

**О. И. ВЕСЕЛИЦКИЙ**

старший преподаватель кафедры экономики городского хозяйства и жилищного права Университета Правительства Москвы

O. I. VESELITSKY

Senior Lecturer with the Chair of City Economy and Housing Law of Moscow Metropolitan Governance Yury Luzhkov University

**В. Р. ОРЛОВА**

студентка бакалавриата Университета Правительства Москвы, направление «Государственное и муниципальное управление», профиль «Управление городским хозяйством»

V. R. ORLOVA

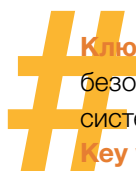
Undergraduate student at Moscow Metropolitan Governance Yury Luzhkov University, direction "State and Municipal Administration", profile "Urban Management"

Правовые аспекты использования биометрических данных

Legal Aspects of Using Biometric Data

Использование биометрических данных при получении государственных услуг гражданами строго регламентировано и обеспечено правовой и технологической поддержкой государства. В то же время на бытовом уровне растет интерес к сервисам, использующим биометрию. Владельцы бизнесов, как правило, не вводят строгую регламентацию при использовании и хранении биометрических данных. Вместе с тем наборы биометрических данных, используемых в государственном секторе и в бизнесе, нередко коррелируют друг с другом. Поэтому в частном секторе возникает риск угрозы информационной безопасности. Разделение наборов биометрических данных для государственного и частного секторов может стать способом минимизации названных рисков.

Use of biometric data at state services delivery to citizens is rigorously regulated and enjoys legal and technological support of the State. At the same time there's a notable proliferation of interest towards services that use biometric data to provide services at the mundane level. Businesses' owners do not as a rule observe strict regulation of the use and biometric data storage. It is not uncommon that sets of biometric data used by the State and the private sector correlate with each other. Due to inadequately formalized data storage conditions in private sector it runs the risks of information security threats. Separation of biometric data in two sets that don't overlap for using them in the state and the private sectors could be a way to minimize the above mentioned risks.



Ключевые слова: биометрические данные, персональные данные, информационная безопасность, идентификация гражданина, государственная услуга, интернет вещей, единая система идентификации и аутентификации (ЕСИА), единая биометрическая система.

Key words: biometric data, personal data, information security, citizen identification, public service, Internet of things, Unified Identification and Authentication System (UIAS), unified biometric system.

Для цитирования: Веселицкий О. И., Орлова В. Р. Правовые аспекты использования биометрических данных // Вестник Университета Правительства Москвы. 2020. № 1. С. 53–58.

For citation: Veselitsky O. I., Orlova V. R. Legal Aspects of Using Biometric Data. *MMGU Herald*, 2020, no. 1, pp. 53-58. (In Russ.).

Уже больше года в России под эгидой федеральных властей собирают, фиксируют и используют биометрические данные граждан. Разработана подробная нормативно-правовая база в данной сфере деятельности. Так, постановлением Правительства Российской Федерации от 30.06.2018 № 772 [2] определен состав биометрических персональных данных, размещаемых в единой информационной системе, где происходят их обработка, сбор и хранение. Согласно постановлению размещается следующая биометрическая информация о гражданах Российской Федерации: «данные изображения лица человека, полученные с помощью фото- и видеоустройств; данные голоса человека, полученные с помощью звукозаписывающих устройств» [2]. Суть названного постановления сводится к выполнению определенной процедуры. После проведения идентификации с согласия гражданина информация о нем вносится в единую систему идентификации и аутентификации (ЕСИА) и единую биометрическую систему (ЕБС). Гражданин, прошедший процедуру идентификации, может открывать счета (вклады) в банках, осуществлять некоторые банковские операции и получать другие услуги, включая государственные, без личного присутствия. Иначе говоря, если гражданин зарегистрирован в ЕСИА и его биометрические данные хранятся в ЕБС, он может, получая удаленно ту или иную услугу, пройти идентификацию с помощью биометрии. Проведенная проверка личности не будет вызывать сомнений ни у организации, услугу оказавшей, ни у органов правопорядка, если к ним обратится гражданин в случае возникновения конфликтной ситуации. Считается, что вероятность ошибки при использовании биометрических данных составляет 1:10 000 000. При такой минимальной степени риска ошибочной идентификации можно с успехом осуществлять и финансовые операции, и выдачу документов.

На государственном уровне процесс первичного сбора биометрических данных, их хранения и использования максимально формализован

Здесь справедливо будет задать вопрос: каковы полнота и содержание базы биометрических данных, где она хранится, кто ее поддерживает и на каких условиях использует? Наполнение базы биометрических данных происходит в соответствии с требованиями, указанными в постановлении Правительства Российской Федерации от 14.07.2018 № 820 [3]. Здесь изложены условия предоставления персональной информации, исключающие случайное либо преднамеренное попадание в базу данных сведений, не относящихся к идентифицируемому гражданину. Все действия в системе обработки биометрических данных должны быть строго регламентированы и зафиксированы согласно постановлению Правительства Российской Федерации от 29.06.2018 № 747 [1]. Более того, чтобы избежать теоретически возможных ошибок при внесении биометрических данных в базу, Минкомсвязи России издало приказ от 21.06.2018 № 307 [4]. Согласно этому документу оператор ЕБС обеспечивает обработку биометрических сведений, включая сбор и хранение, их проверку и передачу информации о степени соответствия биометрическим персональным данным, содержащимся в ЕБС. Оператор должен занимать существенное положение в сфере связи общего пользования на территориях не менее чем двух третей субъектов Российской Федерации. В настоящее время таким оператором связи является ПАО «Ростелеком». Именно эта организация отвечает за наполнение и поддержание работоспособности всех компонентов единой информационной системы. Платформа системы размещена в облачной защищенной инфраструктуре «Ростелекома», к которой государственные структуры и коммерческие организации получают доступ через специальные каналы связи системы межведомственного электронного взаимодействия.

Как следует из вышеизложенного, на государственном уровне процесс первичного сбора биометрических данных, их хранения и использования максимально формализован. Он рассчитан на обеспечение наибольшего доверия граждан к механизмам идентификации с помощью биометрии. Тем не менее существует и в этой строгой схеме слабое звено, не позволяющее до конца быть уверенным в стопроцентной безопасности проце-

дур. Речь идет о неконтролируемом участке в цепочке идентификации на стороне клиента. Современные технологии позволяют незаметно для гражданина подменить его данные в процессе идентификации либо использовать их модифицированные копии. Качество копий так высоко, что третьи лица могут несанкционированно получить услуги либо доступ к закрытой персональной информации. К примеру, уже обычным явлением стало применение технологии Deepfake, позволяющей с помощью обработки в нейросети заменить реальное видеоизображение на синтезированное, весьма реалистичное. В начале марта 2019 г. компания McAfee, занимающаяся проблемами кибербезопасности, сообщила, что замещение изображений реальных людей на виртуальные образы в видео уже невозможно определить невооруженным глазом [12]. Специалисты McAfee считают, что методика замены изображений представляет серьезную угрозу общественной безопасности, так как ее можно использовать в целях искажения работы классификатора изображений¹. Подделка голосовых сообщений тоже не является затруднением для злоумышленников. Так, известен факт мошенничества с применением технологии Deepfake для имитации голоса. По данным страховой компании Euler Hermes Group SA в марте 2019 г. преступник позвонил в одну британскую энергетическую компанию, выдавая себя за главу материнской компании из Германии [11]. Директор энергетической компании, узнав знакомый голос по телефону, решил, что разговаривает со старшим руководителем. «Руководитель» попросил директора отправить средства венгерскому поставщику. Потери компании от действий злоумышленников составили 243 тыс. долл.

Данный эпизод не ставит крест на применении биометрии в финансовой сфере. В настоящее время получены определенные результаты синтеза систем идентификации голоса, которые свидетельствуют о достаточно точной идентификации и верификации дикторов [5].

Однако существенные риски, безусловно, возможны. Поэтому, к примеру, «Тинькофф Банк» использует идентификацию по голосу параллельно с первичной верификацией клиента по имеющимся у банка метаданным: голос – только дополнительный критерий опознания личности.

Ввиду изложенного можно сделать вывод, что главный фактор, препятствующий появлению полного доверия к технологиям биометрии, – вероятность несанкционированного доступа к биометрическим данным граждан. Вместе с тем согласно отчетам «Ростелекома» утечка информации о биометрии граждан из баз данных подведомственной структуры маловероятна. «Ростелеком» использует технологию распределения данных: случайное или преднамеренное раскрытие одного из фрагментов персональной информации не приводит к обнаружению всех биометрических сведений о человеке.

Если система распознавания биометрических данных опирается на сервисы, контролируемые государственными структурами, она довольно безопасна

Примером надежности хранения информации может служить механизм доступа к биометрическим данным, реализованный для Москвы. В московском метрополитене запущено испытание «умных» турникетов, оборудованных видеокамерами [8]. Сейчас их используют при идентификации сотрудников ряда государственных и муниципальных учреждений в целях обеспечения безопасности [7]. В перспективе пассажирам для прохода через такой турникет не надо будет предъявлять проездные документы. Все сведения, необходимые для оплаты проезда, автоматически будут формироваться в момент распознавания лица пассажира. Новая технология позволяет идентифицировать клиента и связаться с платежным функционалом за одну миллисекунду. За этот промежуток времени система управления турникетом обратится к ЕБС и примет решение, открывать турникет или нет.

¹ Программа, которая отвечает за сличение изображений, поступающих в систему, с изображениями, имеющимися в базе системы.

Таким образом, если система распознавания биометрических данных опирается на сервисы, контролируемые государственными структурами, она довольно безопасна и обеспечена как с технической стороны, так и с нормативно-правовой. Поэтому необходимо обратить внимание на те области, где биометрические данные активно используются, но их сбор и применение не столь строго регламентированы, как в случае с ЕБС. В первую очередь стоит упомянуть технологии, стремительно развивающиеся и вошедшие в наш обиход как неперенный атрибут комфорта. Речь идет о направлении, которое обобщенно называется «интернет вещей». «Умные» вещи, которые окружают нас, – это прежде всего неприметные коммуникаторы, сборщики разнообразной информации, позволяющей успешно выполнять назначенные им функции. Технологии «умного» энергоснабжения, «умного» видеонаблюдения, «умного» ресурсосбережения и т. д. круглосуточно помогают людям, незримо управляя различными процессами. В этом огромном количестве электронных «умных» «менеджеров» стали появляться устройства, работающие с биометрическими данными. «Умные» холодильники, светильники, телевизоры с голосовым управлением распознают голос владельца и готовы 24 часа в сутки выполнять голосовые команды, получая и записывая голосовые сообщения. По сути, голосовые команды при условии идентификации владельца являются биометрическими персональными данными. «Умные» агрегаты объединяются в единую систему с другими устройствами и облачными сервисами либо работают автономно.

С появлением «умных» систем доступа на предприятиях внедряются «умные» домофоны, «умные» шлагбаумы, снимающие показания видеокамер и сравнивающие их с корпоративной базой данных сотрудников. Каким образом все эти данные защищены? Кто является оператором данных? Эти и многие другие вопросы вызывают тревогу. Представители бизнеса говорят о добровольном согласии граждан на использование подобного оборудования. Обычно при заключении договора на сервисное обслуживание граждане указывают в соответствующем пункте, что они предупреж-

дены о возможных последствиях использования их персональных данных, в том числе биометрических. Однако люди, подписывая договор на обслуживание шлагбаума или иного оборудования, далеко не всегда правильно понимают все последствия и угрозы потери биометрических данных. От кибератак в сфере интернета вещей страдает все больше коммерческих компаний и их клиентов [10]. Это происходит не только потому, что растут объемы потребления «умных» девайсов и пропорционально – число нападений хакеров, но и потому, что компании часто не уделяют достаточного внимания выбору производителя устройств, не настраивают их должным образом.

Масштабная проблема состоит в том, что биометрические данные, собираемые частными компаниями для осуществления бизнес-процессов, идентичны данным, которые от граждан поступают в единую электронную систему персональных данных (ЕСИА и ЕБС). Если произойдет утечка биометрических сведений из банка данных частной компании, будут нивелированы значительные усилия государственных структур по сохранению персональных данных граждан и ограничению доступа третьих лиц к услугам, для них не предназначенным. Последствия нелегитимного использования похищенной информации при пользовании государственными услугами будут намного серьезнее, чем потеря управления шлагбаумом. Разработчики ЕСИА утверждают, что пока нет поводов для волнений, поскольку не было прецедентов реализации угроз информационной безопасности при помощи биометрических данных. Возможности механизмов сохранности данных не вызывают сомнений, но ради предупреждения возможных конфликтов необходимо разработать и внедрить также и превентивные меры сохранности информации. Самым простым и логичным решением описанной проблемы видится отделение списка биометрических данных, используемых на бытовом уровне, от списка данных, задействованных в процессе идентификации при получении государственных услуг и в банковской сфере. Тут уместно провести аналогию с электронно-цифровой подписью (ЭЦП). В современной практике используют ЭЦП двух видов – простую и усиленную. Про-

стая ЭЦП позволяет удостоверить личность, усиленная ЭЦП – совершать юридически значимые действия.

Сами биометрические данные, используемые в современных технологиях, также различаются по своей надежности. Как видно из диаграммы на рисунке 1, кроме традиционных и привычных для бытового уровня биометрических параметров, существует еще ряд персональных характеристик, пока мало используемых, которые могут существенно повысить уровень безопасности при получении доступа к критически важной информации или услугам.

Таким образом, если при оказании официальных услуг будет использован определенный список биометрических данных, не задействованных в обычной бытовой практике, то в этом случае гражданин будет надежно застрахован от рисков при взломе информационных баз окружающих его «умных» сервисов.

С 2018 г. в Москве активно развивается проект «Умный город – 2030» [6]. В рамках этой концепции впервые для Российской Федерации внедряются технологии, которые определяют облик города будущего. Среди них предусмотрены и возможности для оказания услуг с помощью

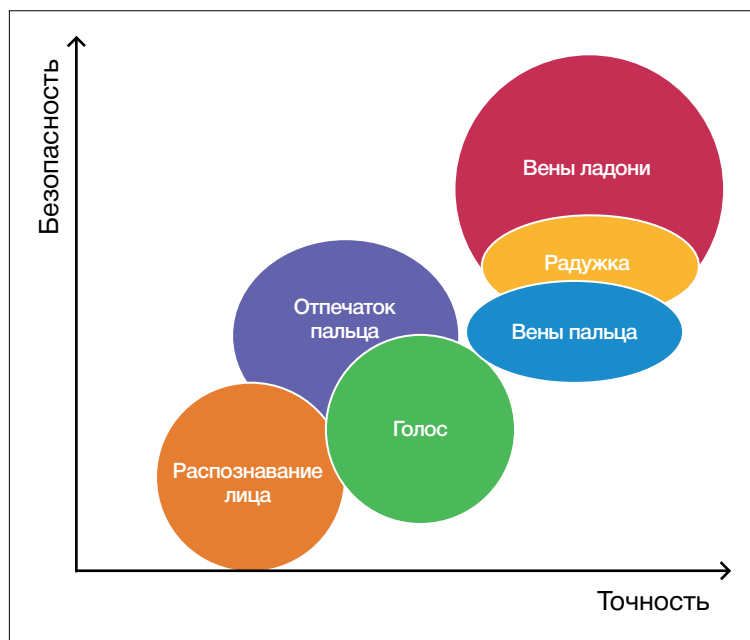


РИС. 1.

Надежность биометрических данных (по Черноусовой Т. Г. [9])

биометрических данных, в том числе посредством использования «умных» сервисов и устройств². Необходимо, прогнозируя растущую популярность названных технологий, на законодательном уровне решить проблему, обусловленную применением биометрической персональной информации. Нужно позаботиться о минимизации последствий при реализации возможных рисков. Важную роль при этом будет играть нормативно-правовое регулирование, разграничивающее и регламентирующее использование биометрических данных в разных условиях.

§ ИНФОРМАЦИОННЫЕ ИСТОЧНИКИ

1. Постановление Правительства РФ от 29.06.2018 № 747 «Об установлении требований к фиксированию действий при размещении в электронной форме в единой системе идентификации и аутентификации сведений, необходимых для регистрации гражданина Российской Федерации в указанной системе, и иных сведений, предусмотренных федеральными законами...». Режим доступа: СПС «КонсультантПлюс».
2. Постановление Правительства РФ от 30.06.2018 № 772 (ред. от 13.09.2019) «Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных». Режим доступа: СПС «КонсультантПлюс».
3. Постановление Правительства РФ от 14.07.2018 № 820 «Об установлении требований к проведению идентификации гражданина Российской Федерации государственными органами и организациями...». Режим доступа: СПС «КонсультантПлюс».
4. Приказ Минкомсвязи России от 21.06.2018 № 307 «Об утверждении методик проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой информационной системе персональных данных...». Режим доступа: СПС «КонсультантПлюс».
5. Маслова М. А. Усовершенствование системы защиты данных в информационных системах методом голосовой биометрии // Новая наука: стратегии и векторы развития. 2016. № 2-1 (64). С. 20–22.

² См. также: Вестник Университета Правительства Москвы. 2019. № 4. С. 2–43, 59–63. – *Прим. ред.*

6. Москва. «Умный город – 2030». URL: https://2030.mos.ru/netcat_files/userfiles/documents_2030/concept.pdf (дата обращения: 20.12.2019).
7. Посыпкина А., Балашова А. Столичный метрополитен начал оборудовать турникеты видеокамерами // РБК. Технологии и медиа. 11.04.2019, 06:00. URL: https://www.rbc.ru/technology_and_media/11/04/2019/5cade2489a7947544a9ac580?from=from_main (дата обращения: 10.01.2020).
8. Турникеты с видеонаблюдением появятся на 26 станциях Московского метрополитена // Официальный сайт Мэра Москвы. 06.11.2019, 11:13. URL: <https://www.mos.ru/news/item/64838073> (дата обращения: 10.01.2020).
9. Черноусова Т. Г. Биометрия и аутентификация // Мир современной науки. 2017. № 3 (43). С. 20–24.
10. Davis D. B. ISTR 2019: Internet of Things Cyber Attacks Grow More Diverse // Symantec.Blogs / Expert Perspectives. 09.04.2019. URL: <https://www.symantec.com/blogs/expert-perspectives/istr-2019-internet-things-cyber-attacks-grow-more-diverse> (дата обращения: 10.01.2020).
11. Stupp C. Fraudsters Used ai to Mimic CEO's Voice in Unusual Cybercrime Case // The Wall Street Journal. 30.08.2019. URL: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402?utm_source=morning_brew (дата обращения: 10.01.2019).
12. Takashi D. McAfee Shows How Deepfakes Can Circumvent Cybersecurity // VentureBeat. 05.03.2019, 10:35. URL: <https://venturebeat.com/2019/03/05/mcafee-shows-how-deep-fakes-can-circumvent-cybersecurity> (дата обращения: 10.01.2020).

REFERENCES

1. Executive Order of the Government of the Russian Federation of 29.06.2018 no.747 "On Establishing Requirements to Documenting Activities of Electronic Data Storing in the Unified Identification and Authentication System, Necessary for Registering a Russian Federation Citizen in That System, as well as Other Data Prescribed by Federal law...". Available at: "ConsultantPlus". (In Russ.).
2. Executive Order of the Government of the Russian Federation of 30.06.2018 no.772 (as amended on 13.09.2019) "On Defining the Scope of Data to be Stored in the Unified Personal Data Information System, Responsible for Processing Biometric Personal Data, Including Its' Accumulation and Storage". Available at: "ConsultantPlus". (In Russ.).
3. Executive Order of the Government of the Russian Federation of 14.07.2018 no. 820 "On Establishing Requirements for Identification of a Russian Federation Citizen by State Bodies and Organizations...". Available at: "ConsultantPlus". (In Russ.).
4. Order of the Ministry of Communications of the Russian Federation of 21.06.2018 no. 317 "On Approval of Discrepancy Tests Methodology Regarding a Private Individual's Personal Biometric Data Versus Private Biometric Data of That Individual Contained in the Unified Personal Data Information System...". Available at: "ConsultantPlus". (In Russ.).
5. Maslova M. A. Upgrading Data Protection Systems in Information Systems Through Methods of Voice Biometrics. *Novaya Nauka: Strategii i Vektory Razvitiya*, 2016, no. 2-1 (64), pp. 20-22. (In Russ.).
6. Moscow. "Smart City – 2030". Available at: https://2030.mos.ru/netcat_files/userfiles/documents_2030/concept.pdf (accessed: 20.12.2019). (In Russ.).
7. Posypkina A., Balashova A. The Capital's Subway Specialists Have Begun to Equip the Pay-gates with Video Cameras. *RBC. Technologies and Media*, 11.04.2019, 06:00. Available at: https://www.rbc.ru/technology_and_media/11/04/2019/5cade2489a7947544a9ac580?from=from_main (accessed: 05.03.2020). (In Russ.).
8. Pay-gates Complete with Video Cameras will Appear in 26 Stations of Moscow Subway. *Moscow Mayor's Official website*. 06.11.2019. Available at: <https://www.mos.ru/news/item/64838073> (accessed: 10.01.2020). (In Russ.).
9. Chernousova T. G. Biometrics and Authentication. *Mir Sovremennoj Nauki*, 2017, no. 3 (43), pp. 20-24. (In Russ.).
10. Davis D. B. ISTR 2019: Internet of Things Cyber Attacks Grow More Diverse. *Symantec.Blogs / Expert Perspectives*, 09.04.2019. Available at: <https://www.symantec.com/blogs/expert-perspectives/istr-2019-internet-things-cyber-attacks-grow-more-diverse> (accessed: 10.01.2020).
11. Stupp C. Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. *The Wall Street Journal*, 30.08.2019. Available at: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402?utm_source=morning_brew (accessed: 10.01.2019).
12. Takashi D. McAfee Shows How Deepfakes Can Circumvent Cybersecurity. *VentureBeat*, 05.03.2019, 10:35. Available at: <https://venturebeat.com/2019/03/05/mcafee-shows-how-deep-fakes-can-circumvent-cybersecurity> (accessed: 10.01.2020).