УДК 34.096

ПРАВОВЫЕ АСПЕКТЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ ЛИЧНОСТИ В УСЛОВИЯХ ЦИФРОВОЙ ЭКОНОМИКИ

М.М. Зинченко

Национальный исследовательский
Нижегородский государственный университет им. Н.И. Лобачевского

Анализируется проблема идентификации пользователей в информационном пространстве, проводится обзор единой биометрической системы, выявляются проблемы безопасности персональных данных при идентификации и аутентификации при совершении транзакций и получении государственных и муниципальных услуг с помощью биометрических данных.

Ключевые слова: информация, биометрические данные, безопасность, персональные данные, единая система биометрических данных, идентификация, аутентификация.

М.М. Зинченко
Магистрант юридического факультета Национального исследовательского Нижегородского государственного университета им. Н.И. Лобачевского

В век информационных технологий информация в большей части представляется в электронной форме без прямой взаимосвязи между субъектами, поэтому можно предположить, что требуется самостоятельный институт в информационном праве. Его актуальность определяется тем, что технологии ушли далеко вперед их правового регулирования, определяющего статус субъектов в информационном пространстве, – сейчас пользователи зачастую действуют анонимно под «никнеймами» и порой невозможно определить участников взаимодействия в социальных сетях, от кого и кому совершаются банковские и иные операции, с каким субъектом взаимодействует государство при блокировке неразрешенного контента.

В настоящий момент остро стоит проблема идентификации пользователей в информационном пространстве, с одной стороны, и проблема безопасности персональных данных субъектов, с другой стороны.

На сегодня в стране существует правовой режим персональных данных, представляющий собой правовую систему регулирования, которую, однако, не всегда эффективно можно реализовывать в сети Интернет, где может происходить как полное рассекречивание персональных данных, так и непредоставление таковых совсем – достаточно использовать данные для идентификации технических устройств. Действующее законодательство позволяет действовать анонимно, не требуя полной самоидентификации в целях сохранения неприкосновенности частной жизни, – в этом случае необходимо указание в законе, является ли обязательной идентификация в тех или иных правоотношениях. Самоидентификация, несмотря на императивный характер правовых норм, представляет собой в современных социальных реалиях не принудительную, а «добровольную» идентификацию, поскольку ответственность за нарушение норм указанной статьи не предусмотрена; однако обязательная идентификация предусмотрена для физических и юридических лиц, осуществляющих предпринимательскую деятельность.

Как подчеркивает в своих статьях В.Б. Наумов[1], в судебной практике по проблеме идентификации выносятся решения по факту распространения сведения конкретным лицом на основе косвенных сведений или свидетельских показаний, так как далеко не все при регистрации указывают свои персональные данные и используют Интернет анонимно.

Идентификация пользователей в информационном пространстве в первую очередь происходит при получении государственных и муниципальных услуг.

Первые шаги во взаимодействии субъектов и государства были сделаны в 2013 году с принятием Федерального закона от 7 июня 2013 года № 112-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и защите информации»[2] и Федерального закона «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»[3]: был определен статус субъектов информационных отношений в сфере оказания государственных услуг.

Была создана Единая система идентификации и аутентификации (ЕСИА) – федеральная государственная информационная система, порядок функционирования которой был установлен Правительством РФ и которая обеспечивала санкционированный доступ к информации, содержащейся в информационных системах, в предусмотренных законом случаях.

Систему модернизировали и в 2014 году Приказом Министерства связи и массовых коммуникаций РФ от 30 июня 2014 г. № 179 ввели в эксплуатацию. Распоряжением Правительства РФ от 9 июня 2014 г. № 991-р утвержден план мероприятий («Дорожная карта») по реализации Концепции развития механизмов предоставления государственных и муниципальных услуг в электронном виде (СЗ РФ. 2014. № 24. Ст. 3136). В последнем квартале 2015 года интегрированы информационные системы многофункциональных центров, давно используемых в России, с Единой системой идентификации и аутентификации.

К системе ЕСИА существуют требования, утвержденные Постановлением Правительства РФ от 28 ноября 2011 г. № 977, – «Требования к Федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»[4], где были заложены правовые и технологические основы идентификации в сфере государственной координации и государственных и муниципальных услуг. В требованиях установлены правовые дефиниции, не определенные федеральными законами. Так, дается определение авторизации участников информационного воздействия, так как для получения государственных и муниципальных услуг требуется ее пройти, то есть подтвердить наличие у участника прав на получение доступа к инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем. В настоящий момент эти определения представляют ограниченную терминологическую базу, которая нуждается в доработке и развитии, так как из-за растущего объема информации появляется масса новых терминов и понятий, которые будут противоречить друг другу, если их иерархично не определить на законодательном уровне.

Авторами научных статей подчеркивается, что уже сейчас можно выделить несостыковки между актуальным законодательством и только формируемым правовым регулированием персональных данных. Второе не содержит ссылок на категории о персональных данных и оперирует собственными терминами, а первое не содержит четкого обозначения, в какой момент идентификации сведения становятся персональными данными. Также согласно пункту 6(1) требований к ЕСИА[5] система должна обеспечивать потенциальную возможность применения различных методов идентификации пользователей при обеспечении доступа к информации для наибольшей безопасности лиц.

В данный момент развитие информационных технологий также позволяет использовать биометрические данные для получения государственных и муниципальных услуг, удаленных операций с транзакциями, других различных банковских операций. Перспективы развития предполагают дальнейшее использование биометрии в здравоохранении, расширенном спектре финансового сектора.

Биометрия лежит в основе и идентификационных документов (биометрических паспортов, идентификационных карт), стандартизацией которых в мире занимается Международная организация гражданской авиации (ИКАО)2 при ООН. Такие биометрические паспорта уже используются во многих странах: в Беларуси, Казахстане, Молдавии, Монголии, Пакистане, США, Израиле, Туркмении, Узбекистане, Украине, в странах Евросоюза.

В России также активно развиваются информационные технологии в области биометрических систем.

В 2017 году SecurityLab.ru опубликовало информацию от журнала «Известия»[6] о появлении национальной биометрической платформы на портале государственных услуг со ссылкой на главу Минкомсвязи Николая Никифорова. Такая интеграция предполагает расширение спектра

юридических услуг, которые можно оказывать в онлайн-режиме, и в первую очередь в данной технологии заинтересованы банки, которые смогут распознавать клиента через камеру смартфона. Также проводились попытки дополнения государственных услуг биометрией – вследствие отсутствия национальных карт предполагалось использовать голос и лицо пользователя.

Единая биометрическая система – это цифровая платформа, которая является одним из ключевых элементов механизма удаленной идентификации человека по его биометрическим характеристикам. Указанная система создается по инициативе Министерства связи и массовых коммуникаций Российской Федерации и Центрального банка Российской Федерации.

Был принят приказ Минкомсвязи России «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации»[7], в соответствии с которым собранные биометрические образцы голоса и изображения собираются в единую биометрическую систему и хранятся в соответствии со ст. 19 Федерального закона № 152-ФЗ[8] не менее 50 лет. В соответствии с пунктом 18 приказа, «использование биометрических персональных данных, в том числе размещенных в единой биометрической системе, в целях идентификации, осуществляется в течение 3 лет с момента их размещения в указанной системе». Биометрические данные при регистрации и обновлении, хранящиеся в единой биометрической системе, подписываются квалифицированной электронной подписью.

В приказе не установлены случаи и сферы применения биометрических данных, а указан только порядок получения и обработки биометрических данных, которые подписываются квалифицированной подписью. Можно сделать вывод, что обработка данных не станет заменой квалифицированной подписи, однако для повышения безопасности в сфере банковского обслуживания они могли бы существовать одновременно, представляя собой двухступенчатую идентификацию пользователя.

На XI Уральском форуме «Информационная безопасность финансовой сферы»[9], прошедшем в феврале 2019 года, на пленарном заседании, посвященном теме «Кибербезопасность в цифровой экономике», выступила с докладом первый заместитель председателя Банка России Ольга Скоробогатова.

Она отметила, что безопасность фокусируется по трем областям: 36% внимания приходится на сетевую безопасность, 30% – безопасность приложений и 34% – безопасность данных, и подчеркнула: «При этом в кулуарах международных форумов в основном, конечно, говорят о том, насколько сложно обеспечивать безопасность именно в части данных».

В фокусе внимания докладчика находятся биометрическая идентификация, система быстрых платежей, при этом биометрическая идентификация названа довольно сложным проектом. По информации Скоробогатовой, «сегодня 95 банков уже начали осуществлять сбор биометрических данных, 4 000 отделений подключено».

В 2017 году Президентом РФ был подписан ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации»[10]. Этот закон предусматривает внесение изменений в закон № 115-ФЗ «О противодействии легализации доходов, полученных преступным путем, и финансированию терроризма». Изменения коснулись самого пункта о необходимости личной явки гражданина для открытия счета в банке, где он раньше не обслуживался.

Использование физическими лицами единой биометрической системы является бесплатным. Оно позволяет сэкономить время на личное открытие счета и дает возможность пользоваться банковскими сервисами в любой момент через логин и пароль от ЕСИА. Запросы пользователя обрабатываются одним из нескольких динамических алгоритмов, что обеспечивает дополнительную защиту от мошенничества, однако в случае компрометации изменить биометрические данные как пароль не представляется возможным, поэтому в случае утечки пользователь не сможет впоследствии воспользоваться этими биометрическими данными.

Что касается развития цифровой платформы единой биометрической системы, то по мере накопления данных будет появляться больше возможностей ее функционирования: она охватит здравоохранение, финансовый сектор, образование, получение государственных и муниципальных услуг.

Удаленная идентификация, согласно сайту ЕБС[11], может применяться для проведения выборов, совершения юридически значимых действий при предоставлении государственных услуг, для обеспечения безопасности граждан.

Эта система является перспективной и в будущем охватит большинство сфер жизни от автоматизации бизнес-процессов взаимодействия с клиентами до бесконтактного прохода посетителей в музеи.

Также указано, что Единая биометрическая система, запущенная 1 июля 2018 года, будет дорабатываться и по мере ее работы оператор системы «Ростелеком»[12] будет ее совершенствовать. Система обладает самообучающимся модулем, который сможет выявлять попытки мошенничества и предотвращать их в дальнейшем. Кроме того, система подразумевает анализ уже существующих биометрических алгоритмов и возможность создания собственных.

Система только начала работать, но перспективы ее развития позволяют предположить, что успешная реализация проекта повысит безопасность электронного документооборота и, возможно, использование технологии электронной подписи станет неактуальным в будущем.

Однако сейчас предполагается использование только двух модальностей для идентификации пользователя – голос и лицо, что позволяет определить «живого человека», отпечаток пальца не предусмотрен, так как для широкого круга пользователей он будет недоступен из-за низкой чувствительности датчика сканера или отсутствия необходимой техники среди широких масс населения.

Таким образом, на данный момент подписание документов и определение автора с помощью биометрии не предполагается, а электронная подпись остается актуальным вариантом для работы с электронным документооборотом.

Однако следует понимать, что у биометрической системы идентификации есть свои, отличные от связки логин/пароль или двухфакторной аутентификации, особенности:

1) биометрические данные находятся в публичном доступе. Существует возможность найти фото-, видеоматериалы практически любого человека и впоследствии использовать их для идентификации;

2) замена голоса или лица невозможна в отличие от логина и пароля;

3) биометрическая идентификация подтверждает личность с вероятностью, близкой, но не равной 100%. Другими словами, система допускает, что человек может в какой-то степени отличаться от своей биометрической модели, сохранённой в базе.

В качестве основных проблем, связанных с биометрической идентификацией, можно выделить фальсификацию, утечки и кражи, низкое качество собранных данных, а также многократный сбор данных одного человека разными организациями. В целях избегания фальсификации посредством масок или технологий айтрекинга (отслеживание движений глазных яблок владельца при вводе пароля), используется технология выявления «живости» – liveness detection – набор проверок, позволяющий определить живого человека перед камерой, но эту технологию также можно обмануть. В представленном на Black Hat-2019 докладе «Biometric Authentication Under Threat: Liveness Detection Hacking»[13] сообщается об успешном обходе liveness detection в Face ID посредством очков, надетых на спящего человека, внедрения поддельных аудиопотоков и видеопотоков, а также других способов.

Так как точность идентификации зависит от качества биометрических данных, сохраненных в системе, необходимо оборудование, способное работать в шумных и неярких отделениях банков, так как бюджетные микрофоны неспособны записать точные образцы голоса, камеры – сделать фотографии для построения биометрической модели, а записанные образцы будут подвержены ложным узнаваниям, при которых система принимает одного человека за другого.

Некоторые банки начали сбор биометрических данных раньше, чем заработала ЕБС, поэтому потребовалась повторная сдача биометрии. В ситуации с несколькими параллельными биометрическими системами можно выделить некоторые риски:

1) повышается возможность утечки данных, так как увеличивается количество возможных каналов доступа к информации;

2) у человека, дважды сдавшего биометрию, скорее всего, уже не вызовет подозрения предложение повторить эту процедуру. Поэтому в будущем он может стать жертвой злоумышленников, которые могут собирать биометрию в преступных целях.

Чтобы максимально обезопасить систему, существуют активные и пассивные методы проверки liveness для лицевой модальности. При пассивных методах нет взаимодействия пользователя с системой, они включают текстурный анализ, оценку бликов, цветовую палитру, микродвижения, соответствие эталону. В активных методах происходит взаимодействие пользователя с системой, методы проверки содержат проверку выражения лица, движение рта, головы, движение и моргание глаз.

Методы проверки liveness для голосовой модальности также делятся на активные и пассивные в зависимости от взаимодействия пользователя с системой. Пассивная проверка включает резкую смену акустической обстановки, интонации, совпадение биометрического отпечатка с эталоном. Активная проверка состоит из динамического пароля и внезапности действий, провоцирующих пользователя на инстинктивные решения.

14 сентября 2019 года в силу вступила директива Евросоюза PSD2 (Open Banking), которая требует от банков многофакторной аутентификации для обеспечения пользователей наибольшей безопасностью при пользовании удаленными транзакциями. Это означает обязательное использование по крайней мере двух из трех элементов:

1) знания – информация, известная только пользователю (к примеру, пароль или контрольный вопрос);

2) владения – устройства, которыми владеет только пользователь (токен или девайс);

3) уникальности – неотделимое, присущее только пользователю, например его биометрические данные.

Эти три элемента должны быть независимы друг от друга, чтобы компрометация одного не повлияла на надежность других.

Применительно к банковской практике это значит, что проведение операций по биометрическим данным должно обязательно сопровождаться дополнительными проверками с помощью пароля, токена или PUSH/SMS-кодов.

На взгляд автора статьи, безопасным будет также хранение биометрических данных в зашифрованном виде у заинтересованного лица – владельца биометрических данных. Так, в случае утечки будут скомпрометированы данные только этого лица, а не всех пользователей в базе данных.

На сегодня у биометрической аутентификации имеются большие перспективы, однако существующие риски безопасности достаточно серьезны, чтобы вызывать опасения, поэтому разработчикам систем нужно оперативно реагировать на новости и новейшие разработки и дорабатывать систему идентификации. Законодательным органам следует изучать новейшие и появляющиеся результаты исследований и активно реагировать для правового регулирования работы биометрических систем. Также законодательное регулирование должно быть направлено на возможность контролирования пользователями своих биометрических данных, чтобы минимизировать вмешательство в частную жизнь.

Наиболее надежной и безопасной техникой остается многофакторная аутентификация, использование ее вместе с биометрией выглядит, по мнению автора статьи, наиболее практичным методом для снижения рисков, а также контролирование и обеспечение безопасности биометрических данных самим пользователем, например, при нахождении в техническом устройстве в собственности пользователя.

Но если биометрическая идентификация, предлагаемая человеку на его устройстве, работает во взаимодействии с удаленными серверами, контролируемыми третьими лицами, то соответствующая организация (разработчик приложения, производитель устройства и т.д.) должна получить санкционирование такой обработки от пользователя.

Таким образом, если все операции с биометрическими данными будут осуществляться только через согласие пользователя и многофакторную аутентификацию, то на данный момент это будет наиболее защищенным и безопасным вариантом использования ЕБС до разработки государством законодательства в этой области и усовершенствования информационных технологий, которые позволят избежать угрозу утечки персональных данных или фальсификации.

Можно полагать, что ключевыми задачами законодательства являются определение терминологии в сфере идентификации персональных данных и формирование единой терминологической базы; совершенствование института правового регулирования технологий идентификации и аутентификации через биометрические данные, а также работа над созданием правового института идентификации субъектов в информационном пространстве.

Библиографический список

1. Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных» (в ред. от 31.12.2017) // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3451.

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

3. Федеральный закон 09.02.2009 № 8-ФЗ (ред. от 28.12.2017) «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства РФ. 2009. № 7. Ст. 776.

4. Федеральный закон от 31.12.2017 № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. 2018. № 1 (ч. 1). Ст. 66.

5. Постановление Правительства РФ от 28.11.2011 № 977 (ред. от 20.11.2018) «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // Интернет-портал Правительства РФ [Электронный ресурс]. URL: http://archive.government.ru/gov/results/17300/ (дата обращения: 15.01.2020).

6. Распоряжение Правительства от 22.02.2018 № 293-р «О возложении на ПАО междугородной и международной электрической связи «Ростелеком» функций оператора единой информационной системы персональных данных» // Официальный сайт Правительства России [Электронный ресурс]. URL: http://static.government.ru/media/files/MbjDAmTYHiwx9JXVvJfNITUGVEA4ThJs.pdf (дата обращения: 15.01.2020).

7. Приказ Минкомсвязи России от 25.06.2018 № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» // Официальный сайт Минкомсвязи России [Электронный ресурс]. URL: https://digital.gov.ru/ru/documents/6214/ (дата обращения: 15.01.2020).

8. Biometric Authentication Under Threat: Liveness Detection Hacking // Black Hat USA. 2019 [Электронный ресурс]. URL: https://www.black-hat.com/us-19/briefings/schedule/#biometric-authentication-under-threat-liveness-detection-hacking-16130 (дата обращения: 15.01.2020).

9. SecurityLab.ru by Positive Technologies [Электронный ресурс]. URL: https://www.securitylab.ru/news/486252.php (дата обращения: 15.01.2020).

10. Единая биометрическая система // Цифровая платформа для удаленной биометрической идентификации / ПАО «Ростелеком» [Электронный ресурс]. URL: https://bio.rt.ru/faq/project/ (дата обращения: 15.01.2020).

11. Наумов В.Б. К вопросу о формировании института идентификации субъектов в системе российского информационного права // Новые вызовы и угрозы информационной безопасности: правовые проблемы / Институт государства и права РАН, Издательство «Канон», 2016. – С. 1–7. [Электронный ресурс]. URL: https://www.russianlaw.net/files/law/doc/aa72.pdf (дата обращения: 15.01.2020).

12. Наумов В.Б. Вопросы развития терминологии в сфере персональных данных // Понятийный аппарат информационного права: Сб. науч. работ / Отв. ред. И.Л. Бачило, Э.В. Талапина. – М., 2015. – С. 124–129.

13. Наумов В.Б. Научные подходы к классификации видов правовой идентификации в информационных правоотношениях // Труды Института государства и права Российской академии наук. – 2016. – С. 104–113. [Электронный ресурс]. URL: https://cyberleninka.ru/article/n/nauchnye-podhody-k-klassifikatsii-vidov-pravovoy-identifikatsii-v-informatsionnyh-pravootnosheniyah (дата обращения: 29.12.2019).

14. Уральский форум XI. Информационная безопасность финансовой сферы 2019 г. // Finversia: портал финансовой информации [Электронный ресурс]. URL: https://www.finversia.ru/news/events/govorim-bankovskaya-sistema-podrazumevaem-sistema-bezopasnosti-53921 (дата обращения: 15.01.2020).

[1] Наумов В.Б. К вопросу о формировании института идентификации субъектов в системе российского информационного права // Новые вызовы и угрозы информационной безопасности: правовые проблемы / Институт государства и права РАН. Издательство «Канон», 2016. – С. 1–7. [Электронный ресурс]. URL: https://www.russianlaw.net/files/law/doc/aa72.pdf (дата обращения: 15.01.2020).

[2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

[3] Федеральный закон 09.02.2009 № 8-ФЗ (ред. от 28.12.2017) «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // Собрание законодательства РФ. 2009. № 7. Ст. 776.

[4] Постановление Правительства РФ от 28.11.2011 № 977 (ред. от 20.11.2018) «О федеральной государственной информационной системе «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме» // Интернет-портал Правительства РФ [Электронный ресурс]. URL: http://archive.government.ru/gov/results/17300/ (дата обращения: 15.01.2020).

[5] Там же.

[6] SecurityLab.ru by Positive Technologies [Электронный ресурс]. URL: https://www.securitylab.ru/news/486252.php (дата обращения: 15.01.2020).

[7] Приказ Минкомсвязи России от 25.06.2018 № 321 «Об утверждении порядка обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядка размещения и обновления персональных данных в единой биометрической системе, а также требований к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации» // Официальный сайт Минкомсвязи России [Электронный ресурс]. URL: https://digital.gov.ru/ru/documents/6214/ (дата обращения: 15.01.2020).

[8] Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных» (в ред. от 31.12.2017) // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3451.

[9] Уральский форум XI. Информационная безопасность финансовой сферы 2019 г. // Finversia: портал финансовой информации [Электронный ресурс]. URL: https://www.finversia.ru/news/events/govorim-bankovskaya-sistema-podrazumevaem-sistema-bezopasnosti-53921 (дата обращения: 15.01.2020).

[10] Федеральный закон от 31.12.2017 № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. 2018. № 1 (1 ч.). Ст. 66.

[11] Единая биометрическая система // Цифровая платформа для удаленной биометрической идентификации / ПАО «Ростелеком» [Электронный ресурс]. URL: https://bio.rt.ru/faq/project/ (дата обращения: 15.01.2020).

[12] Распоряжение Правительства от 22.02.2018 № 293-р «О возложении на ПАО междугородной и международной электрической связи «Ростелеком» функций оператора единой информационной системы персональных данных» // Официальный сайт Правительства России [Электронный ресурс]. URL: http://static.government.ru/media/files/MbjDAmTYHiwx9JXVvJfNITUGVEA4ThJs.pdf (дата обращения: 15.01.2020).

[13] Biometric Authentication Under Threat: Liveness Detection Hacking // Black Hat USA 2019 [Электронный ресурс]. URL: https://www.blackhat.com/us-19/briefings/schedule/#biometric-authentication-under-threat-liveness-detection-hacking-16130 (дата обращения: 15.01.2020).

LEGAL ASPECTS OF BIOMETRIC IDENTITY IN THE DIGITAL ECONOMY

M.M. Zinchenko
First-year Master's degree student of the Law Faculty at the Lobachevsky State University of Nizhny Novgorod

The article analyzes the problem of user's identification in the information space, provides a review of the Unified Biometric System, identifies the problems of personal data security in the identification and authentication of transactions and provision of state and municipal services with the use of biometric data.

Keywords: information, information law, biometric data, security, personal data, unified biometric data, identification, authentication.