https://doi.org/10.17803/lexgen-2025-4-1-24-38

Оригинальная статья / Original article



# Отдельные правовые аспекты биометрической идентификации в банковской сфере

**Ирина Е. Михеева**✉
Университет имени О.Е. Кутафина (МГЮА), Москва, Российская Федерация

## Аннотация

Одним из наиболее перспективных направлений обеспечения дистанционных банковских и иных услуг является развитие удаленной идентификации. На смену традиционным паролям, кодам, сообщениям, использование которых за последние годы серьезно себя скомпрометировало (подтверждается статистикой мошенничества), приходит биометрическая идентификация, которая с более высокой точностью позволяет проводить удаленную идентификацию граждан.

В настоящий момент в мировой практике используются различные способы биометрической идентификации, но наибольшее распространение как в зарубежных странах, так и в России получили изображение лица и голос. При этом развитие искусственного интеллекта позволяет подделывать данные граждан и ставит под сомнение их надлежащую сохранность. Утрата биометрических данных может привести к использованию их мошенниками и причинению вреда физическому лицу.

Законодателем сформированы основные требования к защите биометрических данных граждан, но при этом сохраняются риски, которые возникают при удаленной идентификации и хранении биометрических персональных данных, что является причиной низких показателей передачи гражданами своих биометрических данных в России. Решение указанной проблемы видится в применении совокупности технологических и правовых решений. Важным техническим решением видится использование распределенного реестра (блокчейна), отдельные свойства которого могли бы позволить обеспечить сохранность персональных данных клиентов банков. Кроме того, необходимо усиление гражданско-правовой, административной и уголовной ответственности в отношении лиц, которые осуществляют сбор, обработку и хранение биометрических персональных данных граждан, включая руководителей банков.

✉Email: iemiheeva@msal.ru

**Ключевые слова:** дистанционные банковские услуги, биометрическая идентификация, банки, изображение лица, голос, меры безопасности

**Для цитирования:** Михеева, И.Е. (2025). Отдельные правовые аспекты биометрической идентификации в банковской сфере. *Lex Genetica*, 4(1), 24–38 (In Russ.). https://doi.org/10.17803/lexgen-2025-4-1-24-38

*Поступила в редакцию: 20.02.2025*
*Получена после рецензирования и доработки: 15.03.2025*
*Принята к публикации: 11.04.2025*

# Selected Legal Aspects of Biometric Identification in the Banking Sector

**Irina E. Mikheeva**✉
Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation

## Abstract

One of the most promising areas for providing remote banking and other services is the development of remote identification. Traditional passwords, codes, and messages, the use of which has been seriously compromised in recent years (confirmed by fraud statistics), are being replaced by biometric identification, which helps to remotely identify citizens with a higher degree of accuracy.

Currently, various methods of biometric identification are employed in world practice, but the image of a face and voice are most widespread both in foreign countries and in Russia. At the same time, the development of artificial intelligence makes it possible to forge citizens' data and calls into question their proper security. Biometric data loss can lead to fraudsters using them and causing harm to an individual.

The legislator has formed the basic requirements for the protection of citizens' biometric data. However, the risks that arise from remote identification and storage of biometric personal data remain, which is the reason for the low rates of citizens transferring their biometric data in Russia. The solution to this problem is seen in the application of a combination of technological and legal means. An important technical solution seems to be the use of a distributed registry (blockchain), the individual properties of which could ensure the safety of personal data of bank customers. In addition, it is necessary to enforce civil, administrative and criminal liability against persons who collect, process and store biometric personal data of citizens, including bank managers.

✉Email: iemiheeva@msal.ru

**Keywords:** remote banking services, biometric identification, banks, facial image, security measures

**To cite this article:** Mikheeva, I.E. (2025). Selected legal aspects of biometric identification in the banking sector. *Lex Genetica*, 4(1), 24–38 (In Russ.). https://doi.org/10.17803/lexgen-2025-4-1-24-38

*Received: 20.02.2025*
*Revised: 15.03.2025*
*Accepted: 11.04.2025*

## Введение

Внедрение в банковскую деятельность дистанционных услуг в последнее десятилетие стало причиной широкого распространения в России удаленной идентификации клиентов. Учитывая, что онлайн-обслуживание в перспективе рассматриваются банками как основная форма оказания банковских услуг (Бровкина, 2013), требуется усовершенствование процедур идентификации клиентов банков.

Для удаленной идентификации клиентов традиционно используются пароли, коды, ключи и обмен электронными документами. При этом верно отмечено, что в последние годы общество проделало огромный путь от парольных фраз, сложных печатей, механических замков и ключей до методов автоматической аутентификации (Одиноких, 2019) с использованием биометрических методов идентификации физических лиц, т.е. каких-либо индивидуальных уникальных биологических либо физиологических или физических особенностей конкретного человека (Черняев, 2021).

Ряд авторов считают, что биометрическая идентификация заняла свое место в индустрии безопасности, так как основывается на физиологических особенностях человека (Брюхомицкий, 2019). Биометрические системы идентификации обладают существенными отличиями от традиционных систем контроля и управления доступом (СКУД), включая ключи и пароли (Васильев, 2016). В то же время для идентификации клиентов российские банки продолжают широко использовать пин-коды, ключи, и это объясняется тем, что по российскому законодательству биометрическая идентификация не является обязательной, а клиенты не торопятся добровольно переходить на биометрическую идентификацию (Ефимова, Казаченок, Камалян, 2022). Такие идентификаторы могут быть утеряны, украдены или забыты. Кроме того, эти методы не позволяют провести различие между уполномоченным лицом и самозванцем, который обманным путем получает информацию или «жетон» уполномоченного лица (Yeo, 2007).

Актуальность исследования обусловлена тем, что биометрическая идентификация считается более новым, надёжным и удобным методом идентификации (Утеев, Гибадуллин, 2024), но при этом повсеместного распространения в России так и не получила. Это связывают, прежде всего, с недоверием со стороны граждан, которые опасаются утраты своих биометрических персональных данных.

В этой связи требуется исследование существующих проблем, связанных с биометрической идентификацией клиентов банков, решение которых позволит развивать указанное направление. Одной из таких проблем является отсутствие единообразия

в отношении отдельных терминов в рассматриваемой сфере. Другой проблемой является недостаточное правовое регулирование для обеспечения безопасности.

Однако развитие искусственного интеллекта и технологий ставят перед исследователями новые задачи, требующие современного решения. По мнению Guridi (2024), применение систем искусственного интеллекта для целей биометрической идентификации увеличивает их эффективность в геометрической прогрессии. Но, в то же время, возрастает влияние на права граждан, поскольку инновации в новых технологиях влияют на неприкосновенность частной жизни и основные права человека.

## Результаты и обсуждение

Вопрос о содержании понятия «биометрия» обсуждается различными авторами. При этом признается, что в праве требуется четкость и однозначность отдельных терминов (Соболева, 2007). Единообразие подходов к терминам крайне важно не только для практической деятельности, но и для науки. В то же время в литературе для обозначения понятия «биометрия» используются различные признаки, что приводит к спорным ситуациям, требующим своего разрешения.

Рассмотрим несколько предлагаемых в литературе определений понятия «биометрия».

Так, одни авторы используют слишком общее определение понятия «биометрия», понимая ее как измерение неких отличительных признаков человека для автоматической идентификации (Афанасьев и др., 2022). Биометрическая технология направлена на быстрое и автоматическое распознавание или подтверждение личности человека в режиме реального времени без вмешательства человека (Брюхомицкий, 2019). В данном определении не указано, какие именно характеристики должны учитываться для подтверждения личности, в то же время такими признаками формально может быть, например, ношение определенной одежды, парика и т.д. А.А. Куликов (2021) считает, что в биометрии могут быть задействованы фактически все функциональные особенности человека. Однако понятие «функциональные особенности» также является оценочным и не создает правовую определенность.

Другие авторы рассматривают биометрию более детально, а именно как измерение и анализ уникальных физиологических или поведенческих характеристик человека (Утеев, Гибадуллин, 2024). Схожее понятие предлагает Н.В. Панина (2021), под биометрией понимая не что иное как физиологические или анатомические особенности человека.

Отдельные исследователи считают биометрией область знания, изучающую методы и средства измерения и формализации персональных физических характеристик, поведенческих черт человека и их использование для идентификации или верификации человека (Одиноких, 2019).

Таким образом, можно отметить отсутствие единого понимания термина «биометрия». Рассмотрим признаки биометрии, которые используются в российской практике правоприменения. Параметром биометрии признают некоторую величину, обладающую физическим смыслом, характеризующим сам субъект (Куликов, 2021). Технология биометрической идентификации основана на уникальности биометрической характеристики человека (индивидуума), используемой в качестве идентификатора (Одиноких, 2019).

На мировом рынке биометрических систем активно применяются технологии, основанные на распознавании и использовании

следующих биометрических данных: 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%)[1].

Наиболее широкое применение в биометрической идентификации получили следующие параметры человека: особенности геометрии лица; отпечатки пальцев; геометрия ладони рук; сетчатка и радужная оболочка глаза; голосовые характеристики; особенности подписи и клавиатурный почерк (Гонсалес, Вудс, 2012).

К биометрическим данным относится и геномная информация, что следует из ст. 1 Федерального закона от 03.12.2008 № 242-ФЗ «О государственной геномной регистрации в Российской Федерации»[2], согласно которой «геномная информация – биометрические персональные данные, включающие кодированную информацию об определенных фрагментах дезоксирибонуклеиновой кислоты физического лица или неопознанного трупа».

Согласно ч. 4 ст. 3 Федерального закона от 29.12.2022 № 572-ФЗ в единой биометрической системе размещаются и обрабатываются биометрические персональные данные следующих видов: изображение лица человека, полученное с помощью фотовидеоустройств; запись голоса человека, полученная с помощью звукозаписывающих устройств[3]. Таким образом, в настоящий момент в России используются в качестве биометрических данных только отдельные из возможных способов идентификации, а именно: изображения лица и голос.

## Биометрический метод аутентификации по изображению лица

Изображение лица является наиболее распространенным способом идентификации граждан как в зарубежных странах, так и в России. Уже привычным делом является наличие камер в банках, которые позволяют пройти первичную идентификацию. В последние годы цифровые изображения лица применяются во многих областях, в том числе при визуальной экспертизе и компьютерном автоматическом распознавании лица. Правильно разработанная система распознавания лиц может обеспечить удобный и быстрый доступ к банкомату или компьютеру, контролировать вход в зоны ограниченного доступа, распознавать людей в определенных местах (банки, магазины) (Yeo, 2007).

Требования к формату изображения лица, предназначенного для хранения представлений лица в записи биометрических данных, установлены национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК 19794-5-2013[4].

[1] Банк России. (2018). *Обзор международного рынка биометрических технологий и их применение в финансовом секторе.* Москва. Режим доступа: https://cbr.ru/Content/Document/File/36012/rev_bio.pdf.

[2] *Федеральный закон от 3 декабря 2008 г. № 242-ФЗ «О государственной геномной регистрации в Российской Федерации» (с изменениями и дополнениями)».* Режим доступа: https://base.garant.ru/12163758/.

[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».* Режим доступа: http://www.kremlin.ru/acts/bank/48740.

[4] *Национальный стандарт РФ ГОСТ Р ИСО/МЭК 19794-5-2013 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 6 сентября 2013 г. № 987-ст) (с изменениями и дополнениями).* Режим доступа: https://base.garant.ru/71606576/.

Распознавание лиц основывается на трехмерной модели лица путем анализа его основных черт. По мнению Ю.А. Брюхомицкого, «метод вычисляет расстояния между этими признаками по нескольким изображениям, даже при незначительных изменениях выражения лица или его ориентации. Преимущества метода: отсутствие необходимости физического контакта со сканирующим устройством; низкая чувствительность к внешним факторам; обеспечивается высокий уровень надежности. Недостатки метода: оборудование, необходимое для применения данного метода, может быть дорогостоящим; изменения в выражении лица и наличие препятствий на лице могут снизить статистическую надежность метода» (Брюхомицкий, 2019).

Практика применения распознавания лиц отмечается и зарубежными авторами. Лица богаты информацией об индивидуальности, настроении и психическом состоянии человека, а соотношение положений частей лица, таких как глаза, нос, рот и подбородок, а также их формы и размеры широко используются в качестве отличительных признаков для идентификации (Yeo, 2007).

При этом отмечаются и отдельные недостатки данного способа идентификации. Так, например, в своем диссертационном исследовании Р.А. Васильев (2016) пишет, что «в некоторых случаях применение биометрических характеристик человека осложнено, поскольку геометрии лица свойственна низкая уникальность, для анализа сетчатки и радужной оболочки глаза требуется дорогостоящее оборудование, что недоступно для небольших российских банков».

Среди основных ошибок: ошибки самой системы идентификации; ошибки, возникающие при получении недостаточно полных данных от идентифицируемого лица (фотография плохого качества, не совсем правильный ракурс (лица)); злонамеренные действия нарушителей и т.д. (Левашов, 2018).

Аутентификация по лицу сопряжена со многими проблемами. Несколько изображений одного человека могут сильно отличаться друг от друга из-за изменения ракурса, цвета и освещения или просто потому, что лицо человека выглядит по-разному изо дня в день из-за изменений, связанных с внешностью, таких как макияж, растительность на лице, очки и т.д. (Yeo, 2007).

### Биометрический метод аутентификации по голосу

Метод признается одним из несложных в применении. Этому методу достаточно звуковой платы и микрофона. Исследователи отмечают недостатки данного способа идентификации и аутентификации. Основным и определяющим недостатком метода аутентификации по голосу является низкая точность. Например, человека с простудой система может не опознать. Важную проблему составляет многообразие проявлений голоса одного человека: голос способен изменяться в зависимости от состояния здоровья, возраста, настроения (Утеев, Гибадуллин, 2024).

При этом в последнее время все большее количество потребителей биометрических систем озабочено не только качеством непосредственно голосовой биометрии, но и противодействием различным видам атак, проводимых с целью получения доступа к защищенной информации (Васильев, 2016). Известны случаи, когда с использованием записи голоса мошенникам удавалось обманным путем завладеть денежными средствами граждан.

Как считает Р.А. Васильев (2016), в преобладающем количестве систем идентификации по голосу не присутствует настройка алгоритмов под изменяющиеся условия применения (уровень шума, фонемы речи конкретного человека, ошибки идентификации и т.д.). Для осуществления процедуры идентификации используется спектральный анализ входного звукового сигнала и эталонного сигнала, записанного в базу данных, тем самым существует зависимость от эталонных фраз.

Вместе с тем использование искусственного интеллекта позволяет подделывать голос любого человека. В этой связи данный признак биометрической идентификации не гарантирует защиту граждан и вызывает большую настороженность среди них.

## Правила биометрической идентификации

Общие правила идентификации клиентов банков базируются на положениях Федерального закона от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – ФЗ «О противодействии легализации доходов»)[5].

В ч. 1 ст. 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»)[6] выделено 2 признака биометрических персональных данных:

- сведения, которые характеризуют физиологические особенности человека;
- биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных.

А.И. Савельев (2021) предлагает признать еще один признак биометрических данных, а именно использование оператором специальных технических средств для получения эталонных образцов биометрических данных субъекта и последующего сопоставления вводимых данных с ними.

Удаленная биометрическая идентификация включает Единую биометрическую систему (ЕБС) и Единую систему идентификации и аутентификации (ЕСИА). ЕБС включает биометрические персональные данные гражданина, а ЕСИА – фамилию, имя, отчество, паспортные данные и т.д.

В России согласно Указу Президента РФ от 30.09.2022 № 693[7] Акционерное общество «Центр биометрических технологий» (ЦБТ, г. Москва) является органом, который уполномочен обеспечивать развитие цифровых технологий идентификации и аутентификации, в том числе на основе биометрических персональных данных, а также сервисов подписания и хранения документов, включая создание, развитие и эксплуатацию коммерческих сервисов и типовых решений (далее – оператор).

[5] *Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 07.08.2001 № 115-ФЗ (последняя редакция).* Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_32834/

[6] *Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция).* Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_61801/

[7] *Указ Президента Российской Федерации от 30.09.2022 г. № 693 «Об определении организации, обеспечивающей развитие цифровых технологий идентификации и аутентификации».* Режим доступа: http://www.kremlin.ru/acts/bank/48339

### Преимущества биометрической идентификации

Обращение к биометрическим технологиям идентификации личности происходит, когда речь идет о повышении требований к безопасности совместно с удобством их использования (Одиноких, 2019). Мобильные устройства, стремительно приобретающие универсальность в аспекте проведения всевозможных транзакций, становятся платформой для развёртывания на них сервисов, использующих методы биометрической аутентификации. Значительная часть смартфонов, появившихся на рынке за последние несколько лет, оборудованы компактными сенсорами для аутентификации пользователя.

Использование биометрических данных для удаленной идентификации с использованием мобильных устройств в России поэтапно расширяется. Так, с текущего года использование биометрических персональных данных, размещенных физическим лицом в единой биометрической системе с использованием мобильного приложения единой биометрической системы, позволяет их использовать при заключении договоров об оказании услуг связи; осуществлении продажи алкогольной продукции, безалкогольных тонизирующих напитков (в т.ч. энергетических), табачной продукции или никотинсодержащей продукции, кальянов и устройств для потребления никотинсодержащей продукции[8].

### Безопасность и хранение биометрических данных

Действующим российским законодательством установлены основные правила сбора, обработки, передачи и хранения биометрических персональных данных, обеспечивающих их безопасность.

1. Хранение биометрических персональных данных возможно только централизованно в единой биометрической системе. В соответствии со ст. 15 ФЗ от 29.12.2022 № 572-ФЗ[9] в информационных системах организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц, организаций финансового рынка, иных организаций, индивидуальных предпринимателей, нотариусов по общему правилу запрещена обработка, включая сбор и хранение, используемых в целях идентификации биометрических персональных данных, за исключением обработки, включая сбор, биометрических персональных данных для размещения в единой биометрической системе в соответствии с федеральными законами. Исключения предусмотрены указанным Федеральным законом.

2. Хранение биометрических данных должно осуществляться в обезличенной форме без персональных данных, по которым можно установить личность физического лица (Ф. И. О., паспорт, СНИЛС и так далее).

3. Биометрическим данные не могут обрабатываться без согласия в письменной

[8] *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» (с изменениями и дополнениями).* Режим доступа: https://base.garant.ru/404846015/

[9] *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» (с изменениями и дополнениями).* Режим доступа: https://base.garant.ru/406051675/

форме субъекта персональных данных за исключением случаев, предусмотренных законом. С точки зрения законодательной практики охрана геномной информации происходит персонифицированно (Вихман, Якименко, 2016; Радостева, 2019).

Таким образом, законодателем сформированы основные требования к хранению и защите биометрических данных граждан.

В зарубежной и российской литературе отмечаются проблемы обеспечения сохранности персональных, в том числе биометрических данных, а также их использования, о чем пишут отдельные авторы (Матросов, Карасев, 2023).

Цифровые идентификационные данные конечных пользователей подвергаются все более изощренным атакам.

Рассмотрим некоторые из существующих проблем.

Отмечаются риски, связанные с использованием облачных технологий для хранения биометрической информации, поскольку такие данные требуют повышенной защиты конфиденциальности. В большинстве стран создание записей с биометрией регулируется законами, определяющими условия доступа, хранения, копирования и уничтожения такой информации. Тем не менее сторонники защиты личных данных считают, что действующие правовые нормы, часто сформулированные в общих чертах, недостаточно эффективны против конкретных угроз конфиденциальности, связанных с биометрическими данными (Guridi, 2024).

Также исследуются проблемы мошенничества с банкоматами, несмотря на строгое законодательство и усиление правоприменительной практики, направленные на борьбу с финансовыми преступлениями. Проблема мошенничества с банкоматами имеет глобальный масштаб, и ее последствия ощущаются, в частности, в Австралии (Yeo, 2007).

Проблема обнаружения подделок, связанных с аутентификацией и целостностью, а также с правом собственности на данные и пользователей, постепенно возрастает вместе с беспрецедентным развитием интернета. С развитием аппаратного и программного обеспечения, в результате чего появился интернет вещей (IoT), проверка на подделку станет еще сложнее, поскольку все будет взаимосвязано, как никогда ранее (Kaur и др., 2023).

А.И. Савельев (2021) отмечает, что утечки данных из государственных органов в России — частое явление. Причиной, как правило, становится недостаточная защита персональных данных клиентов, которыми недобросовестные сотрудники (в том числе в банках) злоупотребляют, продавая информацию мошенникам.

В литературе также отмечаются проблемы, которые возникают при удаленной идентификации и хранении биометрических данных. М. Левашов (2018) пишет, что специалисты по информационной безопасности отмечают существенные риски внедрения системы удаленной идентификации при управлении пользователями своими финансовыми и информационными активами. Один из главных рисков — ошибки системы сравнения полученных через интернет биометрических данных человека с его эталонными данными, хранящимися в ЕБС. Источником таких ошибок могут быть различные факторы.

Несмотря на сдержанное отношение граждан к идее сбора биометрических данных, Правительство РФ продолжает стремиться к их более широкому

внедрению[10]. По данным Центра биометрических технологий на январь 2025 г. количество регистраций в ЕБС приближается к трем миллионам[11].

Для успешной реализации государственного проекта необходимо решить ключевую задачу: обеспечение надежной защиты биометрических персональных данных граждан.

### Технологические решения

Одним из перспективных направлений является разработка новых технологических решений для биометрической идентификации. Усовершенствованные системы могут исключать необходимость хранения фактических биометрических образов (например, фотографий лиц или записей голоса). Как отмечает С.В. Черняев (2021), технологии «отменяемой биометрии» накапливают только цифровые отпечатки, которые невозможно преобразовать обратно в исходные данные. Данное решение представляется одним из перспективных, поскольку исключит возможность копирования биометрических данных клиентов и использования их в дальнейшем в мошеннических схемах.

Еще одним технологическим решением видится применение технологии блокчейн в качестве инструмента минимизации рисков несанкционированного использования биометрических персональных данных клиентов банков.

Некоторые эксперты считают, что использование технологии распределенного реестра может существенно повысить безопасность хранения биометрических данных (Генкин, Михеев, 2018). Основные преимущества данной технологии заключаются в ее способности обеспечивать прозрачность и неизменяемость информации (Михеева, 2020).

### Внедрение технологии распределенного реестра в банковской сфере

В рамках пилотного проекта KYC (*Know Your Customer*), основанного на платформе Мастерчейн, создан механизм упрощенной идентификации клиентов между банками (Ahmed и др., 2023). В этой системе:

- информация о клиентах хранится в распределенном виде и доступна только при выполнении строгих условий;
- зашифрованные анкеты сохраняются в блокчейне, а ссылки на них передаются через дополнительные криптографические протоколы;
- только контрагент, имеющий соответствующие права, может получить доступ к данным;
- участники проекта, такие как АК «БАРС» Банк, ПАО «Сбербанк России» и АО Банк «Открытие», успешно протестировали технологию безопасного обмена KYC-анкетами.

Об эффективности использования технологии блокчейн при хранении биометрических данных граждан пишут и зарубежные авторы. Биометрические данные, связанные с распознаванием любого человека, зависят от его поведенческих, физических или психобиологических особенностей, таких как отпечатки пальцев, лицо, радужная

[10] Буйлов М., Гаврилюк А. (2021, 10 марта). Биомеры будут приняты. Сбор данных граждан станет проще и принудительнее. *Коммерсантъ*. https://www.kommersant.ru/doc/4721686

[11] Число пользователей биометрических сервисов приблизилось к 3 млн в РФ. (2025, 20 января). *Известия*. https://iz.ru/1824932/2025-01-20/cislo-polzovatelei-biometriceskih-servisov-priblizilos-k-3-mln-v-rf

оболочка, ухо, подпись, походка, ЭКГ, ЭЭГ и т.д. Поэтому сегодня очень важна безопасность этих биометрических данных. Технология блокчейн – это защищенное и децентрализованное хранилище данных. Модель безопасности 3D-биометрии лица и 3D-биометрии уха с использованием блокчейна обеспечивает прозрачность биометрических данных и передачу данных через распределенный механизм аудита на основе блокчейна (Kaur и др., 2023).

Важно отметить, что применение технологии блокчейн требует соблюдения норм законодательства. Например, действующее законодательство запрещает банкам хранить биометрические данные, их необходимо передавать оператору. Но при этом в момент сбора, который банки уполномочены проводить, также существуют риски, связанные с сохранностью персональных данных до передачи их оператору для хранения. Главная опасность заключается в возможных утечках биометрических данных, что может привести к мошенничеству и нарушению частной жизни граждан. Системы идентификации подвержены ошибкам из-за низкого качества данных или намеренных атак.

Так, например, основываясь на положениях о защите персональных данных, связанных с биометрией, в Европе и Соединенных Штатах, а также на защите персональных данных, связанных с биометрией, в Китае, предлагается улучшить защиту биометрической информации и привести ее в соответствие с существующими законами (Guridi 2024).

*Перспективы развития*

Использование технологии распределенного реестра при биометрической идентификации открывает новые возможности для повышения безопасности данных. В России уже создаются специализированные распределенные хранилища на базе платформы Мастерчейн. Такие хранилища обеспечивают ограниченный временный доступ к данным и позволяют управлять подписками на информацию (Аверина, 2024).

Операции с цифровым рублем, основанные на технологии блокчейн, служат примером успешного применения распределенных реестров в финансовой сфере. Аналогичный подход может быть распространен и на биометрические системы.

*Правовые меры обеспечения безопасности биометрических данных*

Необходимо усилить административную ответственность за нарушение правил обработки биометрических данных, а также ввести уголовную ответственность за их незаконное использование. Это особенно актуально в свете растущего количества мошеннических действий, связанных с персональными данными.

Использование банками при биометрической идентификации клиентов распределенного реестра имеет ряд преимуществ:

- клиенты могут открывать банковские счета в других банках без личного присутствия;
- экономия для банков, что особенно важно для мелких и средних банков, которые не имеют возможности приобрести дорогостоящее оборудование для проведения сбора биометрических данных клиентов;
- значительно сокращаются сроки оказания банковских услуг;
- снижается объем сомнительных, транзитных и иных аналогичных операций;
- технология распределенного реестра не позволяет в одностороннем порядке изменить информацию о платежах (Михеева, 2020).

## Заключение

Внедрение дистанционных банковских услуг привело к широкому распространению удаленной идентификации клиентов в России. Однако, несмотря на перспективность онлайн-обслуживания, биометрическая идентификация, хотя и считается более надежным и удобным методом, пока не получила повсеместного распространения. На данный момент российское законодательство предусматривает использование ограниченного набора биометрических данных для идентификации: изображения лица и записи голоса. Перспективы расширения применяемого инструментария пока не обсуждаются, несмотря на недостатки и возможные риски ошибок, связанных с использованием изображения лица и записи голоса.

Одним из ключевых направлений решения проблем безопасности сохранения биометрических данных является разработка новых технологических решений. Усовершенствованные системы, такие как технологии «отменяемой биометрии», предлагают хранить только цифровые отпечатки вместо фактических биометрических образов, что существенно снижает риск их использования мошенниками. Кроме того, применение технологии блокчейн представляет собой перспективное техническое решение. Блокчейн обеспечивает прозрачность и неизменяемость информации, а его распределенная природа минимизирует риски утечки данных.

Для достижения целей государственного проекта по внедрению биометрических данных необходимо сочетать технологические инновации, усиление правового регулирования и внедрение современных методов защиты информации. Распределенный реестр представляет собой перспективное решение, которое может значительно повысить уровень доверия граждан к биометрии.

В целях совершенствования правового обеспечения сохранности биометрических данных граждан необходимо усилить ответственность лиц, которые занимаются их сбором, обработкой и хранением.

## СПИСОК ЛИТЕРАТУРЫ

Аверина, А.С. (2024). «Умные технологии» масштабирования банковского бизнеса. *Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент*, 14(2), 262–274. https://doi.org/10.21869/2223-1552-2024-14-2-262-274

Афанасьев, С.Д., Терещенко, И.А., Яцкевич, Д.А. (2022). Биометрическая идентификация и права человека: демаркационная линия. *Закон*, (3), 33–46.https://doi.org/10.37239/0869-4400-2022-18-3-33-46

Бровкина, Н.Е. (2013). *Закономерности и перспективы развития кредитного рынка в России* (2-е изд.) Москва: КНОРУС.

Брюхомицкий, Ю. А. (2019). *Биометрические технологии идентификации личности.* Ростов-на-Дону: Южный федеральный университет.

Васильев, Р.А. (2016). *Биометрическая идентификация пользователей информационных систем на основе кластерной модели элементарных речевых единиц.* [Диссертация, Нижегородский государственный университет им. Н.И. Лобачевского]. Нижний Новгород.

Вихман, В.В., Якименко, А.А (2016). *Биометрические системы контроля и управления доступом в задачах защиты информации.* Новосибирск: НГТУ.

Генкин, А., Михеев, А. (2018). *Блокчейн: Как это работает и что ждет нас завтра.* Москва: Альпина Паблишер.

Гонсалес, Р.С., Вудс, Р.Е. (2012). *Цифровая обработка изображений* (3-е изд.). Москва: Техносфера.

Ефимова, Л.Г., Казаченок, О.П., Камалян, В.М. (2022). *Цифровое право в банковской деятельности. Сравнительно-правовой аспект.* Москва: Проспект.

Куликов, А.А. (2021). Применение биометрических систем в технологиях идентификации лиц. *Российский Технологический Журнал*, 9(3), 7–14. https://doi.org/10.32362/2500-316X-2021-9-3-7-14

Левашов, М. (2018). Особенности введения биометрической идентификации. *Бухгалтерия и банки*, (6), 52–55. Режим доступа: https://publications.hse.ru/pubs/share/direct/228207804.pdf

Матросов, С.С., Карасев, П.И. (2023). Биометрические технологии идентификации личности и методы биометрической идентификации. В: *Кибербезопасность: технические и правовые аспекты защиты информации. Сб. науч. тр. I Нац. науч.-практ. конф., Москва, 24–26 мая 2023 г.* (с. 245–248). Москва: МИРЭА Российский технологический университет.

Михеева, И.Е. (2020). Проведение мер по идентификации клиентов с использованием новых цифровых технологий. *Право и цифровая экономика*, 3(09), 21–27.

Одиноких, Г.А. (2019). *Методы и алгоритмы биометрического распознавания человека по радужной оболочке глаза на мобильном устройстве* [Диссертация, Московский государственный университет имени М.В. Ломоносова]. Москва.

Панина, Н.В. (2021). Анализ биометрических характеристик, используемых для информационной безопасности при идентификации пользователя. В: *Моделирование информационных систем. Материалы Междунар. науч.-практ. конф., Воронеж, 19–20 мая 2021 г.* (с. 202–209). Воронеж: Воронежский государственный лесотехнический университет имени Г.Ф. Морозова.

Радостева, Ю.В. (2019). Защита геномной информации в виртуальном пространстве. *Российский юридический журнал*, (3(126)), 42–45.

Савельев, А.И. (2021). *Научно-практический постатейный комментарий к Федеральному закону «О персональных данных».* Москва: Статут. 468 с.

Соболева, А.К. (2007). Законодательная дефиниция как способ преодоления многозначности слова в юридическом дискурсе. *Юридическая техника*, (1), 116–123.

Утеев, Г., Гибадуллин, Р.Ф. (2024). Разработка децентрализованной системы идентификации личности по биометрическим данным с помощью технологии блокчейн и компьютерного зрения. *Международный научно-исследовательский журнал*, (4(142)), 1–16. https://doi.org/10.23670/IRJ.2024.142.6

Черняев, С.В. (2021). Биометрическая идентификация в современном российском законодательстве. *Труды Оренбургского института (филиала) Московской государственной юридической академии*, (4(50)), 55–58.

Ahmed, K.A., Saraya, S.F., Wanis, J.F., Ali-Eldin, A.M. (2023). A blockchain self-sovereign identity for open banking secured by the customer's banking cards. *Future Internet*, 15(6), 208. https://doi.org/10.3390/fi15060208

Guridi, J.F.E. (2024). The Use of Artificial Intelligence (AI) Systems for Remote Biometric Identification in Publicly Accessible Spaces in the European AI Law. *Actualidad jurídica iberoamericana*, (21), 528–565. Available at: https://revista-aji.com/wp-content/uploads/2024/07/AJI21_Art19.pdf. (In Span.).

Kaur, V., Bhatt, D.P., Tharewal, S., Tiwari, P.K. (2023). Blockchain-based secure storage model for multimodal biometrics using 3D face and ear. In: *2023 International Conference on Advancement in Computation & Computer Technologies* (*InCACCT*) (pp. 860–865). IEEE. https://doi.org/10.1109/incacct57535.2023.10141695

Yeo, A.Y. (2007). Stronger authentication: Responding to the crisis of confidence. In: *Managing Information Assurance in Financial Services* (pp. 152–165). IGI Global. https://doi.org/10.4018/9781599041711.ch007

## REFERENCES

Afanasyev, S.D., Tereshchenko, I.A., Yatskevich D.A. (2022). Biometric Identification and Human Rights: the Line of Demarcation. *Zakon*, (3), 33–46. (In Russ.). https://doi.org/10.37239/0869-4400-2022-18-3-33-46

Ahmed, K.A., Saraya, S.F., Wanis, J.F., Ali-Eldin, A.M. (2023). A blockchain self-sovereign identity for open banking secured by the customer's banking cards. *Future Internet*, 15(6), 208. https://doi.org/10.3390/fi15060208

Averina, A.S. (2024). Development Prospects of Modern Banking. *Proceedings of the Southwest State University. Series: Economics. Sociology. Management*, 14(2), 262–274. (In Russ.). https://doi.org/10.21869/2223-1552-2024-14-2-262-274

Brovkina, N.E. (2013). *Patterns and Prospects of Development of the Credit Market in Russia*. (2nd ed.). Moscow: KNORUS Publ. (In Russ.).

Bryukhomitsky, Yu.A. (2019). *Biometric technologies of personal identification*. Rostov-on-Don: Southern Federal University. (In Russ.).

Chernyaev, S.V. (2021). Biometric identification in modern Russian legislation. *Proceedings of the Orenburg Institute (branch) of the Moscow State Law Academy*, (4(50)), 55–58. (In Russ.).

Efimova, L.G., Kazachenok, O.P., Kamalyan, V.M. (2022). *Digital law in banking. Comparative legal aspect*. Moscow: Prospekt Publ. (In Russ.).

Genkin, A., Mikheev, A. (2018). *Blockchain: How it works and what awaits us tomorrow*. Moscow: Alpina Publisher Publ. (In Russ.).

Gonzalez, R.S., Woods, R.E. (2002). *Digital Image Processing*. New Jersey: Prentice Hall. (In Russ.).

Guridi, J.F.E. (2024). The Use of Artificial Intelligence (AI) Systems for Remote Biometric Identification in Publicly Accessible Spaces in the European AI Law. *Actualidad jurídica iberoamericana*, (21), 528–565. Available at: https://revista-aji.com/wp-content/uploads/2024/07/AJI21_Art19.pdf. (In Span.).

Kaur, V., Bhatt, D.P., Tharewal, S., Tiwari, P.K. (2023). Blockchain-based secure storage model for multimodal biometrics using 3D face and ear. In: *2023 International Conference on Advancement in Computation & Computer Technologies* (*InCACCT*) (pp. 860–865). IEEE. https://doi.org/10.1109/incacct57535.2023.10141695

Kulikov, A.A. (2021). Application of biometric systems in face identification technologies. *Russian Technological Journal*, 9(3), 7–14. (In Russ.) https://doi.org/10.32362/2500-316X-2021-9-3-7-14

Levashov, M. (2018). Features of the introduction of biometric identification. *Accounting and Banks*, (6), 52–55. Available at: https://publications.hse.ru/pubs/share/direct/228207804.pdf. (In Russ.).

Matrosov, S.S., Karasev, P.I. (2023). Biometric technologies for personal identification and methods of biometric identification. In: *Cybersecurity: technical and legal aspects of information protection. Collection of academic papers of the I National Scientific and Practical Conference, Moscow, May 24–26, 2023* (pp. 245–248). Moscow: MIREA Russian Technological University. (In Russ.).

Mikheeva, I.E. (2020). Carrying out measures to identify clients using new digital technologies. *Law and Digital Economy*, 3(09), 21–27. (In Russ.).

Odinokikh, G.A. (2019). *Methods and algorithms for biometric human recognition by the iris on a mobile device*. [Dissertation, Lomonosov Moscow State University]. Moscow. (In Russ.).

Panina, N.V. (2021). Analysis of biometric characteristics used for information security during user identification. In: *Modeling of information systems. Proceedings of the International Academic and Practical Conference, Voronezh, May 19–20, 2021* (pp. 202–209). Voronezh: Voronezh State Forest Engineering University named after G.F. Morozov. (In Russ.).

Radosteva, Yu.V. (2019). Protection of genomic information in virtual space. *Russian Law Journal*, (3(126)), 42–45. (In Russ.).

Savelyev, A.I. (2021). *Scientific and practical article-by-article commentary to the Federal Law «On Personal Data»*. Moscow: Statut Publ. (In Russ.).

Soboleva, A.K. (2007). Legislative definition as a means to overcome the polysemy of a word in legal discourse. *Legal technique*, (1), 116–123. (In Russ.).
Uteyev, G., Gibadullin R.F. (2024). Development of the decentralized biometric identity verification system using blockchain technology and computer vision. *International Research Journal*, (4(142)), 1–16. (In Russ.). https://doi.org/10.23670/IRJ.2024.142.6
Vasiliev, R.A. (2016). *Biometric identification of users of information systems based on the cluster model of elementary speech units*. [Dissertation, Lobachevsky State University of Nizhny Novgorod (UNN)]. Nizhny Novgorod. (In Russ.).
Vikhman, V.V., Yakimenko, A.A (2016). *Biometric access control and management systems in information security tasks*. Novosibirsk: NSTU. (In Russ.).
Yeo, A.Y. (2007). Stronger authentication: Responding to the crisis of confidence. In: *Managing Information Assurance in Financial Services* (pp. 152–165). IGI Global. https://doi.org/10.4018/9781599041711.ch007

## ИНФОРМАЦИЯ ОБ АВТОРЕ:

**Ирина Е. Михеева,** кандидат юридических наук, доцент кафедры банковского права, руководитель НОЦ правового регулирования в сфере высоких технологий Университета имени О.Е. Кутафина (МГЮА), Москва, Российская Федерация

## INFORMATION ABOUT THE AUTHOR:

**Irina E. Mikheeva,** Candidate of Science (Law), Associate Professor of the Department of Banking Law, the Head of Scientific Educational Centre of Legal Regulation in the Sphere of High Technology, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation