Государственное и муниципальное управление. Ученые записки. 2024. № 1. С. 231–236
State and Municipal Management. Scholar Notes. 2024;(1):231–236
Проблемы социологии
Научная статья
УДК 316
https://doi.org/10.22394/2079-1690-2024-1-1-231-236 EDN ABUSEC

Биометрические технологии: отношение населения и преодоление рисков

Яна Викторовна Артамонова[1], Сергей Сергеевич Барсуков[2], Анна Андреевна Суханова[3]

[1]Южный федеральный университет, Ростов-на-Дону, Россия,
janaserduchenko@mail.ru, https://orcid.org/0000-0002-9618-0960
[2]Ростовский юридический институт МВД России, Ростов-на-Дону, Россия,
barsukov1982@yandex.ru, https://orcid.org/0000-0001-6043-4124
[3]Санкт-Петербургский университет МВД России, Санкт-Петербург, Россия,
elagin1982@yandex.ru, https://orcid.org/0009-0005-4262-9020

Аннотация. Статья посвящена рассмотрению биометрических систем идентификации населения, используемых сегодня большим количеством информационных платформ. В настоящее время биометрические системы идентификации используются в различных сервисах, вытесняя системы, использующие в качестве идентификаторов логин и пароль человека. Авторы работы в рамках статьи обращаются к рассмотрению социальных и технологических аспектов биометрии. В статье приведена характеристика основных видов биометрических систем, использующих как статические, так и динамические методы. Также авторы выделяют основные причины скепсиса со стороны пользователей среди российского населения, куда можно отнести недоверие граждан к надежности хранения личной информации, что может привести к утечке данных. В статье рассмотрены актуальные в настоящий момент проблемы использования биометрических систем идентификации и варианты их решения.

Ключевые слова: биометрия, идентификация, аутентификация, вены, радужная оболочка, сетчатка, геометрия лица, клавиатурный почерк, сосудистый рисунок, биометрический шаблон

Для цитирования: Артамонова Я. В., Барсуков С. С., Суханова А. А. Биометрические технологии: отношение населения и преодоление рисков // Государственное и муниципальное управление. Ученые записки. 2024. № 1. С. 231–236. https://doi.org/10.22394/2079-1690-2024-1-1-231-236. EDN ABUSEC

Sociology Problems
Original article

Biometric technologies: the attitude of the population and overcoming risks

Yana V. Artamonova[1], Sergey S. Barsukov[2], Anna A. Sukhanova[3]

[1]Southern Federal University, Rostov-on-Don, Russia,
janaserduchenko@mail.ru, https://orcid.org/0000-0002-9618-0960
[2]Rostov Law Institute of the Ministry of Internal Affairs of Russia, Rostov-on-Don, Russia,
barsukov1982@yandex.ru, https://orcid.org/0000-0001-6043-4124
[3]St. Petersburg University of the Ministry of Internal Affairs of Russia, St. Petersburg, Russia,
elagin1982@yandex.ru, https://orcid.org/0009-0005-4262-9020

Abstract. The article is devoted to biometric identification systems. Currently, biometric identification systems are used in various services, replacing systems that use a person's username and password as identifiers. The authors of the work address the social and technological aspects of biometrics in the framework of the article. The article describes the main types of biometric systems using both static and dynamic methods. The authors also identify the main reasons for skepticism on the part of users among the Russian population, which include citizens' distrust of the reliability of storing personal information, which can lead to data leakage. The article discusses the current problems of using biometric identification systems and their solutions.

Keywords: biometrics, identification, authentication, veins, facial geometry, iris, retina, keyboard handwriting, vascular pattern, biometric template

For citation: Artamonova Ya. V., Barsukov S. S., Sukhanova A. A. Biometric technologies: the attitude of the population and overcoming risks. *State and Municipal Management. Scholar Notes.* 2024;(1):231–236. (In Russ.). https://doi.org/10.22394/2079-1690-2024-1-1-231-236. EDN ABUSEC

В настоящий момент во всем мире в различных сферах крайне востребованы системы безопасности с высокой степенью надежности. Еще недавно единственным возможным способом установления личности человека являлась проверка документов. Распространение электронного банковского обслуживания, строгие требования по обеспечению безопасности на рабочих местах, а также многие другие изменения жизни человека в современном мире послужили толчком для начала создания электронных учетных записей с использованием логина (имени пользователя) и пароля (случайной последовательности символов, созданной пользователем) для регистрации и последующей аутентификации в компьютерной системе. Данное событие стало значительным прорывом в направлении защиты информации от несанкционированного доступа.

В связи с непрерывным ростом количества компьютерных систем пользователю необходимо на постоянной основе использовать несколько разных паролей, запоминать их либо записывать в бумажной или электронной форме. Для упрощения запоминания зачастую используются свои же имена или имена близких, даты рождения, номера телефонов, адреса проживания – то, что легче запоминается и фиксируется. Такие логины и пароли ведут к утечке информации либо позволяют путем подбора или использования специальных программ осуществить несанкционированную аутентификацию пользователя, что влечет за собой получение доступа к личной (персональной) информации лица, в то время как подмена личности и мошенничество является значительной проблемой в современном деловом мире [1].

Появление и активное распространение систем, направленных на идентификацию личности на основе биометрии, позволяют совершенствовать многие сферы работы и жизнедеятельности человека, влияют не только на скорость работы, но и на точность процедур.

Активное внедрение данной технологии помимо позитивного влияния на работу различных служб, безусловно, требует особых методов при сборе, хранении, использовании и обработки биометрических данных. В связи с активным использованием данных технологий исследователи обращаются к рассмотрению вопросов о работе биометрических технологий в различных сферах деятельности [2]. Например, исследовательский коллектив из Новосибирского государственного университета экономики и управления касаются изучения пользы от биометрических технологий для банковской, указывают на их защищенность, удобство, стоимость и другие характеристики [2]. Поскольку вопрос применения биометрии тесно связан с использованием персональных данных гражданина, то исследователи не могут обойти стороной вопросы возникновения правовых проблем, связанных с данными технологиями [3]. Помимо этого, ученые обращаются к изучению биометрических технологий с точки зрения использования данных методик в рамках правоохранительной деятельности [4].

Поскольку информационно-коммуникационные технологии в последние годы стали занимать одну из лидирующих позиций в различных сферах деятельности, то это вызывают неподдельный интерес со стороны научного сообщества.

В рамках данной работы рассматривается роль биометрии в жизни населения России, а также их отношения к внедрению и использованию данных технологий.

«Биометрия – наука, основанная на описании и измерении физиологических и поведенческих характеристик организмов живых существ. В применении к системам автоматической идентификации биометрическими являются системы и способы, основанные на использовании для верификации и идентификации уникальных характеристик организма» [5].

Верификацией называется сравнение нового биометрического образца с ранее сохраненным образцом. Выполнив сравнение двух образцов, система может вынести решение, является ли данный человек действительно тем, за кого себя выдает, то есть произвести аутентификацию – проверку подлинности.

Идентификация – сравнение измеренного параметра со всеми имеющимися записями из базы данных. Таким образом, особенностью биометрической идентификации является большой размер биометрической базы данных.

Идентификация состоит из четырех стадий. Первая стадия – запись, во время которой система запоминает физический или поведенческий образец. Вторая стадия – выделение, составляется биометрический образец на основе записанной уникальной информации. Далее осуществляется сравнение, образец сравнивается с представленными в базе. Завершающий этап – определение совпадения или несовпадения.

Системы по типу используемых биометрических параметров разделяются на две группы. Статический метод позволяет осуществить распознавание физических параметров человека. Динамический метод дает возможность проанализировать особенности поведения в момент выполнения какого-либо повседневного действия.

При помощи биометрии современные компьютеры и различные мобильные устройства, а также банковские и другие приложения имеют возможность осуществить аутентификацию пользователя, а организации имеют возможность разграничить доступ работников в зависимости от должности, помимо этого ограничивают доступ к секретным объектам. Несмотря на удобство использования биометрии, многие предпочитают использовать старые методы.

Среди основных причин, которые активно препятствуют внедрению биометрических технологий, можно выделить следующие: слабая информированность населения, риск осуществления несанкционированного доступа к биометрическим параметрам, возможность изменения характеристик с течением времени или из-за болезней, высокая стоимость аппаратного обеспечения, отсутствие надежного способа обеспечения взаимодействия между работой системы и защиты используемых биометрических показателей [6].

Действительно, уникальные возможности биометрической идентификации ценятся не только пользователями за удобство, но и мошенниками – киберпреступниками. При этом несомненным является тот факт, что скомпрометированные пароли можно всегда сменить на новые, а изменить собственные биометрические данные не представляется возможным. Также следует отметить, что некоторые системы биометрической идентификации подтверждают личность с вероятностью, близкой, но не равной 100%, следовательно, допускается возможность, что человек может незначительно отличаться от своей биометрической модели, которая была сохранена в базе.

Для лучшего понимания достоинств и недостатков биометрии остановимся на некоторых наиболее популярных в настоящее время системах.

К основным видам статистического метода относится идентификация по папиллярному узору, радужной оболочке, сетчатке, геометрии и термографии лица, расположению вен на кистях (васкулярная идентификация).

Дактилоскопия – наиболее популярная технология, которая основана на сканировании и распознавании папиллярных узоров, которые формируются в сосочковом слоем дермы под эпидермисом. Данный метод легок в использовании, надежен универсальностью данных и активно используются правоохранительными органами для наполнения учетов электронными образцами. Используемые сканеры имеют небольшой размер и относительно небольшую стоимость.

Папиллярные узоры обладают уникальностью, восстанавливаемостью и устойчивостью, что позволяет использовать данный метод в криминалистике, финансовой сфере и в быту: последнее время производится множество устройств (ноутбуков, смартфонов, клавиатур и пр.) со встроенным сканером папиллярных узоров. Однако в данном случае можно говорить лишь об относительной восстанавливаемости и устойчивости. В случае глубоких повреждений, захватывающих дерму, образуются шрамы. А вследствие поверхностных порезов, особенностей выполнения работ

у людей некоторых профессий (аграрное производство, строительство), сезонных температурных изменений папиллярные узоры могут временно становиться непригодными для идентификации. В связи с использованием сложных алгоритмов распознавания мельчайших папиллярных линий, система требует полный контакт пальца со сканером. Кроме того, систему можно обмануть с помощью качественного муляжа.

Аутентификация по геометрии лица подразделяется на двухмерное и трехмерное распознавание. В процессе сканирования построение шаблона происходит на основании неизменных характеристик головы (форма черепа, надбровных дуг, высота и ширина скул и т.д.).

Аутентификация по радужной оболочке. Рисунок радужки является относительно устойчивым в течение всей жизни, дополнительной надежности способствует различие рисунков радужки левого и правого глаза [7–8]. Устройства, считывающие изображение радужки, являются не сканерами, а специализированными камерами, выполняющими определенное количество снимков в секунду. При этом считывающая камера может находиться на расстоянии до 1 метра, что увеличивает комфорт пользователя. Однако возможность дистанционного снятия изображения радужки увеличивает вероятность кражи биометрического параметра злоумышленниками. Поэтому использовать данный метод, как и аутентификацию по геометрии лица, необходимо одновременно с дополнительными программами защиты от подделок – например с системой, определяющей реакцию зрачка на поток света.

Надежность аутентификации по сетчатке гораздо выше, чем по папиллярным узорам, геометрии лица и радужной оболочке, так как в данном случае в качестве ключа используется биометрический параметр, расположенный внутри глаза. В отличие от радужки, уникальное изображение глазного дна, то есть неповторимое для каждого человека расположение кровеносных сосудов, невозможно снять дистанционно. Сканирование предусматривает направление к глазному дну через зрачок инфракрасного излучения низкой интенсивности или мягкого лазера для выявления уникального сосудистого рисунка. Сканеры данного вида имеют высокую стоимость. Для прохождения аутентификации пользователю необходимо максимально приблизить лицо к устройству и направить взгляд на определенную метку на дисплее, находясь в одном положении некоторое время. Данный метод обладает невысоким уровнем комфорта, также не представляется возможным им воспользоваться в случаях, когда необходимо провести аутентификацию большого количества людей за короткое время (например, на проходных) в связи с относительно долгим сканированием.

Схожая методика используется при аутентификации по васкулярному рисунку кистей рук, когда в качестве идентификатора используется уникальное расположение поверхностных вен [9]. Васкулярный рисунок устойчив во времени, подвержен изменению лишь в случае некоторых заболеваниях (например, при артрите). Метод также является высоко надежным (ключ расположен внутри тела), при этом стоимость данных систем значительно ниже тех, что работают с сетчаткой.

Основными на всемирном рынке биометрической защиты долгое время являлись системы, использующие статистический метод. Динамическая аутентификация и комбинированные системы занимали лишь незначительную долю рынка. Однако в последние годы наблюдается активное развитие именно динамических методов. Среди них наиболее распространены следующие: идентификация по голосу, подписи и клавиатурному почерку.

Формирование персонального шаблона при идентификации по голосу происходит по нескольким характеристикам: тональности, модуляции, интонации, отличительным особенностям произношения определенных звуков.

Клавиатурный почерк – биометрическая совокупная характеристика скорости ввода, время зажатия клавиш, частоты произведенных ошибок при вводе, степени аритмии при наборе символов, продолжительности интервалов между нажатиями и т.д.

Точную верификацию подписи обеспечивает специальное оборудование: световые перья и сенсорные экраны. При этом, биометрический метод аутентификации может использовать анализ, как визуальных характеристик подписи, так и динамических, учитывающих статистические и периодические характеристики написания.

Серьезными недостатками динамических методов является зависимость характеристик от текущего психоэмоционального и физиологического состояния пользователя в момент сдачи биометрии. Усталость, возрастные изменения и заболевания могут значительно изменять биометрические показатели, что приводит к ошибкам аутентификации. К тому же данные методы используют идентификаторы, которые нельзя назвать скрытыми, что сказывается на их надежности.

Как мы видим, существуют различные биометрические методы со своими плюсами и недостатками. Но также мы можем обратить внимание и на то, что из результатов опросов населения видно, многие люди до сих пор предпочитают старые методы аутентификации (использование логина и пароля) вместо использования биометрии.

На наш взгляд, для популяризации данных технологий среди российского населения, а также основным стимулом для сдачи биометрических данных должно быть четкое понимание пользователем того, для чего эти данные будут использоваться, и гарантия их надежной защиты.

То есть гражданам в доступной форме необходимо объяснять, что отличительной особенностью биометрических систем является хранение в их базах наборов цифр, характеризующих контрольные точки, по которым определяются индивидуальные характеристики биометрической модели. Так, в базе Единой биометрической системы персональные данные хранятся в обезличенном и зашифрованном виде, по которому восстановить фотографию или голос невозможно, можно лишь сравнить поступающие в систему запросы с данными моделями. Для идентификации пользователя система строит биометрическую модель и сравнивает ее с хранящимся в базе образцом. Обмануть систему с помощью похищенных из нее данных невозможно.

В целях увеличения надежности защищенности данных также следует отдавать предпочтения тем системам, которые используют скрытые идентификаторы, то есть располагающиеся внутри организма, например, идентификации по сетчатке или васкулярному рисунку кистей. В настоящее время обязательным требованием является и многофакторность аутентификации, но в данном случае необходимо решить, какие именно системы должны быть задействованы в данном процессе.

Разработчикам и законодательным органам следует на основе новейших исследований уязвимостей данных систем оперативно доработать решения по самой идентификации, например, сконцентрироваться на поиске совместимости биометрических данных и протоколов с нулевым разглашением, так и нормативные акты, регулирующие их работу.

На наш взгляд, если будут проведены дополнительные разъяснения населению о принципах работы биометрии, о возможностях ее использования, например, посредством рекламных роликов, а со стороны разработчиков системы будут проработаны надежные механизмы защиты данных, то пользователи с большей уверенностью будут прибегать к использованию данных методик.

Список источников

1. Глинская Е. В. Биометрическая технология васкулярной идентификации личности // Инженерный вестник. 2013. № 5.

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

3. Рассолов И. М., Чубукова С. Г., Микурова И. В. Биометрия в контексте персональных данных и генетической информации: правовые проблемы // Lex Russica. 2019. №1 (146). URL: https://cyberleninka.ru/article/n/biometriya-v-kontekste-personalnyh-dannyh-i-geneticheskoy-informatsii-pravovye-problemy (дата обращения: 14.12.2023).

4. Дивольд В. Е. 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.

5. Болл Р., Коннел Д., Панканти Ш., Ратха Н., Сеньор Э. Руководство по биометрии. М.: Техносфера, 2007. 368 с.

6. Макшанова А. О., Зимнуров М. Ф., Астраханцева И. А., Астраханцев Р. Г. Анализ рисков и перспективы использования биометрических технологий в цифровой экономике // Проблемы экономики, финансов и управления производством. 2021. № 48. С. 101–104.

7. Барсуков С. С. Криминалистическая идентификация по радужной оболочке и сетчатке глаза: современные возможности и проблемы применения // Юристъ-Правоведъ. 2021. №1 (96). URL: https://cyberleninka.ru/article/n/kriminalisticheskaya-identifikatsiya-po-raduzhnoy-obolochke-i-setchatke-glaza-sovremennye-vozmozhnosti-i-problemy-primeneniya (дата обращения: 17.12.2023).

8. Гришенкова Н. П., Лавров Д. Н. Обзор методов идентификации человека по радужной оболочке глаза // Математические структуры и моделирование. 2014. № 1 (29). URL: https://cyberleninka.ru/article/n/obzor-metodov-identifikatsii-cheloveka-po-raduzhnoy-obolochke-glaza (дата обращения: 17.12.2023).

9. Баранов С. О., Абрамов Д. Б. Технология биометрической аутентификации пользователя по венозному рисунку кистей рук // Вестник Вестник Сибирской государственной автомобильно-дорожной академии. 2017. №2 (54). URL: https://cyberleninka.ru/article/n/tehnologiya-biometricheskoy-autentifikatsii-polzovatelya-po-venoznomu-risunku-kistey-ruk (дата обращения: 17.12.2023).

References

1. Glinskaya E.V. Biometric technology of vascular identity identification. *Engineering Bulletin*. 2013;(5). (In Russ.)

2. Zhukov Ya. V., Lysenko R.Y., Protas N. G., Tarasova G. M. Biometrics. How does it work and what risks does it carry? *Modern Economy Success*. 2020;(3):13–19. (In Russ.)

3. Rassolov I. M., Chubukova S. G., Mikurova I. V. Biometrics in the context of personal data and genetic information: legal problems*. Lex Russica*. 2019;1(146). Available from: https://cyberleninka.ru/article/n/biometriya-v-kontekste-personalnyh-dannyh-i-geneticheskoy-informatsii-pravovye-problemy [Accessed 14 December 2023]. (In Russ.)

4. Divold V. E. Prerequisites for the creation of a national biometric identification system. *Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia*. 2021;2(81):139-143. DOI 10.24412/1999-625X-2021-2-139-143. (In Russ.)

5. Ball R., Connell D., Pankanti Sh., Ratha N., Senior E. *Guide to biometrics.* Moscow: Technosphere; 2007. 368 p. (In Russ.)

6. Makshanova A. O., Zimnurov M. F., Astrakhantseva I. A., Astrakhantsev R. G. Risk analysis and prospects for the use of biometric technologies in the digital economy. *Problems of economics, finance and production management*. 2021;(48):101–104 (In Russ.)

7. Barsukov S. S. Criminalistic identification by the iris and retina of the eye: modern possibilities and problems of application. *Jurist-Pravoved*. 2021;1(96). Available from: https://cyberleninka.ru/article/n/kriminalisticheskaya-identifikatsiya-po-raduzhnoy-obolochke-i-setchatke-glaza-sovremennye-vozmozhnosti-i-problemy-primeneniya [Accessed 17 December 2023] (In Russ.)

8. Grishenkova N. P., Lavrov D. N. Review of methods for identifying a person by the iris of the eye. *Mathematical structures and modeling*. 2014;1(29). Available from: https://cyberleninka.ru/article/n/obzor-metodov-identifikatsii-cheloveka-po-raduzhnoy-obolochke-glaza [Accessed 14 December 2023] (In Russ.)

9. Baranov S. O., Abramov D. B. Technology of biometric authentication of the user by the venous pattern of the hands. *Bulletin of the Siberian State Automobile and Road Academy*. 2017;2(54). Available from: https://cyberleninka.ru/article/n/tehnologiya-biometricheskoy-autentifikatsii-polzovatelya-po-venoznomu-risunku-kistey-ruk [Accessed 17 December 2023] (In Russ.)

Информация об авторах

Я. В. Артамонова – кандидат социологических наук, доцент, Институт социологии и регионоведения ЮФУ.

С. С. Барсуков – старший преподаватель кафедры криминалистики и оперативно-разыскной деятельности, подполковник полиции, РЮИ МВД России.

А. А. Суханова – старший преподаватель кафедры деятельности ОВД в особых условиях, подполковник полиции, Санкт-Петербургский университет МВД России.

Information about the authors

Ya. V. Artamonova – Cand. Sci. (Sociol.), Lecturer, Southern Federal University, Institute of Sociology and Regional Studies.

S. S. Barsukov – Senior Lecturer, Police Lieutenant Colonel, Department of Criminalistics and Operational-Investigative Activities, Rostov Law Institute of the Ministry of Internal Affairs of Russia.

A. A. Sukhanova – Senior Lecturer, Police Lieutenant Colonel, Department of Internal Affairs in Special Conditions, St. Petersburg University of the Ministry of Internal Affairs of Russia.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Статья поступила в редакцию 09.01.2024; одобрена после рецензирования 25.01.2024; принята к публикации 26.01.2024.

The article was submitted 09.01.2024; approved after reviewing 25.01.2024; accepted for publication 26.01.2024.