

DOI: 10.17803/1729-5920.2020.164.7.115-126

Д. А. Ловцов*,
Л. В. Терентьева**

Правовое регулирование международных коммерческих электронных контрактов. Технологические и правовые аспекты электронной подписи¹

Аннотация. В современных реалиях перевода документооборота в цифровую плоскость вопросы действительности договоров, заключаемых в электронной форме, а также условия признания электронной подписи приобретают особую значимость. В этой связи авторы обращаются к исследованию положений Нью-Йоркской конвенции об использовании электронных сообщений в международных договорах 2005 г., а также иных международных торговых договоров для выяснения вопроса их применимости к трансграничным контрактам, заключенным в электронной форме.

В статье авторами ставится вопрос о действительности электронной трансграничной сделки, подпадающей под регулирование Венской конвенции о договорах международной купли-продажи товаров 1980 г., оговорка к которой о недопустимости заключения договора не в письменной, а в любой форме, сделанная СССР, продолжает действовать. В этой связи авторы исследуют возможность толкования ст. 13 Венской конвенции 1980 г., содержащей определение понятия «письменная форма», вне общего правила толкования положений Венской конвенции 1980 г., предусмотренного в ст. 7.

В результате сравнительного анализа национальных и международно-правовых норм, а также норм «мягкого права», регулирующих электронный документооборот, авторы выявляют ряд проблем, возникающих вследствие отсутствия конкретизации механизма признания иностранной электронной подписи в РФ, а также выдвигают предложения по их решению. С этой целью авторы исследуют возможности разработки международных стандартов совместимости технологических алгоритмов электронных цифровых подписей, использующих асимметричную схему, на основе которых может быть осуществлено признание иностранных сертификатов ключей электронных подписей.

Ключевые слова: международный коммерческий контракт в электронной форме; электронный документооборот; электронная подпись; электронная цифровая подпись; сертификат ключа подписи; удостоверяющий центр; блокчейн; письменная форма; местонахождение коммерческих предприятий сторон; международные стандарты.

Для цитирования: Ловцов Д. А., Терентьева Л. В. Правовое регулирование международных коммерческих электронных контрактов. Технологические и правовые аспекты электронной подписи // Lex russica. — 2020. — Т. 73. — № 7. — С. 115—126. — DOI: 10.17803/1729-5920.2020.164.7.115-126.

¹ Статья подготовлена при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16061.

© Ловцов Д. А., Терентьева Л. В., 2020

* Ловцов Дмитрий Анатольевич, доктор технических наук, профессор, заведующий кафедрой информационного права, информатики и математики Российского государственного университета правосудия Новочеремушкинская ул., д. 69а, г. Москва, Россия, 117418
dal-1206@mail.ru

** Терентьева Людмила Вячеславовна, кандидат юридических наук, доцент, доцент кафедры международного частного права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993
terentevamila@mail.ru

Legal Regulation of International Commercial Electronic Contracts. Technological and Legal Aspects of Electronic Signature²

Dmitriy A. Lovtsov, Dr. Sci. (Technical Sciences), Professor, Head of the Department of Information Law, Informatics and Mathematics, Russian State University of Justice
ul. Novocheryomushkinskaya, d. 69a, Moscow, Russia, 117418
dal-1206@mail.ru

Lyudmila V. Terenteva, Cand. Sci. (Law), Docent, Associate Professor of the Department of International Private Law, Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
terentevamila@mail.ru

Abstract. In the modern realities of converting document flow to the digital plane, the issues of validity of contracts concluded in electronic form, as well as the conditions for recognizing an electronic signature, are of particular importance. In this regard, the authors turn to the study of the provisions of the United Nations Convention on the Use of Electronic Communications in International Contracts of 2005, as well as other international trade agreements to clarify their applicability to cross-border contracts concluded in electronic form.

In the paper, the authors raise the question of the validity of an electronic cross-border transaction that falls under the regulation of the Vienna Convention on Contracts for the International Sale of Goods of 1980, the USSR reservation to which on the inadmissibility of concluding a contract not in writing, but in any form, continues to apply. In this regard, the authors explore the possibility of interpreting article 13 of the 1980 Vienna Convention containing the definition of the "written form", outside of the general rule of interpretation of the provisions of the 1980 Vienna Convention provided for in article 7.

Based on the comparative analysis of national and international legal norms, norms of soft law regulating electronic documents, the authors reveal a number of problems arising from the lack of specificity of the mechanism of recognition of foreign electronic signatures in Russia and put forward proposals for their solution. To this end, the authors explore the possibilities of developing international standards for the compatibility of technological algorithms for electronic digital signatures using an asymmetric scheme, based on which foreign certificates of electronic signature keys can be recognized.

Keywords: international commercial contract in electronic form; electronic document; electronic signature; digital signature; signature key certificate; certification authority; blockchain; writing; location of business of the parties; international standards.

Cite as: Lovtsov DA, Terenteva LV. Pravovoe regulirovanie mezhdunarodnykh kommercheskikh elektronnykh kontraktov. Tekhnologicheskie i pravovye aspekty elektronnoy podpisi [Legal Regulation of International Commercial Electronic Contracts. Technological and Legal Aspects of Electronic Signature]. *Lex russica*. 2020;73(7):115-126. DOI: 10.17803/1729-5920.2020.164.7.115-126. (In Russ., abstract in Eng.)

I. Понятие «письменная форма» в соответствии с национальными и международными нормами

До ноября 2013 г. гражданское законодательство РФ предусматривало недействительность внешнеэкономической сделки вследствие несоблюдения ее простой письменной формы. Исключение данного положения из гражданского законодательства тем не менее не предполагает допущения, что внешнеэкономическая или международная коммерческая сделка может быть заключена в устной или иной форме, альтернативной письменной. В отношении международных

коммерческих сделок будет действовать общее правило, предусмотренное в п. 1 ст. 161 ГК РФ, о том, что если сделки заключаются юридическими лицами между собой и/или с гражданами, то данные сделки должны совершаться в простой письменной форме. Если же письменная форма не соблюдена, то в соответствии со ст. 162 ГК РФ стороны в случае спора не могут ссылаться в подтверждение сделки и ее условий на свидетельские показания, но в то же время вправе приводить письменные и другие доказательства.

Таким образом, требования о необходимости соблюдения письменной формы междуна-

² The reported study was funded by RFBR according to the research project № 18-29-16061.

родных коммерческих сделок фактически не снимаются. Перестают действовать последствия в виде недействительности договора при несоблюдении его письменной формы.

Следует заметить, что, несмотря на либерализацию гражданского законодательства в отношении формы заключения внешнеэкономических сделок, оговорка, сделанная СССР, о неприменимости положения Венской конвенции о договорах международной купли-продажи товаров 1980 г. (далее — Венская конвенция 1980 г.), предусматривающего возможность заключать договор не в письменной, а в любой форме, если хотя бы одна из сторон договора имеет свое коммерческое предприятие в СССР (постановление ВС СССР от 23.05.1990 № 1511-1)³, продолжает действовать.

В этой связи возникает вопрос о возможности применения Венской конвенции 1980 г. к трансграничной сделке, совершенной в электронной форме. Статья 11 Венской конвенции 1980 г. предусматривает общий порядок, включающий требование о заключении и подтверждении договора в письменной форме, а также подчинении иному требованию в отношении формы. В том случае, если в законодательстве государства-участника содержатся императивные положения о недопустимости заключения, изменения, расторжения договора не в письменной форме, государство вправе сделать оговорку к указанной Конвенции о неприменинии к договорам с участием стороны, имеющей местонахождение коммерческого предприятия в данном государстве, статей, допускающих возможность совершения сделок не в письменной, а любой иной форме.

В Венской конвенции 1980 г. предложено понятие «письменная форма», под которой в ст. 13 понимаются «также сообщения по телеграфу и телетайпу».

В контексте произошедших изменений национального законодательства (исключение из ГК РФ понятия «внешнеэкономическая сделка» и отмена последствий в виде недействительности в результате несоблюдения письменной формы внешнеэкономической сделки) В. А. Канашевский полагает, что правило об

обязательной письменной форме контракта купли-продажи (подпадающего под действие Венской конвенции 1980 г. с участием российского лица) должно соблюдаться до тех пор, пока Россия не отозвала свое заявление о неприменимости заключения, изменения или расторжения договора не в письменной, а в любой иной форме⁴. В этой связи, по мнению ученого, факсимильная связь в соответствии с буквальным толкованием Венской конвенции 1980 г. не относится к письменной форме, хотя автор и допускает оспоримость данной позиции в связи с тем, что в момент разработки Венской конвенции 1980 г. факсимильная связь не была распространена. Следует отметить, что в момент разработки Венской конвенции 1980 г. способы заключения контрактов, альтернативные бумажному документообороту, не исчерпывались лишь перечисленными в ст. 13 телеграфом или телетайпом. Так, уже после 1978 г., когда была утверждена унификация международного стандарта электросвязи МСЭ (ССИТ) в отношении факсимильных аппаратов, факсимильная связь стала массовым видом связи, позволившим многим коммерческим и государственным организациям начать активно использовать ее возможности в своей работе⁵.

Формулировка ст. 13 Венской конвенции 1980 г. «для целей настоящей Конвенции под «письменной формой» понимаются также сообщения по телеграфу и телетайпу» представляется несколько противоречивой. С одной стороны, статья содержит в себе словосочетание «для целей настоящей Конвенции», которое указывает на необходимость толкования понятия письменной формы в соответствии с общим правилом толкования положений Венской конвенции, предусмотренным в ст. 7, а именно учитывая ее международный характер и необходимость содействовать достижению единообразия в ее применении и соблюдению добросовестности в международной торговле. С другой стороны, использование слова «также» явно указывает на неполный перечень допустимых форм письменных документов и возможность в связи с этим дополнять его в

³ Ведомости Съезда народных депутатов СССР и Верховного Совета СССР. 23.05.1990. № 23. Ст. 428.

⁴ Канашевский В. А. Международные сделки: правовое регулирование. М. : Международные отношения, 2019. С. 229.

⁵ Альтергоп А., Панфилов Д., Шаронин С. Факсимильная связь на базе компьютерной телефонии // Сети/Network world. 1997. № 1. URL: <https://www.osp.ru/nets/1997/01/142127/> (дата обращения: 16.04.2020) ; Все о факсах // URL: http://www.imperium.ru/new_page_20.htm (дата обращения: 16.04.2020).

соответствии с национальным правом соответствующего государства.

На открытый неисчерпывающий перечень письменных сообщений, предусмотренных в ст. 13 Венской конвенции 1980 г., указывал в свое время М. М. Розенберг, решая вопрос о допустимости причисления факсимильных сообщений к письменной форме⁶. Аналогичного подхода придерживаются арбитражные суды, признающие заключенными в письменной форме контракты, представленные заявителем в форме факсимиле-документа, при толковании положений о письменной форме Венской конвенции 1980 г., опираясь на российское гражданское законодательство⁷.

В данном случае должно действовать общее правило, закрепленное в доктрине, в рамках которого предусмотрено, что, поскольку обязательность соблюдения письменной формы вытекает из норм национального права государств, сделавших оговорку, этими нормами (а не Венской конвенцией) определяются и требования к ее соблюдению⁸. Таким образом, толкование понятия «письменная форма» не должно осуществляться в соответствии с общим правилом толкования положений Венской конвенции, предусмотренным в ст. 7, учитывая ее международный характер. Если та или иная форма заключения сделки не предусмотрена в ст. 13 Венской конвенции 1980 г., контракт не может считаться заключенным не в письменной форме при условии, что такая форма удовлетворяет требованиям национального законодательства государства, сделавшего оговорку в отношении обязательности письменной формы. Если национальный закон допускает факсимильную или электронную форму заключения сделок, то заключен ли договор в письменной форме, будет решаться в соответствии с правом государства, сделавшего данную оговорку.

Возникает также вопрос, можно ли заявление СССР при присоединении к Венской конвенции 1980 г. о неприменимости ее положений, допускающих заключение, изменение или прекращение соглашения сторон не только в письменной форме, считать основанием несоблюдения простой письменной формы, которое

в силу п. 2 ст. 162 ГК РФ является прямым указанием в законе, обуславливающим недействительность сделки. Иными словами, должна ли сделка международной купли-продажи товаров быть признана недействительной в силу того, что ее форма не удовлетворяет требованиям Венской конвенции 1980 г., или же к данной сделке должны быть применены последствия несоблюдения простой письменной формы, предусмотренные пунктом 1 ст. 162 ГК РФ, в виде лишения сторон права в случае спора ссылаться в подтверждение сделки и ее условий на свидетельские показания.

Статья 12 Венской конвенции 1980 г. оговаривает недопустимость заключения договора не в письменной форме, если одна из ее сторон имеет коммерческое предприятие в государстве, сделавшем оговорку относительно обязательности письменной формы сделки, но не указывает на последствия несоблюдения этого правила. Поскольку Венская конвенция 1980 г. не применяется к действительности самого договора в соответствии с п. «а» ст. 4, в данном случае, как представляется, вопрос относительно заключения договора и средств доказывания будет решаться в соответствии с национальным законодательством. Если таковым будет российское право, то факт заключения договора будет доказываться на основании письменных и иных доказательств в соответствии с п. 1 ст. 162 ГК РФ. В то же время представляется сомнительным применение к такой сделке положений Венской конвенции 1980 г., в которой предусмотрена недопустимость ее применения к заключению договора не в письменной форме, если об этом государством сделана оговорка.

II. Сделки, заключаемые в электронной форме

Следует заметить, что до 1 октября 2019 г., когда вступили в силу изменения в абз. 2 п. 1 ст. 160 ГК РФ, в доктрине неоднозначно решался вопрос о допустимости приравнивания договора, заключенного путем обмена электронными документами, к письменной форме. По мнению В. А. Канашевского, в соответствии с п. 2 ст. 434

⁶ Розенберг М. Г. Международная купля-продажа товаров : Комментарий к законодательству и практике разрешения споров. М. : Контракт: Инфра-М, 2001. С. 36.

⁷ Постановление Федерального арбитражного суда Поволжского округа от 4 декабря 2007 г. № А65-10280/2006.

⁸ Венская конвенция о договорах международной купли-продажи товаров : комментарий / под ред. М. М. Богуславского. М., 1994. С. 42—43 ; Розенберг М. Г. Указ. соч. С. 36.

ГК РФ договор в письменной форме может быть заключен также путем обмена электронными документами, передаваемыми по каналам связи (включая электронную почту), позволяющими достоверно установить, что документ исходит от стороны по договору⁹. В то же время А. И. Савельев отмечал, что соблюдение требований п. 2 ст. 434 ГК РФ, а вместе с тем наличие или отсутствие простой письменной формы в договоре, заключенном посредством сети Интернет, зависит от того, имел ли место какой-либо из предусмотренных законодательством видов электронной подписи¹⁰.

Абзац 1 п. 1 ст. 160 ГК РФ, предусматривающий, что сделка должна быть совершена путем составления документа, выражающего ее содержание и подписанного лицом или лицами, совершающими сделку, либо должным образом уполномоченными ими лицами, и пункт 2 ст. 434 ГК РФ соотносятся как общая и специальная норма, где специальной является норма, регулирующая порядок заключения договора как вид сделки. В то же время ст. 434 ГК РФ, регламентирующая форму заключения договора до 2019 г., не содержала понятия письменной формы, следовательно, при решении вопроса относительно формы заключения договора статьи 434 и 160 ГК РФ должны были применяться комплексно.

Именно данный подход был учтен при внесении изменений в п. 2 ст. 434 ГК РФ, который предусматривает, что договор в письменной форме может быть заключен путем составления одного документа (в том числе электронного), подписанного сторонами, или обмена письмами, телеграммами, электронными документами либо иными данными в соответствии с абз. 2 п. 1 ст. 160 ГК РФ.

В соответствии с редакцией п. 2 ст. 160 ГК РФ до 2019 г. использование при совершении сделок электронной подписи либо иного аналога собственноручной подписи допускалось только в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон.

В этой связи из тех видов электронной подписи, которые предусмотрены в Федеральном законе от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»¹¹, для удовлетворения

требований п. 2 ст. 160 ГК РФ, при отсутствии специального соглашения сторон об определенном виде подписи, в соответствии с п. 2 ст. 160 ГК РФ в редакции до 2019 г. подходила исключительно усиленная квалифицированная подпись, которая в силу п. 1 ст. 6 Федерального закона «Об электронной подписи» признается равнозначной собственноручной подписи.

Измененная редакция п. 1 ст. 160 ГК РФ позволяет сделать допущение, что письменная форма электронной сделки будет считаться соблюденной и при использовании простой и/или неквалифицированной электронных подписей, в отношении которых законодателем принят обратный подход, а именно: электронные документы, подписанные такими видами электронной подписи, признаются равнозначными подписанным вручную документам на бумажном носителе, если это установлено федеральным законом или соглашением сторон.

В соответствии с п. 1 ст. 160 ГК РФ письменная форма сделки, заключаемая электронным способом, будет считаться выполненной, если возможно воспроизведение сделки на материальном носителе и возможна достоверная идентификация лица, выразившего волю на ее заключение.

В определенной степени такой порядок использования электронной подписи воспроизводит положения Нью-Йоркской конвенции «Об использовании электронных сообщений в международных договорах» 2005 г. (далее — Нью-Йоркская конвенция 2005 г.), в ст. 9 которой предусмотрено, что договор в виде электронного сообщения данных будет считаться заключенным в письменной форме, если содержащаяся в нем информация является доступной для ее последующего использования. Требования же в отношении подписи будут считаться выполненными, если:

- а) использован какой-либо способ для идентификации этой стороны и указания намерения этой стороны в отношении информации, содержащейся в электронном сообщении; б) и этот способ:
 - либо является настолько надежным, насколько это соответствует цели, для которой электронное сообщение было подготовлено или передано, с учетом всех обстоятельств,

⁹ Канашевский В. А. Указ. соч. С. 58.

¹⁰ Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. М. : Статут, 2014.

¹¹ СЗ РФ. 2011. № 15. Ст. 2036.

включая любые соответствующие договоренности;
— либо, как это фактически продемонстрировано на основании самого способа или с помощью дополнительных доказательств, позволил выполнить функции, описанные в пп. «а».

В доктрине отмечено, что, поскольку сама Нью-Йоркская конвенция 2005 г. не решает вопрос о том, какое право должно быть применено при решении вопроса о соблюдении предусмотренных в Конвенции правил, в качестве такового предложено применимое к договору право¹².

Конвенционная модель совпадает с национальной в части требования в отношении идентификации лица, выразившего волю на заключение сделки. Различия в данных подходах заключаются в формах выражения доступности информации для последующего использования. Если национальный закон предусматривает необходимость воспроизведения на материальном носителе, то в Нью-Йоркской конвенции 2005 г. не уточняется, в каком виде должна быть представлена информация, чтобы считаться доступной для последующего использования. Дополнительно в Нью-Йоркской конвенции 2005 г. предусматривается необходимость проверки надежности способа идентификации лица, который должен отвечать цели, для которой электронное сообщение было подготовлено или передано, либо с помощью дополнительных доказательств позволять осуществлять идентификацию данных лиц. Следует отметить, что в абз. 2 п. 1 ст. 160 ГК РФ способы идентификации не перечислены, но, как представляется, надежность данных способов презюмируется.

В этой связи международный подход к пониманию письменной формы документа представляется более широким по сравнению с национальным. В том случае, если стороны предусмотрят в своем соглашении применение Нью-Йоркской конвенции 2005 г., требования к признанию иностранной электронной подписи будут основаны именно на положениях данной конвенции, а не Федерального закона «Об электронной подписи» и ст. 160 ГК РФ.

III. Признание иностранной электронной подписи

Федеральный закон «Об электронной подписи» 2011 г. предусматривает порядок признания электронных подписей, созданных в соответствии с нормами иностранного права и международными стандартами. Статья 18 ранее действовавшего Федерального закона «Об электронной цифровой подписи» 2002 г. предусматривала необходимость выполнения установленных законодательством РФ процедур признания юридического значения иностранных документов при признании удостоверенного в соответствии с законодательством иностранного государства иностранного сертификата ключа подписи, в котором этот сертификат ключа подписи зарегистрирован.

Процедура признания юридического значения иностранных документов происходит посредством консульской легализации или апостилирования в соответствии с Гаагской конвенцией, отменяющей требование легализации иностранных официальных документов, 1961 г. Указанное положение вносило определенную неясность: во-первых, в отношении объекта признания юридического значения — должен ли это быть иностранный сертификат или сама электронная подпись, и, во-вторых, каким образом могла бы осуществляться данная процедура в отношении иностранного сертификата, имеющего электронную форму.

В настоящий момент процедура признания юридического значения документов, имеющих отношение к электронной подписи, в действующей редакции Федерального закона «Об электронной подписи» 2011 г. не предусмотрена. В пункте 2 ст. 7 указанного Закона закреплен общий подход недискриминации электронной подписи и подписанного ею электронного документа только на том основании, что сертификат ключа проверки электронной подписи выдан в соответствии с нормами иностранного права.

Данный подход в определенной степени созвучен с п. 1 ст. 12 Типового закона ЮНСИТРАЛ об электронных подписях 2001 г. (далее — Типовой закон ЮНСИТРАЛ 2001 г.), в соответствии с которым при определении того, обладает ли сертификат или электронная подпись юридической силой, не должны учитываться ни место выдачи сертификата либо создания или исполь-

¹² Стригунова Д. П. Правовое регулирование международных коммерческих договоров : монография : в 2 т. 2-е изд., перераб. и доп. М. : Юстицинформ, 2018. Т. 2.

зования электронной подписи, ни местонахождение коммерческого предприятия эмитента или подписавшего.

Имеют место различия в условиях признания подписей, созданных в соответствии с иностранным правом или международными стандартами, в Федеральном законе «Об электронной подписи» и Типовом законе ЮНСИТРАЛ 2001 г. Так, пункты 2 и 3 ст. 12 Типового закона ЮНСИТРАЛ 2001 г. предусматривают равную юридическую силу иностранного сертификата и электронной подписи с сертификатом и электронной подписью соответствующего государства, если они обеспечивают по существу эквивалентный уровень надежности. При определении того, обеспечивает ли сертификат или электронная подпись по существу эквивалентный уровень надежности, пункт 4 ст. 12 Типового закона ЮНСИТРАЛ 2001 г. рекомендует учитывать признанные международные стандарты и любые другие соответствующие факторы.

В пункте 1 ст. 7 Федерального закона «Об электронной подписи» 2011 г. также говорится о признании электронных подписей, созданных в соответствии с нормами права иностранного государства и международными стандартами, но при этом данные подписи будут относиться к электронным подписям того вида, признакам которого они соответствуют на основании Федерального закона «Об электронной подписи» 2011 г. Таким образом, вопрос функционального назначения иностранной электронной подписи, а именно, подтверждает ли подпись только факт ее формирования (простая электронная подпись) или позволяет также определить подписавшее лицо и факт отсутствия внесения изменений в электронный документ после момента его подписания (усиленная неквалифицированная подпись), будет решаться в соответствии с российским правом. Следует отметить, что решение данного вопроса может быть весьма затруднительным в отношении квалифицированной электронной подписи, которая в соответствии с федеральным законом должна отвечать требованиям, предусмотренным для усиленных неквалифицированных

подписей, а также двум дополнительным условиям. К таковым относятся необходимость получения квалифицированного сертификата, в котором указывается ключ проверки такой электронной подписи, а также использование средств электронной подписи для создания и проверки электронной подписи, получивших подтверждение соответствия требованиям, установленным в Федеральном законе «Об электронной подписи» 2011 г.

Проблематичность соблюдения данных требований видится в том, что в разных государствах используются различные стандарты криптографических алгоритмов, лежащих в основе формирования открытого и закрытого ключа электронной подписи. Квалифицированный сертификат ключа проверки электронной подписи выдается аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи. Аккредитация удостоверяющего центра, в свою очередь, проводится уполномоченным федеральным органом Минкомсвязи России. Подобные сложности отмечены и в Рекомендации Европейской экономической комиссии № 37 в отношении функциональной совместимости подписанных цифровых документов. Указанные в документе сложности могут иметь место при обеспечении функциональной совместимости электронных подписей из-за разного восприятия программами форматов полученной цифровой подписи; при определении назначения подписи, а именно, удостоверяет ли подпись подлинность документа или же только обозначает согласие подписанта с содержанием документа, и т.п.¹³

В доктрине отмечено, что признание иностранных сертификатов часто обеспечивается методом «перекрестной сертификации», для которой характерно, чтобы в основном эквивалентные друг другу сертификационные органы признавали услуги, оказываемые каждым из них¹⁴. В то же время авторы отмечают возможность возникновения проблем в связи, напри-

¹³ ECE/TRADE/C/CEFACT/2010/14/Rev.1 Рекомендация ЕЭК ООН № 37 в отношении функциональной совместимости подписанных цифровых документов // URL: <http://docplayer.ru/81871052-Rekomendaciya-37-rekomendaciya-v-otnoshenii-funkcionalnoy-sovmestimosti-podpisannyh-cifrovyyh-dokumentov.html> (дата обращения: 16.04.2020).

¹⁴ Коржов В. Ю., Захарова Н. А. Комментарий к Федеральному закону от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» / под ред. Н. Н. Ковалевой. Гарант, 2016.

мер, с определением того, кто допустил нарушения, приведшие к убыткам, и на чьи именно заверения полагался пользователь¹⁵.

В доктрине проведена классификация подходов к признанию иностранных электронных подписей. Наиболее гибкой исследователям представляется американская модель принципа недискриминации иностранных электронных подписей, а также права сторон избирать приемлемые способы аутентификации и доказывать в суде их действительность при безусловном соблюдении публичного порядка страны признания¹⁶.

В то же время при решении вопроса относительно возможности переноса указанного подхода на российскую правовую почву необходимо понять, не будет ли принцип недискриминации иностранных подписей, применительно к которым может быть снижен порог технологических требований, в свою очередь, дискриминировать порядок признания электронных подписей, созданных в соответствии с требованиями российского законодательства.

Способ оценки эквивалентного уровня надежности электронной подписи и сертификата, предусмотренный в ст. 12 Типового закона ЮНСИТРАЛ 2001 г., также требует дополнительной конкретизации в отношении разработки международных стандартов, подтверждающих соответствующий уровень надежности электронной подписи.

В этой связи для поиска адекватной правовой основы признания иностранной электронной подписи в РФ необходимо исследовать проблему международной стандартизации условий совместимости технологических алгоритмов электронных подписей и сертификатов, принимая во внимание их различное функциональное назначение, которое может как ограничиваться только подтверждением согласия подписанта с содержанием документа, так и наряду с этим предусматривать подтверждение подлинности и неизменности документа после подписания.

IV. Проблема совместимости технологических алгоритмов электронных подписей и сертификатов

Признание иностранных сертификатов ключей электронных цифровых подписей (усиленных и квалифицированных) на основе разработки «продуктивных» международных стандартов условий совместимости технологических алгоритмов электронных подписей, использующих асимметричную схему шифрования, в настоящее время и в обозримом будущем не представляется возможным.

Технологические алгоритмы цифровых электронных подписей опираются на сложные математически задачи, вычислительная сложность которых теоретически еще не доказана, поэтому рассчитать уровень их криптостойкости невозможно. Поэтому на международном уровне часто возникают неразрешимые противоречия в части признания иностранных стандартов в данной сфере.

Кроме того, получившая международное признание типовая асимметричная схема применения электронной цифровой подписи включает следующие три процесса:

1. Генерация на основе применения датчика псевдослучайных чисел ключевой математически зависимой пары, включая:

- закрытый ключ (private key), который сохраняется его владельцем в режиме тайны и используется им для подписи;
- открытый ключ (public key), который может быть опубликован владельцем в справочнике открытых ключей и может использоваться для проверки подписи владельца закрытого ключа.

При этом по закрытому ключу легко вычислить открытый ключ, но наоборот — практически невозможно.

2. Вычисление и формирование электронной подписи в электронном документе на основе применения закрытого ключа в качестве степени односторонней функции зашифрования — функции дискретного возведения в степень в модульной арифметике хеша¹⁷ (сверт-

¹⁵ Коржов В. Ю., Захарова Н. А. Указ. соч.

¹⁶ Козинец Н. В. Вопросы правового регулирования электронных подписей в рамках осуществления трансграничной электронной торговли // Фундаментальные и прикладные исследования в современном мире. 2017. № 18-3. С. 70—73.

¹⁷ Полученного хешированием (от англ. hash — превращать в мешанину; свертка сообщения в его дайджест) — преобразованием массива данных произвольной длины в битовую строку определенной длины в шестнадцатиричном коде согласно принятому стандарту, например: ГОСТ Р 34.11-2012. Ин-

ки, сигнатуры, хеш-суммы, хеш-кода) массива данных документа (или самого массива данных документа), обратить которую практически не представляется возможным.

3. Проверка и верификация подписи в принятом электронном документе на основе применения открытого ключа (из ключевой пары) в качестве степени той же самой функции дискретного возведения в степень в модульной арифметике для расшифрования и сравнения полученного результата — хеша данных (сигнатуры) с рассчитанным хешем (сигнатурой) массива данных полученного электронного документа. В случае их равенства принимается решение, что подпись верна.

В результате обеспечивается целостность и аутентичность переданной информации и снимается организационно-техническая проблема управления (включая распространение, хранение, доставку) множеством ключей для многоабонентских информационных систем (сетей).

Вместе с тем сохраняется ряд технологических проблем, ограничивающих возможности кросс-сертификации криптоалгоритмов электронной подписи, среди которых следующие:

- Как обеспечить стабильность источника случайных чисел, используемого для генерации ключевой пары?
- Как обеспечить надежное хранение и своевременность смены закрытых ключей?
- Как оценить уровень надежности и криптостойкости (необратимости с точки зрения извлечения как корней, так и логарифмов) используемых стандартизованных функций зашифрования в различных криптоалгоритмах в условиях роста производительности современных вычислительных средств, приближающейся к условному порогу, равному приблизительно 10^{40} операций в секунду (и, возможно, более, если верить иностранным источникам, что существуют вычислительные возможности обеспечения обратимости стандартизованных функций зашифрования)?

- Как обеспечить оптимальное сочетание требований к производительности (быстроте передачи информации) и криптостойкости криптографических алгоритмов путем перехода к быстрым алгоритмам электронной подписи, основанным на принципиально других методах расчета (например, на теории графов вместо модульной арифметики), еще недостаточно хорошо изученных?

В связи с наличием перечисленных еще теоретически не решенных технологических проблем универсальная международная стандартизация условий совместимости технологических алгоритмов электронных подписей и сертификатов представляется преждевременной.

Вместе с тем опыт правовой регламентации взаимодействия международных субъектов в неопределенных условиях в других предметных областях¹⁸ позволяет сделать вывод о надежном способе взаимного признания иностранных сертификатов с технологической точки зрения — это привлечение коммерческими организациями при заключении контрактов третьей квалифицированной стороны. В качестве такого арбитра может выступать крупная частная или государственная организация, имеющая международный авторитет в сфере кибербезопасности. Например, Национальный центр кибербезопасности Германии, Национальный центр кибербезопасности Великобритании (оказывает, в частности, поддержку частному сектору в вопросах промышленной кибербезопасности) и др.

Но более перспективным представляется способ заключения и выполнения международных коммерческих сделок (договоров, соглашений) в электронной форме на базе технологии блокчейн¹⁹, для которой в принципе отсутствует проблема взаимного признания и совместимости иностранных алгоритмов электронных подписей и сертификатов, поскольку используются децентрализованные одноранговые P2P-сети²⁰ для записи информации в распределенном реестре на всех компьютерах сети одновремен-

формационная технология. Криптографическая защита информации. Функция хэширования. М. : Стандартиформ, 2013. С. 25.

¹⁸ Например, в области воздушных перевозок — на основе признания сторонами стандартов и рекомендуемой практики (SARPs — Standards and Recommended Practices) ИКАО (от англ. ICAO — International Civil Aviation Organization — Международная организация гражданской авиации) со штаб-квартирой в Монреале, Канада.

¹⁹ От англ. block chain — цепочка блоков.

²⁰ От англ. peer-to-peer — равный к равному.

но. В частности, за последние 10 лет созданы и успешно функционируют частные трансграничные платформы: Cyber Fund, Satoshi Fund, «Голос» (Golos) и др.

Современные блокчейн-технологии, первоначально (в 2009 г.) созданные исключительно для *оперативного децентрализованного* (без доверенных посредников и ненужных звеньев) электронного обращения криптовалюты (биткоина), широко используются в различных сферах экономики и социальной сферы, включая электронную коммерцию, банковскую сферу, госуправление, страхование, здравоохранение и др., поскольку обладают рядом преимуществ, в том числе и в отношении *живучести* (информационно-физической безопасности) и повышенной *информационной защищенности*. Это обусловлено тем, что блокчейн-технологии, наряду с использованием электронных цифровых подписей и мультиподписей, используют последовательно взаимосвязанные цепочки зашифрованных блоков данных, в частности сетевых финансовых транзакций (записей), хранимых одновременно у всех независимых участников (простых пользователей и майнеров — создателей блоков) блокчейн-платформы, поэтому взлом системы (т.е. географически распределенно хранимого множества взаимодействующих идентичных копий единой базы данных) чрезвычайно затруднен. А взламывать каждый зашифрованный блок (содержит заголовок, ключи текущего и предыдущего блоков для обеспечения связности и целостности, набор записей-транзакций) и множество его копий, которые хранятся в разных местах, достаточно долго и дорого. Причем каждая попытка взлома любого блока из цепочки обязательно будет замечена другими участниками системы. Да и физически разрушить такие системы практически невозможно в связи с использованием значительного числа узлов (компьютеров) для хранения соответствующих копий с интерфейсами для доступа и подробной документацией, часто территориально разбросанных по всему миру.

Предположим, пользователь узла-компьютера P2P-сети, представляющий сторону А (первого контрагента), которая хочет заключить трансграничный коммерческий контракт со стороной В (вторым контрагентом), передает необходимую информацию на узел-компьютер

представителя стороны В, с которого передается ответная информация. В P2P-сети с помощью специальных алгоритмов осуществляется сетевая проверка данной транзакции (она проходит процедуру валидации) и статуса неизвестных (анонимных) пользователей. Подтвержденная транзакция, к слову, может содержать не только информацию о контракте, но и криптовалюту, записи о том или ином событии или вещи, и вообще другую, не связанную с финансами, информацию. Данная транзакция вместе с другими проверенными транзакциями в сети объединяется в очередной блок, который имеет свой хеш-код (контрольную сумму) данных и хеш-код предыдущего блока. Причем простые хеш-функции используются при проверке целостности передачи пакетов, например, по протоколу TCP/IP. А сложные хеш-функции, как в данном случае, используются для криптографических преобразований и электронной подписи, и главные условия для них — невозможность по конечному результату вычислить начальный, а также стойкость к «коллизиям», т.е. невозможность получения двух одинаковых хеш-функций из двух разных массивов данных при обработке.

После сборки блоки рассылаются автоматически всем участникам P2P-сети для проверки, и если проблем или ошибок нет, то новый блок добавляется к существующей цепочке блоков таким образом, чтобы оставаться постоянным и неизменным. Так формируется цепочка блоков (блокчейн), содержащая информацию обо всех предыдущих и текущих транзакциях. Вся эта информация открыта и публична, и каждый человек может легко ее просмотреть (для этого существуют программы-парсеры²¹ или онлайн-сервисы), но она не содержит сведений об участниках транзакций. То есть обеспечивается полная анонимность (при этом существует возможность у самих участников от анонимности отказаться).

Прагматические достоинства хранения данных о заключении и выполнении трансграничных контрактов на блокчейн-платформе: абсолютная достоверность данных (это особенно ценно, когда блоки какого-либо процесса выполняются разными операторами), высокая надежность, исключая возможность потери, искажения или уничтожения данных;

²¹ Парсер (от англ. parser — синтаксический анализатор) — это программа, сервис или скрипт, который собирает открытую («белый», т.е. незапрещенный парсинг) интернет-информацию (о ценах, товарах, конкурентах, контрактах и др.) с указанных веб-ресурсов.

принципиальная открытость данных, простота доступа и проверки базы данных на блокчейн-платформе устраняют возможность совершения коррупционных сделок с объектами недвижимости и др.; сокращаются издержки на ведение реестров, повышается оперативность предоставления данных сторонам договора, в том числе за счет исключения традиционных «посредников».

Заключение

Либерализация гражданского законодательства РФ в 2013 г. в отношении отмены положений о последствиях несоблюдения письменной формы внешнеэкономической сделки не исключила требования заключения международных коммерческих сделок в письменной форме в силу общего правила, предусмотренного в п. 1 ст. 161 ГК РФ. Сохраняет свою силу и оговорка, сделанная СССР, о неприменимости положения Венской конвенции 1980 г., предусматривающего возможность заключать договор не в письменной, а в любой форме, если хотя бы одна из сторон договора имеет свое коммерческое предприятие в СССР.

Анализ содержания ст. 13 Венской конвенции 1980 г. позволил авторам прийти к выводу о заложенном в ней противоречии, которое проявляется в том, что, с одной стороны, словосочетание «для целей настоящей Конвенции» указывает на необходимость толкования данной статьи в соответствии со ст. 7 этой же Конвенции, а именно принимая во внимание ее международный характер. С другой стороны, использование слова «также» явно указывает на неполный перечень возможных форм письменных документов. Авторы приходят к выводу, что в данном случае должно действовать общее правило, в рамках которого предусмотрено, что, поскольку обязательность соблюдения письменной формы вытекает из норм национального права государств, сделавших оговорку, этими нормами (а не Венской конвенцией) определяются и требования к ее соблюдению.

Соответственно, международные коммерческие сделки, заключенные в электронной форме, также будут включаться в сформулированное в Венской конвенции 1980 г. понятие «письменная форма», если таковая удовлетворяет требования национального законодатель-

ства государства, сделавшего оговорку в отношении обязательности письменной формы.

С 2019 г. в ГК РФ получила закрепление письменная форма электронной сделки, которая в соответствии с п. 1 ст. 160 ГК РФ будет считаться выполненной при возможности воспроизведения сделки на материальном носителе и идентификации лица, выразившего волю на ее заключение. Измененная редакция п. 1 ст. 160 ГК РФ позволяет сделать допущение, что письменная форма электронной сделки будет считаться соблюденной и при использовании простой и/или неквалифицированной электронных подписей, в отношении которых законодателем принят обратный подход, а именно электронные документы, подписанные такими видами электронной подписи, признаются равнозначными подписанным вручную документам на бумажном носителе, если это установлено федеральным законом или соглашением сторон.

В то же время сравнительный анализ указанного положения с положениями Нью-Йоркской конвенции 2005 г. позволил сделать заключение, что в последней предусмотрен более широкий подход к понятию письменной формы, в которой доступность информации для последующего использования не ограничивается возможностью воспроизведения сделки на материальном носителе.

В результате анализа п. 1 ст. 7 Федерального закона «Об электронной подписи» 2011 г., в которой предусмотрено отнесение иностранной подписи к тому виду, признакам которого она соответствует на основании указанного Закона, выявлены проблемы данного подхода ввиду того, что в разных государствах используются различные стандарты криптографических алгоритмов, лежащих в основе формирования открытого и закрытого ключа электронной подписи. Решение вопроса о признании иностранных электронных подписей (усиленных и квалифицированных) на основе международных стандартов условий совместимости технологических алгоритмов электронных подписей, использующих асимметричную схему шифрования, в настоящее время не представляется возможным. Технологические алгоритмы цифровых электронных подписей опираются на сложные математические задачи, вычислительная сложность которых теоретически еще не доказана, поэтому рассчитать уровень их криптостойкости невозможно. Вместе с тем опыт правовой регламентации взаимодействия международных субъектов в неопределенных условиях в других

предметных областях позволяет сделать вывод о надежном способе взаимного признания иностранных сертификатов с технологической точки зрения — это привлечение коммерческими организациями при заключении контрактов третьей квалифицированной стороны. В качестве такого арбитра может выступать крупная частная или государственная организация, имеющая международный авторитет в сфере кибербезопасности. Наиболее перспективным

представляется способ заключения и выполнения международных коммерческих сделок (договоров, соглашений) в электронной форме на базе технологии блокчейн, для которой проблема взаимного признания и совместимости иностранных алгоритмов электронных подписей и сертификатов снимается в силу использования децентрализованных одноранговых P2P-сетей для записи информации в распределенном реестре на всех компьютерах сети одновременно.

БИБЛИОГРАФИЯ

1. Венская конвенция о договорах международной купли-продажи товаров : комментарий / под ред. М. М. Богуславского. — М., 1994. — 382 с.
2. Канашевский В. А. Внешнеэкономические сделки: основные регуляторы, их соотношение и взаимодействие : автореф. дис. ... д-ра юрид. наук. — М., 2009. — 56 с.
3. Козинец Н. В. Вопросы правового регулирования электронных подписей в рамках осуществления трансграничной электронной торговли // *Фундаментальные и прикладные исследования в современном мире*. — 2017. — № 18-3. — С. 70—73.
4. Коржов В. Ю., Захарова Н. А. Комментарий к Федеральному закону от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» / под ред. Н. Н. Ковалевой. — СПС «Гарант», 2016.
5. Розенберг М. Г. Международная купля-продажа товаров : Комментарий к законодательству и практике разрешения споров. — М. : Контракт : Инфра-М, 2001. — 224 с.
6. Савельев А. И. Электронная коммерция в России и за рубежом: правовое регулирование. — М. : Статут, 2014.
7. Стригунова Д. П. Правовое регулирование международных коммерческих договоров : монография : в 2 т. — 2-е изд., перераб. и доп. — М. : Юстицинформ, 2018. — Т. 2.

Материал поступил в редакцию 5 мая 2020 г.

REFERENCES

1. Boguslavskiy MM, editor. Venskaya konventsia o dogovorakh mezhdunarodnoy kupli-prodazhi tovarov : kommentariy [The Vienna Convention on Contracts for the International Sale of Goods: Commentary]. Moscow; 1994. (In Russ.)
2. Kanashevskiy VA. Vneshneekonomicheskie sdelki: osnovnye regulatory, ikh sootnoshenie i vzaimodeystvie : avtoref. dis. ... d-ra yurid. nauk [Foreign economic transactions: the main regulators, their correlation and interaction. Abstract of the Dr. Sci. (Law) Dissertation]. Moscow; 2009. (In Russ.)
3. Kozinets NV. Voprosy pravovogo regulirovaniya elektronnykh podpisov v ramkakh osushchestvleniya transgranichnoy elektronnoy trgovli [Issues of legal regulation of electronic signatures in the framework of cross-border electronic commerce]. *Fundamentalnye i prikladnye issledovaniya v sovremennom mire*. 2017;18-3:70-73. (In Russ.)
4. Korzhov VYu, Zakharova NA. Kommentariy k Federalnomu Zakonu ot 6 aprelya 2011 g. № 63-FZ «Ob elektronnoy podpisi» [Commentary to Federal Law No. 63-FZ of April 6, 2011 "On electronic signatures"]. Kovaleva NN, editor. Computer-based legal reference system "Garant"; 2016. (In Russ.)
5. Rosenberg MG. Mezhdunarodnaya kuplya-prodazha tovarov: kommentariy k zakonodatelstvu i praktike razresheniya sporov [International sale and purchase of goods: Commentary on the law and practice of dispute resolution]. Moscow: Contract: Infra-M; 2001. (In Russ.)
6. Savelyev AI. Elektronnaya kommertsia v Rossii i za rubezhom: pravovoe regulirovanie [E-Commerce in Russia and abroad: Legal regulation]. Moscow: Statute; 2014. (In Russ.)
7. Strigunova DP. Pravovoe regulirovanie mezhdunarodnykh kommercheskikh dogovorov: monografiya: v 2 t. [Legal regulation of international commercial contracts: monograph: in 2 vol.]. 2nd ed., rev. and suppl. Moscow: Justicinform; 2018. Vol. 2. (In Russ.)