DOI: 10.24412/2070-1381-2022-93-134-149

Варианты использования Единой биометрической системы как инструмента доступа к цифровому профилю гражданина[1]

Долганова Ольга Игоревна
Кандидат экономических наук, доцент, Финансовый университет при Правительстве Российской Федерации, Москва, РФ.
E-mail: oidolganova@fa.ru
SPIN-код РИНЦ: 5350-5145
ORCID ID: 0000-0001-6060-5421

Чистякова Дарья Александровна
Студент бакалавриата, Финансовый университет при Правительстве Российской Федерации, Москва, РФ.
E-mail: 190705@edu.fa.ru
ORCID ID: 0000-0002-6132-4135

Аннотация
Биометрические системы идентификации начинают использоваться государством и бизнесом в ходе оказания услуг, а также в рамках реализации процессов контроля и обеспечения общественной и корпоративной безопасности. Эта тенденция характерна для России так же, как и для других стран. Разработка и введение в действие в нашей стране цифрового профиля гражданина порождают риски утечки, несанкционированного доступа и использования данных физических лиц. Единая биометрическая система, создаваемая в России, становится не только надежным средством защиты данных, содержащихся в цифровом профиле гражданина, но и позволяет расширить варианты их использования органами власти, медицинскими учреждениями, финансовыми структурами и прочими организациями. В рамках данного исследования был рассмотрен зарубежный опыт и специфика применения биометрии в РФ, а также проведен опрос 186 российских представителей поколения Z для выявления их понимания, восприятия биометрической системы и намерений использовать ее для идентификации. На основании полученных результатов были разработаны предложения по расширению возможностей применения Единой биометрической системы в рамках сервисов цифрового профиля гражданина РФ, а также сформулированы рекомендации по учету опасений. Данная работа может быть полезна для более глубокого исследования вариантов применения Единой биометрической системы совместно с цифровым профилем гражданина в сфере реализации государственных функций и услуг, а также при разработке мероприятий по снижению негативного отношения граждан к более активному использованию подобных решений в разных жизненных ситуациях.

Ключевые слова
Биометрия, идентификация личности, проверка личности, Единая биометрическая система, цифровой профиль гражданина.

Use Cases of Unified Biometric System as a Tool for Accessing Citizen's Digital Profile[2]

Olga I. Dolganova
PhD, Associate Professor, Financial University under the Government of the Russian Federation, Moscow, Russian Federation.
E-mail: oidolganova@fa.ru
ORCID ID: 0000-0001-6060-5421

Darya A. Chistyakova
Bachelor student, Financial University under the Government of the Russian Federation, Moscow, Russia Federation.
E-mail: 190705@edu.fa.ru
ORCID ID: 0000-0002-6132-4135

Abstract
Biometric identification systems are beginning to be used by the state and business when providing the services, as well as in the framework of implementing control processes and ensuring public and corporate security. This trend is typical both in Russia and abroad. The development and implementation in Russia of citizen's digital profile of generate new risks of leakage, unauthorized access, and use of personal data. The Unified Biometric System being created in Russia is not only becoming a reliable means of protecting the data contained in citizen's digital profile, but also allows expanding the options for their use by authorities, medical institutions, financial structures, and other organizations. As part of this study, the world experience of the use of biometrics, and the specifics of its use in Russia were considered. A survey of 186 Russian representatives of the Z generation to identify their understanding, perception and intentions to use biometric identification systems was carried out. Based on the results obtained, proposals were developed to expand the possibilities of using the Unified Biometric System within the framework of the services of citizen's digital profile, and recommendations were formulated to consider the related concerns. This work may be useful for a deeper study of the options for using the Unified Biometric System in conjunction with citizen's digital profile in the sphere of implementing government functions and services, as well as developing the measures to reduce the negative attitude of citizens to active use of such solutions in various life occasions.

Keywords
Biometrics, personal identification, identity verification, Unified Biometric System, citizen's digital profile.

[1] Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансового университета при Правительстве Российской Федерации.
[2] The article was prepared based on the results of a research carried out at the expense of budgetary funds under the state assignment of the Financial University.

Введение

Биометрия используется человечеством с давних времен. По некоторым оценкам, первое ее применение было зафиксировано еще в VI веке нашей эры в Китае [Кузьминых, Маслова 2021]. Тогда начали применять дактилоскопические методы для идентификации людей. Биометрические технологии стремительно входят в повседневную жизнь людей во всем мире. Новые решения для сбора и обработки биометрических данных призваны ограничить возможности использования поддельных документов и кражи личных данных, терроризма и киберпреступности. Биометрия уже используется в медицине, банковских услугах, маркетинговых исследованиях и многих других отраслях, в которых требуется идентификация личности. Биометрические системы продолжают развиваться и расширять границы применения, что сопровождается возникновением правовых, организационных и технических проблем их эксплуатации, которые требуют решения [Дивольд 2021].

Данные вопросы довольно активно изучаются учеными разных стран. Так, например, в базе Scopus за период с 2017 по 2021 год по словосочетанию «Biometrics, personal identification» находится 669 статей. Из них 23 публикации написаны российскими учеными. При этом подавляющее большинство исследований (71%) относятся к физико-математическим, инженерным и компьютерным наукам. При поиске статей и тезисов конференций за этот же период в Научной электронной библиотеке elibrary по аналогичному запросу, но на русском языке («биометрия, идентификация личности») было найдено 58 публикаций. В них также в основном рассматриваются технологические аспекты разработки и применения биометрических систем. Вопросы прикладного характера в части совершенствования, одновременного повышения эффективности и упрощения контрольных и идентификационных процедур при взаимодействии граждан с органами власти и бизнесом с помощью биометрических систем в российской научной литературе разбираются крайне мало. Поэтому цель данного исследования — выявление перспективных вариантов использования Единой биометрической системы в качестве доступа к сервисам цифрового профиля гражданина Российской Федерации.

Основными задачами являются рассмотрение зарубежного опыта эксплуатации биометрических информационных систем, изучение особенностей использования биометрии в России, а также изучение мнения представителей поколения Z о возможностях и рисках применения биометрических систем в повседневной жизни.

Назначение и особенности применения биометрических систем идентификации

Согласно Международной организации по стандартизации (ISO), биометрия определяется как средство биологического процесса для распознавания и анализа человека на основе его физиологических (отпечатки пальцев, лицо, радужка, отпечатки ладоней) и поведенческих характеристик (подпись, походка, нажатие клавиш, голос/речь)[3]. Технологии биометрической идентификации совершенствуются настолько быстро, что сложно предсказать, какими они будут через несколько лет. Предполагается, что пароли, которые было сложно использовать, менять и запоминать, останутся в прошлом. Более того, пластиковые карты скоро также отойдут на второй план. Безопасность в будущем будет обеспечиваться за счет биометрии, что, вероятно, связано с простотой использования для граждан и более высоким уровнем точности идентификационных процедур для проверяющих органов.

[3] ГОСТ ISO/IEC 2382-37-2016 Информационные технологии (ИТ). Словарь. Часть 37. Биометрия // Электронный фонд правовых и нормативно-технических документов [Электронный ресурс]. URL: http://docs.cntd.ru/document/1200144206 (дата обращения: 10.04.2022).

Биометрия уже используется во многих сферах жизни общества: например, в сфере обеспечения общественного порядка и безопасности, для проверки физических лиц в ходе осуществления пограничного, выездного и миграционного контроля, гражданской идентификации (на выборах, голосованиях и т.д.), в здравоохранении. Данные технологии используются также в рамках организации физического и логического доступа к различным объектам в коммерческих структурах (в банках и крупных высокотехнологичных компаниях).

Возникает много вопросов этического характера, поскольку биометрические данные, как правило, обрабатываются с помощью технологий искусственного интеллекта и машинного обучения. И здесь возникает ряд вопросов: насколько используемые алгоритмы и системы этически корректно работают и не нарушает ли их применение права граждан на неприкосновенность личной жизни и частной информации [Долганова 2021]? Другим важным аспектом является обеспечение соразмерности запрашиваемых биометрических данных целям, для которых они собираются [Castellano, Ferrer 2022].

Открытые биометрические данные — это лишь часть всевозможных биометрических параметров. Согласно анализу IMARC Group[4], биометрические системы быстро развиваются из-за увеличения числа нарушений безопасности и мошенничества с транзакциями по всему миру. Это подтолкнуло производителей к переходу от однообразных верифицирующих устройств, таких как лицо, отпечаток пальца, радужка и голос, к широкому спектру мультимодальных, полностью автоматизированных систем распознавания. Одной из таких тенденций является использование аутентификации по венам, которая учитывает уникальный рисунок, образованный кровеносными сосудами [Safiullina, Maturov 2021]. Другим идентификационным параметром может быть походка [de Rosa et al. 2022], манера речи человека.

Наиболее распространенной является классификация биометрических характеристик на физиологические и поведенческие. Физиологические, в свою очередь, подразделяют на морфологические и поведенческие. Отпечатки пальцев, форма рук, рисунок вен, радужная оболочка и сетчатка глаз, форма лица — морфологические параметры для идентификации. В качестве биологических идентификаторов используются слюна, кровь, другие биологические выделения, однако стоит отметить, что данные идентификаторы используются преимущественно в правоохранительной среде при расследовании преступлений. Поведенческие измерения — наиболее новый формат биометрических данных, который все чаще задействуют в различных биометрических системах. Они позволяют накапливать информацию о голосе, динамике подписи, нажатия клавиш, походке, звуке шагов, жестов и т.д.[5] Согласно опросу ИТ-специалистов, распознавание отпечатков пальцев на сегодняшний день является самым популярным типом биометрической аутентификации, за которым следует распознавание лиц[6]. Отмечается, что поведенческие характеристики становятся основным трендом биометрии. Анализ походки или нажатия клавиш позволяет осуществлять непрерывную аутентификацию, чтобы гарантировать, что лицо, получающее доступ к данным компании, учетным записям или другим ресурсам, по-прежнему получает их, иными словами, не была произведена подмена пользователя. По этим причинам поведенческая биометрия все чаще используется для выявления мошенничества и управления инсайдерскими угрозами [Liang et al. 2020].

[4] Top Players in the Biometrics Market // Imarc [Электронный ресурс]. URL: https://www.imarcgroup.com/biometrics-manufacturing-companies (дата обращения: 12.04.2022).
[5] What is biometrics? // Thales [Электронный ресурс]. URL: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics (дата обращения: 15.04.2022).
[6] Data Snapshot: Biometrics in the Workplace Commonplace, but Are They Secure? // Spiceworks [Электронный ресурс]. URL: https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-inthe-workplace-commonplace-but-are-they-secure (дата обращения: 17.04.2022).

К определению характеристик для идентификации предъявляется ряд требований. На концептуальном уровне они были сформулированы следующим образом[7]:

- универсальность: этой характеристикой должны обладать все. Это связано с тем, что биометрическое устройство будет инклюзивным, позволяющим использовать его как можно большему количеству пользователей;
- уникальность: по данной характеристике люди не могут быть похожи. Потому что мы должны количественно определить характеристики, которые отличают одного человека от другого, если мы хотим их идентифицировать;
- постоянство: выбранная характеристика должна быть неизменной во времени. Крайне важно, чтобы любая характеристика, которую мы выбираем, вычислялась последовательно, иначе человек может казаться другим человеком в разное время;
- измеримость: выбранная характеристика должна быть количественно измеримой. Это должно быть определено, чтобы устранить всю двусмысленность в отношении того, что измеряется.

Этим характеристикам стремятся соответствовать большинство современных биометрических систем.

Однако идентификация по одной характеристике не является надежной, хотя и активно используется. Многие системы распознавания реализованы на основе одномодальных биометрических данных, таких как распознавание лица или распознавание голоса. Решения, использующие одномодальный режим, имеют ограничения, главным образом когда данные содержат выбросы и поврежденные наборы данных. Мультимодальные биометрические системы привлекают внимание исследователей из-за их превосходства — лучшей безопасности по сравнению с одномодальной биометрической системой и высокой эффективности распознавания [Joseph et al. 2022].

Так как характеристики в биометрических системах являются уникальными и постоянными, получение доступа злоумышленников к ним может привести к непоправимым последствиям. «Лаборатория Касперского» еще в 2016 году обнаружила 12 продавцов, которые предлагали устройства для кражи отпечатков пальцев, и 3 исследователей, разрабатывающих системы распознавания рисунка вен и радужной оболочки глаз. К 2022 году ситуация ухудшилась и количество хакерских атак на биометрические системы лишь возросло[8].

Помимо очевидных рисков по получению несанкционированного доступа к биометрическим данным, существуют и иные виды, которые включают в себя потенциальное злоупотребление персональными данными со стороны организаций, имеющих к ним доступ, или психологический стресс населения, вызванный постоянным мониторингом [Hoffmann, Mariniello 2021]. Эти риски также необходимо учитывать при внедрении биометрических технологий, так как они способны спровоцировать массовый отказ граждан от биометрической идентификации.

Международный опыт использования биометрических систем

Компания ReportLinker в марте 2022 года выпустила отчет с анализом рынка биометрических систем. По их оценкам, прогнозируется рост объема мирового рынка биометрических систем с 42,9 млрд долларов США в 2022 году до 82,9 млрд долларов США к 2027 году при среднегодовом

[7] Biometrics Simplified // Towards Data Science [Электронный ресурс]. URL: https://towardsdatascience.com/biometrics-simplified-e9ed096d0025 (дата обращения: 17.04.2022).
[8] Технологии биометрической идентификации // TAdviser [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Технологии_биометрической_идентификации (дата обращения: 10.04.2022).

темпе роста 14,1%[9]. Более того, сегмент бесконтактных биометрических систем будет расти самыми высокими темпами среднегодового темпа роста в течение прогнозируемого периода. Эксперты связывают такой подъем с интеграцией с прорывными цифровыми технологиями.

Несмотря на существенный рост рынка биометрических систем, Европейский парламент и Еврокомиссия относятся к подобным технологиям с осторожностью. В 2021 году было рекомендовано наложить запрет на использование систем распознавания лиц в общественных местах правоохранительными органами. Предложенный Еврокомиссией законопроект призван также наложить ряд запретов и на использование других технологий биометрической идентификации[10].

Анализ Европейской комиссии в 2020 году по отдельным технологиям показывает, что биометрические технологии являются плохо используемыми технологиями: обработка естественного языка (распознавание речи, машинные переводы или чат-боты) была принята только каждой десятой фирмой, 9% предприятий используют компьютерное зрение (визуальная диагностика, распознавание лиц или изображений), а использование анализа настроений (анализ эмоций и поведения) встречается еще реже — 3%. Каждая десятая из всех компаний ЕС полагается на биометрическую аутентификацию и верификацию на рабочем месте, при этом показатели использования колеблются от 24% на Мальте до 4% в Словении и Болгарии[11].

Тем не менее ряд стран активно использует биометрические технологии в различных целях. Крупнейшая биометрическая система идентификации жителей Индии Aadhaar, содержит в себе фотографию, десять отпечатков пальцев и два скана радужной оболочки глаз. По информации на 11 июля 2022 года, в Индии было выдано более 1, 3 млрд удостоверений личности Aadhaar (более 93 % населения Индии)[12]. По словам министра финансов Аруна Джейтли, Aadhaar предоставляет каждому индусу профиль, что делает ряд услуг более доступными для граждан[13]. В качестве преимуществ от внедрения системы выделяют:

— снижение уровня коррупции;

— снижение стоимости оказания коммунальных услуг;

— исключение ряда посредников при оказании различных государственных и негосударственных услуг.

Aadhaar позволяет осуществлять процедуру KYC (Know Your Customer, идентификация личности клиента) для мобильных подключений и банковских счетов, что позволяет, с одной стороны, выявлять и идентифицировать финансовые преступления, а с другой — предоставить гражданам возможность открывать банковские счета удаленно. UIDAI (Единый орган

[9] Biometric System Market with COVID-19 Impact Analysis by Authentication Type, Type, Offering Type, Mobility, Vertical & Region — Global Forecast to 2027 // ReportLinker [Электронный ресурс]. URL: https://www.reportlinker.com/p04397168/Biometric-System-Market-by-Authentication-Type-Component-Function-Application-and-Region-Global-Forecast-to.html?utm_source=GNW (дата обращения: 20.04.2022).
[10] Биометрическая идентификация (мировой рынок) // TAdviser [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Биометрическая_идентификация_(мировой_рынок) (дата обращения: 12.04.2022).
[11] European enterprise survey on the use of technologies based on artificial intelligence // European Commission [Электронный ресурс]. URL: https://op.europa.eu/en/publication-detail/-/publication/f089bbae-f0b0-11ea-991b-01aa75ed71a1/language-en (дата обращения: 17.04.2022).
[12] Macdonald A. UIDAI CEO lauds successes of Aadhaar biometric ID at India Digital Week 2022 // Biometric Update.com [Электронный ресурс]. URL: https://www.biometricupdate.com/202207/uidai-ceo-lauds-successes-of-aadhaar-biometric-id-at-india-digital-week-2022 (дата обращения: 19.04.2022).
[13] Budget 2018: Govt. To Launch an Aadhaar Like Unique Identity for Enterprises Too // Inc42 [Электронный ресурс]. URL: https://inc42.com/buzz/budget-2018-aadhaar-unique-identity/ (дата обращения: 13.04.2022).

идентификации Индии) изначально предоставлял всем службам аутентификации бесплатные услуги, чтобы снизить входной барьер. С 2019 года из-за его высокой востребованности сервис стал платным[14].

Согласно NYmag, в США ритейлеры также используют распознавание лиц. Данная технология набирает популярность в этой области в части идентификации покупателей, в том числе с целью предупреждения краж. Если система на входе в магазин распознает вора или, наоборот, покупателя премиум-сегмента, то она уведомляет менеджера. Данная технология станет также важнейшим инструментом маркетинга в ближайшем будущем. Однако законы о конфиденциальности в Иллинойсе, Техасе, Вашингтоне и Калифорнии стали серьезным препятствием для внедрения подобных биометрических систем[15]. При этом прогнозируют, что на долю США к 2024 году будет приходиться более 30% от биометрического рынка. Предполагается, что рост будет наблюдаться и в Азиатско-Тихоокеанском регионе[16].

Согласно исследованию, проведенному среди 96 стран[17], Китай был признан самым «злостным преступником» в мире из-за инвазивного использования биометрических данных. Китай был самым быстрорастущим пользователем камер наблюдения в мире, и эта тенденция в основном обусловлена использованием этих технологий правительственными органами. Относительно новый арсенал Китая включает проекты массового видеонаблюдения, включающие технологию распознавания лиц; программное обеспечение для распознавания голоса, которое может идентифицировать говорящих во время телефонных звонков; и обширную программу сбора ДНК и отпечатков пальцев. Кроме того, чиновники работают над развитием общенациональной системой социального кредита (SCS), предназначенной для оценки поведения каждого гражданина Китая. Через SCS китайские власти могут объединять с национальным идентификационным кодом гражданина информацию по различным вопросам: от налоговых платежей, личных финансов и регистрации бизнеса до нарушений правил дорожного движения, поведения в общественных местах (курение, распитие алкогольных напитков, дебоширство и пр.)[18].

Южноафриканская система ABIS — это тип биометрической поисковой системы, которая выполняет сравнение образца с образцами в базе данных, содержащей множество биометрических шаблонов. Это позволяет сопоставлять живой образец со многими существующими биометрическими шаблонами, чтобы найти запись конкретного человека и подтвердить его личность. Сегодня в государственном секторе используются два основных типа ABIS: криминальный ABIS и гражданский ABIS. Ключевой отличительной чертой криминальной ABIS является ее способность обрабатывать и анализировать «скрытые» отпечатки пальцев и изображения лиц. Варианты использования гражданской ABIS включают добровольную отправку

[14] Aadhaar: Start Paying Rs20 for Each eKYC, 50 paisa for Yes/No Authentication Now! // Moneylife [Электронный ресурс]. URL: https://www.moneylife.in/article/aadhaar-start-paying-rs20-for-each-ekyc-50-paisa-for-yes-no-authentication-now/56557.html (дата обращения: 19.04.2022).
[15] There Will Be No Turning Back on Facial Recognition // Intelligencer [Электронный ресурс]. URL: https://nymag.com/intelligencer/2019/11/the-future-of-facial-recognition-in-america.html (дата обращения: 13.04.2022).
[16] Global Biometrics Market Predicted to Flourish by 2028 Due to Increasing Utilization of Smartphones and the Rising Integration of Biometric Systems with IoT Devices // GlobeNewswire [Электронный ресурс]. URL: https://www.globenewswire.com/en/news-release/2022/05/16/2444019/0/en/Global-Biometrics-Market-Predicted-to-Flourish-by-2028-Due-to-Increasing-Utilization-of-Smartphones-and-the-Rising-Integration-of-Biometric-Systems-with-IoT-Devices-215-Pages-Procl.html (дата обращения: 20.05.2022).
[17] Biometric data collection: China is the most invasive user in the world, according to a 96-country study // South China Morning Post [Электронный ресурс]. URL: https://www.scmp.com/news/people-culture/article/3122187/biometric-data-collection-china-most-invasive-user-world (дата обращения: 15.04.2022).
[18] China's Social Credit System // Institute for Social Capital [Электронный ресурс]. URL: https://www.socialcapitalresearch.com/chinas-social-credit-system-social-capital/ (дата обращения: 17.05.2022).

биометрических данных в учреждения системы здравоохранения для идентификации пациента, в различные организации для идентификации клиентов и сотрудников и для использования банковских сервисов[19].

Существует и ряд других биометрических систем, которые находятся на разных стадиях развития и применения. Европейским научным сообществом принято выделять следующие состояния биометрической системы[20]:

— предрыночная разработка технологии;

— регистрация физических лиц;

— сбор и обработка живых шаблонов;

— сравнение живых шаблонов с сохраненными шаблонами и вычисление соответствующего балла;

— реакция системы в соответствии с политикой принятия решений (например, предоставление доступа/отказ в доступе, запрос дополнительных учетных данных, арест);

— цикл обратной связи, уточнение сохраненного шаблона и совершенствование технологии в целом;

— хранение и обработка данных для будущих целей, помимо идентификации.

Общие характеристики прослеживаются и в вариантах использования биометрических технологий, наиболее распространенными из которых являются:

— пограничный контроль и безопасность аэропорта;

— управление посещаемостью со стороны работодателя;

— финансовые данные и защита личных данных;

— решения для физического или логического доступа к материальным значимым объектам.

Электронная биометрическая система в Российской Федерации

В России существует собственная государственная система биометрии — Единая биометрическая система (ЕБС). Оператором Единой биометрической системы по распоряжению правительства № 293-р от 22 февраля 2018 года назначен «Ростелеком»[21].

С 2020 года идентификация посредством ЕСИА (Единая система идентификации и аутентификации) и ЕБС приравнивается к идентификации по паспорту. Согласно планам в рамках программы «Цифровая экономика Российской Федерации» в инициативе «Цифровой профиль гражданина», в 2022 году доступ к услугам по биометрии должны получить 20 млн граждан, в 2023 г. — 30 млн, а в 2024 г. — уже 50 млн. К 2030 году планируется обеспечить возможность идентификации 75 млн россиян (51% населения страны) с помощью данных государственной Единой биометрической системы на добровольной основе для получения услуг[22].

[19] Delays persist in South Africa's automated biometric identification project completion // Biometric update.com [Электронный ресурс]. URL: https://www.biometricupdate.com/202103/delays-persist-in-south-africas-automated-biometric-identification-project-completion (дата обращения: 18.04.2022).
[20] Biometric Recognition and Behavioural Detection // European Parliament [Электронный ресурс]. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf (дата обращения: 18.04.2022).
[21] О единой биометрической системе // Ростелеком [Электронный ресурс]. URL: https://bio.rt.ru/about/ (дата обращения: 10.04.2022).
[22] Мониторинг СМИ. С. 5. // Data Economy Russia [Электронный ресурс]. URL: https://files.data-economy.ru/Digest/2022-01-26-digest.pdf (дата обращения: 18.04.2022).

Единая биометрическая система построена на ряде принципов: мультимодальность, мультивендорность, liveness, выявление аномалий, безопасность данных. При проектировании ЕБС в качестве идентификаторов были выбраны изображение лица и голос, что связано, во-первых, с уникальностью этих параметров, во-вторых, с реализуемостью, то есть сканирование и анализ лица и голоса не требуют специфического оборудования и каких-либо временных затрат и не вызывают сложностей у граждан.

ЕБС обеспечивает безопасность, так как стандарты согласованы с ФСБ России и размещение происходит на отечественном ПО — ОС Astra Linux Special Edition[23]. В общем виде архитектура ЕБС представлена на Рисунке 1.

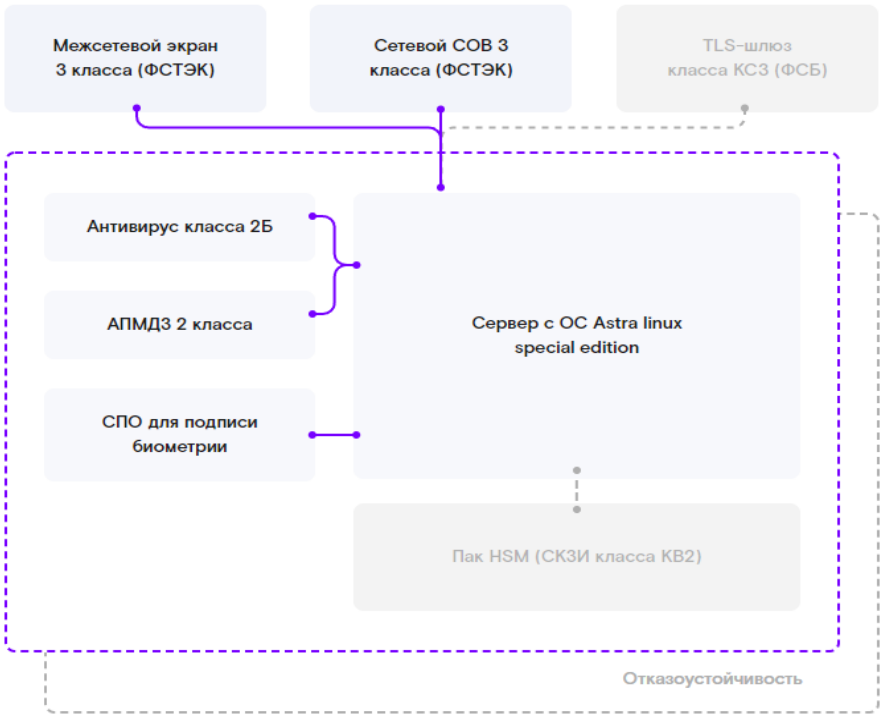

Рисунок 1. Архитектура ЕБС[24]

ЕБС отличается и своей доступностью. Зарегистрировать биометрию можно в 13 300 отделениях 231 банка в 95% городов России[25]. ЕБС напрямую связан с порталом Госуслуг, что позволяет расширять его функционал. ЕБС выделяет наиболее перспективные отрасли применения биометрии: предоставление госуслуг, дистанционное заключение договоров, оплата проезда, удаленная сдача экзаменов, участие в судебных заседаниях по видеосвязи, СКУД (Система контроля и управления доступом), оплата покупок, предоставление услуг в нотариате и т.д. В некоторых сферах технология уже реализована.

На данный момент ЕБС готова к применению в таких сферах, как банковские услуги, квалифицированная электронная подпись, нотариат, БиоСКУДЫ с тепловизорами и детекцией масок, государственные услуги, телеком, образование, интеграция с цифровым профилем гражданина и т.д. В разработке находятся следующие проекты: транспорт, телемедицина,

[23] О единой биометрической системе // Ростелеком [Электронный ресурс]. URL: https://bio.rt.ru/about/ (дата обращения: 10.04.2022).
[24] Источник: О единой биометрической системе // Ростелеком [Электронный ресурс]. URL: https://bio.rt.ru/about/ (дата обращения: 10.04.2022).
[25] О единой биометрической системе // Ростелеком [Электронный ресурс]. URL: https://bio.rt.ru/about/ (дата обращения: 10.04.2022).

торговля рецептурными лекарственными средствами, торговля алкоголем, судопроизводство, электронное голосование, мобильный идентификатор[26]. В качестве преимуществ для бизнеса и государства можно выделить:

— снижение затрат и сокращение времени на обслуживание;

— неограниченная география присутствия;

— дистанционная идентификация и заключение договора;

— легкий и безопасный перевод услуг из офлайн в онлайн;

— достоверные данные о клиентах;

— бесконтактная технология.

Граждане получают следующие преимущества:

— получение услуг в любом месте и в любое время;

— исключение бумажных договоров;

— усиленная безопасность (ГОСТ, подпись класса КВ2);

— возможность выбора лучших предложений на рынке.

Портал Госуслуги уже содержит паспортные данные, СНИЛС, номер полиса ОМС, сведения о водительских удостоверениях и ряде других документов[27]. А идентификация для части государственных услуг уже обеспечивается с помощью биометрической системы[28], где используются данные лица и голоса человека[29].

Предполагается, что варианты использования сервиса цифрового профиля гражданина будут расширяться, а следовательно, это обеспечит и экспансию биометрии. Она позволит идентифицировать гражданина и получить доступ к части информации о нем. Такое развитие несет в себе ряд преимуществ: снижение числа случаев выдачи себя за другого человека, снижение ошибок при использовании данных документов в связи с человеческим фактором, увеличение скорости обслуживания в различных сферах и так далее.

В первом квартале 2022 года нами был проведен опрос среди граждан Российской Федерации, в котором участвовало 186 респондентов. Респонденты преимущественно относятся к возрастной категории 18–25 лет и проживают в Москве, Санкт-Петербурге и Московской области. Их мнение и отношение к реализуемым цифровым решениям являются наиболее значимыми, поскольку в основном они являются наиболее активными участниками интернет-коммуникаций как с государством, так и с бизнесом [Лапидус и др. 2020]. Результаты опроса представлены на Рисунке 2.

[26] Там же.
[27] Концепция и архитектура Цифрового профиля — ЕСИА 2.0 // Аналитический центр при Правительстве Российской Федерации [Электронный ресурс]. URL: https://clck.ru/TqGTX (дата обращения: 10.05.2022).
[28] Постановление Правительства Российской Федерации № 1376 от 22.12.2012 «Об утверждении Правил организации деятельности многофункциональных центров предоставления государственных и муниципальных услуг» // Гарант [Электронный ресурс]. URL: http://base.garant.ru/70290064/ (дата обращения: 12.04.2022).
[29] Лицо и голос вместо документов // Ростелеком [Электронный ресурс]. URL: https://bio.rt.ru/citizens/ (дата обращения: 15.04.2022).

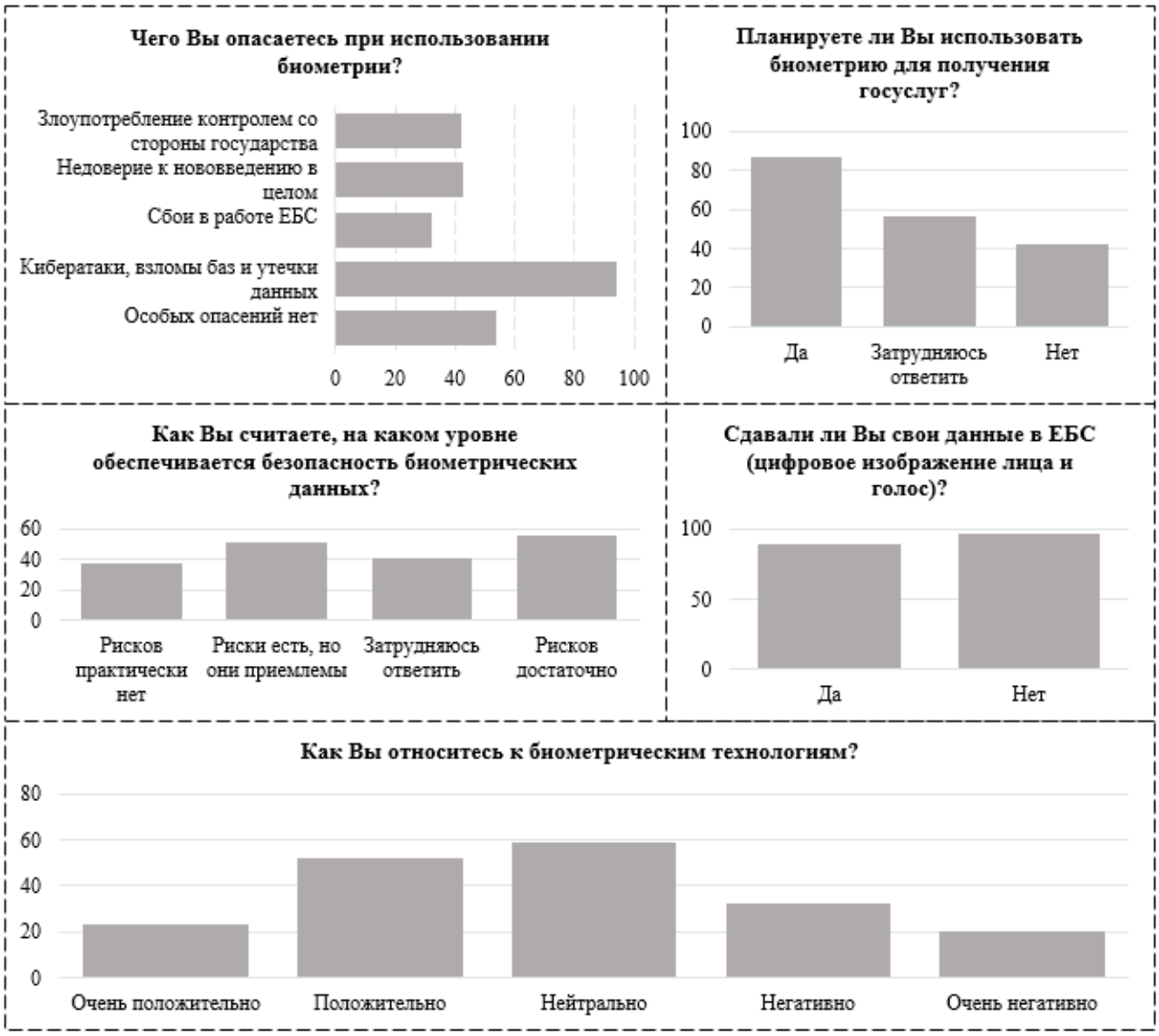

Рисунок 2. Результаты опроса об отношении к ЕБС[30]

Согласно полученным данным, количество людей, которые положительно настроены к биометрическим технологиям, выше, чем тех, кто настроен негативно. Однако большинство респондентов сами не сдавали свои биометрические данные в ЕБС, при этом стоит отдельно отметить, что большинство опрошенных — молодежь из крупнейших мегаполисов, следовательно, среди всего населения России данный показатель намного ниже. Это говорит о недостаточной степени распространенности среди населения биометрических технологий. Тем не менее большинство респондентов готовы использовать биометрию для получения госуслуг, но и эти люди опасаются данного метода идентификации. Большинство считает, что рисков более чем достаточно. Люди боятся кибератак, взломов баз с персональными данными, их утечки, что является особо актуальным и не может не рассматриваться при изучении биометрических технологий. В России, по данным специалистов «Лаборатории Касперского», средняя продолжительность атак за февраль и март 2022 года превышала сутки, составив 29,5 часа, хотя в 2021 году этот показатель равнялся 12 минутам[31]. Эти показатели говорят об обоснованности опасений граждан, поскольку при утечке биометрических данных, в отличие, например, от классических логинов и паролей,

[30] Составлено авторами.
[31] «Касперский» выявил рост числа DDoS-атак на компании России в 8 раз // РБК [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/01/04/2022/624699a89a79473501fa15f9 (дата обращения: 15.05.2022).

они не подлежат смене. Поэтому необходимо принимать меры по снижению данных рисков и убеждению населения в том, что данная система обладает всеми необходимыми средствами защиты персональных данных [Бутов, Карякин 2020].

Возможности расширения применения ЕБС как основы для развития цифрового профиля граждан

Помимо заявленных траекторий для внедрения ЕБС, существует множество иных сфер, которые также нуждаются в идентификации граждан, особенно при наличии связи с цифровым профилем гражданина (ЦПГ) и коммуникации с государственными и коммерческими структурами в режиме онлайн.

Основной документ, который требуется для предъявления во многие учреждения (как государственные, так и негосударственные), — паспорт. На его примере и рассмотрим несколько сфер применения.

Ряд культурных учреждений (музеи, театры, галереи и другие) продают билеты только при наличии документов, подтверждающих личность (чаще всего паспорт): билет оформляется на конкретного человека, и при входе его идентифицируют. В определенные дни это создает очереди, поэтому можно усовершенствовать процесс пропуска через ЕБС, что увеличит скорость прохода людей через пункты контроля и снизит вероятность использования поддельных документов (что критично при проходе на объекты федерального значения: Останкинская башня, Московский Кремль и т.д.). Тем самым повышается безопасность музейных фондов: снижается вероятность кражи, порчи имущества, террористических актов и пр. Более того, систему пропуска можно организовать с помощью аппаратного и программного обеспечения, что позволит высвободить трудовые ресурсы для решения других задач. Аналогично можно предложить использовать биометрию для прохода на крупнейшие стадионы (на мероприятия различного характера: концерты, спортивные соревнования, научные выступления), где основной целью безопасности является снижение вероятности возникновения беспорядков на трибунах и предотвращение террористических актов.

Помимо посещения культурных учреждений, данная проблематика актуальна и в медицинской сфере: выдача справок о заболевании, оформление больничных листов. При создании подобных документов следует выявлять личность пациента, так как возможны ситуации выдачи себя за другого человека. Идентификация через ЕБС позволит не только определить гражданина, но и получить быстрый доступ к ЕГИСЗ (Единая государственная информационная система здравоохранения), где уже накапливается информация о пациенте. Кроме того, это снимает необходимость предъявлять полис ОМС и другие документы для подтверждения личности.

В государственном секторе также возможно использование ЕБС в качестве проверки сотрудниками ГИБДД. При интеграции системы биометрической идентификации с цифровым профилем гражданина ГИБДД может получить доступ, например, к водительскому удостоверению и сопутствующим документам, что позволит снизить частоту использования поддельных документов гражданами и увеличить скорость и эффективность проверки данных сотрудником ГИБДД на дороге.

В перспективе возможно использование биометрии в негосударственных организациях. Самый распространенный пример в мировой практике — оплата при посещении магазина.

Подобные пилотные проекты уже реализованы и в России[32]. Однако на данный момент эта услуга не очень распространена, в том числе из-за опасений граждан: связь биометрии и финансов является очень рискованной и требует длительного времени для принятия обществом. В перспективе биометрия может быть использована как инструмент для анализа покупательской корзины с целью формирования специальных индивидуальных предложений, но такой вариант должен осуществляться исключительно при согласии гражданина и в любой момент может быть им запрещен, то есть должна быть обеспечена возможность просматривать организации, у которых есть доступ к ЕБС, и при желании закрывать/разрешать доступ к своим биометрическим данным гражданином самостоятельно. Такой подход, когда человек сам управляет своими персональными данными, активно пропагандируется во Франции, Эстонии и Швейцарии.

Возможно также использование ЕБС и в других целях. Один из вариантов — процесс приема на работу. Гражданин для оформления должен передать множество информации и документов: паспортные данные, СНИЛС, номер полиса ОМС, трудовую книжку, данные об образовании и так далее. Однако при связи с ЦПГ эти данные можно предоставить в любой момент, даже находясь в самой компании, при реализации в сервисах ЦПГ соответствующих функциональных возможностей. Это позволит снизить трудозатраты отделов по управлению персоналом и служб безопасности на проверку подлинности документов, повысить скорость передачи информации, снизить количество ошибок при переносе данных. Более того, биометрические технологии можно использовать и при прохождении тестирований/собеседований при приеме на работу с целью идентификации претендующего на рабочее место гражданина. На особо значимых объектах, где безопасность должна обеспечиваться на высоком уровне, ЕБС можно использовать и как инструмент для прохождения пункта контроля на рабочее место.

Все эти варианты использования обеспечивают полное вхождение в нашу жизнь биометрических технологий, что вызывает ряд споров относительно безопасности и целесообразности такого вмешательства в личное пространство человека. Поэтому в рамках проводимого исследования мы попытались оценить мнение граждан о целесообразности широкого применения биометрии. Согласно проведенному опросу (см. Рисунок 3), большая часть людей затрудняется ответить, поскольку им не хватает информации для формирования мнения и принятия решения. При этом доля граждан, которые не хотят связывать биометрию с финансами, выше, чем тех, кто готов оплачивать покупки в магазинах. Следовательно, для принятия гражданами данной технологии важной кажется реализация мер по продвижению биометрии, объяснению населению ее возможностей, преимуществ, угроз и рисков.

В то же время ситуация с интеграцией с ЦПГ иная: количество граждан, которые готовы идентифицировать себя для передачи документов, наиболее высокая. Причем это касается и государственных, и негосударственных организаций (хотя для государственных структур этот показатель значительно выше, чем для коммерческих). Однако ситуация с идентификацией гражданина для проверки сотрудником МВД кардинально отличается: большинство не готово идентифицироваться через биометрию. Возможно, это связано с опасением по поводу злоупотребления полномочиями (и как результат увеличение времени при проверке). Но в целом граждане готовы использовать биометрию в различных жизненных ситуациях, так как они воспринимают данную технологию как удобную. Основным критерием доверия населения к биометрии станет безопасность системы, что будет подтверждаться при отсутствии утечек информации и злоупотребления ее использованием. В качестве одного из вариантов решения

[32] В «Перекрестках» и «Пятерочках» запустят оплату по лицу // РБК [Электронный ресурс]. URL: https://www.rbc.ru/finances/10/03/2021/604790869a7947641c7dd930 (дата обращения: 15.04.2022).

данной проблемы может стать применение методов дифференциальной деидентификации биометрических данных человека. Примером может стать решение, предлагаемое корейскими учеными для систем, содержащих медицинские биометрические данные граждан [Kim, Park 2022].

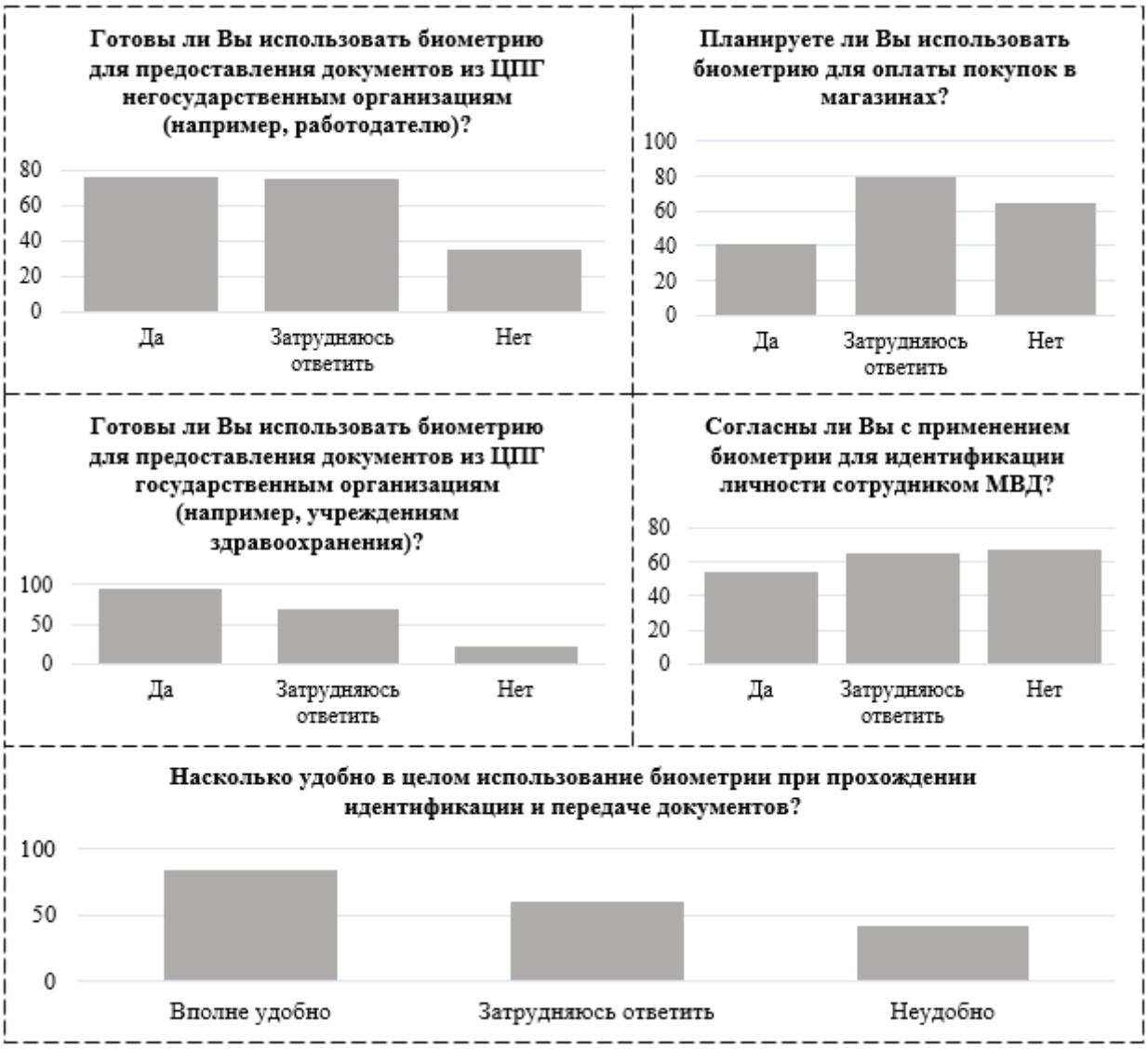

Рисунок 3. Данные опроса по целевому состоянию ЕБС[33]

Для использования сервисов цифрового профиля гражданина через мобильное приложение портала Госуслуг, как это предполагается реализовать в ближайшем будущем, можно рассмотреть возможность применения мультимодальной поведенческой биометрической системы идентификации с учетом траектории нажатия клавиш [Tse, Hung 2022]. Это будет представлять собой более сложную систему защиты персональных данных человека и существенно снизит риск утечки личной информации.

Заключение

Развитие ЕБС приводит к повышению безопасности и удобства для граждан в различных сферах жизни общества: оказание банковских, медицинских, судебных и других государственных и негосударственных услуг, в том числе онлайн, а также обеспечивает быструю идентификацию гражданина сотрудниками органов государственной власти.

[33] Составлено авторами.

Созданная в России ЕБС позволяет провести интеграцию с цифровым профилем гражданина, что означает потенциальную возможность передачи ряда документов заинтересованным лицам с помощью биометрии при согласии гражданина.

В качестве направления возможного развития ЕБС были выделены варианты использования в государственном и негосударственном секторе: проход на культурные и спортивные мероприятия, идентификация в медицинских учреждениях и связь с электронными медицинскими картами, проверка сотрудниками МВД (в частности, сотрудниками ГИБДД, которые проверяют водительское удостоверение), проверка кандидатов на вакансии и последующая передача ряда документов в организации, расширение использования в коммерческом сегменте при оплате покупок.

Таким образом, были рассмотрены процессы, которые могут включать в себя идентификацию посредством биометрии и последующую передачу информации из цифрового профиля гражданина. В перспективе можно рассмотреть возможность идентификации граждан с целью анализа различных аспектов, например покупательской способности, и предоставления дальнейших специальных предложений гражданину. Однако для реализации подобного предложения необходимо согласие граждан, обеспечение прозрачности сбора информации, перепроектирование ряда существующих государственных информационных систем и существенная корректировка соответствующей нормативно-правовой базы.

Результаты данного исследования могут быть использованы для более глубокого изучения вариантов применения Единой биометрической системы совместно с цифровым профилем гражданина в сфере реализации государственных функций и услуг. В качестве развития данного исследования видится возможность рассмотрения методов и приемов по применению разных биометрических систем в ходе идентификации и для обеспечения защиты личной информации людей в рамках ее применения при взаимодействии с различными бизнес-структурами и некоммерческими организациями в ходе взаимодействия с ними. Третьим направлением является разработка перечня конкретных мероприятий по снижению негативного отношения граждан к более активному использованию подобных решений в повседневной жизни.

Список литературы:

Бутов А.В., Карякин А.М. Проблемы развития биометрии как основы цифровизации отечественной экономики и пути их решения // Известия высших учебных заведений. Серия: экономика, финансы и управление производством. 2020. № 1 (43). С. 48–52.

Дивольд Е.В. Предпосылки создания национальной системы биометрической идентификации личности // Научный вестник Омской академии МВД России. 2021. Т. 27. № 2 (81). С. 139–143. DOI: 10.24412/1999-625X-2021-2-139-143

Долганова О.И. Улучшение клиентского опыта взаимодействия с искусственным интеллектом путем соблюдения этических принципов // Бизнес-информатика. 2021. Т. 15. № 2. С. 34–46. DOI: 10.17323/2587-814X.2021.2.34.46

Кузьминых Е.С., Маслова М.А. Анализ и сравнение биометрических способов идентификации личности человека // Научный результат. Информационные технологии. 2021. Т. 6. № 4. С. 13–19. DOI: 10.18413/2518-1092-2021-6-4-0-2

Лапидус Л.В., Гостилович А.О., Омарова Ш.А. Особенности проникновения цифровых технологий в жизни поколения Z: ценности, поведенческие паттерны и потребительские привычки интернет-поколения // Государственное управление. Электронный вестник. 2020. № 83. С. 271–291. DOI: 10.24411/2070-1381-2020-10119

Castellano P.S., Ferrer X.D. Límites y garantías constitucionales frente a la identificación biométrica // IDP. Revista de Internet, Derecho y Política. 2022. № 35. P. 1–13. DOI: 10.7238/idp.v0i35.392324

de Rosa G.H., Roder M., Papa J.P. Neighbour-Based Bag-of-Samplings for Person Identification through Handwritten Dynamics and Convolutional Neural Networks // Expert Systems. 2022. Vol. 39. Is. 4. DOI: 10.1111/exsy.12891

Hoffmann M., Mariniello M. Biometric Technologies at Work: A Proposed Use-Based Taxonomy // Policy Contribution. 2021. Is. 23. URL: https://www.bruegel.org/sites/default/files/wp-content/uploads/2021/11/PC-23-171121-1.pdf

Joseph A., Lian A.N.H., Kipli K., Chin Kh.L., Mat D.A.A., Voon Ch.S.Ch., Ngie D.Ch.S., Song N.S. Person Verification Based on Multimodal Biometric Recognition // Pertanika Journal of Science & Technology. 2022. Vol. 30. Is. 1. P. 161–183. DOI: 10.47836/pjst.30.1.09

Kim J., Park N. De-Identification Mechanism of User Data in Video Systems According to Risk Level for Preventing Leakage of Personal Healthcare Information // Sensors. 2022. Vol. 22. Is. 7. DOI: 10.3390/s22072589

Liang Y., Samtani S., Guo B., Yu Z. Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective // IEEE Internet of Things Journal. 2020. Vol. 7. Is. 9. P. 9128–9143. DOI: 10.1109/JIOT.2020.3004077

Safiullina L.K., Maturov R.R. Image Processing for Biometric Scanning of the Palm Vein Pattern // Society 5.0: Cyber-Social System as a Model of Narrative Management / ed. by A.G. Kravets, A.A. Bolshakov, M. Shcherbakov. Cham: Springer International Publishing, 2021. P. 25–34.

Tse K.-W., Hung K. Framework for User Behavioural Biometric Identification Using a Multimodal Scheme with Keystroke Trajectory Feature and Recurrent Neural Network on a Mobile Platform // IET Biometrics. 2022. Vol. 11. Is. 2. P. 157–170. DOI: 10.1049/bme2.12065

References:

Butov A.V., Karyakin A.V. (2020) Problems in the Development of Biometrics as a Basis for Digitalization of the Domestic Economy and Ways to Solve Them. *Izvestiya vysshikh uchebnykh zavedeniy. Seriya: ekonomika, finansy i upravleniye proizvodstvom*. № 1 (43). P. 48–52.

Castellano P.S., Ferrer X.D. (2022) Límites y garantías constitucionales frente a la identificación biométrica. *IDP. Revista de Internet, Derecho y Política*. № 35. C. 1–13. DOI: 10.7238/idp.v0i35.392324

de Rosa G.H., Roder M., Papa J.P. (2022) Neighbour-Based Bag-of-Samplings for Person Identification through Handwritten Dynamics and Convolutional Neural Network. *Expert Systems.* Vol. 39. Is. 4. DOI: 10.1111/exsy.12891

Divold V.E. (2021) Prerequisites of Creating a National System of Biometric Personal Identification. *Nauchnyy vestnik Omskoy akademii MVD Rossii*. Vol. 27. № 2 (81). P. 139–143. DOI: 10.24412/1999-625X-2021-2-139-143

Dolganova O.I. (2021) Improving Customer Experience with Artificial Intelligence by Adhering to Ethical Principles. *Biznes-informatika.* Vol. 15. № 2. P. 34–46. DOI: 10.17323/2587-814X.2021.2.34.46

Hoffmann M., Mariniello M. (2021) Biometric Technologies at Work: A Proposed Use-Based Taxonomy. *Policy Contribution.* Is. 23. URL: https://www.bruegel.org/sites/default/files/wp-content/uploads/2021/11/PC-23-171121-1.pdf

Joseph A., Lian A.N.H., Kipli K., Chin Kh.L., Mat D.A.A., Voon Ch.S.Ch., Ngie D.Ch.S., Song N.S. (2022) Person Verification Based on Multimodal Biometric Recognition. *Pertanika Journal of Science & Technology*. Vol. 30. Is. 1. P. 161–183. DOI: 10.47836/pjst.30.1.09

Kim J., Park N. (2022) De-Identification Mechanism of User Data in Video Systems According to Risk Level for Preventing Leakage of Personal Healthcare Information. *Sensors.* Vol. 22. Is. 7. DOI: 10.3390/s22072589

Kuzminykh E.S., Maslova M.A. (2021) Analysis and Comparison of Biometric Methods of Identification of a Person. *Nauchnyy rezul'tat*. *Informatsionnyye tekhnologii*. Vol. 6. № 4. P. 13–19. DOI: 10.18413/2518-1092-2021-6-4-0-2

Lapidus L.V., Gostilovich A.O., Omarova Sh.A. (2020) Features of Digital Technologies Penetration into Generation Z Life: Values, Behavioral Patterns and Consumer Habits of the Internet Generation. *Gosudarstvennoye upravleniye. Elektronnyy vestnik*. № 83. P. 271–291. DOI: 10.24411/2070-1381-2020-10119

Liang Y., Samtani S., Guo B., Yu Z. (2020) Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective. *IEEE Internet of Things Journal.* Vol. 7. Is. 9. P. 9128–9143. DOI: 10.1109/JIOT.2020.3004077

Safiullina L.K., Maturov R.R. (2021) Image Processing for Biometric Scanning of the Palm Vein Pattern. In: Kravets A.G., Bolshakov A.A., Shcherbakov M. (eds.) *Society 5.0: Cyber-Social System as a Model of Narrative Management*. Cham: Springer International Publishing. P. 25–34.

Tse K.-W., Hung K. (2022) Framework for User Behavioural Biometric Identification Using a Multimodal Scheme with Keystroke Trajectory Feature and Recurrent Neural Network on a Mobile Platform. *IET Biometrics.* Vol. 11. Is. 2. P. 157–170. DOI: 10.1049/bme2.12065

Дата поступления/Received: 29.05.2022