ПРОБЛЕМА БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ БИОМЕТРИЧЕСКИХ ДАННЫХ ГРАЖДАН

Таранков Олег Игоревич,
Порошкина Татьяна Сергеевна

Цель: *провести анализ современных угроз при использовании биометрических данных граждан для их авторизации в различных электронных системах, а также разработать механизмы минимизации рисков.*

Методология: *дедукция, формально-юридический метод, сравнительно-правовой метод.*

Выводы: *В 21 веке технологии входят в повседневную жизнь очень быстро, что зачастую ставит под вопрос как корректную работу данных механизмов, так и их безопасность. Сегодня ряд государственных и коммерческих институтов предлагает доступ к своему инструментарию с помощью биометрической идентификации по отпечатку узоров пальцев рук, радужной оболочки глаза или голосу. Система кажется совершенной, ключ, который невозможно забыть, украсть или подделать открывает новые страницы в истории компьютерной безопасности. Но так ли надежна биометрическая аутентификация? Действительно ли данные граждан под надежной защитой? Существуют ли механические, электронные и юридические методы защиты? Авторы уверены, что подобные технологии несовершенны. Мировой опыт показывает, что биометрические данные, это такая же информация, хранящаяся в виде двоичного кода в базах данных, которые так же подвержены хакерским атакам. Одновременно с этим сложный механизм сбора этой информации создает ряд слабых мест, которыми могут воспользоваться злоумышленники. Авторы рассматривают совершенствование законодательной базы, позволяющее допускать до процедуры сбора, хранения и использования биометрических данных граждан лишь специализированные государственные организации как единственную возможность минимизации рисков кражи персональных данных.*

Научная и практическая значимость. *Выделение слабых мест в цепочке сбора, передачи, хранения и использования биометрических данных позволяет разработать механизм минимизации рисков при использовании данной технологии.*

Ключевые слова: *Россия, биометрические данные граждан, биометрическая идентификация, аутентификация, безопасность.*

В последнее время тема биометрической идентификации личности находится в центре внимания российского сообщества, которое старается следовать мировым тенденциям в области защиты информации при помощи биометрических данных граждан как надежного способа идентификации их личности. Прорывом в области биометрической идентификации личности в России стало принятие Федерального закона от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» *(СЗ РФ. 2018. №1. Ст. 66.)*, который установил основы для развития в Российской Федерации Единой биометрической системы. Говоря о востребованности и актуальности данной темы, стоит отметить, что Центробанк уже довольно давно прилагает усилия к тому, чтобы стимулировать банки к применению таких систем удостоверения личности.

Стоит упомянуть, что правовое регулирование биометрических данных граждан на данный момент проработано не в достаточной мере:

Исторически первое законодательное упоминание о биометрии содержалось в Федеральном законе от 15 августа 1996 г. № 114-ФЗ «О порядке выезда из Российской Федерации и въезда

DOI 10.31085/2310-8681-2020-4-208-159-164

в Российскую Федерацию» *(СЗ РФ. 1996. №34. Ст. 4029.)*, где говорилось, что паспорта граждан «могут содержать электронные носители информации с записанными на них персональными данными владельца паспорта, включая биометрические персональные данные». Стоит, впрочем, заметить, что выдача заграничных паспортов с такими носителями фактически началась лишь через 10 лет после появления этого закона [1].

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» *(СЗ РФ. 2006. №31. Ст. 3451.)*. В нем имелась статья 11 «Биометрические персональные данные», которая существует по сей день с некоторыми дополнениями. Изначально законодатели определили предмет статьи как «сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность». В актуальной на данный момент редакции (от 31.12.2017) сведения уже не только физиологические, но и биологические; кроме того, указано, что они не только позволяют установить личность, но и используются для этого. В общем случае обработка биометрических ПД разрешается лишь с письменного разрешения субъекта, хотя есть ряд исключений – в основном связанных с охраной порядка, противостоянием терроризму и оборонными задачами. Также авторы закона упомянули о биометрических данных в статье 19 «Меры по обеспечению безопасности персональных данных при их обработке». Статья с тех пор была значительно расширена (с 4 пунктов до 11), но положения, связанные с биометрией, остались прежними: требования к хранению биометрических ПД устанавливаются Правительством РФ.

Далее в нормотворческий процесс включилась стандартизация: в 2007 году были введены в действие ГОСТ Р ИСО/МЭК 19795-1–2007 *(См.: URL: http://docs.cntd.ru/document/1200067413 (дата обращения: 27.10.2019))* «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 1. Принципы и структура» и ГОСТ Р ИСО/МЭК 19784-1–2007 «Автоматическая идентификация. Идентификация биометрическая. Биометрический программный интерфейс. Часть 1. Спецификация». С тех пор постепенно переводились и утверждались разные части международных стандартов, имеющих отношение к сбору биометрических данных, их использованию и обработке. Одним из ключевых документов здесь можно назвать стандарт ГОСТ Р ИСО/МЭК 19794, который определяет требования ко всем основным биометрическим параметрам и к их измерению. Так, например, части 2-4 и 8 касаются отпечатков пальцев, часть 5 – изображения лица, а часть 14 – данных ДНК. Кстати, эта последняя часть относится к наиболее свежим – она утверждена в 2017 г. По названиям стандартов можно видеть, что все они идентичны международным.

Глобальная рамка информационного законодательства – Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» – изначально указаний на биометрию не содержал. 31 декабря 2017 г. он пополнился статьей 14.1 «Применение информационных технологий в целях идентификации граждан Российской Федерации», которая составляет фундамент для единой биометрической системы (ЕБС) и ее применения, а также увязывает ее с единой системой идентификации и аутентификации (ЕСИА), знакомой любому пользователю ресурсов электронного правительства. Установлено, что организации разного рода (например, банки) идентифицируют пользователя в его присутствии и с его согласия, а затем передают его биометрические ПД в ЕБС. Порядок этого процесса и состав сведений определяются Правительством РФ; оно же назначает государственный орган, ответственный за регулирование этой сферы и за разработку конкретных регламентов – обработки данных, их размещения, требований к техническим средствам и т. п. [2]. В этой же статье вводится понятие оператора ЕБС, функции которого возлагаются на крупного оператора связи (т.е. такого, который «занимает существенное положение» в 2/3 регионов страны). Закон требует применять криптографическую защиту информации при передаче биометрических ПД через интернет; если физическое лицо отказывается пользоваться такой защитой, то идентификацию без шифрования можно будет провести только с персонального компьютера и после уведомления о рисках. С мобильного устройства, в том числе планшетного компьютера, удаленная биометрическая идентификация без криптозащиты будет невозможна. Нарушение требований статьи 14.1 влечет гражданскую, административную или уголовную ответственность.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» *(ред. от 31.12.2017)* в ст. 11 устанавливает понятие биометрических персональных данных и основания, по которым обработка персональных данных может осуществляться с согласия и без согласия носителей биометрических данных: Сведения, которые характеризуют физиологические и биологические особенности

человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи. Обработка биометрических персональных данных может осуществляться без согласия субъекта персональных данных в связи с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации.

В современной правовой действительности, как было отмечено раннее, ведущим законом в сфере обработки и идентификации персональных данных является Федеральный закон от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», так как он устанавливает правовые основания сбора биометрических персональных данных граждан РФ и их размещения в Единой биометрической системе, устанавливает механизмы идентификации физического лица без его лично присутствия с использованием информационных технологий (удаленная биометрическая идентификация).

Согласно вышеуказанному НПА на ФОИВ в зависимости от сферы применения возлагаются обязанности по сбору, хранению, надзору и дальнейшему использованию биометрических персональных данных: так, например:

1. Минкомсвязь России – является уполномоченным ФОИВ в сфере идентификации граждан РФ на основе биометрических персональных данных (постановление Правительства РФ от 28 марта 2018 г. № 335);

2. ПАО «РОСТЕЛЕКОМ» осуществляет функции оператора Единой биометрической системы (распоряжение Правительства РФ от 22 февраля 2018 г. № 293-р);

3. ФОИВ, в том числе МВД России, органы государственных внебюджетных Фондов имеют обязанность по направлению сведений о гражданах РФ в целях их обновления в ЕСИА в соответствии с порядком регистрации гражданина РФ в ЕСИА;

4. Центральный Банк РФ надзор за соблюдением банками порядка размещения и обновления сведений в ЕСИА, а также сведений, размещаемых в единой биометрической системе функции нормотворчества и правоприменительные [3].

В результате с начала июля 2018 г. в некоторых банках начала работать единая биометрическая система, созданная «Ростелекомом» по инициативе Министерства цифрового развития, связи и массовых коммуникаций и Центрального банка РФ. Единая биометрическая система была создана, чтобы сделать более доступными услуги, которые требуют юридически значимого подтверждения личности – в первую очередь для жителей отдаленных регионов и маломобильных граждан. Сервис удаленной идентификации, в основе которого лежит Единая биометрическая система, позволяет получать банковские услуги удаленно, при наличии смартфона или компьютера с интернетом. В настоящее время сферами применения ЕБС являются: социальные сервисы, телемедицина, торговля, образование, государственные и муниципальные услуги [4].

Однако, в настоящее время, В России безопасная и практичная ЕБС – это лишь «мечта», уровень защиты биометрических персональных граждан не на самом высоком уровне. Так, например, затрагивая банковскую систему: официальный представитель ЦБ России Артем Сычев, возглавляющий департамент информационной безопасности Банка России в одном из интервью сообщил, что «на данный момент Российские банки не смогут обеспечить тот уровень защиты биометрических данных граждан, который от них требуют власти. Вся проблема заключается в том, что у российских кредитных организаций просто нет оборудования для выполнения условия ФСБ – криптографической защиты на уровне государственной тайны» *(См.: URL: https://www.anti-malware.ru/news/2018-11-29-1447/28160 (дата обращения: 27.10.2019))*.

Исходя из всего вышесказанного, мы приходим к выводу, что вопрос регулирования биометрической идентификации персональных данных недостаточно проработан и имеет много пробелов, поэтому до сих пор в России нет отлаженного, а главное – безопасного, механизма биометрической идентификации личности. Поэтому, к сожалению, правоприменительная практика фик-

сирует случаи хищения биометрических данных граждан с целью завладения чужим имуществом из корыстных побуждений.

За рубежом существует термин IDENTITY THEFT, грубо и дословно переведенный как «Кража личности». Он применяется для случаев хакерских атак, направленных на похищение личных биометрических данных человека, будь то отпечатки пальцев или радужная оболочка глаза, схема сосудов человека, модели лица или голоса.

В марте этого года издание The Wall Street сообщило, что в результате мошеннических действий в Великобритании пострадала крупная страховая компания. Хакер, воспользовался продвинутой программой для модуляции голоса, сумев подделать речевые образцы генерального директора предприятия. Это позволило злоумышленнику связаться с бухгалтерией организации и «подтвердить» личность. Далее были совершены три перевода денежных средств на австрийские банковские счета. В результате этих действий, со счета компании были украдены, по данным источника 234 тысячи долларов США. О произошедшем в самой компании узнали лишь после проведения очередной аудиторской проверки.

В силу меньшей распространенности и только растущей популярности, Российскую федерацию еще не потрясали известия об утечках личных биометрических данных граждан, не из государственных, не из коммерческих структур. Однако, случаи утечек паспортных и иных персональных данных, с последующим использованием их в корыстных целях не редки. А биометрия, какие бы надежды на нее не возлагались в последние годы, храниться в том же электронном виде на серверах в соответствующих информационных базах, которое могут быть подвержены хакерским атакам. Однако кража биометрических данных, этой «виртуальной модели человека», представляется куда более серьезной, нежели простая утечка логинов и паролей от банковских клиентов или клиентов для доступа к государственным услугам. Ведь, в случае похищения, злоумышленник будет иметь в руках универсальный ключ, который позволит от имени гражданина получить доступ к государственным услугам, банковским счетам, прочей информации защищенной самыми современными и казавшимися безопасными системами компьютерной безопасности.

Сторонники же введение повсеместной биометрической идентификации утверждают, что система установления личности по биометрическим данным, работает по весьма сложной схеме, менее подверженной взлому. В качестве доводов приводятся:

1. Использование биометрических данных, похищенных из одной биометрикой системы, не позволит обмануть другую, так как они работают по разным методикам. В случае с распознаванием отпечатка пальца или радужки глаза, разные системы будут брать разные участки для сканирования и занесение в базу данных «эталонной модели». Однако данный принцип оставляет лазейку для использования украденных данных к системе, из которой они и были украдены. При этом в случае кражи целой виртуальной модели, например, схемы кровеносных сосудов, и предъявлении ее, система сможет провести аутентификацию необходимого ей участка.

2. Использовать данные, полученные из одной базы данных, для ее собственного обхода не получится, так как стопроцентное совпадение с «эталонной моделью» система будет автоматически отсеивать. Но современные технологии, а также понимание как работает конкретный механизм аутентификации, позволят злоумышленнику внести незначительные изменения в украденный шаблон, чтобы система не выявила стопроцентного сходства.

3. Любая система запросит проверку «на живость». Предъявленный для сканирования палец должен иметь температуру близкую к температуре человеческого тела, сканируемая радужка глаза реагировать на свет, лицо – иметь объем. Все данные барьеры обходятся современным программным обеспечением, от дешевого китайского ZAO позволяющее анимировать лицо компьютерного персонажа, обладающего всем чертами лица эталона, до более дорогих и совершенных.

Есть и другие «болезненные моменты» биометрической индикации в повседневной жизни. Главная из них (с которой вероятнее всего удастся побороться при введении Единой Базы Биометрических данных), разрозненность хранилищ таких данных на сегодняшний день, а соответственно многократный сбор биометрии. У человека, однажды принявшего участие в процедуре сдачи данных, может не возникнуть подозрения при поступлении нового предложения, которое в свою очередь может оказаться отправленным мошенниками для получения данных для незаконного использования. А также децентрализованность баз хранящих биометрические данные граждан, делает их более уязвимыми перед атаками хакеров, ведь не у каждой организации, занимающейся сбором данных, будут в распоряжении необходимое количество ресурсов для обеспечения безопасности [5]. А как мы уже определили, при должных навыках, похищенные в одном месте данные, могут стать

угрозой для их владельца в целом: банковские и государственные услуги, документация, участие в гражданском обороте окажутся под угрозой.

Не стоит недооценивать и человеческий фактор в сборе биометрических данных. Плохо подготовленный и некачественно обученный специалист, способен с легкостью совершить ошибку в этом процессе, как итог компьютерная биометрическая модель будет иметь изъян, который впоследствии превратится в лазейку для злоумышленника.

В рамках контекста данной работы мы провели открытый опрос для выявления осведомленности людей о самой технологии биометрической аутентификации, а также доверия к ней. При этом опрос был разделен на две части. В первой принимали участия специалисты, осуществляющие свою трудовую деятельность в сфере компьютерной безопасности, а также люди, обучающиеся по современной программе ИУ-10 – будущее специалисты данной сферы. Вторую часть опроса проходили лица, непричастные к теме защиты информации, в основном простые обыватели, обучающиеся и работающие в разных сферах. Суммарно в опросе поучаствовало более ста пятидесяти человек.

Общей чертой в ответах обеих групп можно выделить стопроцентное знакомство всех опрошенных с понятием биометрической идентификации. В первой группе так же все участники применяли ее в своей трудовой и повседневной деятельности. Среди второй группы данной технологией 17 процентов ответили, что использую ее регулярно, а 43 прибегали к ней хотя бы раз в жизни. Среди обеих групп лица, которые использовали биометрические данные для собственной идентификации, делали это в рамках государственных услуг, а также в банковской сфере, для получения доступа к банковским продуктам.

Наиболее разительно отличались ответы респондентов двух групп при ответь на вопрос, считают ли они сбор и дальнейшее применение биометрических данных безопасным. Среди ответов практикующих и будущих специалистов сферы компьютерной безопасности бóльшая часть опрошенных (более 85 процентов) ответили, что это скорее безопасно, хоть и имеет ряд достаточно серьезных уязвимостей, устранение которых помогло бы развитию данной технологии. Остальные 15 процентов однозначно ответили, что данные системы ненадежны. Опрос же лиц, не связанных со сферой защиты баз данных, показал, что пока люди не доверяют сбору биометрических данных, и крайне неохотно используют биометрическую аутентификацию, менее половины опрошенных использовали биометрическую идентификацию и лишь треть доверяет ей, считая ее достаточно безопасной. Респонденты обоих групп сталкивались с проблемами, описанными выше.

Сегодня цена биометрической аутентификации остается краеугольным камнем в вопросе ее повсеместного, а главное безопасного и эффективного применения. Всевозможная обеспечительная аппаратура: ридеры, сканеры и идентификационные серверы для обработки биометрических данных стоят значительно дороже, чем применение привычных методов аутентификации. Это одновременно ставит под угрозу биометрические данные лиц, сдающих их в организации экономящих на безопасности, закупающих менее надежное и защищенное оборудование, и вместе с тем сдерживает популяризацию данной технологи, а соответственно и сдерживает распространение киберприступников, желающих завладеть данными граждан. Во многом, именно благодаря тому факту, что аутентификация по биометрическим данным пользователя лишь набирает обороты в нашей стране, мы говорим о проблемах преступности в этой сфере по единичным случаям, рассматривая ее в большей степени как потенциальную. Однако меры по предупреждению возникающей проблемы стоит начать применять уже сейчас.

Такими мерами против возникающей угрозы кражи или подделки биометрических данных мы видим в комплексном подходе к данному вопросу. Вместе с созданием Единого государственного центра сбора и хранения персональных биометрических данных, необходимо ограничить доступ к данной деятельности со стороны коммерческих участников. Гражданину придется сдать биометрическую информацию один раз, в специализированный центр, что позволит как исключить некачественную фиксацию биометрических данных, так как будет использоваться качественное оборудование под управлением квалифицированного специалиста, так и гарантирует, что гражданин не станет откликаться на иные, предложения оставить биометрические данные. Так же, хранение баз данных содержащих биометрические сведения граждан в едином, максимально защищенном архиве, позволит свести риск утечек к минимуму.

Механизм же использования биометрической идентификации в данной модели будет выглядеть следующим образом:

Гражданин при авторизации, например, в банковском клиенте, проводит сканирование по биометрическим показателям (будь то голос, отпечатки пальцев или радужки глаза). Банк, для удостоверения клиента, связывается с единым

архивом, и передает туда полученные показатели. Они сравниваются с хранящейся в архиве эталонной моделью, и в случае совпадения, банк получает назад только удостоверение гражданина от самого архива. В этой цепочке организация не имеет непосредственного контакта с эталонной моделью биометрических данных гражданина, а значит и утечки с этой стороны быть не может. Сравнение представленных образцов с «оригиналом» также проходит вне организации, что позволит избежать ошибки на этом этапе.

Аутентификация человека при помощи биометрических данных уже совсем скоро плотно войдет в повседневную жизнь людей. Уже сегодня крупные организации представляют своим клиентам возможности установления их личности с помощью данной технологии. Ее удобство трудно переоценить, однако России стоит обратить внимание на международный опыт, а также проблемы, с которыми уже столкнулись как организации, так и физические лица. Учитывая, что преступления в сфере компьютерной безопасности очень сложны для расследования, защита данных во многом строиться именно на предупреждении. Грамотно составленная нормативно правовая база, рабочие механизмы реализации, позволят свести к минимум потенциальные угрозы и минимизировать возможный ущерб.

Литература

1. *Покаместова Е.Ю.* Правовая защита конфиденциальности персональных данных несовершеннолетних: автореф. дис. ... канд. юрид. наук. Воронеж, 2006. 204 с.

2. *Кривогин М.С.* Особенности правового регулирования биометрических персональных данных // Право. Журнал Высшей школы экономики. 2017. № 2. С. 80–89.

3. *Попкова А.Р.* Правовой режим использования биометрических персональных данных при удаленной идентификации физических лиц банками // Молодой ученый. 2020. № 1 (291). С. 183–185.

4. *Заболотный Е.Ю.* Перспективы развития средств аутентификации в банковской сфере // Право. Журнал «Инновационная наука». 2019. № 1. С. 25–28.

5. *Рассолов И.М.* Информационное право: учебник для магистров. М.: Юрайт, 2012. 444 с.

References

1. *Pokamestova E.Yu.* Pravovaya zashchita konfidentsial'nosti personal'nykh dannykh nesovershennoletnikh [Legal protection of the confidentiality of personal data of minors]. Dis. ... k.yu.n. 05.13.19. Voronezh, 2006. 204 p. (In Russian)

2. *Krivogin M.S.* Osobennosti pravovogo regulirovaniya biometricheskikh personal'nykh dannykh [Peculiarities of Legal Regulating Biometric Personal Data]. *Pravo. Zhurnal Vysshey shkoly ekonomiki [Law. Journal of the Higher School of Economics],* 2017, no. 2. pp. 80–89. (In Russian, abstract in English)

3. *Popkova A.R.* Pravovoi rezhim ispol'zovaniya biometricheskikh personal'nykh dannykh pri udalennoi identifikatsii fizicheskikh lits bankami [Legal regime for the use of biometric personal data for remote identification of individuals by banks]. *Molodoi uchenyi [The young scientist],* 2020, no. 1 (291), pp. 183–185. (In Russian)

4. *Zabolotnyi E.Yu.* Perspektivy razvitiya sredstv autentifikatsii v bankovskoi sfere [Prospects for the development of authentication tools in the banking sector]. *Pravo. Zhurnal Innovatsionnaya nauka [Law. Innovation science],* 2019, no.1, pp. 25–28. (In Russian)

5. *Rassolov I.M.* Informatsionnoe pravo: Uchebnik dlya magistrov [Information law: Textbook for the masters]. Moscow, Yurait Publ., 2012. 444 p. (In Russian)