ИНФОРМАТИКА

УДК 57.087.1+612-087 DOI 10.25730/VSU.0536.20.038

Биометрия в России

В. Н. Белов[1], М. О. Акимкин[2]

[1]кандидат педагогических наук, доцент, Арзамасский филиал Нижегородского государственного университета. Россия, г. Арзамас. E-mail: bwn.arz@list.ru

[2]магистрант 2 курса, Арзамасский филиал Нижегородского государственного университета. Россия, г. Арзамас

Аннотация. Людям давно известны неповторимости человеческого тела. В XX веке с ростом технического прогресса было сделано множество открытий, таких как уникальность генов, параметров глаза и других биометрических данных. В тот же период эти данные стали широко использоваться в сфере безопасности. С развитием компьютерных технологий распознавание личности автоматизируется и совершенствуется. Эффективная защита персональных данных – важнейшая задача современности. На данный момент специалисты считают, что биометрия по совокупности параметров подходит лишь как один из факторов комплексной защиты. В данной статье рассматриваются современное развитие биометрических технологий в России, актуальные вопросы биометрии, законодательная база, сферы и особенности применения. Приведены основные нормативные документы, направления использования биометрических технологий, а также критерии регламентирования биометрических систем.

Ключевые слова: Биометрия, биометрическая система, аутентификация, идентификация, FAR (FalseAcceptenceRate), FRR (FalseRejectionRate), единая биометрическая система.

Уже давно мы видим в фильмах, как где-нибудь «на секретной базе секретные агенты секретной организации» идут по коридору к двери, подносят глаз к оптическому датчику или прикладывают ладонь к специальному сканеру, идентифицируются системой и получают доступ в самую секретную часть базы. Всё чаще методы распознавания личности с помощью характеристик тела (иначе говоря – биометрии) стали появляться и в реальной жизни.

Биометрия – способ распознавания людей по одной или более физическим или поведенческим чертам. Физические (физиологические) черты – это те черты, которые относятся к форме тела. К поведенческим чертам относят походку, особенности речи. Осуществляется разделение черт на статические (сетчатка глаза) и динамические (голос).

Биометрические системы – системы, использующие для определения личности людей их биометрические данные. Существует два варианта работы биометрической системы: аутентификация и идентификация. Аутентификация – сравнение один к одному с биометрическим шаблоном, может также осуществляться по ID- и смарт-карте. Идентификация – сравнение один ко многим: сравнение для определения личности [1; 2; 6; 7].

Для успешного использования к системам предъявляются требования:

1) универсальность – каждый субъект должен обладать данной характеристикой;
2) уникальность – индивидуальность каждого субъекта с биометрической точки зрения;
3) постоянство – мера изменчивости биометрических черт (процесс старения);
4) измеримость – возможность провести измерения параметра каким-либо способом для занесения в базу данных;
5) достоверность – низкая вероятность ошибки в распознавании;
6) возможность замены параметра;
7) приемлемость для общества.

Схемы работы биометрических систем практически одинаковы.

Этап 1. Введение биометрической информации в систему:

- получение одного или нескольких образцов (запись);
- извлечение необходимых данных из образца с последующим преобразованием в код по определенным алгоритмам – создание шаблона (выделение). При этом нерелевантные для распо-

знавания характеристики не сохраняются, что делает невозможным восстановление исходных данных из шаблона, защищая личность регистрируемого;

- привязка образцов к профилю субъекта.

Этап 2. Идентификация или аутентификация:

- получение образца;
- создание шаблона – аналогично процедуре из этапа введения данных в систему;
- сравнение шаблона полученного образца с шаблонами в базе данных;
- результат – совпадение или несовпадение [1; 6; 7].

В отличие от прочих методов аутентификации биометрический метод – вероятностный, так как существует шанс, что биометрические характеристики двух людей могут совпасть. Поэтому введены следующие понятия:

FAR (FalseAcceptenceRate) – процентный порог, определяющий вероятность того, что один человек может быть принят за другого (коэффициент ложного доступа, также именуется «ошибкой 2 рода»). Величина 1-FAR называется специфичность.

FRR (FalseRejectionRate) – вероятность того, что человек может быть не распознан системой (коэффициент ложного отказа в доступе, также именуется «ошибкой 1 рода»). Величина 1-FRR называется чувствительность [1; 2; 6; 7].

Необходимо учитывать вероятность возникновения ошибок FAR/FRR: искусственным снижением уровня «требовательности» системы (FAR), как правило, уменьшают процент ошибок FRR и наоборот.

Критичным минимальным порогом для FAR специалисты называют шанс допуска постороннего в 10^{-5}, что соответствует десятеричному 4-разрядному коду. Для FRR всё зависит от пропускной способности системы. В масштабах небольшого предприятия минимальным порогом может быть 10^{-2}, то есть 1 отказ в доступе из 100 легитимных попыток, для более нагруженных систем этот параметр более критичен. В целом отказ в доступе менее опасен, чем ошибочный доступ стороннего субъекта.

Для повышения точности и надежности распознавания и уровня безопасности системы применяют комбинированные биометрические системы, использующие несколько биометрических характеристик. Например, систему распознавания папиллярных линий на пальцах рук можно сочетать со сканированием руки. Подделать целый ряд биометрических характеристик – сложная задача. Также для повышения комбинируются варианты аутентификации с помощью биометрии и сторонних устройств.

На данный момент специалисты считают, что биометрия по совокупности параметров подходит лишь как один из факторов комплексной защиты [5].

К плюсам биометрических систем можно отнести удобство для пользователей. В отличие от паролей, ключей и иных средств подтверждения личности, которые могут быть украдены, утеряны и скопированы, биометрические характеристики всегда находятся при субъекте. Также невозможна их передача третьим лицам. Кроме того, в век цифровых технологий многие сервисы используют парольный доступ. Часто пользователи забывают сложные комбинации символов, поэтому для облегчения работы используют одинаковые пароли. Поэтому шанс получения несанкционированного доступа возрастает даже при утечке одного пароля [2].

К минусам можно отнести утрату биометрических характеристик в результате травмы, а также целенаправленного нападения с целью принудительной аутентификации. Некоторые биометрические характеристики, например, голос, заменить нельзя, в отличие от отпечатков пальцев в пределах десяти раз, что делает их компрометацию еще большей проблемой.

А как же регламентируется использование биометрии в России? Нормативно правовая база в России в этом вопросе еще молода, поэтому начать обзор стоит с Федерального закона от 27.07.2006 № 152-ФЗ в редакции от 31.12.2017 «О персональных данных» (далее ФЗ № 152). Он регулирует отношения, связанные с обработкой персональных данных, в том числе с использованием средств автоматизации или без таковых, если такая обработка позволяет осуществлять поиск по заданному алгоритму [4].

ФЗ № 152 определяет персональные данные как любую информацию, относящуюся к прямо или косвенно определенному или определяемому физическому лицу. Определяются такие понятия, как оператор и информационная система персональных данных. Также даются определения основным операциям с персональными данными – обработка, автоматизированная обработка, предоставление, распространение, блокирование, уничтожение, обезличивание, трансграничная передача.

Вместе с тем определены права субъектов персональных данных, обязанности оператора, органы государственного контроля и надзора за обработкой персональных данных, ответственность за нарушение настоящего федерального закона.

Одним из ключевых законов, регулирующих обработку персональных данных, является Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.06.2018) «Об информации, информационных технологиях и о защите информации» (далее ФЗ № 149) [4].

Настоящий федеральный закон регулирует отношения, возникающие при:

– осуществлении права на поиск, передачу, производство и распространение информации;

– применении информационных технологий;

– обеспечении защиты информации.

Статья 14.1 настоящего закона определяет применение информационных технологий в целях идентификации граждан Российской Федерации. Данная статья регламентирует порядок получения биометрической информации, ее размещения в единой биометрической системе персональных данных и идентификации клиента с ее помощью. Определяются оператор ЕБС, а также регулирующие, надзорные и контролирующие органы.

Статья 17, пункт 1 гласит, что «лица, виновные в нарушении требований статьи 14.1 настоящего ФЗ в части обработки, включая сбор и хранение, биометрических персональных данных, несут административную, гражданскую и уголовную ответственность в соответствии с законодательством РФ».

Важную роль в биометрической идентификации играет Федеральный Закон от 07.08.2001 N 115-ФЗ (ред. от 23.04.2018) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Настоящий закон регламентирует отношения различных категорий субъектов, участвующих в операциях с денежными средствами, в целях предупреждения, выявления и пресечения деяний, связанных с легализацией (отмыванием) доходов, полученных преступным путем, финансированием терроризма и финансированием распространения оружия массового уничтожения.

Статья 7 определяет права и обязанности организаций, осуществляющих операции с денежными средствами или иным имуществом.

Пункт 5.6 регламентирует порядок биометрической регистрации клиентов банков с занесением биометрических данных в информационные системы персональных данных, в том числе в ЕСИиА и в ЕБС.

Пункт 5.8 определяет условия применения биометрической идентификации в отношении клиентов банка.

Пункт 5.9. устанавливает порядок взаимодействия между банками и оператором единой биометрической системы в области оплаты банками услуг по предоставлению биометрических данных, хранящихся в ЕБС.

Также стоит отметить следующие документы, регламентирующие различные аспекты применения биометрических технологий:

– Организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных регламентируются приказами Федеральной службы по техническому и экспортному контролю (далее ФСТЭК) России от 18.02.2013 N 21 (ред. от 23.03.2017) и Федеральной службы безопасности (далее ФСБ) России от 10.07.2014 N 378;

– Постановление Правительства Российской Федерации № 152 от 06.07.2008 (в ред. Постановления Правительства РФ от 27.12.2012 N 1404) «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

– ГОСТ Р ИСО/МЭК 19784 «Информационные технологии. Биометрия. Биометрический программный интерфейс»;

– ГОСТ Р ИСО/МЭК 19785 «Автоматическая идентификация. Идентификация биометрическая. Единая структура форматов обмена биометрическими данными»;

– ГОСТ Р ИСО/МЭК 19794 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными». Различные части ГОСТа – о разных способах идентификации (отпечаток, радужная оболочка глаза и т. д.);

– ГОСТ Р ИСО/МЭК 19795 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии»;

– ГОСТ Р ИСО/МЭК 24708–2013 «Информационные технологии. Биометрия. Протокол межсетевого обмена БиоАПИ»

– ГОСТ Р ИСО/МЭК 24709 «Автоматическая идентификация. Идентификация биометрическая. Испытания на соответствие биометрическому программному интерфейсу (БиоАПИ)» (части);

– ГОСТ Р ИСО/МЭК 24713 «Информационные технологии. Биометрия. Биометрические профили для взаимодействия и обмена данными»;

– ГОСТ Р ИСО/МЭК 29109 «Информационные технологии. Биометрия. Методология испытаний на соответствие форматам обмена биометрическими данными, определенным в комплексе стандартов ИСО/МЭК 19794»;

– ГОСТ Р ИСО/МЭК 29141 «Информационные технологии. Биометрия. Одновременное получение изображений отпечатков десяти пальцев с помощью БиоАПИ»;

– ГОСТ Р ИСО/МЭК 29794 «Информационные технологии. Биометрия. Информационные технологии. Биометрия. Качество биометрических образцов»;

– ГОСТ Р 54411–2011/ISO/IEC TR 24722:2007 «Информационные технологии. Биометрия. Мультимодальные и другие мультибиометрические технологии»;

– ГОСТ Р 54412–2011/ISO/IEC TR 24741:2007 «Информационные технологии. Биометрия. Обучающая программа по биометрии» [3; 4; 6; 7].

Данный список можно продолжить и другими документами, но они мало значимы в контексте биометрии.

Применение биометрии в России представлено в различных сферах жизни. Если в финансовой сфере биометрия только развивается, хоть и большими темпами, то в сфере медицины и правоохранительной системе биометрия имеет богатую историю.

Биометрия в сфере охраны правопорядка используется давно. Снятие отпечатков пальцев, фотографирование, измерение роста и иные способы измерения и сохранения характеристик применяются для последующей идентификации граждан, вызывающих интерес у правоохранительных органов. В отличие от гражданского сегмента, где биометрические параметры хранятся в виде шаблонов, не позволяющих восстановить информацию о личности, в сфере обеспечения безопасности правопорядка биометрические данные хранятся целиком и служат именно для этой цели.

Важным новшеством в обеспечении общественной безопасности стало создание биометрических паспортов. В биометрический паспорт встроена специальная микросхема, содержащая личные данные владельца. Стандарты предусматривают возможность хранения в микросхеме специальной биометрической информации. Отличием биометрического паспорта от обычного является наличие информации, недоступной его владельцу, и, в теории, возможности ее дистанционного считывания. Главным преимуществом такого паспорта является ускорение процедуры установления личности при наличии специального оборудования. Но и это не обеспечивает 100 % безопасности, установлены случаи успешной подделки биометрических паспортов. Также известна и уязвимость чипов, находящихся в паспортах, к дистанционному отслеживанию владельца паспорта.

Развитие гражданской биометрической идентификации получило широкое распространение в банковской сфере. Была создана единая биометрическая база данных.

Единая биометрическая система – цифровая платформа идентификации по голосу и изображению лица, разработанная компанией «Ростелеком» по инициативе Министерства связи и массовых коммуникаций РФ и Центрального Банка РФ. Благодаря единой биометрической системе граждане России могут дистанционно открывать счета в российских банках. Планируется, что работы не будут ограничены только единой биометрической системой, но со временем внедрят дистанционную аутентификацию и в других сферах.

Идентификация пользователя в единой биометрической системе происходит по двум параметрам – голосу и лицу, одновременное использование которых позволяет определить реально существующего человека. Для регистрации в ЕБС гражданину необходимо всего один раз прийти в банк и сдать биометрические образцы. В последствии для дистанционного получения услуг гражданину необходимо пройти аутентификацию с помощью смартфона, планшета или компьютера, оснащенных веб-камерой и имеющих доступ в интернет. Аутентификация проходит в два этапа: ввод пары логин – пароль от ЕСИиА и биометрическая аутентификация, путем произнесения сгенерированной контрольной фразы глядя в камеру.

Стоит отметить, что российское законодательство не отстает и достаточно оперативно вносит корректировки, в частности, применение удаленной идентификации клиентов в финансовой сфере регламентировано Федеральным законом № 482-ФЗ от 31 декабря 2017 г., который вносит изменения в Федеральный закон от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [4].

В 2016 году правительство поставило задачу разработки технологии идентификации граждан при помощи биометрических данных. При этом эксперты не видели технических сложностей

в реализации такой системы, однако была определена необходимость единой базы биометрических данных для наиболее оптимальной работы системы.

В течение 2017 года шло межведомственное обсуждение реализации проекта. В ходе реализации пилотного проекта биометрической идентификации клиентов банков – физических лиц оператором национальной биометрической платформы был выбран «Ростелеком». Были подготовлены законопроекты, регламентирующие работы банков в России по формированию единой биометрической системы. 20 декабря 2017 г. Госдума РФ приняла в третьем чтении поправки к закону, позволяющие банкам идентифицировать и аутентифицировать пользователей удаленно с помощью биометрических данных и сведений из Единой системы идентификации и аутентификации.

В 2018 году была представлена первая рабочая версия ЕБС производства компании «Ростелеком». По данным экспертов, в ближайшие 2-3 года единая биометрическая система в полном объеме востребована не будет, в связи с невысоким темпом сбора биометрических данных.

Развитие гражданской биометрической идентификации не ограничивается единой биометрической системой. Подобные технологии применяются в контроле доступа работников в отдельные помещения, авторизации пользователей на выполнение определенных операций, отслеживании соблюдения рабочего графика сотрудниками предприятия.

Использование таких систем позволяет не только облегчить жизнь работников, но и повысить безопасность. Исчезают такие явления, как утеря пароля, передача его третьим лицам, запись пароля в незащищенном месте. Кроме того, сквозное использование таких систем на предприятии упрощает расследование инцидентов безопасности. Если с использованием пароля доступ может получить неавторизованный пользователь, то при биометрической аутентификации и авторизации такой шанс гораздо ниже.

Биометрическая идентификация также встречается в сотовых телефонах, планшетах, где реализована разблокировка устройства по распознаванию отпечатка пальца или лица, что позволяет более надежно защитить свои персональные данные от посягательств извне.

Следует отметить, что биометрические технологии в России быстро развиваются. Государство, банки и крупный бизнес заинтересованы в развитии и массовом применении данных технологий. Соответствующие ведомства, такие как ФСБ, Роскомнадзор, Минкомсвязи, Центробанк и другие, а также правительственные структуры РФ разрабатывают законопроекты, регламентирующие все аспекты применения биометрии.

Для использования биометрических технологий в организациях с целью идентификации людей необходимо соблюдение действующих нормативных и методических документов, таких как ФЗ № 149, ФЗ № 152, ФЗ № 115.

Обязательным требованием, согласно статье 22 ФЗ № 152, является уведомление уполномоченного органа по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных, кроме случаев, предусмотренных частью 2 настоящей статьи. На данный момент таким уполномоченным органом является Роскомнадзор.

Отдельным пунктом идет защита персональных данных. В информационном сообщении от 6 июня 2018 г. № 240/13/2549 «О некоторых вопросах по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», в связи с многочисленными обращениями граждан, ФСТЭК информирует, «что в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» и Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» обработка персональных данных не является лицензируемым видом деятельности. В соответствии с пунктом 5 части 1 статьи 12 Федерального закона от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности» лицензированию подлежит деятельность по технической защите конфиденциальной информации. Вместе с тем в соответствии с частью 1 статьи 19 Федерального закона «О персональных данных» от 27 июля 2006 г. № 152-ФЗ оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры для защиты персональных данных» [4].

Помимо лицензирования деятельности, к области обеспечения безопасности относится и сертифицирование средств защиты информации. На данный момент в реестре на сайте ФСТЭК фигурируют 3 средства, использующих биометрические технологии: программно-аппаратный комплекс «АССаД-ID», программный комплекс «Системабиометрия», программный комплекс «Программное обеспечение системы BiolinkIDenium». Все три средства сертифицированы на защиту от недекларированных возможностей, а «АССаД-ID» еще на автоматизированную систему физической защиты.

В личных целях использование биометрической технологии не регламентируется, достаточно соблюдения прав субъектов персональных данных и действующих законов РФ.

Сложность соблюдения всех требований, финансовые затраты, особые требования к надежности и прохладное, недоверчивое отношение широких слоев населения к биометрическому установлению личности все еще могут отпугнуть желающих опробовать новые технологии на базе своей организации. Но с каждым годом технологии совершенствуются, рынок биометрических технологий растет высокими темпами и скоро многие компании и предприятия смогут выбрать решение, подходящее под их задачи.

Однако многие специалисты, как уже говорилось ранее, считают, что популяризация и применение биометрических технологий может привести нас к обществу тотального контроля. Если пессимистично пофантазировать на тему концепции вшитых в тело чипов и прочих перспектив кибернизации организма как логического продолжения биометрического установления личности и авторизации, то, возможно, наступит момент, когда мысль в нашей голове может быть уже и не нашей собственной.

Список литературы

1. *Абалмазов Э. И*. Энциклопедия безопасности. Справочник-каталог, 1997.

2. *Белов В. Н., Ковалёв А. И.* Некоторые аспекты использования электронных ключей в подходах защиты информации // Математический вестник педвузов и университетов Волго-Вятского региона : периодический межвузовский сборник научно-методических работ. Киров, 2015. С. 318–324.

3. Все ГОСТы. URL: http://vsegost.com.

4. Информационно правовой портал. URL: http://www.garant.ru.

5. *Татарченко Н. В., Тимошенко С. В.* Биометрическая идентификация в интегрированных системах безопасности // Специальная техника. 2002.

6. *Тихонов В. А., Райх В. В.* Информационная безопасность: концептуальные, правовые, организационные и технические аспекты : учеб. пособие. М. : Гелиос АРВ, 2006.

7. Электронный фонд правовой и нормативно-технической документации. URL: http://docs.cntd.ru/ document/550594669 (дата обращения: 20.02.2020).

Biometrics in Russia

V. N. Belov[1], M. O. Akimkin[2]

[1]PhD in Pedagogical Sciences, associate professor, Arzamas Branch of Nizhny Novgorod State University. Russia, Arzamas. E-mail: bwn.arz@list.ru

[2]master student of the 2nd year, Arzamas Branch of the Nizhny Novgorod State University. Russia, Arzamas

Abstract. People have long known the uniqueness of the human body. In the twentieth century, with the growth of technological progress, many discoveries were made, such as the uniqueness of genes, eye parameters, and other biometric data. During the same period, this data became widely used in the field of security. With the development of computer technologies, personality recognition is being automated and improved. Effective protection of personal data is the most important task of our time. At the moment, experts believe that biometrics in terms of a set of parameters is suitable only as one of the factors of comprehensive protection. This article discusses the current development of biometric technologies in Russia, current issues of biometrics, the legislative framework, the scope and features of application. The main regulatory documents, directions for the use of biometric technologies, as well as the criteria for regulating biometric systems are presented.

Keywords: Biometrics, biometric system, authentication, identification, FAR (FalseAcceptenceRate), FRR (FalseRejectionRate), Unified biometric system.

References

1. *Abalmazov E. I. Enciklopediya bezopasnosti* [Encyclopedia of security]. Spravochnik-catalog. 1997.

2. *Belov V. N., Kovalyov A. I. Nekotorye aspekty ispol'zovaniya elektronnyh klyuchej v podhodah zashchity informacii* [Some aspects of the use of electronic keys in information security approaches] // *Matematicheskij vestnik pedvuzov i universitetov Volgo-Vyatskogo regiona : periodicheskij mezhvuzovskij sbornik nauchno-metodicheskih rabot* – Mathematical herald of pedagogical universities and universities of the Volga-Vyatka region : periodic interuniversity collection of scientific and methodological works. Kirov. 2015. Pp. 318–324.

3. All state standards. Available at: http://vsegost.com.

4. Information and legal portal. Available at: http://www.garant.ru.

5. *Tatarchenko N. V., Timoshenko S. V. Biometricheskaya identifikaciya v integrirovannyh sistemah bezopasnosti* [Biometric identification in integrated security systems] // *Special'naya tekhnika* – Special technics. 2002.

6. *Tihonov V. A., Rajh V. V. Informacionnaya bezopasnost': konceptual'nye, pravovye, organizacionnye i tekhnicheskie aspekty : ucheb. posobie* [Information security: conceptual, legal, organizational and technical aspects : textbook]. M. Helios ARV. 2006.

7. Electronic fund of legal and normative-technical documentation. Available at: http://docs.cntd.ru/ document/550594669 (date accessed 20.02.2020).