

© **Андрей Викторович Барinov**,
кандидат юридических наук, доцент
заведующий кафедрой гражданско-
правовых дисциплин
Владимирский филиал РАНХиГС
г. Владимир
e-mail: barinov-vlad@inbox.ru

A. V. Barinov,
Candidate of Legal Sciences,
Assistant Professor
Head of the Civil Law Disciplines
Department Vladimir branch of the
RANEPA, Vladimir

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЭЛЕКТРОННОЙ ИДЕНТИФИКАЦИИ ГРАЖДАН КАК ОСНОВА ПРАВООТНОШЕНИЙ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

Legal regulation of electronic identification of citizens as the basis of legal relations in the information society

***Аннотация:** в статье исследуется становление и развитие правового обеспечения электронной идентификации граждан как необходимого элемента для установления правоотношений в условиях информационного взаимодействия субъектов права. На основе анализа норм законодательства в сфере информации и информационных технологий последовательно раскрываются особенности и недостатки таких средств электронной идентификации граждан, как электронная подпись, электронная идентификационная карта, биометрические данные. В работе сделан вывод о публично-правовом подходе в решении вопроса электронной идентификации граждан, что может оказать отрицательное влияние на развитие частных правоотношений.*

***Abstract:** The article examines the formation and development of legal support for electronic identification of citizens, as a necessary element for establishing legal relations in the context of information interaction of subjects of law. Based on the analysis of legislation in the field of information and information technology, the features and disadvantages of such means of electronic identification of citizens as an electronic signature, an electronic identification card, and biometric data are consistently revealed. The paper draws a conclusion about the public-law approach to solving the issue of electronic identification of citizens, which can have a negative impact on the development of private legal relations.*

***Ключевые слова:** правовое регулирование, электронная идентификация гражданина, идентификация и аутентификация, электронная подпись, электронная идентификационная карта, биометрические данные, государственные услуги, информационно-телекоммуникационная сеть.*

***Keywords:** legal regulation, electronic identification of a citizen, identification and authentication, electronic signature, identification document, biometric data, public services, information and telecommunication network.*

Появление в последнее время многочисленных фундаментальных исследований [1-6], посвященных вопросам регулирования правоотношений в условиях внедрения информационных технологий, расширения общественных отношений в сети «Интернет» и развития цифровой экономики, говорит о том, что вопросы информатизации и цифровизации оказывают существенное влияние на формирования новой системы правового регулирования общественных отношений.

В условиях перехода общественных отношений в информационное пространство ключевое значение приобретает вопрос надежной идентификации субъектов в информационно-телекоммуникационной среде. Причем использование традиционных идентификаторов, средств и способов идентификации участников общественных отношений в информационной системе, таких как фамилия, имя, отчество гражданина, номер паспорта и адрес места жительства, затруднительно. Случаи, когда граждане выдавали себя за других путем подделки паспорта, возникали и до появления сети «Интернет». С переходом общественных отношений в информационное пространство сети «Интернет» для многих граждан стало обычным делом регистрироваться на сайтах и вступать в отношения с другими лицами под чужим именем, под разными именами или вообще анонимно. И если такие обстоятельства при получении гражданином информации с сайтов или общении в социальных сетях юридического значения не имеют, то при совершении юридически значимых действий проблема идентификации становится наиболее острой, так как необходимо решить ключевой вопрос: как достоверно установить, с кем ты в действительности имеешь дело. Проблема состоит в том, что субъект права в сети «Интернет» может быть вообще неидентифицированным, вместо этого создается юридическая фикция (или презумпция) определенного лица, что требует новых подходов и к теории правоотношений [7]. В этой связи с целью расширения возможностей субъектов совершать юридические действия в информационно-телекоммуникационной сети необходимо не только техническое решение проблемы идентификации участников через создание цифровой личности, но и их нормативное закрепление. Без этого невозможно построение доверительных отношений между субъектами цифрового пространства как общества взаимосвязанных и доверяющих друг другу лиц, каждый из которых может на основе персональных и биометрических данных однозначно установить настоящих участников этого сообщества.

Работы по созданию системы электронной идентификации личности и ее правового регулирования в информационно-телекоммуникационной сети ведутся в РФ более 10 лет. Начало этому процессу было положено принятием законов о цифровой подписи, сначала в 2002 году [8], а потом заменившего его в 2011 году [9]. В настоящее время в РФ установлено три вида электронной подписи (ЭП), причем только квалифицированная электронная подпись (КЭП), выданная аккредитованным удостоверяющим центром, признается аналогом собственноручной. Электронный документ, подписанный такой подписью, признается равнозначным документу на бумажном носителе и может использоваться как в частных, так и в публичных правоотношениях. Кроме того,

КЭП можно не только подписывать документы, но и использовать ее в системах, в которых требуется идентификация через единую систему идентификации и авторизации (ЕСИА). Используя КЭП, пользователь может входить на портал госуслуг и сайты государственных органов, подключенные к системе ЕСИА. В этом случае юридические действия, совершенные на этих сайтах с КЭП, приравниваются к действиям, заверенным собственноручной подписью. Достоинством КЭП является то, что с ее помощью можно быстро провести защищенную идентификацию, причем не только физического лица, но и юридического, что крайне важно для гражданского оборота. Так как КЭП - это информация в электронной форме на электронном носителе, а средства КЭП – это шифровальные (криптографические) средства, используемые для ее создания, то и уязвимость КЭП связана с необходимостью обеспечения конфиденциальности ключа ЭП и ее носителя и устареванием алгоритмов шифрования. Даже самую защищенную электронную подпись гарантированно можно «взломать» и фальсифицировать удостоверенный ею документ [10]. Кроме того, создание и выдача сертификатов КЭП возложены на аккредитованные удостоверяющие центры, которых в РФ более 500 [11], и до сих пор нет единого реестра таких центров. Проблема получения незаконного доступа к ключу проверки КЭП через удостоверяющие центры с последующей подачей в Росреестр заявления от имени собственника в электронной форме привела в свое время к возникновению мошеннических схем по завладению чужой недвижимостью. Законодателю удалось вовремя скорректировать соответствующие нормы [12] и предотвратить реализацию этой мошеннической схемы, что в целом не решает проблемы использования КЭП, например, регистрации на чужое имя юридического лица. Можно согласиться с мнением, что в силу правового нигилизма и недостаточной компьютерно-технической образованности населения электронная подпись является довольно рискованным способом взаимодействия с государством и частными лицами [13]. С целью усиления правовой защиты лиц, использующих КЭП, были внесены изменения в закон об ЭП [14]. Так, с 01.01.2021 вводится новый участник электронного взаимодействия для лиц, подписавших электронный документ, – это доверенная третья сторона. В законе об ЭП даются ее определение и требования к ней, порядок проверки электронной подписи и перечень услуг, оказываемых доверенной третьей стороной. В частности, доверенная третья сторона подтверждает действительность электронных подписей, используемых при подписании электронного документа, проверяет соответствие всех квалифицированных сертификатов, используемых при подписании электронного документа, и, самое главное, проверяет полномочия участников электронного взаимодействия. Вступившие в силу нововведения являются одним из элементов формирования цифровой личности в информационно-телекоммуникационной сети и будут способствовать развитию доверия при взаимодействии органов государственной власти, органов местного самоуправления, юридических и физических лиц с применением ЭП.

Другой проблемой, связанной с ЭП, является ее использование только в правоотношениях по обмену электронными документами, это не охватывает

другие юридически значимые действия в информационно-телекоммуникационной сети, в частности выражение согласия на совершение действия в адрес лица или совершение пользователем конклюдентных действий, в том числе перевод денежных средств. Кроме того, срок действия ключа КЭП ограничен (12 месяцев), а его выдача требует денежных расходов.

Можно согласиться с рядом авторов, которые считают, что КЭП в ее традиционном понимании уходит в прошлое. Современные технологии позволяют идентифицировать человека по биометрическим данным, по голосу, по видеозаписи и т.д. Даже по видеозаписи раскрытого паспорта можно программно установить, настоящий паспорт или поддельный [15]. Поэтому в законодательстве должны быть урегулированы различные способы электронной идентификации.

Если проанализировать зарубежный опыт, то идентификация граждан и юридических лиц при взаимодействии между собой и с государственными органами реализуется с использованием различных электронных идентификационных карт (ЭИК). Причем в большинстве стран используются либо ЭИК (ID-карта - Identity Document), либо специализированные: платежные карты, комбинированные с ID-картой, карты государственных услуг (Public Service Card - PSC), карты доступа к услугам здравоохранения, карточка социального страхования (Social Security Card, SSC), а в ряде стран реализованы проекты, связанные с электронными паспортами. Как правило, такие ЭИК содержат биометрические данные о гражданине (цифровой код изображения лица, группу крови, сканы отпечатков пальцев) и включают следующие цифровые сертификаты: для идентификации самой карты; для аутентификации, который гарантирует однозначную идентификацию гражданина в процессе выполнения онлайн-транзакций; сертификат ЭП, который используется в процессе постановки ЭП на документах, что гарантирует их целостность и факт того, что он был подписан именно данным лицом [16]. Удобство ЭИК состоит в том, что она носит универсальный характер, так как содержит как персональные и биометрические данные, необходимые для идентификации личности, так и ЭП для удостоверения электронных документов.

Таким образом, системы идентификации/аутентификации граждан функционируют в большинстве развитых стран, основной целью данных систем является снижение рисков управления данными пользователей и обеспечение особой доверительной информационной среды [17].

С 1 января 2012 г. в РФ была предпринята попытка выдачи универсальной электронной карты (УЭК), которая совмещала два инструмента: идентификацию пользователя для доступа к госуслугам и совершения юридически значимых действий в электронной форме, в том числе могла использоваться и как платежный инструмент (глава 6 закона о госуслугах [18]). Реализация проекта УЭК предполагалась в форме частно-государственного партнерства с привлечением юридических лиц, и в первую очередь банков. Но потенциальная несовместимость идентификационного и платежного приложений, отсутствие на момент реализации национальной платежной системы и большие финансовые затраты на выпуск карты, которые не вызвали интереса у бизнеса, привели к тому

что необходимый частным лицам, но непроработанный проект был закрыт, выпуск и выдача УЭК прекращена с 1 января 2017 года.

Одновременно с проектом по выдаче УЭК в РФ приступили к созданию единой системы электронной идентификации граждан. Для этих целей еще в 2011 г. была создана федеральная государственная информационная система «Единая система идентификации и аутентификации» (ЕСИА), обеспечивающая информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме [19]. В качестве идентификаторов в такой системе используется простая ЭП, которую граждане могут получить при регистрации на портале госуслуг [20]. И если первоначально ЕСИА была создана для доступа к информации, содержащейся в государственных и муниципальных информационных системах, в том числе для предоставления государственных и муниципальных услуг, то согласно изменениям, внесенным в постановление Правительства РФ № 977 в 2020 г., в этой системе возможно и взаимодействие государственных и муниципальных информационных систем с иными информационными системами коммерческих и некоммерческих организаций.

С целью расширения возможностей ЕСИА в части достоверной электронной идентификации граждан - в 2018 году приступили к созданию Единой биометрической системы (ЕБС) как составной части единой информационной системы персональных данных, которая предназначена для сбора, обработки и хранения биометрических данных гражданина (данные изображения лица человека, полученные с помощью фотовидеоустройств, и данные голоса человека, полученные с помощью звукозаписывающих устройств) [21], а также проверки их соответствия первично сданным биометрическим образцам по запросам государственных органов и организаций (процесс аутентификации). По Распоряжению Правительства РФ № 293-р от 22 февраля 2018 года в качестве оператора ЕБС определено ПАО «Ростелеком» [22]. С момента создания использование ЕБС предполагалось исключительно только для банковского обслуживания граждан, т.е. возможности удаленного открытия счета, вклада, получения кредита.

В декабре 2020 г. правовое регулирование электронной идентификации граждан получило новое развитие. Поправки, внесенные в закон об информации и информационных технологиях, вступившие в силу с 01.01.2021 [23], существенно изменили нормы ст. 14.1 «Применение информационных технологий в целях идентификации физических лиц» [24], установив принципиально новые подходы в процедуре идентификации и аутентификации пользователей информационно-телекоммуникационной сети.

Кроме того, в закон об информации и информационных технологиях введены два важнейших понятия - это идентификация и аутентификация, которые включают совокупность мероприятий по установлению сведений о лице. Для реализации мероприятий по электронной идентификации граждан необходимо сформировать систему (базу данных) сведений о гражданах, включающую уникальные обозначения (идентификаторы – биометрические данные), принадлежащие им, а далее при контакте в информационно-

телекоммуникационной сети с гражданином, сведения о котором внесены в систему, можно будет проверить, отвечает ли гражданин, с которым вы контактируете, его идентификаторам в системе, и, используя аутентифицирующие признаки (идентификаторы), установить, правомерно ли он владеет идентификаторами, в результате чего гражданин считается установленным.

С 01.01.2021 г. возможности использования ЕБС значительно расширяются. Пройдя идентификацию и аутентификацию, граждане могут получать различный спектр услуг, причем не только от государственных и муниципальных органов и финансовых организаций, но и от других организаций, при условии их включения в перечень прошедших идентификацию и аутентификацию участников информационного взаимодействия. Это говорит о том, что в РФ будет создана публичная информационно-телекоммуникационная система для организации информационного взаимодействия граждан и юридических лиц, причем не только с государственными органами, но и между собой.

Таким образом, в настоящее время в РФ созданы правовые основы для формирования регистров единой системы идентификации и аутентификации как граждан, так и юридических лиц, которые позволят частным субъектам осуществлять права в рамках информационного взаимодействия с использованием информационно-телекоммуникационной сети.

Насколько эффективна и безопасна будет электронная идентификация через ЕСИА с ЕБС и правильно ли выбрано направление правового регулирования идентификации граждан, пока судить трудно. Пока, по данным аналитического центра НАФИ, половина из опрошенных россиян не поддерживают создание ЕБС [25], а на август 2020 года в ЕБС были зарегистрированы 150 тыс. пользователей [26].

Кроме того, в отличие от распространенной во многих странах идентификации граждан с использованием ЭИК, от которой мы отказались, электронная идентификация через ЕСИА с ЕБС имеет и ряд недостатков, связанных с использованием биометрических данных гражданина.

В частности, при информационном взаимодействии через ЕСИА отправка идентификационной информации - пароля, записи голоса и изображения лица может осуществляться при воздействии третьих лиц, либо с использованием поддельного изображения и имитации голоса [3]. Хотя в последнем случае представители ПАО «Ростелеком» уверяют, что алгоритмы распознавания имеют очень высокую точность и могут распознавать при физиологических изменениях голоса или лица (болезнь, травмы и т. п.) и даже близнецов [27]. Другой недостаток биометрических данных связан с их устареванием, чего нельзя сказать об ЭИК, где может устанавливаться только срок действия. Поэтому обновление биометрических данных в ЕБС в целях идентификации должно осуществляться каждые 3 года [28], и для граждан эта процедура бесплатна.

Вся информация о персональных данных гражданина, в том числе биометрических с использованием ЭИК, хранится на карте, а не у оператора, как

в ЕСИА, поэтому база представляет определенный интерес для компьютерных взломщиков. Хотя представители ПАО «Ростелеком» утверждают, что в ЕСИА реализовано распределенное хранение данных: биометрический шаблон хранится в обезличенной форме отдельно от персональных данных [27], но и в этом случае нельзя исключить человеческий фактор.

Кроме того, избрав для идентификации и аутентификации граждан в ЕСИА персональные и биометрические данные, законодателем проигнорированы такие идентификаторы, как логин, пароль и абонентский номер клиента, пользующегося услугами подвижной радиотелефонной связи, или IP-адрес технологического оборудования или IP-адрес узла сети, с которых гражданин имеет доступ в информационно-телекоммуникационную сеть. Такой способ идентификации широко используется в предпринимательской деятельности при оказании услуг, и в частности в системе платежей. Более того, в перспективе абонентский номер, технологическое оборудование и IP-адреса можно использовать для электронной идентификации граждан с целью направления им юридически значимых сообщений (например, писем, извещений, повесток) вместо используемого в настоящее время адреса места жительства.

Таким образом, в регулировании отношений, связанных с электронной идентификацией граждан, можно видеть императивный подход, состоящий в приоритете ЕСИА и ЕБС при информационном взаимодействии частных субъектов с использованием информационно-телекоммуникационной сети. В этой связи совершенно справедливо утверждение авторов, что «нормативные правовые акты должны предусматривать равный статус различных способов идентификации и аутентификации физических и юридических лиц, иных участников цифровой экономики» [29]. Поэтому законодательство должно обеспечивать возможность идентификации и аутентификации субъектов любыми технически возможными способами: электронной подписью; персональными и биометрическими данными; ЭИК; абонентским номером клиента - физического лица, пользующегося услугами подвижной радиотелефонной связи; совершением действий, однозначно идентифицирующих лицо и позволяющих достоверно установить его волеизъявление на совершение юридически значимых действий. Что касается граждан и субъектов предпринимательской деятельности, то формирование ЕСИА не влияет на их возможности использовать свои способы идентификации клиентов при заключении договоров и пополнять сведения о клиентах, пользоваться уже созданными базами клиентов в целях идентификации, а став участником информационного взаимодействия в рамках ЕСИА, они получают достоверные сведения о клиентах, что станет важным элементом в формировании доверия в информационном обществе.

Список литературы

1. Правовое регулирование экономических отношений в современных условиях развития цифровой экономики: монография / А. В. Белицкая, В. С. Белых, О. А. Беляева и др.; отв. ред. В. А. Вайпан, М. А. Егорова. – М.: Юстицинформ, 2019. – 376 с.

2. Финансовое право в условиях развития цифровой экономики: монография / К. Т. Анисина, Б. Г. Бадмаев, И. В. Бит-Шабо и др.; под ред. И. А. Цинделиани. – М.: Проспект, 2019. – 320 с.

3. Морхат П. М. Право и искусственный интеллект: монография. – М.: ЮНИТИ-ДАНА, 2018. – 544 с.

4. Энтин В. Л. Авторское право в виртуальной реальности (новые возможности и вызовы цифровой эпохи). – М.: Статут, 2017. – 216 с.

5. Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. – 2-е изд. – М.: Статут, 2016. – 640 с.

6. Жарова А. К. Право и информационные конфликты в информационно-телекоммуникационной сфере: монография. – М.: Янус-К, 2016. – 248 с.

7. Носов С. И. Право и информатизация // Юрист. – 2019. – № 4. – С. 6-13.

8. Об электронной цифровой подписи: Федеральный закон от 10 января 2002 г. № 1-ФЗ (утратил силу) // Собр. законодательства Рос. Федерации. – 2002. – № 2, ст. 127.

9. Об электронной подписи: Федеральный закон от 6 апреля 2011 г. № 63-ФЗ // Собр. законодательства Рос. Федерации. – 2011. – № 15, ст. 2036.

10. Лисаченко А. В. Идентификация субъектов гражданских правоотношений: новые проблемы и некоторые решения // Российский юридический журнал. – 2019. – № 5.

11. URL: https://digital.gov.ru/ru/activity/govservices/certification_authority.

12. О внесении изменений в Федеральный закон "О государственной регистрации недвижимости": Федеральный закон от 2 августа 2019 г. № 286-ФЗ // Собр. законодательства Рос. Федерации. – 2019. – № 31, ст. 4445

13. Дарькина М. М. Практика использования электронной цифровой подписи в предпринимательской деятельности // Право и цифровая экономика. – 2020. – № 3. – С. 28-35.

14. О внесении изменений в Федеральный закон "Об электронной подписи" и статью 1 Федерального закона "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля": Федеральный закон от 27 декабря 2019 г. № 476-ФЗ // Собр. законодательства Рос. Федерации. – 2019. – № 52, ч. I, ст. 7794.

15. Наумов В., Авакян Е., Чубурков А., Янковский Р., Белова С., Тевс М., Махносов Э., Рыбалко В. Цифровая среда доверия // Закон. – 2019. – № 9. – С. 25-38.

16. Шевцова Г. А. Опыт зарубежных стран в создании системы электронного правительства и формировании единого информационного ресурса // Делопроизводство. – 2020. – № 3. – С. 97-105.

17. Жарова А. К. Особенности процесса правовой идентификации человека в Интернете // Информационное право. – 2016. – № 3. – С. 30-35.

18. Об организации предоставления государственных и муниципальных услуг: Федеральный закон от 27 июля 2010 г. № 210-ФЗ // Собр. законодательства Рос. Федерации. – 2010. – № 31, ст. 4179.

19. 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»: Постановление Правительства РФ от 28 ноября 2011 г. № 977 // Собр. законодательства Рос. Федерации. – 2011. – № 49, ч. V, ст. 7284.

20. Об использовании простой электронной подписи при оказании государственных и муниципальных услуг: Постановление Правительства РФ от 25 января 2013 г. № 33 // Собр. законодательства Рос. Федерации. – 2013. – № 5, ст. 377.

21. Об определении состава сведений, размещаемых в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации, включая вид биометрических персональных данных, а также о внесении изменений в некоторые акты Правительства Российской Федерации: Постановление Правительства РФ от 30 июня 2018 г. № 772 // Собр. законодательства Рос. Федерации. – 2018. – № 28, ст. 4234.

22. Распоряжение Правительства РФ от 22 февраля 2018 г. № 293-р // Собр. законодательства Рос. Федерации. – 2018. – № 11, ст. 1640.

23. О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 29 декабря 2020 г. № 479-ФЗ // Собр. законодательства Рос. Федерации. – 2021. – № 1, ч. I, ст. 18.

24. О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31 декабря 2017 г. № 482-ФЗ // Собр. законодательства Рос. Федерации. – 2018. – № 1, ч. I, ст. 66.

25. URL: <https://nafi.ru/analytics/bolshinstvo-rossiyan-ne-khotyat-sdavat-dannye-dlya-edinoi-biometricheskoj-sistemy-/>.

26. URL: https://www.rbc.ru/society/07/03/2021/6044a5ff9a7947abb6a642b4?utm_source=yxnews&utm_medium=desktop.

27. Единая биометрическая система [Сайт]. URL: <https://bio.rt.ru/>.

28. Об утверждении порядка обработки, включая сбор и хранение, параметров персональных данных в целях идентификации, порядка размещения и обновления биометрических 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: Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 25 июня 2018 г. № 321 [Электронный ресурс] // Официальный интернет-портал правовой информации [Сайт]. URL: www.pravo.gov.ru.

29. Вайпан В. А. Правовое регулирование цифровой экономики // Предпринимательское право. Приложение «Право и Бизнес». – 2018. – № 1. – С. 12-17.