УДК 543.054
DOI 10.33764/2618-981X-2024-8-2-167-175

Е. А. Овчинникова[1*]

К вопросу о методах защиты персональных данных

[1]Сибирский государственный университет телекоммуникаций и информатики,
г. Новосибирск, Российская Федерация
*e-mail: 9538685137@mail.ru

Аннотация. Рассматриваются отдельные методы, соответствующие областям использования биометрических персональных данных (ПДн). Возможность доступа злоумышленников к информации, обрабатываемой в финансовых организациях, в составе которой, на сегодняшний день, могут находиться, в том числе, и биометрические ПДн, свидетельствует о существенности вероятных потерь, в частности, для субъектов персональных данных. Также увеличивается объем утечек хешированных паролей, позволяющих восстановить исходные пароли. Применение технологий получения доступа с использованием биометрических данных позволяет обеспечить высокий уровень защиты особо важной для гражданина информации.

Ключевые слова: персональные данные, информационная система персональных данных, государственная информационная система

E. A. Ovchinnikova[1*]

On the Issue of Methods for Protecting Personal Data

[1] Siberian State University of Telecommunications and Informatics, Novosibirsk,
Russian Federation
*e-mail: 9538685137@mail.ru

Abstract. Individual methods corresponding to the areas of use of biometric personal data are considered. The ability of attackers to access information processed in financial organizations, which today may include biometric personal data, indicates the significance of the likely losses, in particular for subjects of personal data. There is also an increase in the number of leaks of hashed passwords that allow recovery of the original passwords. The application of access technologies using biometric data allows us to ensure a high level of protection of information that is especially important for a citizen.

Keywords: personal data, personal data information system, state information system

Введение

Биометрические данные, как и любые другие значимые сведения, не застрахованы от хищений. В силу особой значимости, интерес преступного мира к биометрии только увеличивается. В 2023 году произошел резкий рост утечек персональных данных, что на 60% выше уровня 2022 года. Объем утечек в 2023 году составил 1,12 млрд записей. Кроме того, повышение мер ответственности приводит к замалчиванию организациями незначительных объемов утечек данных, что указывает на более высокий реальный масштаб. Конечно, в общий доступ чаще всего попадают иные персональные данные, которые не дают прямой воз-

можности определить субъекта, в частности: телефоны, адреса электронной почты. Вместе с тем, на четвертом месте по уровню утечек находится довольно защищенная финансовая сфера (160,9 млн), что свидетельствует о высоком уровне современных нарушителей. Таким образом, практика свидетельствует о значительном росте возможностей нарушителей, соответственно, для обеспечения защищенности информации возможности по защите информации должны, как минимум, на шаг опережать арсенал нарушителей [1].

Распространенными становятся случаи финансового мошенничества с использованием верификации по голосу. Телефонные мошенники звонят клиенту банка с простой просьбой: дать однозначный утвердительный или отрицательный ответ на предложенный вопрос, после чего происходит списание денежных средств клиента.

Опасность применения биометрии заключается в статичности таких данных. Скомпрометированные пароли или электронные пропуска могут быть заблокированы и оперативно заменены, в отличие от биометрии, которая является неизменной неотъемлемой частью человека. Таким образом, статус защищаемой информации, а также активное применение биометрических методов идентификации усиливает интерес мошенников к данной области и расширяет их возможности.

Система защиты биометрических персональных данных (далее – СЗИБПДн) может быть сформирована по принципу, применяемому ко всей группе сведений, который заложен в требованиях к защите персональных данных при их обработке в информационных системах персональных данных [2]. Таким образом, СЗИБПДн объединяет в себе элементы обработки данных (ИС), элементы транспортировки данных (инфо-телекоммуникационные сети) и элементы защиты данных (систему защиты). Развернутую структуру СЗИБПДн представим на рис. 1.

Рис. 1. Структура СЗИБПДн

Далее рассмотрим подробнее некоторые элементы в аспекте применяемых методов защиты биометрических данных.

Состав биометрических данных разнообразен, к ним относятся:

– геометрия лица – изображение лица человека, полученное с помощью фото-, видеоустройств;

– папиллярный рисунок на пальцах (отпечаток пальца);

– образец голоса человека, полученный с помощью звукозаписывающих устройств;

– образец почерка;

– радужная оболочка глаза;

– геометрия руки;

– сетчатка глаза;

– анализ ДНК;

– фотография на пропуске согласно Определению Верховного Суда РФ от 05.03.2018 № 307-КГ18-101 по делу № А42-342/2017 [5];

– сердечный ритм и другие.

С точки зрения защищенности обеспечиваемых юридически значимых действий аутентификация с помощью биометрических систем является современным и эффективным способом. Но, как это зачастую случается, в особенности со сложными механизмами, она не лишена уязвимостей. К ним относится публичность и статичность биометрии. Публичностью в той или иной степени обладают все биометрические персональные данные, но в большей степени – голос и геометрия лица, что повсеместно используется сегодня мошенниками. Уязвимость технологий использования отпечатка пальца, в том числе, связана с его статичностью. Следовательно, методы, обеспечивающие безопасность применения биометрических данных, должны учитывать их особенности.

Относительно права, области применения биометрии должны быть сегментированы, унифицированы и обеспечены последовательным, прозрачным комплексом правового инструментария.

Также при формировании методов защиты должны учитываться все стадии процессов применения биометрических технологий:

– регистрация биометрии;

– хранение биометрии;

– установление личности посредством биометрии.

Рассмотрим области обработки и использования биометрических персональных данных субъекта:

– информационные системы, обрабатывающие биометрические персональные данные субъекта (далее – ИСПДн);

– государственные (муниципальные) информационные системы (далее – ГИС (МИС));

– хранение данных на машинных носителях;

– обработка биометрических персональных данных с использованием электронной подписи;

– обработка биометрических персональных данных при осуществлении идентификации субъекта через Единую биометрическую систему (далее – ЕБС).

Риски, актуальные при обработке данных в ЕБС, в том числе сборе и пересылке, зафиксированы в Приказе Минцифры России от 12.05.2023 №453 [8], к ним, в частности относятся:

– нарушение целостности;
– подмена данных;
– нарушение конфиденциальности;
– удаление данных.

В соответствии с ПП РФ от 01.11.2012 № 1119 [2] обработка биометрических персональных данных (далее – ПДн) осуществляется в информационных системах персональных данных, защита которых обеспечивается посредством определения актуальных угроз безопасности информации. Для систем биометрических персональных данных 1–3-го уровней защищенности, для которых актуальны 3 типа угроз безопасности информации (1–3), методы криптографии применяются в целях защиты машинных носителей информации. Следует отметить, что основной документ, регламентирующий защиту ИСПДн, – Приказ ФСТЭК от 18.02.2013 № 21 [2] – не закрепляет использование методов криптографической защиты, их выбор осуществляется согласно выписке из перечня средств защиты информации, сертифицированных ФСБ России на основании Приказа ФСБ России от 10.07.2014 № 378 [4].

В рамках электронного документооборота повсеместно применяются технологии электронной подписи. Для получения квалифицированной электронной подписи необходимо сгенерировать закрытый ключ проверки электронной подписи, подтвердив свою личность по биометрии. Квалифицированная электронная подпись используется при документировании социально-значимых действий, например, оформление ипотеки или кредита, ведение финансовой документации, получение налогового вычета и другое. Защита электронной подписи осуществляется посредством применения криптографических методов.

Квалифицированная электронная подпись также используется в государственных информационных системах (далее – ГИС) в соответствии с правилами, установленными оператором по результатам проверки содержащегося в квалифицированном сертификате идентификатора на основе модели угроз для ГИС. Следует отметить, что Приказ ФСТЭК России от 11.02.2013 № 17, равно как и ранее упомянутый Приказ № 21, не регламентирует применение криптографических методов защиты. Их необходимость устанавливается, исходя из актуальных угроз безопасности информации, руководствуясь соответствующими нормативными актами ФСБ России.

Далее рассмотрим методы защиты биометрических персональных данных (изображение лица, запись голоса человека), применяемые в Единой биометрической системе, в соответствии с ФЗ РФ от 29.12.2022 № 572. ЕБС является государственной информационной системой, которая обладает исключительной возможностью хранить «сырую биометрию»: изображение лица, запись голоса.

Следовательно, все организации, обладающие названными выше данными, еще в 2023 году должны были передать их в ЕБС или получить аккредитацию в Минцифры, соответственно, и право их обрабатывать.

ЕБС, оператором которой является Ростелеком, осуществляет обработку около 70 млн данных. Сфера возможностей, предоставляемых ЕБС, достаточно обширна, что отражено на рис. 2.

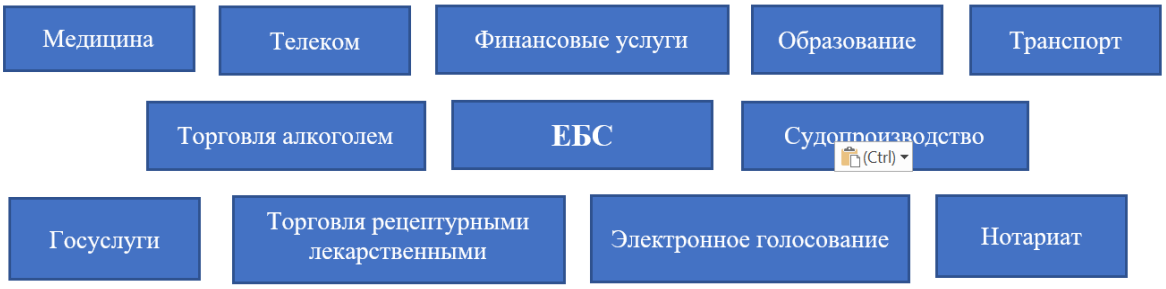

Рис. 2. Услуги, предоставляемые посредством ЕБС

Подходы к управлению ЕБС вызывают активные дискуссии, в особенности, ее жесткая регламентация и единоначалие. У каждого – свое мнение, что для одних является положительным аспектом, для других, скептически настроенных участников отношений, – негативным. Мнение скептиков, что «зарегулированность» системы не позволит ей стать массовой в своем сегменте, уже опровергнуто временем. В 2023 году число напрямую зарегистрировавшихся в ЕБС лиц выросло почти в шесть раз, количество собранных слепков превысило 1,5 млн [9].

Федеральный закон предусматривает применение ряда существенных методов правовой защиты, минимизирующих организационные (человеческий фактор) риски. Рассмотрим основные правовые аспекты функционирования ЕБС.

Аккредитация организаций. Организации, осуществляющие аутентификацию субъекта на основе его биометрических данных с использованием векторов Единой биометрической системы, должны пройти аккредитацию в соответствующем установленном порядке.

Ограничение субъектного состава. Состав организаций, осуществляющих аутентификацию на основании данных ЕБС, ограничен. По общему правилу к ним относятся: государственные и муниципальные органы, а также организации финансового сектора.

Использование шифровальных средств. Криптографические методы защиты, в частности, используются при взаимодействии Единой биометрической системы с информационными системами персональных данных по защищенным криптографическими средствами шифрования каналам связи, либо другими информационными системами соответствующих субъектов – аккредитованных операторов. Мобильное приложение, используемое для обработки биометрических ПДн, функционирует с применением шифровальных средств.

Средства обработки информации в ЕБС находятся в распоряжении РФ и передаются только соответствующему оператору для использования в установленных целях. Данные средства не могут отчуждаться третьим лицам.

Использование сертифицированного оборудования. Для транспортировки биометрических данных в ЕБС должно использоваться сертифицированное оборудование, что подтверждает определенный, требуемый уровень защищенности.

Письменное согласие субъекта персональных данных. Согласие физического лица необходимо для размещения и обработки его биометрических персональных данных в ЕБС, а также для осуществления аутентификации с использованием векторов ЕБС. Согласие не требуется в связи с использованием биометрии в целях осуществления социально-значимых действий, например:

– осуществление правосудия или исполнение судебных актов;

– проведение обязательной государственной дактилоскопической регистрации;

– в случаях, предусмотренных законодательством об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности.

Несомненным плюсом ЕБС является то, что каждый субъект может контролировать свой биометрический профиль, управляя онлайн своими согласиями на обработку персональных данных. Онлайн согласие фиксируется электронной подписью в соответствии с требованиями ФЗ РФ.

В аспекте правового регулирования использования биометрических технологий, следует отметить актуальные для них простейшие требования, основанные на сущности понятия «персональные данные». Так, персональными данными в сфере действия ФЗ РФ от 27.07.2006 № 152 [6] является любая информация о человеке, которая используется оператором в установленных целях. Причем достижение целей возможно только при непосредственном сопоставлении субъекта и его данных, например, оказание услуги конкретному определенному лицу. В связи с этим, изображения, полученные с камер наружного наблюдения, не признаются биометрическими персональными данными, поскольку определение личности субъекта ПДн не является целью видеофиксации. Данное утверждение сделано по сути ФЗ РФ № 152, а также прямо следует из Разъяснения Роскомнадзора от 30.09.2013 [7]. Именно поэтому судебная практика расценивает фотографию на пропуске, как биометрические персональные данные. А вот получение согласия субъекта для осуществления его фото- и видеофиксации городскими камерами те же суды не считают необходимым, поскольку отсутствует изначально прямая цель идентифицировать конкретное, заранее определенное, лицо. Таким образом, необходимость получения согласия на обработку ПДн, в том числе и биометрических, обуславливается как содержанием непосредственно сведений, так и целями их получения и обработки.

Ответственность за инциденты информационной безопасности в ЕБС. Важным правовым вопросом остается распределение ответственности в случае неадекватного распознания личности (ошибки системы), в особенности, если результатом такой ошибки становится финансовый ущерб, например, выдача кредита лицу, не являющемуся обладателем биометрических данных.

Далее рассмотрим ряд технических аспектов функционирования ЕБС.

Раздельное хранение баз биометрических данных. Разграничение баз данных предусмотрено требованиями к защите ИСПДн [2]. Для надежности хранения именно биометрических данных для их размещения должен использоваться отдельный сервер.

Порядок импортирования данных в ЕБС. Существует два способа передачи данных в ЕБС:

1) самим субъектом ПДн с помощью приложения ЕБС, что подтверждается сканированной копией загранпаспорта с биометрией;

2) биометрические данные передаются организациями-операторами.

Осуществление идентификации личности посредством двух факторов доступа:

1) биометрия;

2) логин и пароль от Госуслуг.

Такой метод обеспечивает максимальную надежность осуществления процессов идентификации и аутентификации лица посредством ЕБС.

Двухфакторная аутентификация усложняет возможность доступа к данным, поскольку злоумышленнику в таком случае необходимо пройти два уровня защиты: взломать пароль и пройти биометрическую аутентификацию. Такой метод, конечно, не дает абсолютной гарантии защиты, но значительно сокращает круг нарушителей до лиц, обладающих высокими техническими возможностями.

Обезличенное хранение в ЕБС биометрических данных. ЕБС хранит только математические модели биометрии – векторы единой биометрической системы (данные, полученные в результате математического преобразования). Восстановить по ним фото или голос человека невозможно.

Статичность биометрических данных является серьезной, но не непреодолимой проблемой, которая решается посредством «отменяемой биометрии», то есть изменения не самих данных, а алгоритма их хранения и использования.

Мультивендорный подход основан на одновременном использовании нескольких постоянно изменяющихся алгоритмов.

Параллельная идентификация через ЕБС и ЕСИА. Значительно повышает защищенность действий субъектов одновременное применение биометрической идентификации посредством ЕБС и идентификации на сайте Госуслуг. Также Ростелеком обеспечивает защиту канала связи между телефоном клиента и базой биометрических данных.

Заключение

Таким образом, функционирование СЗИБПДн основывается на комплексном использовании правовых, организационных и технических методов защиты данных. Правовая защита биометрических данных предполагает унификацию действующего законодательства в области защиты биометрических персональных данных, обрабатываемых в различных системах, установление ограничений на формирование банков биометрических данных, жесткую регламентацию и

контроль государства, гармонизацию правоустановительной и правореализационной практики. Техническая защита биометрических данных в своей основе стремится к применению отечественных средств и технологий, а также к установлению и контролю соответствия применяемых средств обработки, передачи и защиты. Наиболее надежным способом защиты информации представляется параллельное применение двух методов: идентификации по биометрическим персональным данным и использование квалифицированной электронной подписи при совершении юридически значимых действий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Утечки данных в России. 2024. [Электронный ресурс] URL: https://www.tadviser.ru/index.php/Статья:Утечки_данных.

2. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных утв. Постановлением Правительства РФ 1 нояб. 2012 г. № 1119. [Электронный ресурс] URL: http://www.consultant.ru/document/cons_doc_LAW_137356/.

3. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ ФСТЭК России от 18 февр. 2013 г. № 21. [Электронный ресурс] URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18- fevralya-2013-g-n-21.

4. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности: Приказ ФСБ России от 10 июля 2014 г. № 378. [Электронный ресурс] URL: https://base.garant.ru/70727118/.

5. Определение Верховного Суда РФ от 05.03.2018 № 307-КГ18-101 по делу № А42-342/2017. [Электронный ресурс] URL: https://www.v2b.ru/documents/opredelenie-verhovnogo-suda-rf-ot-05-03-2018-307-kg18-101/.

6. О персональных данных [Федер. закон: принят Гос. Думой 8 июля 2006 г.: по состоянию на 25 ноября 2009 г.]. – М.: Собрание законодательства Российской Федерации, 2006. – № 31. – Ч. 1. – Ст. 3451.

7. Разъяснения по вопросам отнесения фото-, видеоизображений, дактилоскопических данных и иной информации к биометрическим персональным данным и особенностей их обработки. [Электронный ресурс] URL: https://www.garant.ru/products/ipo/prime/doc/70342932/.

8. О порядке обработки биометрических персональных данных и векторов единой биометрической системы в единой биометрической системе и в информационных системах аккредитованных государственных органов, Центрального банка Российской Федерации в случае прохождения им аккредитации, организаций, осуществляющих аутентификацию на основе биометрических персональных данных физических лиц. [Электронный ресурс] URL: https://docs.cntd.ru/document/1301709238.

9. Лицевой счет: почему растут регистрации в Единой биометрической системе. 2024. [Электронный ресурс] URL: https://www.forbes.ru/tekhnologii/511272-licevoj-scet-pocemu-rastut-registracii-v-edinoj-biometriceskoj-sisteme.

10. Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные за-

конодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации: Федеральный закон РФ от 29 декаб. 2022 г. № 572-ФЗ. URL: https://internet.garant.ru/#/document/406051675/paragraph/1/doclist/1550/1/0/0/%D1%84%D0%B7%20572:22.