УДК 347.1 DOI: 10.22394/2074-7306-2020-1-2-97-103

ПРОБЛЕМЫ ПРИМЕНЕНИЯ ЦИФРОВОЙ ПОДПИСИ В ЭЛЕКТРОННОМ ДОКУМЕНТООБОРОТЕ РОССИИ

Гончаров Евгений Иванович кандидат юридических наук, доцент, Ростовский институт (филиал) ВГУЮ (РПА Минюста России) в г. Ростове-на-Дону (344000, Россия, г. Ростов-на-Дону, ул. 9-я линия/ Советская, 2/32). E-mail: ei06@bk.ru

Шатковская Татьяна Владимировна доктор юридических наук, профессор, Южно-Российский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации (344002, Россия, г. Ростов-на-Дону, ул. Пушкинская, 70/54); профессор кафедры гражданского права, Ростовский государственный экономический университет (РИНХ) (344002, Россия, Ростов-на-Дону, ул. Большая Садовая, 69). E-mail: shatkovskaya.tv@gmail.com

Аннотация

В статье рассматриваются вопросы использования цифровой подписи в условиях расширения электронного документооборота в Российской Федерации.

На основе анализа действующего российского законодательства определено назначение цифровой подписи, используемой участниками гражданского оборота. Авторами выявлены положительные и отрицательные последствия использования электронного документооборота, а также особенности его правового регулирования. В статье определены пробелы и иные недостатки действующего законодательства, регламентирующего применение цифровой подписи и указаны пути их преодоления

Ключевые слова: *электронный документооборот, цифровая подпись, гражданский оборот, цифровая безопасность, информационная безопасность, электронный обмен информации, электронная коммерция, цифровая экономика, электронный документ, информационные технологии.*

Развитие цифровой экономики в Российской Федерации (далее РФ) привело к тому, что повседневная жизнь граждан, функционирование государственных институтов и гражданского общества становится немыслимым без применения информационных технологий, в том числе, использования электронного документооборота. Сегодня цифровые технологии повсеместно внедрены в деятельность государственных органов, организаций и граждан. Расширение электронного документооборота требует соответствующего правового регулирования прежде всего для обеспечения безопасности частных и публичных интересов.

Особая социальная значимость данной проблемы и ее государственный уровень подтверждается фактом принятия В.В. Путиным указа, согласно которому обозначены приоритетные направления в развитии информационного общества в Российской Федерации

в условиях тотальной цифровизации социально-экономических отношений[1]. Для гражданского общества сформирована возможность получения онлайн-услуг в образовании, медицине, социальном секторе, а также при взаимодействии с органами государственной власти и муниципалитетами.

Активное использование хозяйствующими субъектами в гражданском обороте средств электронного документооборота, дистанционного взаимодействия с контрагентами при помощи электронного обмена информацией посредством сети Интернет, электронных платежей вызвало потребность в обеспечении достоверности сведений электронных документов, передаваемой информации и совершенных платежей.

Для реализации указанной потребности государством вводятся новые правовые средства - электронный документооборот и электронная (цифровая) подпись, выступающие не только инструментами гражданского оборота, но и приемами защиты прав и законных интересов участников правоотношений в информационно-телекоммуникационных сетях.

С формально-юридической точки зрения внедрение цифровой подписи следует рассматривать как процедуру реализации юридической нормы, направленную на достижение поставленных участниками правоотношений целей техническими средствами цифровой подписи по своему усмотрению [1, с. 87]. Иными словами, использование цифровой подписи следует отождествлять с деятельностью, направленной на достижение юридически значимых действий.

При этом обеспечение достоверности сведений электронных документов, передаваемой информации и совершенных платежей возможно достичь, применяя криптографические средства защиты [2, с. 52]. По сути, цифровая подпись и является одним из средств применения криптографии, используемым в качестве подтверждения волеизъявления участников гражданского оборота как аналог собственноручной подписи на обычном документе.

Вообще, криптография – наука, изучающая средства и способы защиты информации, существующей как на бумажном, так и на электронном носителе. В качестве таких средств и способов применяются специальные алгоритмы для шифрования и дешифрования информации, в основе которых имеется секретный ключ. Таким образом, цифровая подпись и есть тот ключ, который будет придавать достоверность и обеспечивать безопасный обмен информации.

В пределах российской юрисдикции использование цифровой подписи при заключении сделок допускается в случаях, прямо предусмотренных гражданским законодательством или соглашением участников гражданского оборота. Поэтому указание в договоре на возможность применения сторонами цифровой подписи предполагает его действительность. Так, с 1 июля 2020 года вступает в силу новая редакция закона об электронной подписи[2], согласно которой цифровую подпись допускается использовать как средство, удостоверяющее волеизъявление стороны, желающей заключить сделку с помощью электронного обмена информации[3].

---

[1] Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Официальный интернет-портал правовой информации. URL: http://www.pravo.gov.ru, 10 мая 2017 г.

[2] Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 23.06.2016) «Об электронной подписи» // Российская газета. № 75. 08.04.2011.

[3] Федеральный закон от 27.12.2019 № 476-ФЗ «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» // Российская газета. № 296. 31.12.2019.

Выбор того или иного вида цифрового подписания сделки предусматривает п. 1 ст. 160 ГК РФ[1]. В случае достижения соглашения стороны оговаривают, какая цифровая подпись будет использоваться при заключении сделки. Кроме того, соглашение может быть дополнено пунктом о порядке проверки цифровой подписи. В число обязанностей стороны сделки входит соблюдение конфиденциальности метаданных цифровой подписи, если речь идет о простой электронной подписи.

Нормативно-правовое регулирование электронной подписи как правового средства находит свое отражение в ряде нормативных актов. Основой для правового регулирования цифровой подписи выступает закон об электронной подписи, где регламентирован порядок использования и применения настоящего правового средства в гражданско-правовых отношениях при оказании государственных или муниципальных услуг, выполнении юридически значимых действий государственными органами, должностными лицами и организациями.

Определение понятийного аппарата по электронному документообороту дает закон об информации информационных технологиях и о защите информации, согласно которому формулируется значение электронного документа. Так, п. 11.1 ст. 2 указанного закона под электронным документом понимается задокументированные сведения в электронном виде, восприятие которых возможно осуществить посредством электронно-вычислительных технических средств, а также через Интернет сеть или базы данных[2].

В нотариальной деятельности при совершении юридически значимых действий с использованием электронных документов, нотариус вправе использовать усиленную квалифицированную электронную подпись в соответствии со ст. 11 Основ законодательства РФ о нотариате[3]. Так, нотариусы с 1 июля 2014 года могут удостоверять равнозначность электронного документа и бумажного носителя, переводить один вид носителя в другой и передавать гражданам на расстоянии данные документы для совершения юридически значимых действий.

Росреестр с июля 2016 года перестал выдавать документы на бумажном носителе о праве собственности на недвижимость, с этого времени сведения о недвижимости хранятся в электронном виде. Кроме того, совершать сделки с недвижимостью теперь могут лица, имеющие усиленную квалифицированную электронную подпись. В связи с этим были известны случаи мошеннических действий с недвижимостью, собственники которых и не подозревали о совершении этих сделок. Поэтому в августе 2019 года законодатель внес соответствующие изменения, согласно которым, Росреестр, перед тем как совершать действия по внесению записей в ЕГРН по поводу недвижимости, уведомляет об этом собственника, который должен подать соответствующее заявление (согласие) на подобные действия. После этого волна мошеннических действий была сведена к минимуму.

Таким образом, можно прийти к выводу, что цифровая подпись может рассматриваться в качестве юридического средства, обладающего следующими свойствами:

- универсальность, проявляющаяся в процессе реализации права как инструмент идентификации любой личности, осуществляющей подписание электронного документа;
- законность, выражающаяся в том, что адресат субъективного права, осуществляющий деятельность по применению цифровой подписи, действует в рамках дозволенного поведения, регламентированного законодательством РФ;

[1] Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 16.12.2019) // Российская газета. № 238-239. 08.12.1994.

[2] Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 02.12.2019) «Об информации, информационных технологиях и о защите информации» // Российская газета. № 165. 29.07.2006.

[3] Основы законодательства Российской Федерации о нотариате (утв. ВС РФ 11.02.1993 № 4462-1) (ред. от 27.12.2019) // Российская газета. № 49. 13.03.1993.

- волевой характер, означающий, что субъекты, реализующие права на электронную подпись, принимают волевые, а не властные решения, присущие субъектами правоприменительной деятельности;
- юридико-технического упорядочивания правоотношений гражданского оборота, состоящее в том, что процесс совершения юридически значимых действий с использованием цифровой подписи направлен на свободное и беспрепятственное пользование материальными и социальными благами.

При изучении вопросов правового регулирования цифровой подписи необходимо обратить внимание и на требования, предъявляемые к созданию, использованию, а также проверке подлинности электронной подписи. В этой связи следует отметить, что отношения по применению электронного документооборота будут иметь юридическую значимость и последствия, если используемая цифровая подпись обладает действительностью.

Простую цифровую подпись можно использовать в личном кабинете налогоплательщика или на портале Госуслуг. Она как правила находится в самом электронном документе и защищается посредством логина и пароля. В общем виде это называется метаданными. Для входа в систему электронного документооборота гражданин должен ввести уникальный логин и пароль. Возникает справедливый вопрос о безопасности хранения этих метаданных как у гражданина, так и в информационной среде, где происходит процесс идентификации и допуск к соответствующей базе данных.

Методика хранения логина и пароля в системе электронного документооборота разработана еще в 2011 году Приказом Минкомсвязи России[1]. Настоящим документом закрепляется законодательное определение метаданных, согласно которым они представляют собой как средства идентификации данных, так и историю, совершенную с документами.

Если проводить аналогию с хранением документов на бумажном носителе, то безопасность данных при таком хранении обеспечивается посредством специальных помещений – архивов, находящихся под охраной и к которым устанавливается специальный допуск уполномоченных должностных лиц.

С электронными документами ситуация иная, это информационное пространство, к которому имеют доступ неограниченное количество лиц, если данная информация хранится на серверах в сетях Интернет.

При работе с электронными документами нередко возникает неопределенность в применимости таких понятий, как: «копия», «подлинник» или «дубликат» документа. Даная терминология однозначно использовалась к документам на бумажном носителе. Однако электронный документ не может рассматриваться в этих значениях, так как в любом случае его передачи или копирования, сохраняются исходные данные содержащиеся в свойствах этого документа (например, формат, размер файла, подлинность сертификата электронной подписи) [3, с. 22].

По мере развития электронного документооборота в системе государственной власти и местного самоуправления происходит и увеличение объема хранимой электронной информации. Во избежание потери данных постоянно совершается их резервирование, применяются разновидности носителей информации, которые в свою очередь ограничены по времени и объему хранения. Любой сбой носителя приводит к потере большого объема данных. При этом присутствует и потенциальная возможность взлома или перехвата информации злоумышленниками.

---

[1] Приказ Минкомсвязи РФ от 02.09.2011 № 221 «Об утверждении Требований к информационным системам электронного документооборота федеральных органов исполнительной власти, учитывающих в том числе необходимость обработки посредством данных систем служебной информации ограниченного распространения» // Российская газета. № 261. 21.11.2011.

Возрастающий риск утраты сведений электронного документооборота, заставляет государство и других участников документооборота совершенствовать средства защиты и хранения информации.

Одним из серьезных шагов в этом направлении считаем разработку новейших средств идентификации личности, а также замену метаданных - биометрическими данными. К примеру, в нотариальной системе США, в частности, в штате Вирджиния с 2012 года осуществляется технология дистанционного получения нотариальных услуг гражданином при помощи средств удаленной видеофиксации личности гражданина [4, с. 31].

Как верно отмечается в юридической литературе, биометрию можно считать не обычными персональными данными, а результатом проведенной обработки данных при помощи физиологических или поведенческих параметров людей как средства идентификации личности [5, с. 109]. Изначально биометрия использовалась в криминалистике, теперь эта возможность интегрирована в гаджетах, используемыми гражданами для входа в устройство.

Сегодня можно совершать ряд онлайн-платежей и пользоваться онлайн-услугами при помощи идентификации с помощью отпечатка пальца, радужной оболочки глаза, распознавания лица человека или данных ДНК.

При этом, с одной стороны, отпадает необходимость хранения логина и пароля гражданина, а также возможность их утраты или хищения. С другой стороны, это не является препятствием для злоумышленников перехватить (скопировать) процедуру идентификации личности при помощи средств биометрии, так как процесс распознавания личности моделируется при помощи специального кода или ключа, записанного в базе. Поэтому опять возникает проблема хранения метаданных в информационном пространстве, так как биометрия есть прообраз логина и пароля, выраженных в зашифрованном виде с применением того же криптографического алгоритма.

В связи с этим, идентификация гражданина посредством биометрии должна получить особую правовую регламентация. Законодателем должна быть проведена тщательная работа по внедрению в повседневную жизнь российского общества новых средств идентификации личности, обеспечив ее надежными юридическими средствами защиты [8, с. 31-32].

Сегодня биометрические данные гражданина могут использоваться в соответствии с положениями ст. 11 закона о персональных данных[1], где упоминается об их обработке только с согласия гражданина. Однако есть случаи, предусмотренные законом, когда это согласие не требуется.

Кроме того, в действующем законодательстве можно обратить внимание на множество подзаконных актов, регламентирующих использование в России биометрии в Единой системе идентификации и аутентификации (ЕСИА) и Единой биометрической системе (ЕБС). Однако со стороны законодателя не уделяется внимание обеспечению безопасности процедуры идентификации личности и хранения криптографического алгоритма в информационных системах или базах данных государства.

Безусловно, что отмечается многими авторами, биометрическая идентификация позволит беспрепятственно принимать участие во всех сферах жизни общества, в том числе и в сфере предоставления услуг населению [6, с. 43]. И это общемировая тенденция развития современного цивилизованного общества. Поэтому наряду с новыми средствами идентификации личности и обмена информацией, следует и рецепировать зарубежный опыт, и создавать собственные разработки по защите такой информации. Тогда это будет соответствовать конституционным основам Российского государства и обеспечивать конституционные права и свободы человека и гражданина в РФ.

---

[1] Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) «О персональных данных» // Российская газета. № 165. 29.07.2006.

Подводя итоги, отметим, что электронный документооборот будет стремительно развиваться в условиях информационной революции и массового распространения цифровых технологий. И акцент в правовом регулировании этого процесса следует делать в первую очередь на защите содержания электронного документа [7, с. 45].

Вышеназванная проблема актуализируется в условиях цифровой безграмотности значительной части российского общества, а также психологической боязни резкого перехода на новый уклад жизни, где в ней не остается ничего бумажного и овеществленного. Поэтому внедрение новых информационных технологий должно проходить последовательно и на основе доверия граждан России.

Такое доверие достигается проведением официальных разъяснений и обучения по порядку применения и пользования средствами цифровой подписи, электронных документов. И самое главное, обеспечением безопасности электронного документооборота, гарантированным государством. Такие гарантии во многом достигаются юридическими средствами. К примеру, разработкой и внедрением нормативной базы, обеспечивающей надежные средства защиты хранимой или передаваемой информации, ключей безопасности, средств электронной идентификации личности.

В этой связи предлагаем разработку и принятие Федерального закона «Об электронном документообороте в Российской Федерации», в котором следует четко закрепить понятийный аппарат в данной сфере, определить область нормативно-правового регулирования, а также необходимые средства защиты электронных документов и средств криптографического шифрования, в том числе и цифровой подписи.

Литература

1. *Николюкин С.В.* Использование электронной подписи как форма реализации права // Современный юрист. 2016. № 1. С. 86 – 103.
2. *Тарасов А.М.* Криптография и электронная цифровая подпись // Российский следователь. 2014. № 1. С. 50 –64.
3. *Гончаров Е.И.* Актуальные проблемы ведения электронного документооборота в Российской Федерации // В сборнике: Наука и технологии: стратегия развития. Сборник научных статей. Под общей редакцией В.А. Козловой, И.В. Кожан. Ростов н/Д., 2019. С. 20 –24.
4. *Даниленков А.В.* К вопросу об интернет-правовом регулировании нотариальной деятельности // Нотариус. 2015. № 7. С. 29 – 33.
5. *Рассолов И.М., Чубукова С.Г., Микурова И.В.* Биометрия в контексте персональных данных и генетической информации: правовые проблемы // Lex russica. 2019. № 1. С. 108 –118.
6. *Чеджемов С.Р., Золоева З.Т.* Биометрические персональные данные человека - средство защиты его прав или тотального контроля государства над личностью? // Конституционное и муниципальное право. 2019. № 11. С. 39 – 43.
7. *Бородин М.В.* Технология цифровой подписи в электронном документообороте // Информационное право. 2015. № 3. С. 42 – 45.
8. Шатковская Т.В. Правовое обеспечение индивидуализации субъектов права как условие инновационного развития российской экономики // Северо-Кавказский юридический вестник. 2016. № 3. С. 24 – 32.

Goncharov Evgeniy Ivanovich, candidate of law, associate Professor Rostov Institute (branch) of Vladimir state University (RPA of the Ministry of justice of Russia), in Rostov-on-don (344000, Rostov region, Rostov-on-Don, 9-ya Liniya street / Sovetskaya, 2/32). E-mail: ei06@bk.ru

Shatkovskaya Tatiana Vladimirovna, Ph.D. Doctor of Law, Professor of the department of theory and history of law and state, the South-Russian Institute of Management – branch of the Presidential Academy of the National Economy and Public Administration (70/54, Pushkinskaya St., Rostov-on-Don, 344002, Russian Federation); Professor, Department of Civil Law, Rostov State University of Economics (RINH) (69, Bolshaya Sadovaya St., Rostov-on-Don, 344002, Russian Federation). E-mail: shatkovskaya.tv@gmail.com

PROBLEMS OF DIGITAL SIGNATURE APPLICATION IN RUSSIA AS ELECTRONIC DOCUMENT

Abstract

The article discusses the use of electronic digital signatures in the context of the expansion of electronic document management in the Russian Federation. Based on the analysis of the current Russian legislation, the purpose of the digital signature used by the participants of the civil turnover is determined. The authors identified the positive and negative consequences of the use of electronic document management, as well as the features of its legal regulation. The article identifies gaps and other shortcomings of the current legislation governing the use of digital signatures and indicates ways to overcome them.

Keywords: *electronic document management, digital signature, civil circulation, digital security, information security, electronic information interchange, electronic commerce, digital economy, electronic document, information technology.*

References

1. Nikolyukin S.V. Ispol'zovanie elektronnoj podpisi kak forma realizacii prava // Sovremennyj yurist. 2016. № 1. P. 86 – 103.
2. Tarasov A.M. Kriptografiya i elektronnaya cifrovaya podpis' // Rossijskij sledovatel'. 2014. № 1. P. 50 – 64.
3. Goncharov E.I. Aktual'nye problemy vedeniya elektronnogo dokumentooborota v Rossijskoj Federacii // V sbornike: Nauka i tekhnologii: strategiya razvitiya. Sbornik nauchnyh statej. Pod obshchej redakciej V.A. Kozlovoj, I.V. Kozhan. Rostov-na-Donu, 2019. P. 20 – 24.
4. Danilenkov A.V. K voprosu ob internet-pravovom regulirovanii notarial'noj deyatel'nosti // Notarius. 2015. № 7. P. 29 – 33.
5. Rassolov I.M., CHubukova S.G., Mikurova I.V. Biometriya v kontekste personal'nyh dannyh i geneticheskoj informacii: pravovye problemy // Lex russica. 2019. № 1. P. 108 – 118.
6. CHedzhemov S.R., Zoloeva Z.T. Biometricheskie personal'nye dannye cheloveka - sredstvo zashchity ego prav ili total'nogo kontrolya gosudarstva nad lichnost'yu? // Konstitucionnoe i municipal'noe pravo. 2019. № 11. P. 39 – 43.
7. Borodin M.V. Tekhnologiya cifrovoj podpisi v elektronnom dokumentooborote // Informacionnoe pravo. 2015. № 3. P. 42 – 45.
8. SHatkovskaya T.V. Pravovoe obespechenie individualizacii sub"ektov prava kak uslovie innovacionnogo razvitiya rossijskoj ekonomiki // Severo-Kavkazskij yuridicheskij vestnik. 2016. № 3. P. 24 – 32.