

УДК 336:339.138
DOI 10.17513/fr.43814

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ КАК ФАКТОР ПОВЫШЕНИЯ БЕЗОПАСНОСТИ И КОНКУРЕНТОСПОСОБНОСТИ В ФИНАНСОВОЙ ИНФРАСТРУКТУРЕ РОССИИ

Храмов Е.Н., Вершинина О.В.

АНО ВО «Российский новый университет», Москва, e-mail: enhram@gmail.com

Рост числа киберугроз делает актуальным внедрение биометрических технологий в финансовом секторе России как инструмента повышения безопасности и доверия пользователей. В особенности значима интеграция таких решений в банковскую инфраструктуру в условиях активной цифровизации. Цель исследования – провести всесторонний анализ динамики применения биометрической идентификации в банковской системе Российской Федерации с учетом технологических перспектив и выявлением основных вызовов, сопровождающих внедрение таких решений. В исследовании были использованы методы монографического анализа, оценки и рефлексивного подхода, а также нормативные правовые акты и актуальные научные публикации, позволяющие оценить влияние биометрических систем на снижение операционных рисков и совершенствование процессов аутентификации. Установлено, что технологии искусственного интеллекта, внедренные в биометрические системы, позволяют повысить точность идентификации и адаптировать системы к изменениям биометрических характеристик пользователей. Выявлены преимущества мультимодальных подходов и обозначены проблемы, связанные с правовым регулированием, рисками утечки данных и низким уровнем доверия населения. Анализ Единой биометрической системы показал наличие значительных технологических и социальных барьеров для масштабного внедрения. Исследование подтверждает перспективность применения биометрии с элементами искусственного интеллекта как инструмента повышения информационной безопасности. Успешная реализация требует комплексного подхода: технологического совершенствования, нормативной базы и повышения доверия граждан к механизмам идентификации.

Ключевые слова: биометрические технологии, безопасность данных, финансовая инфраструктура, киберугрозы, аутентификация, идентификация клиентов, конкурентоспособность, управление рисками, цифровизация, банковская система, искусственный интеллект.

BIOMETRIC TECHNOLOGIES AS A FACTOR IN IMPROVING SECURITY AND COMPETITIVENESS IN RUSSIA'S FINANCIAL INFRASTRUCTURE

Khramov E.N., Vershinina O.V.

Russian New University, Moscow, e-mail: enhram@gmail.com

The growing number of cyber threats highlights the relevance of implementing biometric technologies in Russia's financial sector as a tool for enhancing security and increasing user trust. This is particularly significant in the context of active digitalisation, where integration into the banking infrastructure is essential. The objective of this study is to conduct a comprehensive analysis of the dynamics of biometric identification implementation within the banking system of the Russian Federation, taking into account technological prospects and identifying key challenges associated with its deployment. The research employs methods of monographic analysis, evaluative and reflexive approaches, as well as a review of legal regulations and up-to-date academic publications, enabling assessment of the impact of biometric systems on reducing operational risks and improving authentication processes. The study reveals that artificial intelligence technologies, integrated into biometric systems, significantly enhance identification accuracy and allow systems to adapt to changes in users' biometric characteristics. The advantages of multimodal approaches are identified, along with existing issues related to regulatory frameworks, data leakage risks, and low levels of public trust. An analysis of the Unified Biometric System highlights substantial technological and social barriers to large-scale adoption. The findings confirm the promising potential of biometrics combined with artificial intelligence as an effective tool for strengthening information security. Successful implementation requires a comprehensive approach, involving technological advancement, regulatory development, and increased public confidence in identification mechanisms.

Keywords: biometric technologies, data security, financial infrastructure, cyber threats, authentication, customer identification, competitiveness, risk management, digitalisation, banking system, artificial intelligence

Введение

Активное развитие цифровой экономики в России способствует растущему интересу к биометрическим технологиям, которые становятся важным инструментом для повышения безопасности финансовых операций. Применение методов биометрической идентификации существенно снижа-

ет вероятность мошенничества и упрощает доступ к электронным сервисам, заменяя устаревшие способы аутентификации, такие как пароли и PIN-коды. Использование уникальных биометрических данных позволяет не только укрепить доверие клиентов, но и формировать персонализированные финансовые предложения. Этот подход сти-

мулирует рост инноваций и автоматизацию процессов, что способствует улучшению конкурентных позиций российской экономики на мировом уровне.

Исследование П.В. Мизинова и Н.С. Конновой [1] раскрывает связь биометрических технологий с эволюционными принципами, подчеркивая, что генетическая уникальность каждого человека является основой надежной идентификации. Авторы отмечают, что отсутствует возможность полного совпадения биометрических характеристик между двумя людьми, что гарантирует точность аутентификации. Н.И. Куликов, Ю.В. Кудрявцева и Е.С. Вдовина [2] анализируют внедрение информационных технологий, рассматривая скорость и надежность операций как основные факторы модернизации банковских систем. По мнению исследователей, финтех-ландшафт требует постоянной адаптации и внедрения инноваций, чтобы соответствовать требованиям времени.

Работа А. Мораке и его коллег [3] подчеркивает роль биометрии в автоматизированной идентификации, основанной на анализе таких данных, как черты лица и голос. Биометрические системы моделируют процессы человеческого восприятия, создавая надежные механизмы защиты данных. Вклад физиологических методов аутентификации изучен в работе С.С. Датваса и его команды [4]. Отпечатки ладоней как пример физиологических биометрических данных выделяются высокой точностью и устойчивостью к подделке. И.Н. Карцан [5] подчеркивает, что использование уникальных поведенческих и физиологических характеристик усиливает защиту информационных систем. В то же время М.С. Иванов [6] обращает внимание на недостатки традиционных методов аутентификации и описывает биометрические технологии как более эффективное средство предотвращения несанкционированного доступа.

А.Л. Белоусов и Е.Ю. Левчук подчеркивают стратегическую важность внедрения информационных технологий, включая биометрию, для укрепления конкурентных преимуществ банковских организаций. Использование таких решений способствует созданию инновационных бизнес-моделей, которые позволяют финансовым учреждениям оперативно адаптироваться к изменяющимся условиям и требованиям рынка [7]. Исследования О.М. Аббасовой демонстрируют, что мультимодальные биометрические системы, объединяющие несколько методов идентификации, значительно повышают точность распознавания и надежность обработки данных [8]. Одна-

ко Ю.И. Лукьянникова, А.Р. Мардамшина и Е.В. Каменева подчеркивают, что надежность биометрических систем пока остается предметом дискуссий. По мнению исследователей, необходимо продолжить научные изыскания, чтобы устранить существующие риски и обеспечить более высокий уровень защиты данных [9]. Законодательное регулирование в России в области биометрии опирается на Федеральные законы № 152-ФЗ¹ и № 149-ФЗ², которые накладывают строгие обязательства на организации, занимающиеся сбором и обработкой персональных и биометрических данных. Настоящие нормативные акты обеспечивают защиту информации в цифровой среде и создают базу для безопасного взаимодействия с данными пользователей. Аналогичные стандарты приняты в Европейском союзе: регламент GDPR распространяет свои требования не только на страны ЕС, но и на компании, работающие с данными граждан Европы за пределами Союза, что формирует высокие стандарты защиты информации на глобальном уровне [10].

Ключевую роль в развитии биометрии в банковской сфере сыграл Федеральный закон № 479-ФЗ, который расширил применение биометрических методов идентификации в финансовом секторе. М.А. Орцханова и О.И. Бжеумихова отмечают, что этот шаг значительно усилил потенциал технологии в сфере цифровых услуг [11]. Перспективы развития биометрии подчеркивает Д.Р. Перевертун, указывая, что такие технологии обеспечивают не только безопасность, но и удобство использования, что делает их неотъемлемой частью цифровой инфраструктуры. При этом, как отмечает исследователь, важно сохранять баланс между внедрением новых решений и защитой личной информации пользователей, что требует дальнейшего совершенствования стандартов безопасности [12]. Анализ Я.В. Жукова с коллегами показывает, что банковская безопасность играет важнейшую роль в стабильности российской экономики. Ученые также акцентируют внимание на значительных инвестициях, необходимых для создания и эксплуатации Единой биометрической системы, что подтверждает стратегическое значение биометрии для развития финансовой инфраструктуры страны [13].

¹ Федеральный закон РФ «О персональных данных» от 27.07.2006 № 152-ФЗ (в ред. от 28.02.2025) // Собрание законодательства Российской Федерации. 2006. № 31 (Ч. I). Ст. 3451.

² Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (в ред. от 23.11.2024) // Собрание законодательства Российской Федерации. 2006. № 31 (ч. I). Ст. 3448.

Результаты социологических исследований, проведенных ВЦИОМ, свидетельствуют о положительной динамике в общественном восприятии биометрических технологий в Российской Федерации. В 2024 году доля респондентов, поддерживающих использование таких решений, увеличилась с 27 до 41%. Рост показателя отражает тенденцию усиления доверия к цифровым инструментам идентификации и защиты персональных данных, что создает потенциал для дальнейшего расширения их применения в различных секторах [14]. Однако распространение биометрических решений на территории страны демонстрирует фрагментарный характер. В мегаполисах и крупных городах наблюдается активная интеграция таких систем в повседневную жизнь, тогда как в малых населенных пунктах биометрия воспринимается преимущественно как инновация с элементами научной фантастики, оторванная от текущих реалий. Опросы общественного мнения указывают на наличие устойчивой поляризации оценок: часть граждан рассматривают биометрические технологии как удобный и технологичный инструмент, другая часть выражают обеспокоенность вопросами конфиденциальности и сохранности персональной информации.

Смена общественного отношения к использованию биометрии требует целенаправленных усилий по укреплению доверия и повышению уровня прозрачности всех процессов, связанных с обработкой персонализированных данных. Одной из приоритетных задач становится не столько технологическая доработка соответствующих решений, сколько формирование эффективных механизмов правовой и технической защиты информации. Разработка и реализация безопасных протоколов обращения с биометрическими параметрами приобретают критическое значение в контексте формирования устойчивого пользовательского доверия. Не менее важной задачей выступает внедрение унифицированных стандартов и четких регламентов, определяющих правила использования биометрических данных в различных институциональных и коммерческих контекстах.

Международный опыт показывает, что успешная реализация биометрических инициатив опирается на наличие продуманной нормативной базы, детализирующей все аспекты хранения, обработки и использования персональных сведений. Рост уровня общественного одобрения тесно коррелирует с повышением информированности населения и формированием устойчивого запроса на безопасные и удобные инстру-

менты цифровой идентификации. Консолидация усилий между государственными институтами и представителями бизнеса способна стать основой для формирования устойчивой модели доверительного взаимодействия. С высокой вероятностью в ближайшей перспективе биометрия станет базовым стандартом в процедурах идентификации, однако ее повсеместное внедрение будет возможно лишь при условии преодоления существующих барьеров в виде общественного скепсиса и обеспокоенности вопросами информационной безопасности.

Целью представленного исследования является комплексный анализ динамики применения биометрической технологии в банковской системе России с оценкой перспектив и вызовов, связанных с ее внедрением.

Материалы и методы исследования

Основу исследования составляют актуальные научные публикации, а также нормативные акты, регулирующие сбор и обработку биометрических данных. В рамках методологии применены три основных подхода. Во-первых, монографический анализ позволил изучить текущее состояние биометрической безопасности, выявить ключевые проблемы и существующие практики в этой области. Во-вторых, оценочный подход обеспечил возможность количественной оценки влияния биометрических технологий на снижение операционных рисков, а также на оптимизацию процессов идентификации. Наконец, рефлексивный метод позволил осуществить критическое осмысление предложенного подхода, оценить его эффективность и определить практическую применимость в банковском секторе России.

Результаты исследования и их обсуждение

Рынок биометрической аутентификации набирает обороты, становясь все более востребованным в самых разных секторах. От финансов и медицины до государственных учреждений – везде внедряются системы идентификации по биометрическим данным в качестве меры защиты от неправомерного доступа и кражи персональной информации [15]. Согласно аналитическому отчету, опубликованному на платформе Reportlinker, динамика роста мирового рынка биометрии весьма впечатляющая – с увеличением с почти 33 млрд долл. в 2022 году до прогнозируемых 39,37 млрд долл. в 2023 году, что соответствует годовому темпу роста в 19,4%. К 2027 году спрогнозировано

дальнейшее расширение рынка до уровня 73,5 млрд долл., с годовым темпом роста в 16,9% [16]. Отдельное внимание заслуживают усилия Российской Федерации в этой сфере. В отклик на решение правительственной комиссии по информационным технологиям уполномоченные органы, среди которых Министерство коммуникаций и связи (Минкомсвязи) и Банк России, а также некоторые предприятия, с середины 2016 года активно занимаются исследованиями и разработками, направленными на создание и функционирование Единой биометрической системы (ЕБС).

Единая биометрическая система, разработанная в рамках инициативы Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, занимает центральное место в создании инфраструктуры электронного правительства. Данная система интегрируется с Единой системой идентификации и аутентификации (ЕСИА), которая служит основным порталом предоставления государственных услуг, обеспечивая обработку и объединение различных данных. ЕБС представляет собой масштабный проект национального уровня, направленный на использование биометрических технологий для повышения безопасности и упрощения доступа к различным сервисам. Однако ее внедрение сопровождается рядом серьезных вызовов, влияющих на эффективность функционирования и популяризацию системы. К середине 2023 года объем данных, зарегистрированных в ЕБС, составил лишь несколько сотен тысяч записей, что значительно уступает показателям крупных частных операторов, таких как Сбербанк и другие финансовые организации, где количество биометрических данных исчисляется десятками миллионов.

Разрыв между этими показателями обусловлен несколькими ключевыми причинами, такими как:

- недостаточный уровень информированности населения о преимуществах использования Единой биометрической системы;
- низкий уровень доверия пользователей к обеспечению безопасности персональных данных и отсутствию прозрачности в их дальнейшем использовании;
- ограниченные возможности инфраструктуры для сбора биометрической информации в удаленных регионах Российской Федерации.

Несмотря на декларируемые высокие стандарты защиты, эксперты в области кибербезопасности неоднократно подчеркивали наличие уязвимостей в ЕБС. Одной

из наиболее серьезных проблем является риск несанкционированного доступа к серверным ресурсам с целью хищения персональной информации. Также серьезные опасения вызывает вероятность утечек данных, возникающих из-за недостаточной защиты операционных систем или ненадежных каналов передачи информации. Еще одной сложностью стало ограничение технических возможностей некоторых операторов при обеспечении безопасности на этапе сбора биометрических данных. Кардинальные корректировки в правовом регулировании биометрической отрасли, зафиксированные в декабре 2022 года посредством вступления в силу Федерального закона № 572-ФЗ³, стали отправной точкой для масштабной трансформации инфраструктуры биометрических услуг. С сентября 2023 года все массивы персонализированных биометрических данных, ранее собранные коммерческими операторами, подлежат обязательной передаче в ЕБС. Вне рамок государственной платформы дальнейшее хранение и эксплуатация такой информации были запрещены на законодательном уровне.

Принятые меры обусловили цепочку значимых последствий, в числе которых – прекращение деятельности частных субъектов рынка, ранее осуществлявших функции сбора, обработки и хранения биометрических параметров. Сокращение институционального участия негосударственных операторов повлекло снижение их заинтересованности в развитии соответствующей инфраструктуры, так как дальнейшее использование данных стало возможно исключительно в контуре государственной системы. Возникла потребность в формировании обновленной нормативной архитектуры, способной регламентировать взаимоотношения между органами государственной власти и коммерческими участниками. Реализация политики централизации и усиленного контроля над биометрической информацией оказала глубокое воздействие на рыночную конфигурацию. Помимо изменения институциональной структуры, сформировался комплекс новых вызовов, охватывающих необходимость усиления гарантий информационной безопасности, повышение уровня гражданского доверия и адаптацию участников к обновленной модели взаимодействия.

³ Федеральный закон «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» от 29.12.2022 № 572-ФЗ (в ред. от 28.12.2024) // Собрание законодательства Российской Федерации. 2023. № 1 (ч. I). Ст. 19.

Доверие со стороны населения продолжает оставаться критически значимым фактором, определяющим успешность внедрения ЕБС. Согласно данным социологических опросов, проведенных в 2024 году, лишь 41% респондентов поддерживают распространение биометрических технологий. Значительное число опрошенных демонстрируют настороженность, связанную с ключевыми рисками, включая сомнения в достаточной защите персональных данных, опасения относительно неконтролируемого доступа к ним со стороны государственных структур, а также недостаточную прозрачность процедур внутри системы. Несмотря на первоначальные капиталоемкие вложения, развитие платформы требует дальнейших инвестиций. Для обеспечения масштабируемости необходимо расширение функционала и архитектурной гибкости системы. Постоянная модернизация аппаратно-программного комплекса является необходимым условием повышения надежности и производственной устойчивости. Биометрические технологии, продемонстрировавшие высокую эффективность в финансовом секторе, приобрели универсальный характер применения. Их использование вышло за рамки банковской сферы и активно распространяется на иные отрасли. В здравоохранении они способствуют идентификации пациентов и предоставлению доступа к медицинской информации. В системе образования применяются для контроля посещаемости и регулирования доступа к образовательным ресурсам. Транспортная сфера использует биометрические решения при автоматизации посадки и обработке электронных билетов, а си-

стемы обеспечения безопасности активно внедряют данные технологии для контроля доступа и аутентификации личности (табл. 1).

Технология удаленной идентификации основывается на трехуровневой модели аутентификации, которая сочетает авторизацию через ЕСИА и использование двух биометрических факторов: анализа движения лица и голоса. Для получения доступа к удаленным банковским услугам пользователям, ранее зарегистрировавшим свои биометрические данные, необходимо пройти процесс верификации. Настоящий процесс включает направление камеры устройства на лицо и произнесение заранее определенной системой фразы. Если изображение и голос совпадают с сохраненными данными, предоставляется доступ к необходимым сервисам. Реализация ЕБС нацелена на оптимизацию затратных статей коммерческих банков и упрощение процессов привлечения новых клиентов в рамках дистанционного обслуживания. Инициатива была реализована ПАО «Ростелеком» и функционирует на коммерческой основе, предусматривающей платный доступ к персонализированным данным. Согласно официальным сведениям, стоимость одной аутентификационной операции составляет 200 руб., из которых 50% перечисляются в пользу кредитной организации, изначально обеспечившей сбор и верификацию биометрической информации. Оставшаяся часть суммы перераспределяется между оператором ЕБС, разработчиками технологической инфраструктуры и участниками, обеспечивающими интеграцию с ЕСИА [17].

Таблица 1

Примеры использования биометрии за пределами финансовой сферы

Область применения	Примеры применения	Преимущества
Транспортная отрасль	Идентификация пассажиров, контроль доступа на вокзалах и в аэропортах	Ускорение процессов, повышение безопасности
Образование	Распознавание лиц для учета посещаемости, безопасный доступ в школы	Улучшение контроля, защита учащихся
Системы контроля доступа	Ограничение доступа на рабочие места, идентификация в «умных» домах	Повышение безопасности, удобство пользователей
Сфера услуг	Регистрация гостей в гостиницах, идентификация в фитнес-центрах	Удобство, автоматизация процессов
Здравоохранение	Идентификация пациентов, предотвращение мошенничества при выдаче лекарств	Точность данных, защита от мошенничества
Государственные услуги	Оформление паспортов, регистрация на избирательных участках	Упрощение процедур, повышение доверия граждан

Источник: составлено автором.

По состоянию на начало 2020 год к сервисам, основанным на биометрической идентификации, обратились порядка 110 тыс. граждан, о чем было официально заявлено оператором платформы. Технологическое развитие сопровождалось запуском новых функциональных решений. Так, 13 августа 2020 года в банковской отрасли была представлена инновационная услуга по оформлению кредитов посредством банкоматов, оснащенных биометрическими модулями. Спустя месяц, 28 сентября, в рамках модернизации цифрового интерфейса кредитных организаций была представлена обновленная версия личного кабинета на платформе ЕБС. Осенью 2020 года стартовало внедрение алгоритмов распознавания лиц в целях автоматизации доступа в офисы банковских учреждений. Первыми такие системы интегрировали отделения АО «Альфа-Банк», где биометрические технологии были установлены в пилотном режиме. В дальнейшем планировалось масштабирование решения на более чем 300 филиалов. В марте 2021 года стала доступна возможность удаленной регистрации биометрических параметров через мобильное приложение «Биометрия», что позволило полностью исключить необходимость личного присутствия в банковских отделениях или многофункциональных центрах. Повышение внимания к вопросам информационной безопасности биометрических данных наблюдалось с октября 2021 года, а уже в ноябре платформа была официально включена в состав инфраструктуры электронного правительства, получив статус государственной информационной системы.

В июне 2022 года Министерство цифрового развития инициировало пересмотр нормативной базы с акцентом на усиление юридических гарантий защиты биометрических данных. Законодательные поправки значительно ужесточили ответственность за нарушения в сфере сбора и обработки персонализированной информации. Основные аспекты функционирования ЕБС были конкретизированы в постановлении Председателя Правительства № 1237, подписанном в июле 2022 года⁴. Дальнейшая эволюция правового регулирования позво-

лила выстроить системную модель, обеспечивающую четкое распределение обязанностей между участниками и стандартизированные процедуры обращения с биометрической информацией. Среди значимых нововведений в области регулирования биометрической идентификации следует выделить предоставление гражданам возможности самостоятельно размещать свои биометрические данные в ЕБС посредством специализированного отечественного программного обеспечения. Закон, принятый Государственной Думой 21 декабря 2022 года, гарантировал защиту прав лиц, отказавшихся от передачи биометрических параметров, установив юридический запрет на какую-либо форму дискриминации по этому основанию. В дополнение к этому, документ существенно сузил перечень допустимых к обработке биометрических признаков, ограничив его изображением лица и голосом, а также упростил механизм удаления сведений из базы, тем самым расширив контроль граждан над персональной информацией.

Начиная с февраля 2023 года на платформе государственных услуг была внедрена опция биометрической аутентификации, позволившая пользователям быстрее и безопаснее получать доступ к электронным сервисам. С июня 2023 года введена процедура добровольного отказа от использования биометрических данных, которая реализуется путем подачи заявления в многофункциональном центре. Осенью того же года доступ к регистрации биометрии стал еще более широким за счет запуска мобильного приложения «Госуслуги Биометрия», что позволило проводить верификацию вне офиса банка или МФЦ. С вступлением в силу положений Федерального закона № 572-ФЗ с начала 2024 года управление согласием на обработку персональных биометрических данных было интегрировано в интерфейс портала Госуслуг, что обеспечило более прозрачное и удобное взаимодействие граждан с системой [18]. Обязательная передача всех ранее собранных биометрических данных в ЕБС, предусмотренная тем же нормативным актом, существенно трансформировала механизм функционирования данной государственной информационной платформы (табл. 2). Функцию регистрации биометрических данных уже предоставляют такие крупные банки России, как АО «Почта-Банк», АО «Тинькофф Банк», ООО «Хоум Кредит», АО «Альфа-Банк», ПАО «Совкомбанк» и ПАО «Промсвязьбанк», а перечень участников предсто-

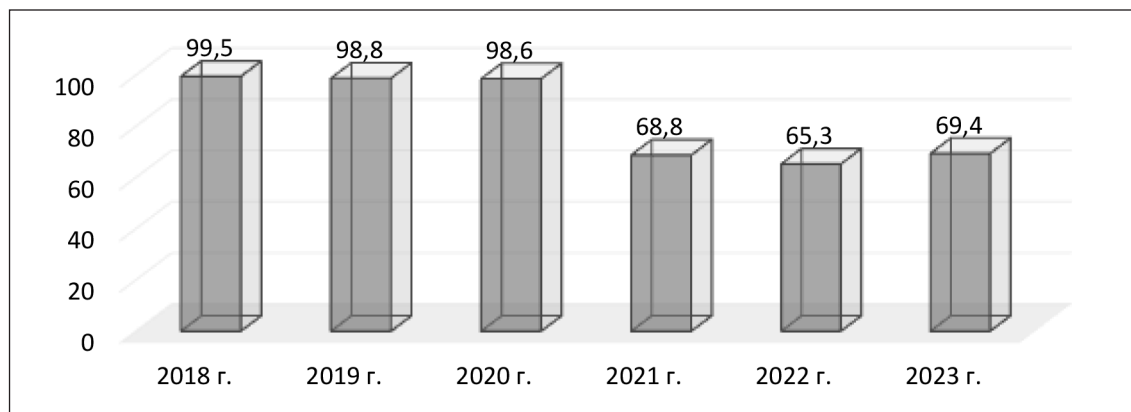
⁴ Постановление Правительства РФ «О внесении изменения в состав сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным физического лица, включая вид биометрических персональных данных» от 12.07.2022 № 1237 // Собрание законодательства Российской Федерации. 2022. № 29 (ч. III). Ст. 5493.

Таблица 2

Влияние передачи данных в ГИС ЕБС

Аспекты влияния	Описание	Последствия
Централизация данных	Хранение данных в единой государственной системе. Частные операторы утратили право самостоятельного хранения данных	Повышение управляемости и защиты данных, но снижение автономии участников
Укрепление безопасности	Доступ к данным только в виде векторов, строгие протоколы взаимодействия минимизируют утечки	Снижение рисков компрометации данных
Снижение конкурентоспособности частных операторов	Частные операторы ограничены в использовании данных, увеличиваются затраты и сложности процессов	Сужение инновационных возможностей, рост затрат для частных операторов
Сложности адаптации участников рынка	Изменения в бизнес-процессах и сложности интеграции инфраструктуры в единую систему	Увеличение времени и ресурсов на адаптацию
Повышение доверия пользователей	Государственная защита данных и меры для повышения прозрачности укрепляют доверие граждан	Повышение лояльности граждан, улучшение имиджа системы

Источник: составлено автором.



Доля банков, зарегистрированных в ЕСИА и ЕБС в общем количестве действующих банков России за 2018–2023 гг., % [20, 21]

Клиенты имеют возможность подключиться к ЕБС через авторизованные банки (рисунок). Для регистрации в системе достаточно однократно пройти процедуру сбора биометрических данных, после чего информация отправляется банком в ЕБС. Оттуда и начинается возможность удаленного доступа к банковским услугам. Важно отметить, что обращаться клиентам следует только в те финансовые учреждения, которые уже интегрировались в ЕБС [19].

Внедрение биометрических технологий в России для идентификации личности через ЕБС свидетельствует о желании государства обеспечить высокий уровень безопасности и удобства для граждан. Для ускорения внедрения биометрической идентификации в банковской сфере России можно использовать несколько ключевых технологий, которые улучшат точность,

безопасность и доступность биометрических систем (табл. 3).

Интеграция искусственного интеллекта (ИИ) в обработку биометрических данных предоставляет новые возможности для повышения точности идентификации. Технологии машинного обучения успешно анализируют биометрическую информацию, включая изображения лиц, голосовые записи и отпечатки пальцев. Адаптивные алгоритмы учитывают изменения характеристик, вызванные возрастом, травмами или заболеваниями, что обеспечивает высокий уровень надежности и устойчивости системы к внешним воздействиям. Применение ИИ в ЕБС создает дополнительные преимущества, среди которых способность обнаруживать аномалии и предотвращать мошенничество в реальном времени.

Таблица 3

Направления развития биометрической идентификации в банковской сфере России

Технология	Описание	Преимущества
Облачные технологии и облачная биометрия	Централизованное хранение и обработка биометрических данных, снижение затрат и упрощение управления	Масштабируемость, централизованная защита данных, быстрая интеграция
Искусственный интеллект и машинное обучение (AI/ML)	Использование AI/ML для повышения точности и снижения количества ложных срабатываний в биометрических системах.	Повышение точности и адаптивность к изменениям в биометрии
Технология блокчейн	Использование блокчейна для обеспечения безопасности и прозрачности обработки биометрических данных	Прозрачность, безопасность и защита от изменений данных
5G-сети	Увеличение скорости и надежности передачи биометрических данных благодаря 5G-сетям	Высокая скорость передачи данных, низкая задержка
Мультимодальная биометрия	Использование нескольких видов биометрических данных для повышения точности идентификации	Более высокая точность, защита от мошенничества
Биометрия с использованием искусственного интеллекта для обнаружения подделок (Liveness Detection)	Технологии, проверяющие подлинность биометрических данных, чтобы избежать использования поддельных изображений	Защита от мошенничества и поддельных данных
Интеграция с мобильными устройствами (Biometrics on Edge)	Использование биометрических сенсоров на смартфонах и других устройствах для локальной обработки данных	Меньше зависимость от сетевых задержек, быстрый доступ к услугам
Безопасные модули на чипах (Secure Enclave / Trusted Execution Environment)	Изоляция биометрических данных внутри защищенной среды на уровне чипов для повышения безопасности	Повышенная безопасность данных и защита от взломов
Распознавание поведения (Behavioral Biometrics)	Мониторинг поведения пользователя для создания дополнительного уровня защиты на основе его привычек	Постоянный мониторинг и дополнительная защита от мошенничества

Источник: составлено автором.

Технологии распознавания лиц на базе глубокого обучения обрабатывают миллионы записей с высокой скоростью, сопоставляя их с базами данных. Такой подход ускоряет идентификацию и укрепляет защиту персональной информации. Внедрение ИИ в процессы удаленной регистрации упрощает взаимодействие пользователей с системой. Регистрация биометрических данных через мобильные устройства позволяет осуществлять сканирование лица или запись голоса в любое время. Дополнительную защиту обеспечивает технология «обнаружения живого лица» (liveness detection), минимизирующая возможность использования поддельной информации. Экономические преимущества использования ИИ в государственной информационной системе ЕБС становятся особенно заметными при оценке временных и финансовых затрат. Согласно данным ВЦИОМ, около 2,2 млн граждан уже зарегистрированы в системе. Оптимизация обработки данных сокращает время на один запрос в среднем на 300 секунд, что эквивалентно

5 минутам. При средней стоимости обработки одного обращения в 200 рублей такая автоматизация снижает операционные издержки банков и организаций. Оценка затрат на внедрение ИИ учитывает расходы на серверное оборудование, разработку программного обеспечения, обучение специалистов и технические сопровождение. Общая стоимость проекта составляет около 4,5 млрд рублей. Автоматизация процессов позволяет значительно сократить нагрузку на персонал. Ежегодная экономия операционных расходов достигает 700 млн рублей. Период окупаемости проекта составляет примерно 7 лет, что подчеркивает его экономическую эффективность и перспективность для дальнейшего развития биометрических технологий (табл. 4).

Внедрение технологий искусственного интеллекта в рамках государственной информационной системы ЕБС сопряжено с рядом значимых рисков, которые требуют комплексного анализа для обеспечения устойчивого функционирования системы.

Таблица 4

Экономический эффект внедрения технологий ИИ в ГИС ЕБС

Параметр	Единица измерения	Значение	Эффект	Полный расчет	Дополнительные пояснения
Общее число пользователей	Человек	2200000	Увеличение эффективности обслуживания	$(2200000 \times 300) / 1000 = 660$ млн	Экономия времени пользователей
Средняя стоимость одного запроса	Рубль	200	Снижение затрат на обработку данных	$660 \text{ млн} \times 0,3 = 198$ млн	Уменьшение времени идентификации
Стоимость внедрения ИИ	Рубль	4500000000	Расходы на оборудование и обучение	–4,5 млрд	Включает закупку серверов и ПО
Ежегодная экономия на операциях	Рубль	700000000	Снижение затрат на персонал	$(700 \text{ млн.} \times 5) = 3,5$ млрд	За 5 лет
Итог			Совокупный эффект: +660 млн.	$3,5 \text{ млрд} - 4,5 \text{ млрд} = -1$ млрд	Окупаемость ожидается через 7 лет

Источник: составлено автором.

Таблица 5

Риски проекта и меры по их нейтрализации

Риск	Вероятность	Последствия	Меры минимизации
Кибератаки и утечка данных	Высокая	Финансовые потери	Использование блокчейна, регулярные тесты на проникновение
Высокая стоимость внедрения	Средняя	Затраты	Привлечение инвесторов, использование грантов, внедрение облачных технологий
Негативное общественное восприятие	Средняя	Замедление внедрения	Информационные кампании, повышение прозрачности
Технические сбои	Низкая	Временные неудобства	Создание резервной инфраструктуры, регулярное обновление системы

Источник: составлено автором.

Одной из наиболее серьезных угроз остается возможность кибератак, способных привести к компрометации биометрической информации. Утечка данных может негативно сказаться на уровне доверия пользователей, что существенно снизит эффективность работы системы. Последствия подобных инцидентов включают не только финансовые убытки, но и ухудшение репутации проекта в целом. Процесс интеграции ИИ требует крупных начальных инвестиций, охватывающих приобретение серверного оборудования, разработку специализированного программного обеспечения и обучение специалистов. Высокие затраты на старте могут стать препятствием для оперативного внедрения технологии. Дополнительно, часть населения сохраняет скептическое отношение к новым цифровым решениям, опасаясь утечек личной информации или ненадежности автоматизированных процессов. Подобные опасения могут за-

медлить масштабирование ИИ в биометрической инфраструктуре. Еще одной важной проблемой является сложность алгоритмов, используемых в системах на базе ИИ. Высокий уровень технологической сложности повышает вероятность технических сбоев, которые способны вызывать временные затруднения в обслуживании пользователей. Для минимизации таких рисков необходимы регулярная модернизация оборудования, тестирование решений и обеспечение надежной технической поддержки.

Комплексное решение описанных вызовов станет ключевым фактором успешной реализации проекта, а также залогом повышения уровня доверия со стороны граждан (табл. 5).

Несмотря на очевидные преимущества, интеграция ИИ в ЕБС сталкивается с рядом вызовов. Одним из основных является высокая стоимость внедрения и обслуживания таких технологий.

Таблица 6

Преимущества и области применения мультимодальной системы идентификации

Параметр	Описание	Преимущества
Физиологические данные	Распознавание лица, отпечатки пальцев, анализ радужной оболочки	Высокая точность идентификации и устойчивость к подделке
Поведенческие особенности	Голосовая идентификация, анализ клавиатурного почерка	Устойчивость к изменениям внешности, дополнительный уровень безопасности
Динамические факторы окружения	Геолокация, реакция кожи, микроподергивания глаз	Снижение вероятности мошенничества, дополнение основных биометрических методов
Искусственный интеллект	Машинное обучение для обработки данных и оценки рисков	Адаптивность системы и минимизация ложных срабатываний
Протоколы безопасности	Шифрование, распределенное хранение, управление доступом	Надежная защита данных от утечек и кибератак

Источник: составлено автором.

Для работы ИИ-систем необходимы значительные вычислительные мощности, современные серверы и программное обеспечение, а также квалифицированные специалисты, способные разрабатывать и обслуживать эти решения. Кроме того, возникают риски, связанные с безопасностью больших данных, особенно если хакерские атаки приведут к утечке биометрической информации. Для минимизации рисков и повышения эффективности ЕБС с использованием ИИ рекомендуется разработка мультимодальных моделей идентификации, которые комбинируют различные типы биометрических данных, такие как лицо, голос и отпечатки пальцев (табл. 6).

Таким образом, проведенный анализ подтвердил значимость биометрических технологий как стратегического ресурса повышения безопасности в финансовой инфраструктуре России, особенно в условиях масштабной цифровизации и растущих угроз информационной безопасности.

Заключение

Выводы исследования подчеркивают ключевую роль биометрических технологий в трансформации финансовой сферы России, ориентированной на обеспечение безопасности данных, сокращение рисков мошенничества и оптимизацию взаимодействия с клиентами. Анализ подтверждает, что интеграция биометрии, дополненной искусственным интеллектом, способствует не только повышению точности идентификации, но и улучшению адаптивности систем в условиях изменения биометрических характеристик пользователей. Вместе с тем выявлены актуальные проблемы, включая недостаточную правовую регламентацию, уязвимость к кибератакам и необходимость

повышения доверия граждан через прозрачность процессов обработки данных. Рекомендации исследования сосредоточены на создании мультимодальных систем идентификации, объединяющих несколько биометрических методов, таких как анализ лицевых характеристик, голоса и отпечатков пальцев. Это направление позволяет повысить надежность и устойчивость систем, а также улучшить пользовательский опыт. Успешная реализация таких решений требует активного взаимодействия между государственными структурами и частными организациями, что станет основой для выработки эффективных стандартов безопасности и создания доверия среди пользователей. Перспективы дальнейших исследований включают разработку высокозащищенных протоколов для управления биометрическими данными и адаптацию технологий к международным требованиям. Возможности расширения применения биометрии в других секторах, таких как медицина, образование и транспорт, открывают дополнительные горизонты для научных разработок, что подчеркивает стратегическое значение этой области в условиях цифровой экономики.

Список литературы

1. Мизинов П.В., Коннова Н.С. К вопросу о значении термина «биометрия» // Гуманитарный вестник. 2023. № 5(103). DOI: 10.18698/2306-8477-2023-5-869.
2. Куликов Н.И., Кудрявцева Ю.В., Вдовина Е.С. Банковский менеджмент. Тамбов: Издательский центр ФГБОУ ВО «ТГТУ», 2019. 95 с. ISBN: 978-5-8265-2098-7.
3. Morake A., Khoza L., Bokaba T. Biometric technology in banking institutions: 'The customers' perspectives' // SA Journal of Information Management. 2021. № 23(1). DOI: 10.4102/sajim.v23i1.1407.
4. Датвасе С.С., Дешмукх Р.Р., Гупта Р.С. Современные доступные базы данных отпечатков ладони: обзор //

Известия ЮФУ. Технические науки. 2022. № 3. С. 27-37. DOI: 10.18522/2311-3103-2022-3-27-37.

5. Карцан И.Н. Биометрические данные: новые возможности и риски // Современные инновации, системы и технологии. 2023. № 3(3). С. 0201-0211. DOI: 10.47813/2782-2818-2023-3-3-0201-0211.

6. Иванов М.С. Анализ уязвимостей и актуальных биометрических методов аутентификации в системах безопасности // Молодой ученый. 2023. № 20 (467). С. 4-7. URL: <https://moluch.ru/archive/467/103000/> (дата обращения: 15.02.2025).

7. Белоусов А.Л., Левчук Е.Ю. Диджитализация банковского сектора // Финансы и кредит. 2018. Т. 24, № 2(770). С. 455-464. DOI: 10.24891/фс.24.2.455.

8. Аббасова О.М. Современные методы биометрии // Символ науки. 2024. Т. 2, № 2-2. С. 20-21.

9. Лукьянникова Ю.И., Мардамшина А.Р., Каменева Е.В. Биометрия: ключевой элемент информационной безопасности // Наукосфера. 2024. № 3-1. С. 195-199. DOI: 10.5281/zenodo.10817189.

10. Куминов В.П. Биометрия и информационная безопасность: аутентификация, идентификация, уязвимости и защита данных // Соискатель – приложение к журналу «Мир транспорта». 2023. № 4(15). С. 6-13.

11. Орцханова М.А., Бжеумихова О.И. Применения технологий биометрии в финансовой сфере проблемы и перспективы // Вестник Академии знаний. 2024. № 1(60). С. 436-439.

12. Перевертун Д.Р. развитие технологий биометрии в сфере аутентификации и защиты данных // Международный журнал информационных технологий и энергоэффективности. 2023. Т. 8, № 9(35). С. 37-40. URL: <http://openaccessscience.ru/index.php/ijcse/article/view/439/420> (дата обращения: 15.02.2025).

13. Жуков Я.В., Лысенко Р.Ю., Протас Н.Г., Тарасова Г.М. Биометрия. Как работает и какие риски несет? // Modern Economy Success. 2020. № 3. С. 13-19.

14. Новиков А. Биометрия в России: от настороженности к доверию? [Электронный ресурс]. URL: <https://www.novostiitkanala.ru/news/detail.php?ID=180671> (дата обращения: 17.02.2025).

15. Размер рынка биометрических датчиков, доля и глобальные тенденции – 2032 [Электронный ресурс]. URL: <https://www.gminsights.com/ru/industry-analysis/biometric-sensors-market> (дата обращения: 18.02.2025).

16. Мировой рынок биометрии – 39,37 млрд долларов в 2023 году [Электронный ресурс]. URL: <https://www.secuteck.ru/news/mirovoj-gynok-biometrii-39-37-mlrd-dollarov-v-2023-godu> (дата обращения: 10.02.2025).

17. Протасов П.А. Биометрия в банковской системе РФ // Вестник Томского государственного университета. Экономика. 2020. № 49. С. 141-148. DOI: 10.17223/19988648/49/10.

18. Единая биометрическая система (ЕБС) [Электронный ресурс]. URL: [https://www.tadviser.ru/index.php/Продукт:Единая_биометрическая_система_\(ЕБС\)](https://www.tadviser.ru/index.php/Продукт:Единая_биометрическая_система_(ЕБС)) (дата обращения: 10.02.2025).

19. Биометрия в банках: что это такое [Электронный ресурс]. URL: <https://brobank.ru/chto-takoe-biometriya/> (дата обращения: 10.02.2025).

20. Рукобратский П.Б., Козырева Н.О. Биометрическая идентификация: базовый компонент цифровой инфраструктуры финансовых рынков // Вестник Тверского государственного университета. 2023. № 2(62). С. 20-32. DOI: 10.26456/2219-1453/2023.2.020-032.

21. Евкина И.И., Шарыпова Т.Н. Киберпреступность как угроза информационной безопасности // Инновации. Наука. Образование. 2021. № 36. С. 375-377.