ЭКОНОМИКА И МЕНЕДЖМЕНТ

УДК 336.71

ОРГАНИЗАЦИЯ БЕЗОПАСНОГО ХРАНЕНИЯ БИОМЕТРИЧЕСКИХ ДАННЫХ: УГРОЗЫ И ВОЗМОЖНОСТИ

К. А. Гуртовая, А. Г. Окунева

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. Автором 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, выявлении уязвимые места в существующих системах хранения.

Ключевые слова: биометрические технологии; финансовые технологии; цифровизация банковской отрасли; Единая биометрическая система; безопасность персональных данных.

В современном мире биометрические технологии стали неотъемлемой частью различных сфер деятельности. Экономия времени и удобство – основные причины активного развития биометрии в государственной, юридической и иных областях. Наибольшее распространение технология получила на финансовом рынке, став инструментом, оптимизирующим получение различных услуг, например, оформления кредита, открытия счёта в банке, оплаты покупок или проезда (рис. 1) [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 является 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 стали причиной изучения новых технологий, альтернативой стало использование биометрических решений [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) [4].

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 ПИН-кода или пароля.

Гуртовая Ксения Анатольевна (ks.gurtovaya@yandex.ru), студент III курса института экономики и управления;
Окунева Алла Геннадьевна (okuneva.ag@ssau.ru), доцент кафедры экономики Самарского университета, 443086, Россия, г. Самара, Московское шоссе, 34.

Для предотвращения негативных последствий необходимо организовать безопасное хранение биометрических данных, что может быть реализовано только во взаимодействии двух аспектов: правового и технического. В рамках законодательного регулирования шагом к созданию надежной биометрической экосистемы стало принятие Федерального закона от 29.12.2022 г. № 572 "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных…».

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 [5]. С 1 июня 2023 года хранить биометрические персональные данные вне ЕБС запрещается (п. 14 ст. 4 № 572-ФЗ). 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. Всё это дает гарантию сохранности биометрических данных на уровне государства.

Также Законом было установлено, что до 30 сентября 2023 года вся собранная государственными и коммерческими системами биометрия должна быть передана в Единую биометрическую систему (п.2 ст. 26 № 572-ФЗ). Благодаря этому к началу 2024 года количество пользователей системы составило 70 миллионов (рис. 3).

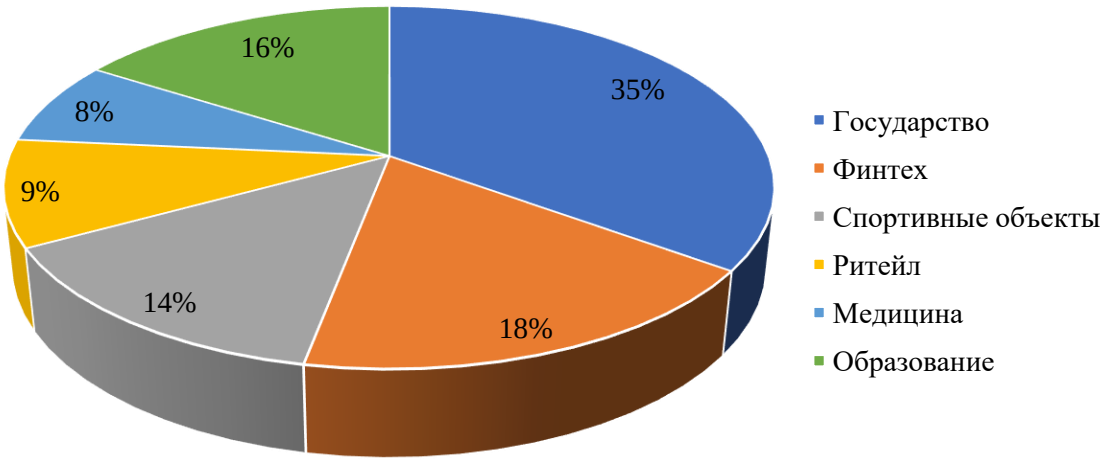

Рис. 1. Российский рынок биометрических технологий в разрезе отраслей, 2023 г. [1]

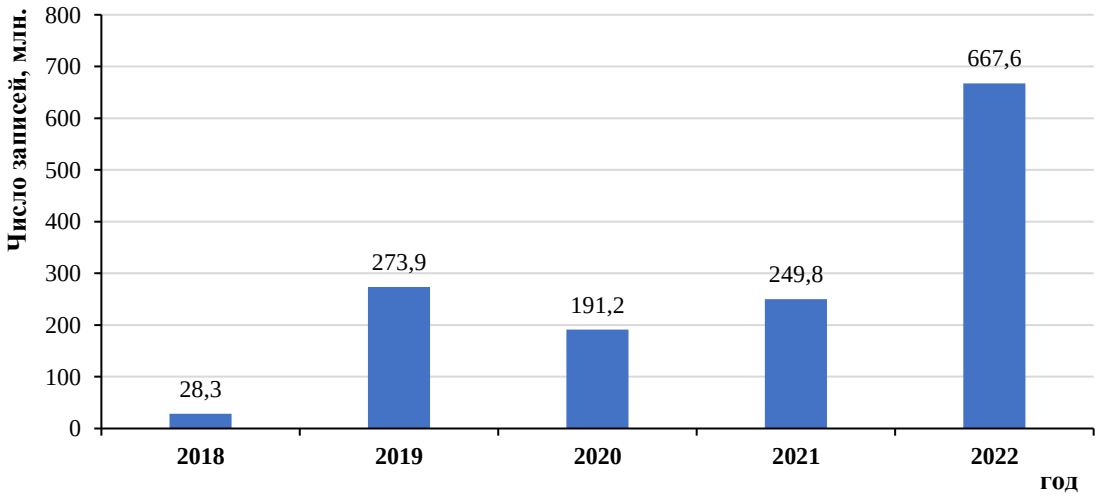

Рис. 2. Количество утекших записей персональных данных и платежной информации в РФ [4]

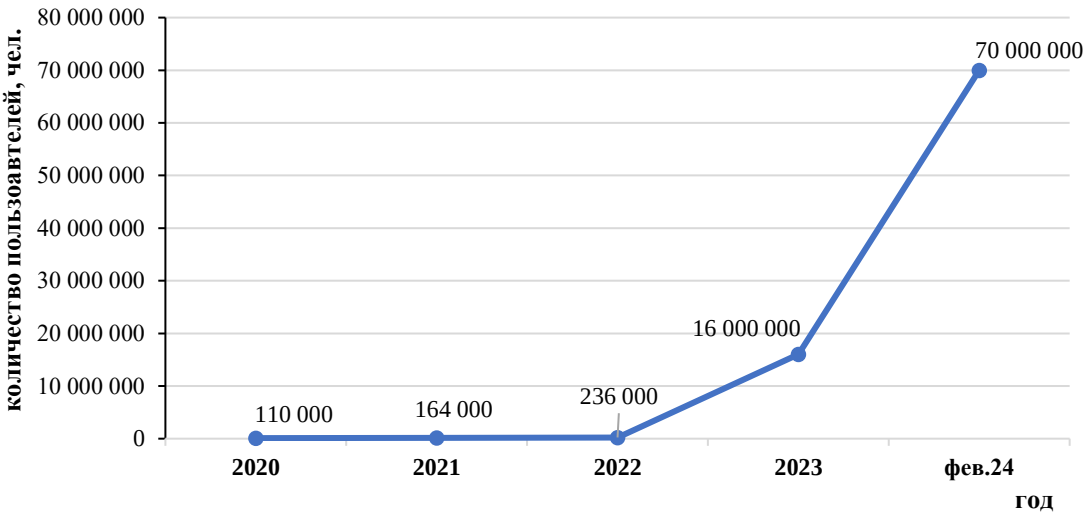

Рис. 3. Количество пользователей, зарегистрированных в ЕБС

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 единой биометрической системе гарантируется путём соблюдения следующих принципов:

• распределенное хранение данных: биометрия хранится в обезличенной форме отдельно от персональных данных;

• хранение данных в системе в зашифрованном виде;

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

• использование мультивендорного подхода: ЕБС использует множество постоянно меняющихся биометрических алгоритмов.

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 таблице (табл. 1).

Таким образом, единственной неосвещённой 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. «Большинство утечек происходит из-за человеческого фактора» – сообщает президент группы InfoWatch Наталья Касперская [6]. 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, допущенных к работе с биометрическими данными. Уполномоченные сотрудники должны проходить процедуру авторизации для получения доступа к базам биометрических данных.

В настоящий момент организация хранения биометрии является исчерпывающей для предотвращения различных угроз. Если злоумышленникам удалось получить оригинальные данные, то риск негативных последствий будет велик, если человек использовал биометрию во многих системах или в качестве единственного способа аутентификации. Однако эти риски нивелируются на других этапах использования биометрических данных, например, в процессе получения услуг таким инструментом является технология liveness, которая обеспечивает проверку живого присутствия человека в кадре.

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 придётся 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, т.к. данные хранятся раздельно
Утечка векторов биометрической системы	Хранение биометрии в зашифрованном виде	Математически обработанные модели бесполезны для злоумышленников
Атака вредоносными программами	Использование программных решений	Антивирусное и антишпионское программное обеспечение помогут обнаружить и заблокировать попытки перехвата данных или внедрение вредоносных программ

Организация безопасного хранения данных позволяет получить множество возможностей для всех участников рынка. Достаточное информирование о безопасности системы повысит доверие граждан, как следствие, больше людей будут готовы к сдаче своей биометрии. В результате пользовали получат 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 как техническими возможностями, так и правовым регулированием. 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.

Литература

1. ВЕДОМОСТИ: деловая газета России. 2023 [Электронный ресурс]. URL: https://www.vedomosti.ru/finance/articles/2023/09/22/996514-pravitelstvo-opredelilo-grafik-vnedreniya-biometrii-v-servisi (дата обращения: 25.03.2024).

2. Frank Media: деловое издание о финансах и экономике. 2020 [Электронный ресурс]. URL: https://frankmedia.ru/25912 (дата обращения: 26.03.2024).

3. ФинТех Ассоциация: официальный сайт. 2020 [Электронный ресурс]. URL: https://www.fintechru.org/analytics/analiticheskaya-zapiska-po-biometrii/ (дата обращения: 30.03.2024).

4. InfoWatch. 2023 [Электронный ресурс]. URL: https://www.infowatch.ru/analytics/analitika/utechki-informatsii-ogranichennog-dostupa-v-rossii-za-2022-god (дата обращения: 30.03.2024).

5. Brace law firm. 2023 [Электронный ресурс]. URL: https://brace-lf.com/informaciya/cifrovoe/1955-biometricheskie-personal-nye-dannye#_edn11 (дата обращения: 30.03.2024).

6. FORBES. 2021 [Электронный ресурс]. URL: https://www.forbes.ru/tekhnologii/442163-s-garantiej-sol-ut-kasperskaa-posovetovala-ne-sdavat-biometriu-iz-za-utecek (дата обращения: 30.03.2024).

ORGANIZATION OF SECURE STORAGE OF BIOMETRIC DATA: THREATS AND OPPORTUNITIES

K. A. Gurtovaya, A. G. Okuneva

The work reveals the scope 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 safe storage is considered based on two aspects: legal and technical. 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 biometrics leakage due to the fault of employees. The author proposes 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, research on this topic will deepen the understanding of the mechanisms and principles of secure storage of biometric data and increase public awareness of the degree of security of biometric storage. The practical significance of the study lies in the development of recommendations for improving secure data storage and identifying vulnerabilities in existing storage systems.

Key words: biometric technologies; financial technologies; digitalization of the banking industry; Unified Biometric System; security of personal data.

Статья поступила в редакцию 31.05.2024 г.

Gurtovaya Ksenia Anatolyevna (ks.gurtovaya@yandex.ru),
3rd year student of the Institute of Economics and Management;
Okuneva Alla Gennadievna (okuneva.ag@ssau.ru),
associate professorof the Department of Economics of Samara University,
443086, Russia, Samara, Moskovskoye shosse, 34.