УДК: 330.341.13
https://doi.org/10.32686/1812-5220-2023-20-1-64-77

Классификация рисков системы цифровой идентификации граждан (на основе иностранного опыта)

ISSN 1812-5220

Башкирова О. В.,
Финансовый университет при Правительстве РФ, 109456, Россия, г. Москва, 4-й Вешняковский пр., д. 4

Аннотация

Данная статья посвящена разработке классификации рисков проектов внедрения и развития систем цифровой идентификации граждан на основе иностранного опыта. При формировании выборки были учтены следующие схожие с российскими условия: уровень цифрового развития, уровень цифровой грамотности и доходов населения, наличие тесного сотрудничества в экономической сфере.

Ранее проведенные исследования по теме носят, как правило, ограниченный и отрывочный характер, посвящены в основном описанию рисков конкретных национальных систем, риски не систематизированы, а также не приведен перечень наиболее существенных рисков для системы цифровой идентификации граждан Российской Федерации.

Методология исследования и описание выборки: критический анализ.

Для разработки классификации использован метод фасетной классификации; оценка наиболее вероятных рисков на пути становления системы в России основана на данных метаанализа исследований уровня цифрового развития и грамотности граждан.

Было обнаружено, что риски носят сложный составной характер; степень сопротивления граждан системам цифровой идентификации не зависит от общего уровня цифровой грамотности населения, однако больше всего негативно настроенных граждан среди людей с высокой цифровой грамотностью или ИТ-специалистов; для проекта, осуществляемого в России, наиболее важны обеспечение безопасности персональных данных граждан и возможности контроля гражданами своих цифровых двойников, обучение пользованию интернет-технологиями, правовые, этические и технологические аспекты процессов.

Ключевые слова: цифровая реальность; цифровой идентификатор личности; риски; технологии защиты персональных данных; безопасность; цифровой двойник.

Для цитирования: Башкирова О. В. Классификация рисков системы цифровой идентификации граждан (на основе иностранного опыта) // Проблемы анализа риска. 2023. Т. 20. № 1. С. 64—77, https://doi.org/10.32686/1812-5220-2023-20-1-64-77

Автор заявляет об отсутствии конфликта интересов.

Digital Identification System's Risk Classification (Based on Foreign Experience)

Olga V. Bashkirova,
Financial University under the Government of the Russian Federation,
4th Veshnyakovsky pr., 4,
Moscow, 109456, Russia

Abstract

This article is devoted to the development of a classification of the risks of projects for the introduction and development of digital identification systems for citizens, based on foreign experience. When forming the sample, the following similar conditions to those in Russia were taken into account: the level of digital development; the level of digital literacy and income of the population; the presence of close cooperation in the economic sphere.

Studies on the topic are limited and fragmentary, devoted mainly to describing the risks of specific national systems, the risks are not systematized, and there is no list of the most significant risks to the digital identification system of citizens of the Russian Federation.

Research methodology and description of the sample: critical analysis.

The faceted classification method was used to develop the classification; the assessment of the most likely risks on the way of the system formation in Russia is based on the data of the meta-analysis of studies of the level of digital development and literacy of citizens.

It was found that the risks are of a complex composite nature; the degree of citizens' resistance to digital identification systems does not depend on the general level of digital literacy of the population, but the most negatively inclined citizens are among people with high digital literacy or IT specialists; for the project being implemented in Russia, it is most important to ensure the security of citizens' personal data and the possibility for citizens to control their digital doubles, training in using Internet technologies, legal, ethical and technological aspects.

Keywords: digital reality; digital identity; risks; personal data protection technologies; security; digital twin.

For citation: Bashkirova O. V. Digital identification system's risk classification (based on foreign experience) // Issues of Risk Analysis. 2023;20(1):64-77, (In Russ.), https://doi.org/10.32686/1812-5220-2023-20-1-64-77

The author declare no conflict of interest.

Содержание

Введение

Начиная с первых попыток внедрения отдельных инструментов цифровой идентификации, таких как цифровой код доступа к банковским продуктам (Lloyds Bank, 1972 г.), удостоверения личности с чипами (Сингапур, 2000 г.) или цифровой код как замена паспорта жителей приграничных территорий (Индия, 1999 г.), имевших место начиная с последней четверти XX в., правительства стран сталкивались с определенными трудностями в реализации и продвижении проектов, связанными как с некорректной работой системы, так и с недовольством и сопротивлением граждан.

Исследование опыта зарубежных, прежде всего развивающихся, стран в вопросах становления систем призвано облегчить путь России в данном направлении.

Следует отметить, что исследователи уделяли внимание, как правило, отдельным аспектам систем — технической или нормативной обеспеченности процесса [1, 2], вопросам морали и права [3—6] при функционировании систем, общей системы рисков работы не содержат.

Система электронной идентификации личности в самом общем виде состоит из определенных акторов — субъекта персональных данных (ПД); оператора, обрабатывающего данные; государственных и коммерческих организаций, идентифицирующих субъект ПД; технических стандартов и технологического обеспечения процессов внесения, хранения и использования ПД; нормативной базы, регулирующей возникающие при работе системы отношения, права и обязанности сторон.

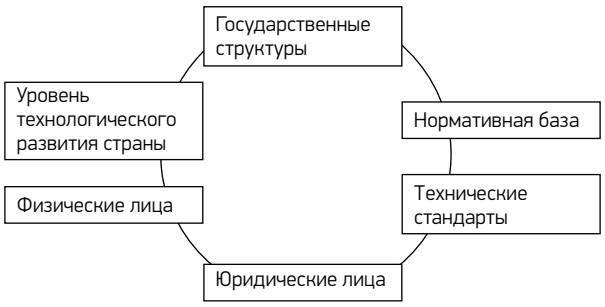

Рис. 1. Основные блоки системы электронной идентификации

Figure 1. The main units of the electronic identification system

Источник: разработано автором по итогам проведенного анализа.

Риски возникают при взаимодействии между указанными элементами системы. Они объясняются либо несогласованностью работы блоков системы, либо проявлением изначально содержащихся в каждом блоке недоработок.

Гипотезами данного исследования являются:

H1. Система цифровой идентификации граждан в развернутом виде являет собой полноценный мир взаимоотношений человека, органов власти и коммерческих структур; следовательно, риски системы носят схожий с обычной реальностью характер.

H2. Ввиду неоднородного состояния элементов системы последствия рисков носят сложный составной характер.

H3. Сопротивление граждан системе не имеет прямой зависимости от общего уровня цифровой грамотности населения.

Для выявления рисков был проведен контент-анализ официальных государственных источников попавших в выборку стран, сайтов и регулирующей нормативной базы национальных проектов цифровизации, периодических публикаций.

Для целей исследования был использован фасетный метод классификации.

Оценка вероятных рисков, несущих наибольшую угрозу для национального проекта, основана на данных метаанализа оценки цифровой грамотности россиян.

Классификация рисков

1. Политические риски

1.1. Международные взаимоотношения и ПД

Основные риски при обмене персональными данными граждан в сфере международных взаимоотношений заключаются в угрозе **неконтролируемого использования** данных граждан **иностранными государствами** и коммерческими организациями. В основе данных рисков лежит неравноправное положение участников отношений — разные уровни технологического и нормативного сопровождения процессов обмена и использования данных.

Большинство нормативных актов, регулирующих обмен данными при международных соглашениях, предусматривающих сотрудничество

в мирных сферах туризма и торговли[1, 2], запрещают предоставление данных резидентов иностранным государствам (страны Евросоюза, Китай, Индия и др.[3]).

Отдельные страны (Китай, страны Евросоюза) в свою очередь требуют предоставления ПД лиц, задействованных в международном экономическом сотрудничестве. Полный гид GDPR[4] содержит пункты, предусматривающие обязательное предоставление данных иностранных граждан; некоторые положения китайского PIPL[5] включают юрисдикцию Long Arm в отношении сбора данных и процессов организаций за пределами Китая. В свою очередь перемещение персональных данных за пределы вышеуказанных стран строго ограничено[6]. Подобные неравные условия выполнимы благодаря технологическому и нормативному превосходству в сфере цифровых технологий указанных стран над странами — партнерами.

Кроме рисков несанкционированного изъятия данных существуют **риски «форматирования данных»**, связанные с разными технологиями передачи, получения и чтения зашифрованной информации[7]. В качестве примера можно привести Бангладеш, где в попытке компенсировать возможные риски данного характера для разработки биометрических паспортов была приглашена немецкая компания[8].

Последние мировые события, сделавшие очевидными различия в видении дальнейшего развития мира, стран и содружеств, а также нарастающие масштабы цифровой реальности повышают риски обмена данными между государствами. Особенно уязвимым автору представляется блок биометрических данных. Необходимо определить минимум ПД, достаточный для осуществления международных транзакций, и обеспечить высокоуровневую нормативную, технологическую и организационную поддержку процессов.

1.2. Социальное согласие граждан

Риски сопротивления населения внедрению систем цифровой идентификации основаны на недоверии и опасениях наблюдения и слежки со стороны государства, а также нецелевого использования данных коммерческими службами [7]. Причем недовольство проявляют граждане как вполне благополучных с точки зрения уровня цифрового развития и цифровой грамотности населения стран, таких как Швейцария[9] и США [8], так и стран, где уровень ИТ-грамотности неравномерен (Индия), однако проявление негативного отношения к проекту отмечено по большей части в интеллектуальных центрах страны. Это позволяет предположить, что основная угроза исходит от граждан с уровнем ИТ-образования выше среднего, в отдельных исследованиях максимальное количество отрицательно на-

---

[1] В 2020 г. Сингапур и Австралия подписали Меморандум о взаимопонимании (MOU) в отношении цифровых удостоверений личности — для облегчения финансовых операций и активизации туристических потоков между странами.

[2] В 2021 г. Сингапур, Новая Зеландия и Чили заключили соглашение о работе над электронными счетами, цифровой идентификацией, финансовыми технологиями, потоками данных, искусственным интеллектом, цифровой торговлей и инвестиционными возможностями. [Alfred Siew. URL: Techgoondu.com (Дата обращения: 17.02.2022)]. Eileen Yu "Singapore, New Zealand, and Chile inch towards digital economy pact." URL: https://www.zdnet.com/article/singapore-new-zealand-and-chile-inch-towards-digital-economy-pact/ (Дата публикации: 21 января 2020 г.).

[3] Глава 4 GDPR (Нормативный акт ЕС о конфиденциальности и безопасности данных, PIPL, Национальный портал государственных услуг Индии).

[4] Complete guide to GDPR compliance (2017), European Commission. URL: https://gdpr.eu/ (Дата обращения: 24.01.2022).

[5] Закон о защите личной информации.

[6] В качестве примера можно привести следующий факт: единственный способ использования цифрового профиля (в виде приложения на смартфоне) за границей для жителя Китая состоит в том, что он может использовать персональный код только для оплаты товаров. Функция доступна с 10 июля 2017 г. Приложение генерирует QR-код, по которому осуществляется оплата [9].

[7] Canada-EU Joint Workshop Series for Enabling Interoperability and Mutual Support for Digital Credentials: Results and next steps (2021). European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/canada-eu-joint-workshop-series-enabling-interoperability-and-mutual-support-digital-credentials (Дата публикации: 22.11.2021. Дата обращения: 25.01.2022).

[8] Государственный портал Народной Республики Бангладеш. Страница онлайн-регистрации электронного паспорта. People's Republic of Bangladesh. Immigration & Passports Department. (на бенгальском языке). URL: https://www.epassport.gov.bd/landing (Дата обращения: 08.02.2022).

[9] Сайт электронного правительства Швейцарии (2022). URL: https://www.egovernment.ch/en/umsetzung/schwerpunktplan/elektronische-identitat (Дата обращения: 08.02.2022).

строенных граждан составляют молодые люди до 30 лет, работающие в ИТ-сфере[10].

Основными методами снижения риска можно назвать разъяснительные мероприятия среди населения и создание атмосферы доверия. Как пример можно привести концепцию «обоюдного доверия»[11], Сингапур[12] и метод, основанный на психологии восприятия и использования новых инструментов, — создание простого и доступного интерфейса страницы приложения[13].

2. Экономические риски

2.1. Экономическая эффективность системы

Вопросы **экономической эффективности** также вызывают споры и критику систем цифровой идентификации граждан. Сомнению подвергается экономическая целесообразность как системы в целом [10], так и отдельных аспектов, связанных с точечным выделением дотаций и выплат [11] и возможностью покрытия расходов на внедрение системы за их счет.

2.2. Возможный рост издержек для бизнеса

Вынужденный функционировать в новых условиях бизнес готовится к **росту издержек**. Новые правила ведения бизнеса, закрепленные в нормативных актах и стандартах работы с персональными данными, предусматривают введение определенных процедур и использование для их проведения новейших технологий. Соблюдение установленных норм по оценке специалистов (доклад, подготовленный по заказу юридической фирмы Baker & McKenzie[14]) вызовет необходимость создать специальный бюджет: 70% компаний ЕС будут вынуждены инвестировать порядка 200 млрд евро в новые процессы и их техническое и документарное обеспечение. Подобные вложения фирм США оцениваются в 41,7 млрд долларов. Эксперты выразили опасения, что малому бизнесу и стартап-компаниям может не хватить финансовых ресурсов, чтобы адекватно соответствовать новым правилам[15].

3. Риски нормативного характера

3.1. Отсутствие законодательного обоснования проекта

Недоработки нормативной базы оказывают значительное влияние на задержку процесса введения систем электронной идентификации.

Самый массовый проект электронной идентификации, вызвавший едва ли не самое большое количество судебных процессов, был осуществлен в Индии[16]. Он столкнулся со значительным сопротивлением со стороны гражданского общества Индии: среди судебных разбирательств чаще всего звучали темы необеспеченности проводимых инициатив законодательной поддержкой, безопасности данных и сохранения добровольного характера регистрации в системе для граждан; в попытках противостоять потоку жалоб подверглась сомнению сама фундаментальность права на неприкосновенность частной жизни граждан Индии [10].

Факт отклонения законопроекта об электронной идентификации в Швейцарии в 2021 г.[17] свидетельствует о недостаточной проработанности темы в законодательном поле страны. Правительством Швейцарии был существенно изменен План реализации электронного правительства на 2022—2023 гг.[18] В новой версии документа содержится подробный перечень акторов системы

[10] НИР «Определение необходимого и достаточного набора персональных данных и разработка рекомендаций по созданию цифрового профиля гражданина» (2022), Финансовый университет при Правительстве РФ.

[11] Когда граждане доверяют государству свои данные, государство, в свою очередь, «доверяет» гражданам, что они предоставили системе правдивые данные.

[12] Портал цифрового правительства Республики Сингапур. GovTechSingapore. Digital Identity. URL: https://www.tech.gov.sg/singapore-digital-government-journey/digital-identity (Дата обращения: 09.02.2022).

[13] Umsetzungsplan 2022–2023. Электронный документ. URL: https://www.digital-public-services-switzerland.ch/en/publications/all-publications (Дата обращения: 16.03.2022).

[14] Отчет 2021/2022 "Digital Transformation and Cloud Survey". URL: https://www.bakermckenzie.com/en/insight/publications/2021/12/2021-digital-transformation-and-cloud-survey

[15] Complete guide to GDPR compliance (2017), European Commission. URL: https://gdpr.eu/ (Дата обращения: 24.01.2022).

[16] Отчет "World Population Prospects. The 2018 Revision" (2018) United Nations. URL: https://desapublications.un.org/working-papers/ (Дата обращения: 13.07.2022).

[17] Сайт электронного правительства Швейцарии (2022). URL: https://www.egovernment.ch/en/umsetzung/schwerpunktplan/elektronische-identitat (Дата обращения: 08.02.2022).

[18] Umsetzungsplan 2022—2023. Электронный документ. URL: https://www.digital-public-services-switzerland.ch/en/publications/all-publications (Дата обращения: 16.03.2022).

(государственных служб, операционной компании eOperations Schweiz AG, ответственной за обеспечение ИТ-систем кантонов), определение границ их ответственности, описание основных процессов технологического и технического обеспечения данных процессов (требования к платформе и ИТ-архитектуре кантонов и муниципальных служб). Также приводится подробная дорожная карта реализации проекта. Инициативы призваны повысить доверие граждан к системе.

3.2. Защита ПД граждан

В качестве необходимой нормативной меры стоит указать принятие законов, обеспечивающих **защиту личной информации граждан**. Одним из наиболее значимых документов в этой области является уже упоминавшийся GDPR — нормативный акт ЕС о конфиденциальности и безопасности данных (дословно — Общее положение о защите данных), введенный 25 мая 2018 г.[19] Он послужил основой для разработки соответствующих документов не только для стран — претендентов на вступление в ЕС, но и для таких далеких от Европы государств, как Китайская Народная Республика [12].

В Китае в 2021 г. был принят Закон о защите личной информации (PIPL), «...первый всеобъемлющий закон Китая, призванный регулировать онлайн-данные и защищать личную информацию» [6]. Закон PIPL входит в тройку наиболее значимых нормативных актов Китая, регулирующих отношения в цифровом пространстве — наряду с законами о кибербезопасности (CSL) и о защите данных (DSL)[20]. Кроме указанных актов нормативная база проекта цифровизации страны представлена общими принципами гражданского законодательства, Постановлением Верховного народного суда от 2017 г.; в 2018 г. была выпущена «Белая книга системы цифровой идентификации eID», в которой определены все основные правила использования (создания, запроса контрагентом и удаления) личной информации граждан по его/ее запросу или после окончания транзакции[21].

Вследствие сопротивления гражданского общества Канады внедрению цифровых идентификаторов личности правительство страны пересмотрело Закон о защите персональных данных и электронных документов от 2013 г. и разработало на основе GDPR акт Consumer Privacy Protection Act (CPPA), ужесточив наказание за нецелевое использование ПД [13]. Всего опыт Канады в области нормативного законотворчества в безопасности цифровых данных своих граждан составляет более 20 лет.

Богатый в части судебных разбирательств и законодательных инициатив опыт зарубежных стран показывает, что при создании нормативной базы системы цифровой идентификации граждан необходимо предусмотреть следующее:

- во-первых, сформировать нормативную основу для проведения процедур разработки и внедрения самой системы;
- во-вторых, четко определить круг действующих лиц, подробно описав их права и обязанности, правила взаимоотношений между сторонами и предусмотрев наказания за их нарушения.

Отдельно стоит выделить очень важный блок законов защиты персональных данных субъекта в цифровой среде. Это позволит избежать многочисленных судебных разбирательств и ускорит процесс перехода к цифровому обществу.

4. Технологические риски

4.1. Риски, связанные с отсутствием единых технических стандартов, при внедрении системы в крупных странах

Крупные страны, состоящие из разных субъектов, Европейский союз, страны, продвигающие наиболее тесное сотрудничество в области обмена цифровыми данными[22] (в том числе и своих граждан), сталкиваются с проблемами, связанными с разным уровнем развития цифровых технологий, используемых на той или иной территории, и отсутствием единых технических стандартов в области работы

[19] Complete guide to GDPR compliance (2017), European Commission. URL: https://gdpr.eu/ (Дата обращения: 24.01.2022).

[20] China Approves PIPL (2021). URL: https://chinapipl.com/china-approves-pipl/ (Дата обращения: 24.01.2022).

[21] Белая книга по системе цифровой идентификации eID (2018 г.) (на китайском языке). Электронный документ. URL: https://eid.cn/digid/introduce.html (Дата обращения: 05.02.2022).

[22] Канада и Нидерланды, Сингапур и Австралия (Портал цифровых государственных услуг Республики Сингапур, 2022).

с данными[23]. Это затрудняет создание единой технологической системы внесения, обработки, хранения, распознавания, верификации данных.

4.2. Проблема обеспечения конфиденциальности данных

Проблема обеспечения конфиденциальности и безопасности ПД остается наиболее острой и для пользователей, и для государственных служб, работающих над созданием и продвижением систем электронной идентификации.

Основной вред, который может быть нанесен субъекту ПД, заключается в неправомерном ознакомлении и использовании ПД, ухудшении качества данных и затруднении доступа к данным [3].

Проблема утечки данных лежит в плоскостях технологических и технических ошибок и недоработок, а также злонамеренного воздействия человека.

Технологии защиты данных должны быть разработаны для всех объектов, с которых возможна утечка данных:

- виртуальных платформ и хранилищ данных;
- приложений в мобильных устройствах;
- физических носителей с чипами, содержащими конфиденциальную информацию.

Для совершенствования систем цифровой идентификации и повышения их безопасности предлагаются следующие технологии считывания и обработки данных (новая биометрия), контроля и шифрования данных:

- технология блокчейна [2], позволяющая пользователям контролировать собственные данные;
- методы биометрического шифрования[24] (цветные штрих-коды) [5], шифрования на основе алгоритмов Advanced Encryption Standard (AES) и SHA-256 [1] призваны повысить безопасность биометрического паспорта от несанкционированного доступа и могут применяться для обеспечения большей безопасности, например, при пересечении границ;
- технологии защиты отпечатков пальцев как более точной по сравнению с паролями и токенами [14];
- биометрия нового поколения [15];
- анонимизированные данные[25] для невозможности определения субъекта ПД [3].

4.3. Риски масштабирования системы

Риски масштабирования связаны с внедрением единых технических регламентов и технологическим обеспечением процессов цифровой идентификации, а также могут быть связаны с человеческим фактором — согласием (или несогласием) различных категорий граждан участвовать в проекте, с процессами обучения их пользоваться своим цифровым идентификатором.

Следует отметить, что нагрузка на систему любой страны будет только расти, учитывая тенденции развития сбора и хранения (использования) данных о человеке и всех его действиях как в сети, так и в реальной жизни. Показатели запросов самой масштабной системы идентификации личности (Aadhaar, Индия) составляют порядка 20 млн транзакций в день[26] (в среднем 100 запросов в секунду с пиковым значением в 500 — в начале и конце рабочего дня госслужащих). Система рассчитана на 40 млн запросов в день, но, учитывая вышеобозначенные тенденции, планируется ее модификация с расчетом ежедневных запросов до 100 млн в день. Всего за время своего существования в системе совершено 2 451 303 296 транзакций[27].

Среди наиболее популярных технологий масштабирования систем эксперты называют техноло-

[23] Canada-EU Joint Workshop Series for Enabling Interoperability and Mutual Support for Digital Credentials: Results and next steps (2021). European Commission. URL: https://digital-strategy.ec.europa.eu/en/library/canada-eu-joint-workshop-series-enabling-interoperability-and-mutual-support-digital-credentials (Дата публикации: 22.11.2021, Дата обращения: 25.01.2022).

[24] Вызывает опасение тот факт, что плотность цветных штрихкодов несет собственные риски трудоемкого исправления ошибок при обработке не только геометрических, но и хроматических искажений, например, при сканировании и печати.

[25] Исследования показывают, что «якобы анонимные сведения при помощи ИИ позволяют идентифицировать физическое лицо с вероятностью 99,8%» [3].

[26] На конец 2020 г. Сайт цифровых государственных услуг Индии. National Government Services Portal Find Government Services Faster. URL: https://services.india.gov.in/service/listing?cat_id=64&ln=en (Дата обращения: 03.02.2022).

[27] На 18:58 18.03.2022 по московскому времени. (Портал государственной программы Aadhaar, Индия, 2022).

гию блокчейна [16], применимую как для продвижения совершенно новых технологий (5G, квантовых вычислений), так и при замене существующих технологий новыми — глубокого обучения, больших данных и пр.

5. Технические риски

5.1. Риски утечки данных с серверов и при проведении транзакций

Проблема утечки данных лежит в плоскостях технологических ошибок и технических недоработок, а также злонамеренного воздействия человека.

Обеспечение безопасности данных должно быть обеспечено как на пути транзакций, так и в хранилище ПД; в технических и правовых документах — прописаны зоны ответственности служб на разных участках движения данных (Aadhaar).

Во избежание утечки данные, вводимые для подтверждения или совершения транзакции, должны быть зашифрованы уже на устройстве ввода, время хранения вводимых данных строго ограничено, иногда временем осуществления транзакции (Aadhaar). Полученные биометрические данные для аутентификации запрещается хранить где-либо. Во время транзакции данные передаются по защищенному каналу, доступ к хранилищу данных строго ограничен (проекты Индии, Китая, Сингапура, Европы).

Псевдонимизация[28] и токенизация[29] как технологии шифрования данных названы обязательным условием хранения данных в GDPR. Положение требует, чтобы дополнительная информация (например ключ дешифрования) хранилась отдельно от псевдонимизированных данных. Данные технологии повышают конфиденциальность данных и рекомендованы для снижения рисков несанкционированного использования данных[30].

5.2. Риски утечки данных с приложений

Приложения часто показывают недостаточную защищенность, особенно если речь идет о кибертерроризме, использующем высококомпетентных специалистов. Как пример можно привести тестовую атаку на французское приложение Alicem, осуществленную ученым Батистом Робером, который подтвердил, что ему удалось получить доступ к данным из общедоступных следов: он взломал приложение с помощью гипертекстовой ссылки с общедоступного сайта [12].

Для снижения данного риска применяется двух-[31] или усиленная двухфакторная идентификация[32], когда при входе в систему субъект проходит двухэтапную проверку личности.

5.3. Уязвимость электронных удостоверений и паспортов

Похищение данных с физических носителей отмечено еще в начале XXI в. — в Италии считывание данных происходило при помощи радиочастотной связи [17]. На данный момент существуют более современные технологии считывания информации с электронных чипов — Chip-off. и JTAG [19], которые представляют угрозу субъекту ПД.

В ряде стран (Индия, Бангладеш), где популярно использование физических носителей (электронных паспортов, пластиковых удостоверений),

---

[28] Псевдонимизация — процесс преобразования персональных данных таким образом, что полученные сведения не могут быть отнесены на конкретный субъект ПД без использования дополнительной информации.

[29] Токенизация — нематематический подход к защите данных в состоянии покоя, который заменяет конфиденциальные данные нечувствительными заменителями, называемыми токенами. Токены позволяют конкретным данным быть полностью или частично видимыми для обработки и анализа, в то время как конфиденциальная информация остается скрытой.

[30] Complete guide to GDPR compliance (2017), European Commission. URL: https://gdpr.eu/ (Дата обращения: 24.01.2022).

[31] Сначала пользователь вводит номер своего цифрового идентификатора (возможно — скан лица или отпечаток пальца, что удобно при использовании приложения), затем пароль, который генерируется токеном системы и высылается через смс на смартфон пользователя. Пароль действителен только во время совершения транзакции. Smart Nation Singapore. URL: https://www.smartnation.gov.sg/initiatives/strategic-national-projects/national-digital-identity (Дата обращения: 09.02.2022).

[32] Цифровая идентификация гражданина Китая eID представляет собой цифровой код, формируемый при помощи криптографического алгоритма, и пароль, выдаваемый «Системой сетевой идентификации гражданина» / Белая книга по системе цифровой идентификации eID (2018 г.) (на китайском языке). Электронный документ. URL: https://eid.cn/digid/introduce.html (Дата обращения: 05.02.2022).

данные защищены при помощи встроенного микропроцессорного чипа, содержат до 41 функции защиты, в том числе голографические изображения (Бангладеш)[33].

5.4. Ошибки при распознавании символов и ввод некорректных данных

Кроме риска утечки данных физические носители несут риски технологического и технического характера при считывании и обработке информации — качество считывающих устройств должно быть обеспечено «на основе сверточных нейронных сетей» [19].

5.5. Проблема адекватности ПД и качества цифровых двойников

Полный набор оцифрованных персональных данных представляет собой «цифровой двойник» человека. В связи с этим возникают вопросы **качества цифрового двойника:** «…качество цифровых двойников определяется адекватностью, достоверностью, полнотой и актуальностью предоставляемых данных» [3].

В самом общем виде проблемы предоставления неадекватных данных можно подразделить на техническую, технологическую неисправность, личную непреднамеренную и злонамеренную. Риски технического и технологического порядка были рассмотрены выше, уточним последние два пункта.

Личная непреднамеренная

Технологические недоработки могут не отследить некорректную информацию либо дублирование информации, ввод некорректных данных человеком (ошибку). **Риски ошибочного предоставления данных** без злого умысла, влияние «человеческого фактора» могут быть снижены путем разработки более тщательной процедуры сбора данных[34].

Личная преднамеренная

В истории становления систем отмечены случаи **предоставления** гражданами **заведомо ложных данных**.

Предоставление ложной информации с целью скрыть истинного носителя данных может осуществляться двумя способами: когда один человек выдает себя за другого реального, либо искажает данные, формируя совершенно новую личность[35].

Подобные риски могут быть минимизированы при использовании единой системы цифровой идентификации [4].

5.6. Слабая чувствительность аппаратуры и неоднородная плотность покрытия сети Интернет

Обеспечение всех центров считывания информации аппаратурой надлежащего качества позволит избежать **рисков отказа работы системы**. В Индии зафиксированы случаи, когда было невозможно провести идентификацию человека по отпечаткам пальцев в связи с тем, что они стерты из-за тяжелой работы или поблекли из-за преклонного возраста [22].

Также стоит учитывать возможные **проблемы с сетью**, особенно в отдаленных районах, где плотность покрытия ниже в сравнении с центральными регионами стран.

6. Гуманистические, морально-этические риски

6.1. Риски «исключения» части населения

Риск исключения населения, не пользующегося Интернетом. Согласно данным отчета[36] ни одна страна мира не показывает 100%-й результат в области использования Интернета населением. В крупных государствах эти проценты в абсолютном выра-

[33] Где содержатся демографические и биометрические данные владельца электронного паспорта: отпечатки пальцев, скан радужной оболочки глаза, фотография, электронная подпись и не только. (Государственный портал Народной Республики Бангладеш. Страница онлайн-регистрации электронного паспорта, 2022).

[34] Без данных инициатив существуют риски дублирования профилей, когда человек неверно ввел данные, либо забыл код, пароль и т.д. и создал профиль снова. С подобной проблемой сталкивались власти Индии, где до введения жестких ограничений на создание более чем одного цифрового профиля гражданина были случаи, когда люди создавали несколько разных профилей.

[35] Основные технологии искажения данных: морфинг — создание одной искусственной фотографии лица, представляющей два различных качества, и использование ее в качестве эталонной на документе [21]; ретушь — манипуляции с пропорциями лица в целом или его частей [22]; face swap (перенос лица) — технология, позволяющая при помощи нейросетей переносить лицо одного человека на изображение другого без потери качества конечного результата [22].

[36] DIGITAL 2022: GLOBAL OVERVIEW REPORT. URL: https://datareportal.com/reports/digital-2022-global-overview-report (Дата обращения: 16.03.2022).

жении составляют миллионы людей: на конец 2021 г. в Северной Америке число людей, не использующих Интернет, составляло 28 млн человек, в Северной и Западной Европе — 16 млн человек, Центральной и Восточной Азии (включая Индию и Китай) — 486 млн человек. В странах Восточной Европы число людей, оторванных от цифровой действительности, составляет 42 млн человек. Вследствие этого возникает риск того, что часть населения будет либо не зарегистрирована в системе и, следовательно, лишена возможности пользоваться предусмотренными законами своей страны услугами, либо будет зарегистрирована (путем предоставления и обмена данными среди государственных органов и служб), но не будет иметь возможности влиять на факт использования своих данных.

Риск, связанный с низким уровнем компьютерной грамотности, характерен для людей старшего (преклонного) возраста и/или живущих в отдаленных и малонаселенных местах. Для полноценного включения населения в цифровую реальность следует предусмотреть образовательные программы для такой категории граждан и не лишать их всех положенных дотаций и выплат. Как пример можно привести Индию, где отмечены случаи непредоставления дотаций на газ и невыдача продовольственного пособия малоимущим из-за проблем с цифровой идентификацией [22].

Риск «исключения» в этнически неоднородных странах может быть вызван тем, что искусственный интеллект (ИИ), задействованный в процессах идентификации граждан по биометрии, научен распознавать лица, как правило, автохтонного населения, что в современном мире может вызвать затруднение для граждан, не принадлежащих к основному этносу. В проекте «Гендерные оттенки» исследователя Джой Буоламвини из Массачусетского технологического института отмечено, что для трех систем распознавания лиц от IBM, Face++ и Microsoft частота ошибок составляет менее 1% для светлокожих мужчин, но более 20% — для темнокожих женщин [12].

6.2. Многоязычность стран

Риск недопонимания контента сайтов существует в странах с несколькими государственными языками и/или населенных многочисленными народностями. Случаи непонимания информации на сайте были отмечены в Индии, где местные языки провинций имеют существенные отличия, а английским языком, как правило, не владеют жители деревенских поселений. Перевод контента на все местные языки стоит важным пунктом в программе «Цифровая Индия»[37].

В Швейцарии Планом реализации электронного правительства на 2022—2023 гг.[38] предусмотрено предоставление информации гражданам на трех государственных языках — немецком, французском, итальянском.

6.3. Контроль за цифровым двойником

Кроме качества цифрового двойника важен вопрос **контроля за двойником**. В цифровой реальности цифровое дополнение (расширение) физической личности и ее среды обитания носит синергический характер[39]. Поскольку данные собираются зачастую без ведома человека [23], встает вопрос контроля человеком данных и осведомленности о выводах, принимаемых на основе этих данных ИИ.

На основе поведения человека в социальных сетях «…рассчитывается его индекс интеллектуального развития» [3]. «Существует реальный риск оказаться маргиналом системы: поскольку решение о рейтинге человека алгоритм принимает на основе статистических корреляций, личности, ведущие себя нетипично, "отбраковываются" машиной». Для контроля над цифровым аналогом личности эксперты считают необходимым сделать все данные о человеке доступными для самого человека [4].

Такое право предусмотрено уже упоминавшимся в данном исследовании актом GDPR, в котором прописано право субъекта предоставлять определя-

---

[37] Сайт государственной программы цифровизации Digital India. URL: https://digitalindia.gov.in/ (Дата обращения: 13.02.2022).

[38] Umsetzungsplan 2022—2023. Электронный документ. URL: https://www.digital-public-services-switzerland.ch/en/publications/all-publications (Дата обращения: 16.03.2022).

[39] В качестве примера можно привести широко известный и обсуждаемый социальный рейтинг (КНР), когда человеку изначально присваиваются баллы, которые растут или падают в зависимости от социального поведения человека, в результате отдельных проступков человеку будет отказано в покупке билета на самолет или возможности записать ребенка в престижную школу. Более того, рейтинг меняется в результате как активных процессов (когда за них ответственен сам человек), так и тех, на которые повлиять не может, — старение, состояние здоровья, факт увольнения и пр.

емый им набор данных, контролировать перечень видимых данных и их использование в каждом конкретном случае. Например, ст. 21 GDPR позволяет физическому лицу возражать против обработки персональных данных в маркетинговых или несервисных целях [12]. Положение содержит перечень ситуаций, когда данные могут быть исследованы и без согласия гражданина.

Наблюдается некоторое противоречие: законодательными актами[40] необходимость использования биометрических данных для идентификации человека не установлена, этот тип данных не является необходимым для получения предоставляемых услуг, но внести свои биометрические данные в систему человек обязан[41] [12].

Законодательство КНР[42] предусматривает согласие граждан на обработку их ПД и отзыв согласия в любое время. Обработчикам не разрешается отказывать в предоставлении продуктов или услуг, если физическое лицо удерживает или отзывает свое согласие на несущественную обработку. Также предусмотрен ряд ситуаций, когда требуется дополнительное согласие граждан[43] на использование персональных данных [6].

Обсуждение и выводы

Анализ рисков внедрения и использования систем цифровой идентификации граждан зарубежных стран показал, что последствия и риски зачастую носят сложный составной характер. Классификация рисков, учитывающая не только тип риска, но и влияние дополнительных рисковых факторов, представлена на рис. 2.

Основные риски выделены и распределены по матрице: по оси ординат указан тип риска, по оси абсцисс — дополнительный фактор влияния.

Так, политический риск неполучения социального согласия граждан на функционирование системы имеет этический аспект (будут ли учтены пожелания населения), наиболее вероятные последствия риска — затягивание процесса внедрения системы во времени, связанный с ним рост издержек (доработка нормативной базы, технологического обеспечения процессов).

Риски несанкционированного использования ПД российских граждан государственными органами другой страны в процессе международного сотрудничества могут быть вызваны разным технологическим ландшафтом стран, применением разных технологий при осуществлении идентичных операций.

Недоработка нормативного обеспечения процессов способна вызвать политические и этические последствия, которые могут быть выражены в проявлении гражданского недовольства.

Проблема обеспечения конфиденциальности ПД помимо технологического имеет также нормативный, политический и этический аспекты.

Проблема качества цифрового двойника и контроля над ним — этический риск — может вызвать политические, технологические и нормативные последствия.

Метаанализ исследований уровня цифровой грамотности россиян[44] [24] позволил выделить наиболее существенные риски внедрения системы цифровой идентификации в России:

1. Социальное согласие граждан и их способность пользоваться системой — общий уровень цифровой грамотности российских граждан ниже среднего (по сравнению со странами Европы) [24], имеющий территориальные и возрастные особенности[45], способен оказать негативное влияние на временные параметры проекта и увеличить его расходную часть (обучение населения и выравнивание ИТ-ландшафта).

2. Риски безопасности ПД и возможность контроля за цифровым двойником — решаются за счет

[40] e-IDAS.

[41] Во Франции отказ от обработки биометрических данных на этапе регистрации в Alicem препятствует созданию и активации учетной записи пользователя.

[42] PIPL.

[43] Передача ПД третьим лицам, публикация ПД, трансграничная передача данных.

[44] Индекс «Цифровая Россия»-2018. Московская школа управления Сколково; «Цифровая грамотность россиян: исследование 2020». НАФИ Аналитический центр. URL: https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020/ (Дата обращения: 10.12.2021); Мониторинг развития информационного общества в Российской Федерации за 2010—2021 гг. Данные по РФ. Росстат.

[45] «Цифровая грамотность россиян: исследование 2020». НАФИ Аналитический центр. URL: https://nafi.ru/analytics/tsifrovaya-gramotnost-rossiyan-issledovanie-2020/ (Дата обращения: 10.12.2021).

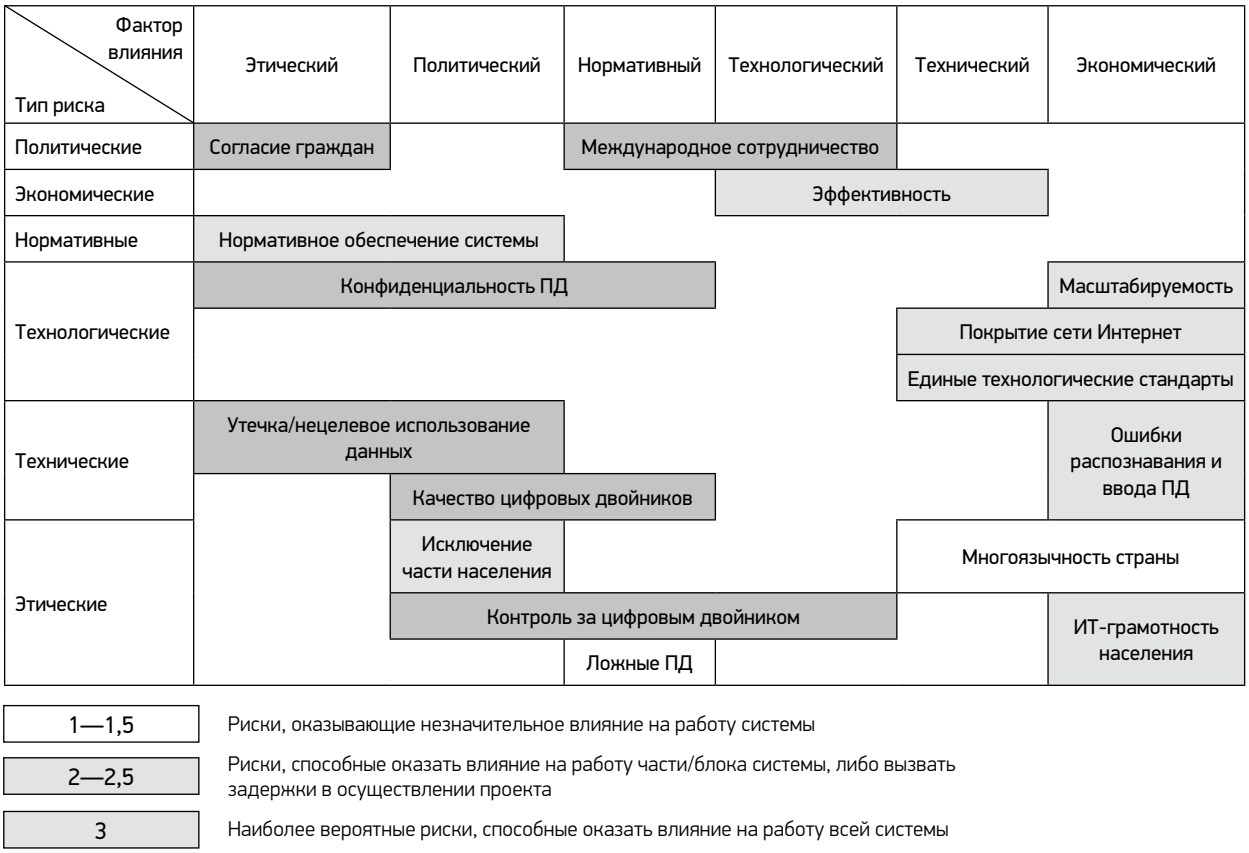

Рис. 2. Классификация рисков становления и функционирования системы цифровой идентификации

Figure 2. Classification of risks of formation and functioning of the digital identification system

Источник: разработано автором по результатам анализа.

нормативного обеспечения и технологической и технической поддержки системы цифрового контроля.

3. Масштабируемость системы и многоязычие страны — особое внимание здесь следует уделить выравниванию ИТ-ландшафта и уровня цифровой грамотности граждан.

Принимая во внимание оценку цифровой зрелости российского общества, а также его социокультурные особенности, наибольшее внимание следует уделить обеспечению безопасности персональных данных и возможности контроля гражданами своих цифровых двойников, правовым, этическим и технологическим аспектам процессов, поскольку их недостаточная проработка способна вызвать негативный отклик в одной части общества и полное игнорирование (неиспользование) системы у другой. Следует уделить значительное внимание разъяснению происходящих изменений, так как было показано выше (п. 2), недовольство работой и самим наличием систем проявляли как граждане стран с высоким уровнем ИТ-грамотности, так и с неравномерным уровнем образования. Риски, относимые к технологическому и техническому сопровождению проекта, значимы, но решаемы, как и повышение цифровой грамотности граждан.

Литература [References]

1. Choudhury Z. H., Munir Ahamed Rabbani M. (2020). Biometric Passport Security by Applying Encrypted Biometric Data Embedded in the QR Code. In: Raju, K., Senkerik, R., Lanka, S., Rajagopal, V. (eds) Data Engineering and Communication Technology. Advances in Intelligent Systems and Computing, vol 1079. Springer, Singapore. https://doi.org/10.1007/978-981-15-1097-7_5

2. Oliveira M., Honório T., Reis C. I., Maximiano M. (2022). Immunity Passport Ledger. In:, et al. Innovations in Bio-Inspired Computing and Applications. IBICA 2021. Lecture Notes in Networks and Systems, vol 419. Springer, Cham. https://doi.org/10.1007/978-3-030-96299-9_50
3. Докучаев В. А., Маклачкова В. В., Статьев В. Ю. Цифровизация субъекта персональных данных // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. №6. С. 27—32.
https://doi.org/10.36724/2072-8735-2020-14-6-27-32
[Dokuchaev V. A., Maklachkova V. V., Statev V.Yu. Digitalization of the personal data subject // T-COMM. 2020;14(6):27-32, (In Russ.),
https://doi.org/10.36724/2072-8735-2020-14-6-27-32]
4. Кондаков А. М., Костылева А. А. Цифровая идентичность, цифровая самоидентификация. Цифровой профиль: постановка проблемы // Вестник Российского университета дружбы народов. Серия: Информатизация образования. 2019. Т. 16. № 3. С. 207—218.
https://doi.org/10.22363/2312-8631-2019-16-3-207-218
[Kondakov A. M., Kostyleva A. A. Digital identity, digital self-identification, digital profile: problem statement // RUDN Journal of Informatization in Education. 2019;16(3):207-218, (In Russ.),
https://doi.org/10.22363/2312-8631-2019-16-3-207-218]
5. Choudhury Z. H., Rabbani M. M. A. (2020). Biometric Passport Security Using Encrypted Biometric Data Encoded in the HCC2D Code. In: Pandian A., Senjyu T., Islam S., Wang H. (eds) Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI — 2018). ICCBI 2018. Lecture Notes on Data Engineering and Communications Technologies, vol 31. Springer, Cham.
https://doi.org/10.1007/978-3-030-24643-3_115
6. Kutner A., Navetta D., Wood Ch. (2021) 'China: China's New National Privacy Law: The PIPL' MONDAQ. URL: https://www.mondaq.com/china/data-protection/1137330/china39s-new-national-privacy-law-the-pipl (Дата обращения: 24.01.2022).
7. Wang Victoria & Tucker John. (2021). 'I am not a number': Conceptualising digital identity in digital surveillance. Technology in Society. 67.
doi: 10.1016/j.techsoc.2021.101772
8. Auxier B., Rainie L., Anderson M., Perrin A., Kumar M., Turner E. (2019) 'Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information' Pew Research Center. URL: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ (Дата обращения: 01.02.2022).
9. Matzkuhn D., (2018) 'China ermöglicht Personalausweis als App' CANCOM.INFO. URL: https://www.cancom.info/2018/01/china-ermoeglicht-personalausweis-als-app/ (Дата обращения: 18.03.2022).
10. Ramakumar R. (2010). The Unique ID Project in India: A Skeptical Note. In: Kumar, A., Zhang, D. (eds) Ethics and Policy of Biometrics. ICEB 2010. Lecture Notes in Computer Science, vol 6005. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-12595-9_20
11. Khera R. (2013). A 'Cost-Benefi t' analysis of UID. 48. 13—15.
12. Hennion Ch., Mis J.-M. (2020) Rapport d'information déposé en application de l'article 145 du règlement en conclusion des travaux de la mission d'information commune sur l'identité numérique. URL: https://www.assemblee-nationale.fr/dyn/15/rapports/micnum/l15b3190_rapport-information (Дата обращения: 14.02.2022).
13. Sookman B., Kerr G., Iatrou N., Leslie P. (2021) "The CPPA's Privacy Law Enforcement Regime". URL: https://www.mccarthy.ca/en/insights/blogs/techlex/cppas-privacy-law-enforcement-regime (Дата обращения: 18.03.2022).
14. Baghel V. S., Prakash S. & Agrawal I. An enhanced fuzzy vault to secure the fingerprint templates. Multimed Tools Appl 80, 33055–33073 (2021).
https://doi.org/10.1007/s11042-021-11325-w
15. Sun Z., Li, Q., Liu Y., Zhu Y. (2021). Opportunities and Challenges for Biometrics. In: China's e-Science Blue Book 2020. Springer, Singapore.
https://doi.org/10.1007/978-981-15-8342-1_6
16. Tchagna Kouanou A., Tchito Tchapga C., Sone Ekonde M. et al. Securing Data in an Internet of Things Network Using Blockchain Technology: Smart Home Case. SN COMPUT. SCI. 3, 167 (2022).
https://doi.org/10.1007/s42979-022-01065-5
17. Auletta V., Blundo C., De Caro A., De Cristofaro E., Persiano G., Visconti, I. (2010). Increasing Privacy Threats in the Cyberspace: The Case of Italian E-Passports. In:, et al. Financial Cryptography and Data Security. FC 2010. Lecture Notes in Computer Science, vol 6054. Springer, Berlin, Heidelberg.
https://doi.org/10.1007/978-3-642-14992-4_9

18. Яковлев А. Н., Данилова А. С. Применение технологий JTAG и Chip-Off в исследовании мобильных устройств // Теория и практика судебной экспертизы. 2018. Т. 13. № 3. С. 109—115, https://doi.org/10.30764/1819-2785-2018-13-3-109-115 [Yakovlev A. N., Danilova A. S. JTAG and Chip-Off Technologies in Computer Forensics // Theory and Practice of Forensic Science. 2018;13(3):109-115. (In Russ.) https://doi.org/10.30764/1819-2785-2018-13-3-109-115]
19. Liu Y., James H., Gupta O. et al. MRZ code extraction from visa and passport documents using convolutional neural networks. IJDAR 25, 29–39 (2022). https://doi.org/10.1007/s10032-021-00384-2
20. Kenneth M. O., Sulaimon B. A., Abdulhamid S. M., Ochei L. C. (2022). A Systematic Literature Review on Face Morphing Attack Detection (MAD). In: Misra S., Arumugam C. (eds) Illumination of Artificial Intelligence in Cybersecurity and Forensics. Lecture Notes on Data Engineering and Communications Technologies, vol 109. Springer, Cham. https://doi.org/10.1007/978-3-030-93453-8_7
21. Tolosana R., Vera-Rodriguez R., Fierrez J., Morales A., Ortega-Garcia J. (2022). An Introduction to Digital Face Manipulation. In: Rathgeb C., Tolosana R., Vera-Rodriguez R., Busch C. (eds) Handbook of Digital Face Manipulation and Detection. Advances in Computer Vision and Pattern Recognition. Springer, Cham. https://doi.org/10.1007/978-3-030-87664-7_1
22. Roychoudhury A. (2016) 'Aadhaar legislation might be a Money Bill' Rediff. URL: https://www.rediff.com/business/report/budget-2016-aadhaar-legislation-might-be-a-money-bill/20160302.htm (Дата обращения: 24.01.2022).
23. Чернышева Е. (2022) «Минцифры предложило собирать биометрию россиян без их согласия, РБК» https://www.rbc.ru/politics/09/08/2022/62f1e7fb9a7947174c3125aa (Дата размещения: 09.08.2022. Дата обращения: 14.08.2022). [Chernysheva E. (2022) "The Ministry of Digital Science proposed collecting biometrics of Russians without their consent from RBC". https://www.rbc.ru/politics/09/08/2022/62f1e7fb9a7947174c3125aa. (Date of placement: 09.08.2022; Accessed: 14.08.2022) (In Russ.)]
24. Левен Е., Суслов А. (2020) «Уровень владения цифровыми навыками в России и странах ЕС», ИСИЭЗ НИУ ВШЭ. URL: https://issek.hse.ru/news/377859466.html (Дата обращения: 13.05.2022). [Leven E, Suslov A. (2020) "Level of digital skills in Russia and EU countries", ISIEZ HSE. (Accessed: 13.05.2022) (In Russ.)]

Сведения об авторе

Башкирова Ольга Владимировна: кандидат экономических наук, старший преподаватель, департамент бизнес-информатики Финансового университета при Правительстве РФ

Количество публикаций: 15, в т. ч. 1 монография

Область научных интересов: цифровая трансформация бизнеса, развитие компании в новых условиях хозяйствования

ORCID: 0000-0002-8505-4328

Контактная информация:

Адрес: 109456, г. Москва, 4-й Вешняковский пр., д. 4

shedu@inbox.ru

Статья поступила в редакцию: 21.11.2022
Одобрена после рецензирования: 16.01.2023
Принята к публикации: 16.01.2023
Дата публикации: 28.02.2023

The article was submitted: 21.11.2022
Approved after reviewing: 16.01.2023
Accepted for publication: 16.01.2023
Date of publication: 28.02.2023