Вестник Самарского государственного экономического университета. 2025. № 1 (243). С. 106–113.
Vestnik of Samara State University of Economics. 2025. No. 1 (243). Pp. 106–113.

Научная статья
УДК 004.056.5:336.71

Актуальные проблемы безопасности хранения персональных данных клиентов

Ксения Анатольевна Гуртовая[1], Алла Геннадьевна Окунева[2]
[1,2] Самарский национальный исследовательский университет имени академика С.П. Королева, Самара, Россия
[1] ks.gurtovaya@yandex.ru
[2] okuneva.ag@ssau.ru

Аннотация. Вопрос безопасности личных данных становится все более актуальным из-за активного внедрения цифровизации в повседневную жизнь. Методы исследования, применяемые в работе, включают в себя анализ литературы, изучение законодательства в сфере биометрии, анализ статистических данных и аналитических материалов. В работе раскрываются сферы применения биометрических решений, роль биометрии в банковском секторе, анализируются риски, связанные с применением биометрии. Организация безопасного хранения рассматривается исходя из двух аспектов: правового и технического. В статье сопоставлены угрозы применения биометрии и существующие методы их предотвращения, данный анализ помогает выявить проблему, решение которой не освещено, – риск утечки биометрии по вине сотрудников. Авторами предлагаются методы предотвращения данной угрозы. Результатом предложенных решений при должном информировании граждан является расширение возможностей для всех участников рынка. С теоретической точки зрения исследование этой темы позволит углубить понимание механизмов и принципов безопасного хранения биометрических данных, повысить осведомленность общественности о степени безопасности хранения биометрии. Практическая значимость исследования заключается в разработке рекомендаций по улучшению безопасного хранения данных, выявлению уязвимых мест в существующих системах хранения.

Ключевые слова: биометрические технологии, финансовые технологии, цифровизация банковской отрасли, Единая биометрическая система, безопасность персональных данных, финансовый рынок, утечка персональных данных, биометрическая идентификация, биометрическая аутентификация

Основные положения:

♦ биометрия получила широкое распространение в финансовых технологиях, которые неразрывно связаны с банковским сектором;

♦ нарушение конфиденциальности личной информации является серьезной проблемой для России;

♦ единственной неосвещенной проблемой в сфере биометрических данных является риск утечки данных по вине сотрудников, имеющих доступ к биометрии;

♦ в настоящее время реализовано достаточно безопасное хранение биометрических данных, что подтверждается техническими возможностями, правовым регулированием и сравнением с международным опытом.

Для цитирования: Гуртовая К.А., Окунева А.Г. Актуальные проблемы безопасности хранения персональных данных клиентов // Вестник Самарского государственного экономического университета. 2025. № 1 (243). С. 106–113.

Original article

Organization of secure storage of biometric data: Threats and opportunities

Ksenia A. Gurtovaya[1], Alla G. Okuneva[2]
[1,2] Samara National Research University named after Academician S.P. Korolev, Samara, Russia
[1] ks.gurtovaya@yandex.ru
[2] okuneva.ag@ssau.ru

Abstract. The issue of personal data security is becoming increasingly relevant due to the active introduction of digitalization into everyday life. The research methods used in the work include literature analysis, study of legislation in the field of biometrics, analysis of statistical data and analytical materials. The work reveals the areas of application of biometric solutions, the role of biometrics in the banking sector, and analyzes the risks associated with the use of biometrics. The organization of secure storage is considered based on two aspects: legal and technical ones. The article compares the threats of using biometrics and existing methods of preventing them, this analysis helps to identify a problem whose solution is not covered - the risk of biometric leakage due to the fault of employees. The authors propose methods to prevent this threat. The result of the proposed solutions, with proper information to citizens, is the expansion of opportunities for all market participants. From a theoretical point of view, the study of this topic will deepen the understanding of the mechanisms and principles of secure storage of biometric data, increase public awareness of the degree of security of storing biometrics. The practical significance of the study is the development of recommendations for improving secure data storage, identifying vulnerabilities in existing storage systems.

Keywords: biometric technologies, financial technologies, digitalization of the banking industry, Unified Biometric System, personal data security, financial market, personal data leakage, biometric identification, biometric authentication

Highlights:

♦ biometrics have become widespread in financial technologies, which are inextricably linked with the banking sector;

♦ violation of the confidentiality of personal information is a serious problem for Russia;

♦ the only unaddressed problem in the field of biometric data is the risk of data leakage due to the fault of employees with access to biometrics;

♦ currently, sufficiently secure storage of biometric data has been implemented, which is confirmed by technical capabilities, legal regulation and comparison with international experience.

For citation: Gurtovaya K.A., Okuneva A.G. Organization of secure storage of biometric data: Threats and opportunities // Vestnik of Samara State University of Economics. 2025. No. 1 (243). Pp. 106–113. (In Russ.).

Введение

В современном мире биометрические технологии стали неотъемлемой частью различных сфер деятельности. Экономия времени и удобство – основные причины активного развития биометрии в государственной, юридической, финансовой и иных областях.

Вопрос безопасности личных данных становится все более актуальным из-за активного внедрения цифровизации в повседневную жизнь людей, в особенности после проникновения биометрических технологий. Биометрия – это особо чувствительные персональные данные, утечка и расшифровка которых могут привести к значительным негативным последствиям. Использование биометрии в качестве единственного способа аутентификации во многих системах может привести к тому, что «цифровая жизнь» человека будет «сломана». В связи с этим особую значимость приобретает вопрос безопасного хранения биометрических данных.

Цель работы – исследовать текущие угрозы при хранении биометрических данных, проанализировать существующие методы организации хранения биометрии и междуна-

родный опыт с целью разработки рекомендаций по повышению безопасности.

Для достижения цели работы поставлены следующие задачи:

♦ оценить значимость биометрических технологий на финансовом рынке;

♦ проанализировать правовой и технический аспекты хранения биометрии;

♦ выявить угрозы, связанные с хранением биометрии, сопоставить им существующие методы обеспечения безопасности;

♦ выявить угрозы, методы предотвращения которых не определены;

♦ изучить международный опыт хранения биометрических данных;

♦ составить рекомендации по совершенствованию системы безопасного хранения биометрии.

Методы

Методы исследования включают в себя анализ литературы, соответствующей теме работы, изучение действующего законодательства о биометрических данных и существующих технологий хранения, анализ статистических данных и аналитических материалов.

С теоретической точки зрения исследование этой темы позволит углубить понимание механизмов и принципов безопасного хранения биометрических данных, повысить осведомленность общественности о степени надежности хранения биометрии. Практическая значимость исследования заключается в разработке рекомендаций по повышению надежности хранения данных.

Таким образом, проведение научно-исследовательской работы по данной теме имеет как теоретическую, так и практическую ценность, способствует развитию науки об информационной безопасности и повышению уровня защиты биометрических данных.

Результаты

Основным понятием в данной работе является понятие «биометрия». Биометрия – уникальные физиологические и биологические характеристики человека, которые используются для установления или подтверждения личности.

Процесс распознавания человека состоит из двух этапов: идентификации и аутентификации. Биометрическая идентификация – это предъявление пользователем своего уникального биометрического параметра и процесс сравнения его со всей базой имеющихся данных. Биометрическая аутентификация – процесс доказательства и проверки подлинности через предъявление пользователем своего биометрического образа [1].

Наибольшее распространение технология получила на финансовом рынке, став инструментом, оптимизирующим получение различных услуг, например, оформление кредита, открытие счета в банке, оплата покупок или проезда (рис. 1).

По представленной диаграмме видно, что биометрия особо активно применяется в финансовых технологиях, которые неразрывно связаны с банковским сектором. Это объясняется тем, что цифровизация банковской отрасли выступает основным трендом последних лет, уровень затрат на IT-решения ежегодно возрастает на 12–14% [2]. Причиной этому является стремление банковской сферы к повышению качества и безопасности предоставляемых услуг.

«Рост числа случаев финансового мошенничества и других киберугроз заставили банки изучать новые технологии, и альтернативой стало использование биометрических решений» – говорится в аналитической записке ФинТех Ассоциации [3]. Несмотря на то что биометрия безопаснее других средств аутентификации, она также подвержена рискам, например, утечке персональных данных.

На сегодняшний день нарушение конфиденциальности личной информации является серьезной проблемой для России (рис. 2).

За последние 5 лет показатель утечки персональных данных вырос в 23,6 раза, с течением времени значение только увеличивается. В связи с проникновением таких персональных данных, как биометрические, эта проблема требует еще большего внимания. Это связано с тем, что ценность биометрии выше, так как изменить ее не представляется возможным, в отличие от PIN-кода или пароля.

Для предотвращения негативных последствий необходимо организовать безопасное хранение биометрических данных, что может быть реализовано только во взаимодействии

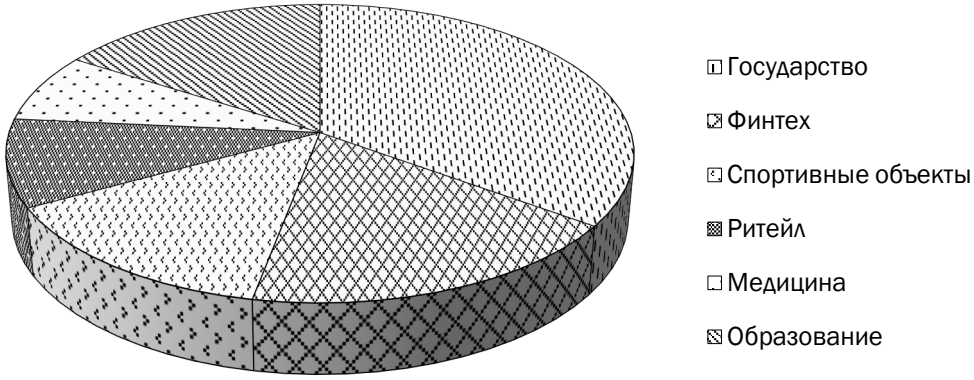

Рис. 1. **Российский рынок биометрических технологий в разрезе отраслей, 2023 г.***

* Правительство определило график внедрения биометрии в сервисы. URL: https://www.vedomosti.ru/finance/articles/2023/09/22/996514-pravitelstvo-opredelilo-grafik-vnedreniya-biometrii-v-servisi (дата обращения: 25.03.2024).

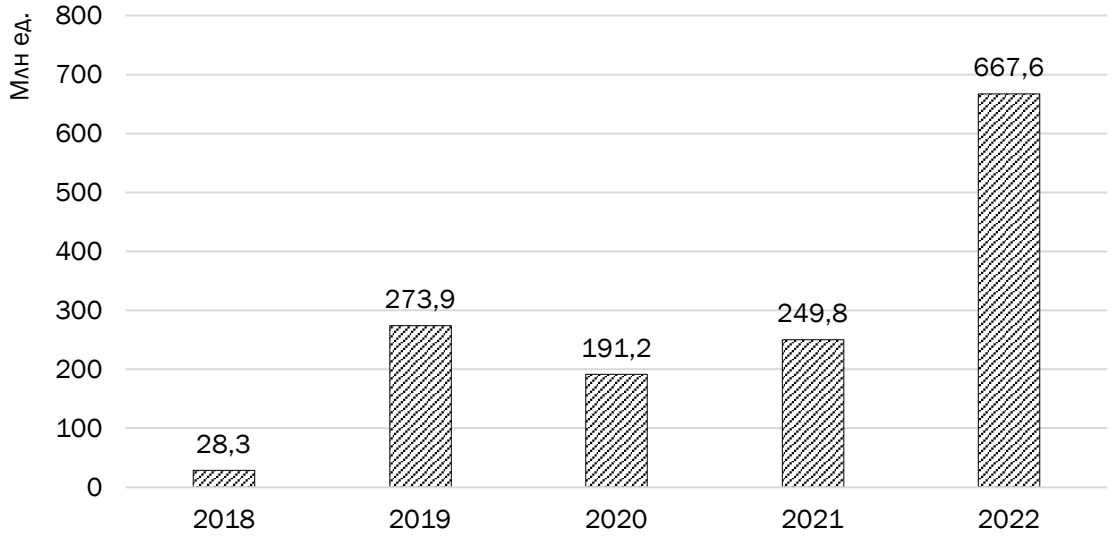

Рис. 2. **Количество утекших записей персональных данных и платежной информации в РФ***

* Утечки информации ограниченного доступа. URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennogo-dostupa-v-rossii-za-2022-god (дата обращения: 30.03.2024).

двух аспектов: правового и технического. В рамках законодательного регулирования шагом к созданию надежной биометрической экосистемы стало принятие Федерального закона от 29.12.2022 № 572 «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных...» (далее – ФЗ № 572).

Данным законом введено понятие «Единая биометрическая система» (далее – ЕБС). ЕБС – государственная информационная система, которая позволяет производить аутентификацию и идентификацию человека по лицу и (или) голосу [4]. С 1 июня 2023 г. хранить биометрические персональные данные вне ЕБС запрещается (п. 14 ст. 4 ФЗ № 572). Таким образом, биометрия может находиться только в государственной информационной системе, а получать доступ к этим данным могут только организации, имеющие аккредитацию или подключившиеся к другой аккредитованной организации. Все это дает гарантию сохранности биометрических данных на уровне государства.

Также законом было установлено, что до 30 сентября 2023 г. вся собранная государ-

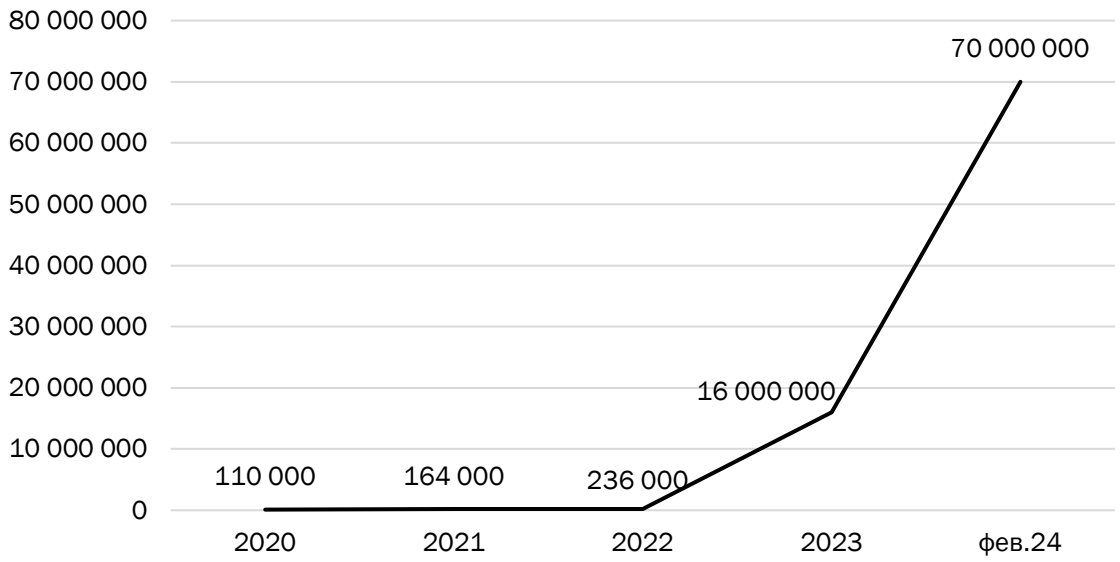

Рис. 3. **Количество пользователей, зарегистрированных в ЕБС**

ственными и коммерческими системами биометрия должна быть передана в Единую биометрическую систему (п. 2 ст. 26 ФЗ № 572) [5]. Благодаря этому к началу 2024 г. количество пользователей системы составило 70 млн человек (рис. 3).

За 5 лет количество биометрических слепков, хранящихся в ЕБС, увеличилось в 636 раз. Концентрация в одном месте такого объема особо чувствительных персональных данных возлагает на систему колоссальную ответственность за их сохранность и предъявляет особые требования к технической части организации безопасного хранения биометрии.

На сегодняшний день безопасность данных в ЕБС гарантируется путем соблюдения следующих принципов:

♦ биометрия хранится в обезличенной форме отдельно от персональных данных (распределенное хранение);

♦ данные хранятся в системе в зашифрованном виде;

♦ аккредитованные организации получают доступ не к самим биометрическим данным, а к их векторам – математически обработанным моделям лица и голоса граждан;

♦ ЕБС использует множество постоянно меняющихся биометрических алгоритмов (мультивендорный подход).

Данные принципы призваны предотвратить различные угрозы, связанные с хранением биометрических данных, самым опасным последствием которых является утечка уникальных и неизменных характеристик человека. Опасности и существующие методы их предотвращения представлены в табл. 1.

Таким образом, единственной неосвещенной проблемой является риск утечки данных по вине сотрудников, имеющих доступ к биометрии, например, с помощью методов социальной инженерии – психологического воздействия с целью получения конфиденциальных данных.

Для совершенствования системы хранения биометрических данных в России стоит обратить внимание на международный опыт и передовые практики в этой области. Для сравнения взяты страны с крупнейшими рынками биометрических технологий – США, Канада и Мексика, а также страны – лидеры по проникновению финтех-технологий – Индия и Китай [6; 7]. Сравнительный анализ приведен в табл. 2.

В Северной Америке (США, Канада, Мексика) схожая система хранения биометрических данных. Рост биометрического рынка в этих странах объясняется внедрением таких программ, как электронные паспорта и электронные визы. Идентификацию преимущественно используют в системах безопасности, миграционных и таможенных целях, а данные хранятся в различных базах данных, а не в единой централизованной системе. С одной

Таблица 1

Угрозы, связанные с хранением биометрии, и способы их предотвращения

Угроза	Способ предотвращения	Принцип защиты
Взлом системы	Мультивендорный подход	Взлом одного алгоритма – сложный и дорогостоящий процесс, злоумышленнику придется изучить десятки алгоритмов, которые постоянно меняются
Утечка ключей шифрования	Распределенное хранение данных	Владея ключами шифрования, злоумышленник будет иметь возможность расшифровать векторы, но не сможет сопоставить их с конкретными людьми, так как данные хранятся раздельно
Утечка векторов биометрической системы	Хранение биометрии в зашифрованном виде	Математически обработанные модели бесполезны для злоумышленников
Атака вредоносными программами	Использование программных решений	Антивирусные и антишпионские программные обеспечения помогут обнаружить и заблокировать попытки перехвата данных или внедрение вредоносных программ

Таблица 2

Сравнение международного опыта хранения биометрии

Страна	Применяемые виды биометрии	Единая централизованная система хранения	Хранение в зашифрованном виде	Особые требования для получения права использовать биометрию
Россия	Изображение лица и запись голоса	+	+	+
США	Различные виды биометрии	-	+	+
Канада	Различные виды биометрии	-	+	+
Мексика	Различные виды биометрии	-	+	+
Индия	Изображение лица, отпечатки пальцев, скан радужной оболочки глаз	+	+	+
Китай	Различные виды биометрии	-	+	+

стороны, наличие множества систем создает риски, связанные с недостаточным контролем за их безопасностью, а с другой – в случае утечки часть биометрии останется нетронутой.

Несмотря на то что в США находится один из крупнейших рынков биометрических технологий, некоторые системы хранения биометрии в этой стране подвергаются критике. Это касается, например, базы данных IDENT, которая лежит в основе центральной системы Министерства внутренней безопасности (DHS). Управление генерального инспектора Министерства считает, что надзор за биометрическими данными децентрализован, а сбор и использование биометрических данных в DHS частично некорректны [8]. Однако США стремятся улучшить свои биометрические системы, например, изучается возможность использования облачных сервисов, которые считаются более безопасными, чем устаревшие правительственные системы.

Особенностью индийского подхода является применение системы идентификации Aadhaar ID – это цифровое удостоверение личности и система биометрической идентификации и аутентификации граждан, представляет собой 12-значный номер, привязанный к цифровому профилю, в котором хранятся биометрические данные и копии некоторых документов владельца [3]. Решение хранить биометрию вместе с другими персональными данными влечет за собой дополнительные риски в случае утечки. В ЕБС эти данные располагаются в разных системах, что обеспечивает более высокую защищенность личной информации.

Обсуждение

В ходе исследования было выявлено, что риск утечки данных по вине сотрудников является неосвещенной проблемой в сфере биометрии. «Большинство утечек происходит из-за

человеческого фактора» – сообщает президент группы InfoWatch Наталья Касперская [9]. Возможными методами предотвращения данной угрозы является блокирование любых способов переноса данных на программном уровне, установка видеонаблюдения для особого контроля за сотрудниками, а также законодательное закрепление требований к лицам, допущенным к работе с биометрическими данными. Также уполномоченные сотрудники должны проходить процедуру авторизации для получения доступа к базам биометрических данных.

Сравнив российский и международный подходы к хранению биометрических данных, можно сделать вывод, что все анализируемые страны хранят биометрию в зашифрованном виде и вводят ограничения для получения возможности собирать и использовать биометрию. Анализ используемых решений для хранения биометрических данных показал, что в большинстве случаев система хранения биометрии в России является более безопасной, чем в других странах.

Заключение

На сегодняшний день в России не существует даже теоретической возможности восстановить фотографию или голос из биометрических данных. Если удалось получить оригинальные сведения, то спектр возможных последствий будет весьма велик, если человек повсеместно использовал эти данные в системах, где они являются единственным фактором аутентификации владельца. Однако эти риски нивелируются на других этапах использования биометрических данных, например, в процессе получения услуг таким инструментом служит технология liveness, которая обеспечивает проверку живого присутствия человека в кадре.

Безопасное хранение данных позволяет получить множество возможностей для всех участников рынка. Достаточное информирование о надежности системы позволит повысить доверие граждан, как следствие, больше людей будут готовы к сдаче своей биометрии. В результате пользовали будут иметь доступ к более удобному и быстрому получению услуг, аккредитованные организации – возможность повысить свою конкурентоспособность и получить дополнительную прибыль за счет предоставления доступа к ЕБС для других организаций, а государство – развитие цифровизации и улучшение экономики.

В результате проведенного исследования можно сделать вывод, что в настоящее время реализовано достаточно безопасное хранение биометрических данных, что подтверждается техническими возможностями, правовым регулированием и сравнением с международным опытом. Требуется незначительное совершенствование законодательной части и повышение контроля за сотрудниками, имеющими доступ к биометрии. Таким образом, ЕБС способна противостоять возможным угрозам, связанным с утечкой биометрических данных.

Список источников

1. Сергеева Л.И. Цифровая экономика. Москва : Юрайт, 2024. 415 с.

2. Deloitte оценила уровень цифровизации банков. URL: https://frankmedia.ru/25912 (дата обращения: 26.03.2024).

3. Ломов Н., Петрова Д., Рязанцева Ю. Биометрия в финансовой сфере 2020: выгоды для потребителей : аналитическая записка. Москва : Финтех ассоциация, 2020. 12 с.

4. Биометрические персональные данные: российское и международное регулирование. URL: https://brace-lf.com/informaciya/cifrovoe/1955-biometricheskie-personal-nye-dannye#_edn11 (дата обращения: 30.03.2024).

5. Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации : федеральный закон от 29.12.2022 № 572-ФЗ. URL: https://www.garant.ru/products/ipo/prime/doc/405951675/ (дата обращения: 30.03.2024).

6. Мировой рынок биометрии: главные тренды. URL: https://habr.com/ru/companies/digitalrightscenter/articles/670126/ (дата обращения: 05.04.2024).

7. Россия на третьем месте в мире по финтеху. URL: https://bcs-express.ru/novosti-i-analitika/rossiia-na-tret-em-meste-v-mire-po-fintekhu-kakie-aktsii-imet-v-vidu (дата обращения: 05.04.2024).

8. Методы DHS для сбора биометрических данных. URL: https://d-russia.ru/metody-dhs-dlja-sbora-biometricheskih-dannyh-podverglis-oficialnoj-kritike.html (дата обращения: 16.04.2024).

9. Утечка биометрических данных. URL: https://www.forbes.ru/tekhnologii/442163-s-garantiej-sol-ut-kasperskaa-posovetovala-ne-sdavat-biometriu-iz-za-utecek (дата обращения: 30.03.2024).

References

1. Sergeeva L.I. Digital economy. Moscow : Yurait, 2024. 415 p.

2. Deloitte assessed the level of digitalization of banks. URL: https://frankmedia.ru/25912 (date of access: 26.03.2024).

3. Lomov N., Petrova D., Ryazantseva Yu. Biometrics in the financial sector 2020: benefits for consumers: analytical note. Moscow : Fintech Association, 2020. 12 p.

4. Biometric personal data: Russian and international regulation. URL: https://brace-lf.com/informaciya/cifrovoe/1955-biometricheskie-personal-nye-dannye#_edn11 (date of access: 30.03.2024).

5. On the implementation of identification and (or) authentication of individuals using biometric personal data, on amendments to certain legislative acts of the Russian Federation and recognition of certain provisions of legislative acts of the Russian Federation as invalid : Federal Law of Dec. 29, 2022 No. 572-FZ. URL: https://www.garant.ru/products/ipo/prime/doc/405951675/ (date of access: 30.03.2024).

6. Global biometrics market: main trends. URL: https://habr.com/ru/companies/digitalrightscenter/articles/670126/ (date of access: 04.05.2024).

7. Russia ranks third in the world in fintech. URL: https://bcs-express.ru/novosti-i-analitika/rossiia-na-tret-em-meste-v-mire-po-fintekhu-kakie-aktsii-imet-v-vidu (date of access: 05.04.2024).

8. DHS methods for collecting biometric data. URL: https://d-russia.ru/metody-dhs-dlja-sbora-biometricheskih-dannyh-podverglis-oficialnoj-kritike.html (date of access: 16.04.2024).

9. Biometric data leak. URL: https://www.forbes.ru/tekhnologii/442163-s-garantiej-sol-ut-kasperskaa-posovetovala-ne-sdavat-biometriu-iz-za-utecek (date of access: 30.03.2024).

Информация об авторах

К.А. Гуртовая – студент Самарского национального исследовательского университета имени академика С.П. Королева;

А.Г. Окунева – кандидат экономических наук, доцент кафедры экономики Самарского национального исследовательского университета имени академика С.П. Королева.

Information about the authors

K.A. Gurtovaya – student of Samara National Research University named after Academician S.P. Korolev;

A.G. Okuneva – Candidate of Economic Sciences, Associate Professor of the Department of Economics of the Samara National Research University named after Academician S.P. Korolev.

Статья поступила в редакцию 16.10.2024; одобрена после рецензирования 23.10.2024; принята к публикации 05.11.2024.

The article was submitted 16.10.2024; approved after reviewing 23.10.2024; accepted for publication 05.11.2024.