Правовая модель электронной подписи в России: история и вызовы современности

Марк Витальевич Терешин
orcid.org/0000-0003-3386-6663

Аннотация: В статье рассмотрены эволюция развития законодательных подходов и нормативных актов, касающихся обращения и использования электронных подписей в России в сравнении с некоторыми зарубежными правопорядками. Определено в соответствии с законодательством понятие электронной подписи, проведено сравнение понятий по действующему и прежнему законам. Обозначены функции электронной подписи, подчёркивающие её ценность и необходимость в использовании. Рассмотрены виды электронных подписей, предусмотренные российским законодательством, порядок использования и особенности каждого из вида подписей. Обозначена содержащаяся в электронной подписи информация, позволяющая установить подписавшее лицо и подлинность документа. Приведена практика использования электронной подписи как в публично-правовых, так и в частноправовых отношениях. Сделан вывод о том, что хоть российское законодательство не вполне успевает за техническими новшествами в сфере электронного документооборота, законодательные новеллы уже вносят свой вклад в формирование цифровой среды доверия в России.

Ключевые слова: электронная подпись; электронный документооборот; цифровая экономика; квалифицированная подпись; облачная электронная подпись; сертификат ключа проверки подписи; доверенная третья сторона; удостоверяющий центр; машиночитаемая доверенность; криптографическая защита.

The Legal Model of Electronic Signature in Russia: History and Contemporary Challenges

Mark Vitalievich Tereshin
orcid.org/0000-0003-3386-6663

Annotation: The article discusses the evolution of legislative approaches and regulations concerning the circulation and use of electronic signatures in Russia in comparison with some foreign jurisdictions. The notion of electronic signature is defined in accordance with the legislation, the notions under the current and former laws are compared. The functions of electronic signatures, which underscore their value and necessity of use, were outlined. Types of electronic signatures provided for

by the Russian legislation were considered, as well as the order of use and the peculiarities of each type of signatures. The information contained in the electronic signature, which makes it possible to identify the signer and the authenticity of the document, was outlined. The practice of using electronic signatures both in public and private legal relations was given. The conclusion is made that though the Russian legislation does not fully keep up with technical innovations in the field of electronic document flow, legislative novelties being introduced already contribute to formation of the digital environment of trust in Russia.

Keywords: electronic signature; electronic document management; digital economy; qualified signature; cloud electronic signature; signature verification key certificate; trusted third party; certification center; machine-readable power of attorney; cryptographic protection.

Введение

Переход к цифровой экономике в России способствовал появлению новых понятий, связанных с появившимися технологиями, потребовал развитие новых правовых институтов, адекватно регулирующих новые отношения. Кроме того, продолжается активное развитие дистанционных сервисов для интернет-торговли, электронного документооборота. В связи с этим начали широко внедряться и применяться электронные подписи (далее — ЭП), которые обеспечили надёжность и скорость современного документооборота.

История практического применения электронной подписи как высокотехнологичного инструмента прослеживается с 1990-х годов с первых её внедрений в западных странах. Само же понятие электронной (цифровой) подписи было предложено американскими криптографами У. Диффи и М. Хеллманом ещё в 1976 году. В отличие от западных стран, институт электронной подписи в Российской Федерации получил своё развитие не сразу. Так, например, первый закон, положившим начало правового режима электронных подписей в России, вступил в силу лишь в 2002 г. (им стал Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи» (далее — Закон № 1-ФЗ)). Для сравнения, одной из первых стран мира, которая ввела в национальное законодательство понятие «электронная подпись», стали Соединённые Штаты Америки ещё в 2000 году. В дальнейшем электронная подпись начала получать отражение и в законодательстве других стран, в том числе на уровне Евросоюза. В дальнейшем в локальных законодательствах получали регулирование новые подвиды электронных подписей (квалифицированные, облачные и т.д.). Национальное законодательство развивалось по мере того, как электронная подпись все более широко

применялась гражданами и бизнесом на практике, и демонстрировало особенности подходов в разных юрисдикциях.

Принятые в России национальная программа «Цифровая экономика Российской Федерации» 2019 г.[1] и Стратегия развития электронной торговли в РФ 2017 г. (на период до 2025 г.)[2] предусматривают организацию правовых условий для всестороннего применения юридически значимых электронных документов во всех сферах экономики РФ, включая цифровое взаимодействие частного бизнеса и государства. Через создаваемые в рамках реализации программ нормативные акты и создаваемые цифровые сервисы, в России активно происходит развитие дистанционных сервисов для дистанционной работы, электронного документооборота, банковской сферы. Кроме того, в публично-правовой сфере активно создаются информационные сервисы, позволяющие физическим и юридическим лицам получать государственные и муниципальные услуги с сохранением юридической значимости при взаимодействии через телекоммуникационные сети.

Типовые законы ЮНСИТРАЛ об электронной торговле 1996 г. и электронных подписях 2001 г. определили установление взаимосвязи между подписью лица и указанием на то, какую волю выражает данное лицо в отношении информации, содержащейся в электронном документе[3]. Схожие положения использованы также в законодательстве Евросоюза (Директиве ЕС 1999 г и заменяющем её Регламенте 2014 г. об электронной идентификации и удостоверительных сервисах[4]). Очевидно, что аналогичный подход был воспринят и в российском законодательстве, что является необходимым фундаментом для международного признания ЭП, выданных в Российской Федерации. Так, например, ст. 7 Федерального закона от 06.04.2011 г. № 63-ФЗ «Об электронной подписи» (далее — Закон № 63-ФЗ) определяет саму возможность признания зарубежных электронных подписей в России, созданных в соответствии с иностранным и международным правом.

С. Мейсон, британский эксперт в области исследования правовой природы электронных подписей, справедливо выделяет три модели развития

---

[1] Утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7.

[2] Стратегия развития электронной торговли в Российской Федерации на период до 2025 года. Проект. Минпромторг России. 2017 г. // URL: http://minpromtorg.gov.ru/common/upload/content/strat_torg.doc (дата обращения: 21.08.2022).

[3] *Kim H.* Globalization and regulatory change: The interplay of laws and technologies in E-commerce in Southeast Asia. // Computer Law & Security Review. 2019. Vol. 35. No. 5. P. 4.

[4] Регламент Европейского Парламента и Совета Европейского Союза 910/2014 от 23 июля 2014 г. об электронной идентификации и удостоверительных сервисах для электронных трансакций на внутреннем рынке… (Принят в г. Брюсселе 23.07.2014).

законодательных подходов в сфере регулирования электронного документооборота и использования электронных подписей[5]:

— «минималистичная модель» (яркий пример — США), позволяющая лицам самостоятельно определять методы своего взаимодействия при подписании соглашений в электронной форме. Эта модель основана на принципах свободы заключения договоров, выбора способов его заключения, в том числе с применением любых информационных технологий;

— «двухуровневая» модель (страны Европы, Сингапур), особенностью которой является установление допустимых форм, которые могут принимать электронные подписи, добровольная сертификация выдачи и применения электронной подписи (в Евросоюзе)[6], а также добавление дополнительного критерия надёжности, соответствующей назначению данных.

— «предписывающая» модель (Россия, Саудовская Аравия, Малайзия), которая предусматривает определенный тип технологии для использования в цифровой среде как эквивалент подписи. Кроме того, в странах с такой правовой моделью электронной подписи деятельность по предоставлению соответствующих услуг зачастую подлежит лицензированию.

Принципы модели электронной подписи, используемой в России, основываются, в частности, на признание непосредственного действия лишь именно цифровой подписи (при этом она должна быть усиленной квалифицированной) в качестве приемлемой формы электронной подписи (в отличие от, например, графического изображения собственноручной подписи). По некоторым мнениям, данный подход неоднозначен, поскольку он ни обеспечивает правовую определённость, ни способствует дальнейшему развитию электронной коммерции. Кроме того, нельзя достоверно утверждать, всегда ли цифровые подписи, обеспечивающие шифрование с помощью пар открытого и закрытого ключей, безопаснее, чем электронные подписи в целом[7]. Таким образом, действующая в Российской Федерации правовая модель электронной подписи имеет свои отличительные особенности, которые будут рассмотрены в настоящей статье.

Предмет исследования данной статьи — анализ особенностей становления и современного состояния законодательства России об электронной подписи.

---

[5] *Mason S.* Electronic Signatures in Law (4th edition). London: University of London Press, 2016. P. 69-70.

[6] *Ловцов Д. А.* Системология правового регулирования информационных отношений в инфосфере: монография. М.: РГУП, 2016. С. 220.

[7] *Ou P., Tsai A., Kaiser N.* The e-signature in Taiwan: consent, integrity and accessibility. // Digital Evidence and Electronic Signature Law Review. 2016. No. 13. P. 153.

1. Понятие и функции электронной подписи

1.1. Эволюция российского законодательства об электронной подписи

В России практика электронной подписи и её правовое регулирование стали развиваться позже, чем в других странах, российское законодательство прошло несколько этапов. Это было обусловлено повышением важности и распространённости электронной подписи в частноправовых и публично-правовых отношениях, а также в связи с бурным ростом дистанционных сервисов.

В настоящее время правовое регулирование института электронных подписей в России осуществляется Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». В отличие от ранее действующего Закона № 1-ФЗ, в нынешнем законе теперь прямо предусмотрены дополнительные виды электронных подписей, что даёт возможность рассматривать соответствующее российское законодательство в качестве двухуровневого, более приближенному к европейскому законодательству об электронной подписи.

Принятый 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…» (далее — Закон № 476-ФЗ) привнёс существенные изменения и дополнения в Закон № 63-ФЗ. Законом была усовершенствована система выдачи квалифицированных сертификатов и использования квалифицированной ЭП при участии в правоотношениях разных субъектов (физических, юридических лиц, нотариусов, государственных служащих, индивидуальных предпринимателей и других категорий лиц). Помимо этого, значительное ужесточены требования к порядку аккредитации удостоверяющих центров (УЦ) и выдачи ими ЭП, расширены полномочия государственных органов по выпуску квалифицированных сертификатов ключей электронной подписи, введены в оборот машиночитаемые доверенности для автоматизированной проверки полномочий, определено понятие института доверенной третьей стороны (ДТС) и метки доверенного времени, а также заложен фундамент для использования облачной электронной подписи и удалённой идентификации-заявителей без необходимости их личной явки в УЦ для выдачи сертификатов. Данные нововведения будут рассмотрены далее.

Закрепление в законодательстве возможности применения электронной подписи при цифровом взаимодействии гарантирует как законность самой ЭП, так и юридическую силу или подписанного с помощью такой подписи электронного документа недействительными юридически, лишь исходя из того,

что такая электронная подпись поставлена не собственноручно, а с использованием технических средств для автоматического создания и (или) проверки электронных подписей в информационной системе (см. ч. 3 ст. 4 Закона № 63-ФЗ).

1.2. Определение и функции электронной подписи

Ранее действующий Закон № 1-ФЗ определяет электронную цифровую подпись как «реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе»[8].

В актуальном Законе № 63-ФЗ слово «цифровая» из легального определения было исключено. Так, в соответствии с п. 1 ст. 2 Закона № 63-ФЗ электронная подпись — «информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию»[9]. Таким образом, законом определены условия признания подписанных ЭП электронных документов, равноценными документам на бумажном носителе, заверенным собственноручной подписью[10] (ст. 6 Закона № 63-ФЗ). Тем не менее, вопрос определения и природы термина «электронная подпись», несмотря на свою кажущуюся однозначность, вызывает некоторые дискуссии в информационно-правовом сообществе. К примеру, исследователь О. В. Танимов полагает, что ЭП является некой фикцией исходя из того, что собственно «подписью» ЭП можно считать только условно. Исследователь комментирует это тем, что подпись «не связана неразрывно с электронным документом так же, как собственноручная подпись с бумажным документом, не является его непосредственной частью, а имеет с ним сложную криптографическую связь»[11]. В свою очередь полагаем, что применение самого слова «подпись» в данном случае условно, и криптографическое заверение аутентичности информации является ближайшим

[8] Федеральный закон от 10.01.2002 № 1-ФЗ (ред. от 08.11.2007) «Об электронной цифровой подписи» // СЗ РФ. 14.01.2002. № 2. Ст. 127.

[9] Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 14.07.2022) «Об электронной подписи» // СЗ РФ. 11.04.2011. № 15. Ст. 2036.

[10] Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 14.07.2022) «Об электронной подписи» // СЗ РФ. 11.04.2011. № 15. Ст. 2036.

[11] *Танимов О. В.* Электронный документ и электронная цифровая подпись как юридические фикции // Информационное право. 2005. № 3. С. 8.

по надёжности аналогом собственноручной подписи документов в цифровом пространстве.

Сравнивая оба определения, отметим, что в каждом из них предусматривается идентификация при помощи электронной подписи конкретного лица-подписанта. При этом мы не считаем данное положение однозначным. Конкретнее, электронная подпись не даёт возможность гарантированно и однозначно установить лицо, фактически поставившее электронную подпись в документ[12]. Из этого мы делаем вывод, что лишь по факту наличия в документе ЭП нельзя установить, что конкретный документ подписан именно владельцем электронной подписи, а не кем-то другим. Соответственно, это даёт пространство для некоторых злоупотреблений и правонарушений (при несанкционированном использовании).

Согласно доктринальным мнениям, электронной подписью может считаться, к примеру, запись голоса, рисунок сетчатки глаза, отпечаток пальца, считанный биометрическими устройствами, скан собственноручной подписи, персональный идентификационный номер (PIN)[13] или даже подпись с именем и фамилией отправителя в сообщении электронной почты. Полагаем, что данное мнение отчасти справедливо, вместе с этим электронная подпись не должна быть излишне подвержена произвольному использованию любым лицом, поэтому как минимум напечатанные на клавиатуре имя и фамилия в электронной почте не должны расцениваться в качестве какого бы то ни было подвида электронной подписи. Некоторые российские авторы, например, Е. В. Шестакова и Н. В. Гурьянова, отграничивают также факсимильные подписи от электронных и собственноручных, подразумевая, что при печати электронная подпись в виде графического изображения собственноручной становится другим типом подписи.

В электронной подписи содержатся метаданные, содержащие сведения о подписанте и техническую информацию, а также криптографические данные. Кроме того, в состав ЭП может включаться дата и время подписания, сведения для дополнительной проверки подписи (которая может производиться как на удалённом сервере, так и на локальном компьютере[14]), дополнительную информацию о подписавшем, его полномочия для подписания, комментарии, файлы, скан-образ собственноручной подписи и другие данные. В новых

---

[12] *Иванов Н. А.* Об электронных документах и электронной цифровой подписи. // Информационное право. 2006. № 3. С. 11.

[13] *Kim H.* Op. cit. P. 3.

[14] *Kazmierczyk Z., Turner I. J.* Self-identification of electronically scanned signatures (ESS) and digitally constructed signatures (DCS). // Forensic Science Research. 2022. Vol. 7. No. 2. P. 261.

поправках к законодательству об электронной подписи отдельное место уделено регламентации механизма использования метки доверенного времени — достоверной зашифрованной информации о дате и времени подписания электронного документа. Причём это не является изобретением именно российского законодателя — наоборот, это стало очередным шагом к гармонизации отечественного и передового зарубежного законодательства, а также легализации существующих технических инструментов.

Касательно функционала электронной подписи, прежде всего, они выполняют в праве доказательную функцию: они удостоверяют, что подписавший одобряет и принимает содержание документа и придают документу юридическую силу, признаваемую всеми подписавшими его сторонами. С. Мейсон отличает электронные подписи от собственноручных[15]: последние, если они подлинные, биологически связаны с конкретным человеком, в то время как первые соотносятся с личностью посредством программного кода и определённых процедур.

Функция электронных подписей, применяемых лицами в своих документах, не ограничивается установлением автора документа. Их функция зависит от характера и содержания документа, к которым она приложена. Подписи выполняют целый ряд функций, таких как удостоверение подлинности заявления, сделанного в документе, декларирование намерения подписанта связать себя правами и обязанностями согласно условиям документа, подтверждение того, что подписант принимает к сведению содержание документа и не может отречься от подписанного, и признание конкретного документа в качестве оригинального. Современные технологии позволяют электронным подписям выполнять эти и другие функции, традиционно присущие собственноручным подписям.

Для осуществления своих функций электронная подпись должна соответствовать определенному перечню требований, в частности, должна обеспечивать возможность достоверного и однозначного установления отправителя (подписанта) информации и становиться недействительной при случайной или намеренной модификации подписываемых данных. Данное требование получило отражение в законодательстве некоторых европейских стран, где понятие «электронная подпись» охватывает самые распространённые виды использования собственноручной подписи для достоверного установления личности подписанта и связи конкретного лица с содержимым документа. Одним из возможных способов защиты прав владельца ЭП является

[15] *Mason S.* Op. cit. P. 69.

обязательная процедура видеофиксации процесса оформления ЭП со сроком хранения записи до окончания действия сертификата ключа такой подписи. Однако, в действующем Законе № 63-ФЗ обязательность такой фиксации не предусмотрена, что повышает шансы потенциального несанкционированного оформления и использования ЭП в мошеннических целях.

2. Виды электронной подписи

Первоначально в законодательстве России не существовало никакого видового деления электронных подписей (согласно Закону № 1-ФЗ). Теперь же, согласно ст. 5 Закона № 63-ФЗ в качестве видов электронной подписи законодательством обозначены простая, усиленная неквалифицированная и усиленная квалифицированная подписи.

Законом определено, что участники электронного взаимодействия вправе использовать электронную подпись любого вида по своему усмотрению, если требование об использовании конкретного вида ЭП в соответствии с целями её использования не предусмотрено федеральными законами (иными нормативными правовыми актами) либо соглашением между участниками электронного взаимодействия. Помимо этого, участники электронного взаимодействия вправе самостоятельно определять любые средства, позволяющие обеспечить выполнение законодательства по использованию конкретных видов ЭП[16]. К примеру, некоторые банки и страховые компании при подписании документов с физическими лицами со своей стороны применяют графическое воспроизведение подписи уполномоченного лица, выполненное типографским способом или с помощью компьютерной программы. При этом физическое лицо, принимая условия договора присоединения с такими организациями, принимает и допустимость использования такого аналога собственноручной подписи во взаимоотношениях сторон.

2.1. Простая электронная подпись

Исходя из законодательного определения, простой ЭП является электронная подпись, которая «посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом»[17] (п. 2 ст. 5 Закона № 63-ФЗ). Простые подписи позволяют идентифицировать автора документа, но не позволяют достоверно проверить

---

[16] *Пешкова (Белогорцева) Х. В. и др.* Комментарий к Федеральному закону от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (постатейный). // СПС КонсультантПлюс. 2020. С. 207.

[17] Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 14.07.2022) «Об электронной подписи» // СЗ РФ. 11.04.2011. № 15. Ст. 2036.

внесение изменений в документ после его подписания. Также отметим, что документы, требующие наличия печати, не могут быть подписаны простой электронной подписью.

В соответствии с п. 2 ст. 6 Закона № 63-ФЗ, аутентичность электронного документа, подписанного простой и (или) усиленной неквалифицированной электронной подписью, должна быть обеспечена наличием в соответствующем соглашении между контрагентами порядка проверки электронных подписей. Требования к порядку проверки нормативными правовыми актами не установлены, поэтому стороны устанавливают его самостоятельно и по своему усмотрению. Например, регламент СПБ биржи[18] предусматривает, что проверка неквалифицированной электронной подписи осуществляется путём сопоставления информации, содержащейся в полученном электронном документе, подписанном неквалифицированной ЭП, и информации, содержащейся в документе на момент его подписания. В свою очередь, результатом проверки неквалифицированной ЭП является заключение о её принадлежности и факте внесения изменений в электронный документ после момента его подписания.

2.2. Усиленная неквалифицированная подпись

Понятие усиленной неквалифицированной ЭП (УНЭП) определено в п. 3 ст. 5 Закона № 63-ФЗ: «Неквалифицированной электронной подписью является ЭП, которая: 1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи; 2) позволяет определить лицо, подписавшее электронный документ; 3) позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания; 4) создаётся с использованием средств электронной подписи»[19].

Усиленная неквалифицированная ЭП не только устанавливает личность отправителя, но и подтверждает, что после подписания документ не подвергался изменениям. При использовании УНЭП сертификат ключа проверки ЭП может не создаваться, если соответствие электронной подписи признакам усиленной неквалифицированной ЭП, установленных Законом № 63-ФЗ, может быть обеспечено без использования сертификата ключа проверки ЭП (п. 5 ст. 5 Закона № 63-ФЗ). Генерирование УНЭП производится при помощи криптографических

[18] Соглашение об использовании электронной подписи ПАО «СПБ Биржа» // URL: https://spbexchange.ru/ru/otc_market/repository/documents/sogl_epodp/soglashenie_ob_ispolzovanii_ep291221.pdf (дата обращения: 28.07.2022).

[19] Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 14.07.2022) «Об электронной подписи» // СЗ РФ. 11.04.2011. № 15. Ст. 2036.

средств, что позволяет не только определить подписанта, но и гарантировать отсутствие несанкционированных правок.

В целом, неквалифицированная подпись превосходно подходит для внутреннего документооборота и отправки электронных данных из одной организации в другую. Более того, так называемые смарт-контракты могут считаться электронными документами, подписанными неквалифицированной электронной подписью[20]. Однако недопустимо подписание с помощью УНЭП электронных документов, подлежащих проверке налоговой службой, без соблюдения всех условий п. 2 ст. 6 Закона № 63-ФЗ.

Отличие усиленной квалифицированной электронной подписи от усиленной неквалифицированной состоит в различной степени защищённости и возможностях применения. По сравнению с усиленной квалифицированной электронной подписью, УНЭП обладает следующими основными преимуществами: во-первых, усиленную неквалифицированную электронную подпись можно получить в неаккредитованном удостоверяющем центре; во-вторых, не нужно за отдельную плату приобретать сертифицированный ключ проверки.

2.3. Усиленная квалифицированная подпись

Следующая разновидность ЭП — усиленная квалифицированная электронная подпись (УКЭП) — аналогична неквалифицированной, но для её создания и проверки используется сертифицированная органами ФСБ криптографическая защита. Как следствие, усиленная квалифицированная ЭП имеет сертификат от аккредитованного удостоверяющего центра. Квалифицированные подписи считаются эквивалентными собственноручной подписи во всех случаях, кроме тех, когда закон допускает только самостоятельно проставленную («живую») подпись. Важно отметить, что Закон № 63-ФЗ признаёт в качестве квалифицированных сертификаты ключей подписей, выданные в соответствии с прежним Законом № 1-ФЗ.

В Законе № 63-ФЗ приводится следующее определение удостоверяющего центра: «юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные настоящим Федеральным

[20] *Kirillova E. A. et al.* Legal status of smart contracts: features, role, significance. // Jurídicas CUC. 2019. Vol. 15. No. 1. P. 294.

законом»[21]. Отметим, что в Законе № 63-ФЗ появляется понятие аккредитации удостоверяющего центра, то есть процедура признания УЦ соответствующего требованиям закона. Это стало нововведением по сравнению с ранее действующим законодательством. Полагаем, это связано с тем, что в предыдущем Законе № 1-ФЗ отсутствовала какая-либо аккредитация УЦ, как следствие, возникали проблемы контроля.

Удостоверяющие центры вправе выдавать усиленную неквалифицированную (УНЭП) и усиленную квалифицированную (УКЭП) электронную подпись, которые создаются методом криптографического преобразования информации. Прежде чем выдать подпись, удостоверяющий центр должен надлежаще установить личность лица, обратившегося за выдачей ЭП. Если это представитель юридического лица, центр проверяет также и его полномочия. В дальнейшем УЦ обеспечивает сохранность ключей электронной подписи. При получении соответствующего обращения он вправе осуществить проверку электронной подписи (п. 1, п. 9 ч. 1, п. 4 ч. 2 ст. 13 Закона № 63-ФЗ). Закон № 476-ФЗ расширил полномочия удостоверяющих центров — а именно, появилась возможность хранить закрытый ключ квалифицированной ЭП на стороне УЦ, как следствие, необходимо было заметно повысить требования к порядку аккредитации и деятельности УЦ. Решение об аккредитации УЦ будет принимать правительственная комиссия. С 1 января 2022 г. сертификаты КЭП, выданные УЦ, которые не прошли аккредитацию по новым правилам, перестали действовать. При этом имеющиеся сертификаты будут действовать до истечения своего срока действия, если он не превышает срок действия аккредитации УЦ, но в любом случае не позже 01.01.2022 г. Повышение требований к финансовому обеспечению и степени респектабельности удостоверяющих центров уже приводит к уменьшению доли рынка УЦ, так, сообщается, что на 5 июля 2021 г. аккредитовано лишь 18 удостоверяющих центров[22].

Теперь в законодательстве получила своё отражение и технология, уже реализованная в российском информационно-правовом пространстве — это так называемая «облачная» электронная подпись. Теперь применение облачных электронных подписей урегулировано и российским законом, ранее такой вид подписей уже успешно применялся в США с 2017 года, когда был запущен первый облачный сервис[23]. Под облачной подписью понимается то, что теперь

---

[21] Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 14.07.2022) «Об электронной подписи» // СЗ РФ. 11.04.2011. № 15. Ст. 2036.

[22] *Митина А.* Новые правила в регулировании рынка электронной подписи // 19.07.2021. URL: https://cryptoarm.ru/news/rynok-ecp/ (дата обращения: 10.08.2022).

[23] *Chong K. W. et al.* A Study of Factors Affecting Intention to Adopt a Cloud-Based Digital Signature Service. // Information. 2021. Vol. 10. No. 7. P. 1.

сама электронная подпись теперь будет храниться на удалённом сервере удостоверяющего центра, там же будут производиться и криптографические процедуры. Для усиления контроля за несанкционированным использованием такой ЭП законодательством было установлено, что удостоверяющий центр обязан информировать владельца квалифицированного сертификата об использовании данного ключа ЭП и предоставление по его требованию информации об использовании указанного ключа электронной подписи (п. 2 ч. 2.2 ст. 15 Закона № 63-ФЗ). Аккредитованный удостоверяющий центр, хранящий ключи подписи владельцев квалифицированных сертификатов, должен соблюдать повышенные требования в части технического оснащения и обеспечения финансовой ответственности (в размере 200 миллионов рублей или более) за понесённые убытки в результате компрометации или нелегитимного использования ключей ЭП, хранящихся в аккредитованных УЦ.

Наиболее очевидным для пользователя преимуществом является его мобильность при использовании электронной подписи: отсутствие привязки к стационарному компьютеру с программным обеспечением для подписания электронных документов. В случае утери контроля над ключом электронной подписи, например в результате его утери, возможно избежать негативных последствий в виде несанкционированного использования ЭП, в отличие от компрометации физического носителя. Благодаря дистанционному характеру использования облачной подписи появилась возможность получить «облачную» подпись без личного присутствия владельца (пп. «б» п. 10 ст. 1 Закона № 476-ФЗ) Идентификация будет проведена через ЕСИА (Единую систему идентификации и аутентификации) или при помощи ЕБС (Единой биометрической системы)[24]. Однако в связи с «революционным» характером этой разновидности электронной подписи бизнес и рынок в целом пока ещё скептически относятся к переходу на облачные подписи, видя в этом риски утери контроля за ЭП и излишней концентрации полномочий у удостоверяющих центров.

В соответствии со ст. 10 Закона № 63-ФЗ, участники электронного взаимодействия при использовании усиленных электронных подписей обязаны обеспечивать конфиденциальность ключей подписи, в том числе обязаны не допускать несанкционированного использования своих ключей, а также не

[24] *Якушкина О.* Перспективы развития облачной подписи // 05.10.2020. URL: https://cryptoarm.ru/news/oblachnoy-podpisi/ (дата обращения: 10.08.2022).

использовать ключ ЭП при наличии оснований полагать, что его конфиденциальность нарушена[25].

Все ранее выданные сертификаты ключей ЭЦП (до 1 июля 2013 года), после 1 января 2014 года были признаны квалифицированными сертификатами ЭП (ст. 19 Закона № 63-ФЗ).

В плане разграничения понятий Закон № 63-ФЗ внёс большую ясность в понятийный аппарат, заложенный Законом № 1-ФЗ. Например, Р. Э. Туркин отмечает в Законе № 1-ФЗ неоднозначность понятия «сертификат ключа подписи», которое в законе применялось к владельцам как закрытого, так и открытого ключей[26]. В Законе № 63-ФЗ данный аспект был разрешён путём разделения понятий ключа электронной подписи и ключа проверки электронной подписи. В дополнение, в законе предусмотрены отдельные понятия сертификата ключа электронной подписи, принадлежащего её владельцу, и сертификата ключа проверки ЭП, переданного для проверки подписи участнику электронного документооборота.

3. Практические аспекты использования электронной подписи в России

3.1. Практика применения электронной подписи в публично-правовой сфере

Виды электронных подписей, использование которых допускается при обращении за получением государственных и муниципальных услуг, и порядок их использования устанавливаются Постановлением Правительства РФ от 25.08.2012 № 852 (ред. от 25.10.2017) «Об утверждении Правил использования усиленной квалифицированной электронной подписи при обращении за получением государственных и муниципальных услуг…». Как обращает внимание М. М. Дарькина, ещё в 2012 г. государственные органы получили право вносить документы в Правительство в электронном виде с использованием ЭП благодаря принятым изменениям в Регламент об электронном документообороте в органах государственной власти[27].

---

[25] *Дарькина М. М.* Практика использования электронной цифровой подписи в предпринимательской деятельности. // Право и цифровая экономика. 2020. № 3. С. 30.

[26] *Туркин Р. Э.* Электронная подпись: опыт комплексного изучения. // 29.03.2013. URL: https://zakon.ru/blog/2013/3/29/elektronnaya_podpis_opyt_kompleksnogo_izucheniya (дата обращения: 14.08.2022).

[27] *Дарькина М. М.* Указ. соч. С. 29.

Далее, правовой эксперимент по использованию усиленной неквалифицированной электронной подписи «Госключ» реализует Минцифры России в рамках Постановления Правительства Российской Федерации «О проведении эксперимента по использованию усиленной электронной подписи при предоставлении услуг» от 15.07.2021 г[28]. В проекте используются сервисы единой цифровой платформы для создания и выдачи ЭП, предоставляемые ПАО «Ростелеком» и Банк ВТБ (ПАО). Доступ к платформе будет у юрлиц и госорганов. Ключ усиленной неквалифицированной электронной подписи создаётся, хранится и используется в приложении, токены не требуются. Через «Единую цифровую платформу подписания» можно будет: 1) бесплатно получить сертификат электронной подписи, 2) подписывать, хранить и управлять документами по единым стандартам. В будущем перечень сделок и юридических документов, которые можно подписывать с помощью «Госключа», будет расширен, в том числе планируется его использование для онлайн-подписания договоров купли-продажи транспортных средств и аренды недвижимости. Однако такое удобство использования УНЭП «Госключ» вызывает опасения у некоторых специалистов по информационной безопасности. Так, есть мнение, что предусмотренный порядок выдачи «Госключа» противоречит положениям Приказа ФАПСИ РФ от 13 июня 2001 г. № 152, регламентирующего порядок генерации и работы с ЭП.

Уже известным Законом № 476-ФЗ изменён порядок подписания документов от имени юридических лиц сотрудниками этих организаций. Для того чтобы подписывать электронные документы от имени юридического лица, лицу, действующему от имени организации без доверенности, необходимо получить УКЭП в уполномоченных органах, например в Федеральной налоговой службе на бесплатной основе. Сотрудники же организаций, которым для исполнения профессиональных обязанностей требуется доверенность, должны использовать квалифицированные сертификаты, выданные на имя физического лица, совместно с машиночитаемыми доверенностями. Сведения о полномочиях в таких доверенностях могут быть указаны в виде машинных кодов или человекочитаемого текста. Личные подписи физические лица могут получить в коммерческих удостоверяющих центрах за плату[29].

[28] Постановление Правительства РФ от 15.07.2021 № 1207 // СЗ РФ. 26.07.2021. № 30. Ст. 5784.

[29] Письмо Минцифры России от 10.08.2021 № ОП-П15-085-33604 «О разъяснении применения положений Федерального закона от 06.04.2011 № 63-ФЗ».

Отметим также, что принятый в 2021 году Федеральный закон от 11.06.2021 г. № 170-ФЗ[30] внёс изменения в Закон № 63-ФЗ в части законодательного определения предмета госнадзора в сфере электронной подписи (новая статья 16.1 Закона № 63-ФЗ).

3.2. Практика применения электронной подписи в частноправовой сфере

Российскими судами уже наработана практика по возможности физического лица оформить личную УКЭП и подписывать с её помощью документы в качестве должностного лица организации. При этом практика складывалась не в пользу физических лиц, так как в сертификате ключа проверки подписи в этом случае не включалась информация о том, что лицо имеет право действовать от имени организации. Например, Нижегородский областной суд в 2018 г. (дело № 33-5337/2018[31]) в лице судебной коллегии по гражданским делам рассматривал ситуацию, связанную с тем, что одна УКЭП, выпущенная на имя юридического лица, использовалась как для подписания договора займа, выданного юридическому лицу, так и договора поручительства, оформленного с руководителем этого же ООО. В апелляционной жалобе, поданной представителем физического лица, было отмечено, что для признания контракта заключённым посредством обмена электронными письмами необходимо было заключить соглашение между участниками электронного взаимодействия на использование электронной подписи и обмена электронными сообщениями. При рассмотрении и оценке доказательств судом не было учтено, что договор займа не включал в себя данные о его обеспечении поручителем, не было доказательств соглашения между физическим лицом и ООО о подписании договора поручительства посредством электронного документооборота с помощью электронных средств связи, и физическое лицо не являлось владельцем электронной подписи. Суд указал, что на основании п. 1 ст. 2 и ст. 18 Закона № 63-ФЗ электронная подпись служит средством идентификации лица, подписавшего информацию. Сертификат ключа проверки электронной подписи ООО был выдан на имя данного гражданина. Договор поручительства от имени физического лица был подписан сертификатом, выданным на имя этого же физического лица, то есть он был заверен электронной подписью, которая доказывает его подлинность и подтверждает авторство подписи гражданина.

---

[30] Федеральный закон от 11.06.2021 № 170-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации...» // СЗ РФ. 14.06.2021. № 24 (Часть I). Ст. 4188.

[31] Апелляционное определение Нижегородского областного суда от 05.06.2018 № 33-5337/2018.

Как видим, суд сделал вывод о том, что если УКЭП юридического лица выдана на конкретное физическое лицо (а, как следствие, его данные включены в сертификат ключа проверки подписи), то это физическое лицо имеет право использоваться им для подписания своих (личных) документов. В то же время полагаем, что в такой ситуации должно быть чётко определено законодательством — можно или нельзя применять УКЭП представителя юридического лица, в личных целях.

Частично этот вопрос решён правками, вносимыми Законом № 476-ФЗ, который ввёл понятие машиночитаемой доверенности (МЧД), а также возможность её приложения непосредственно к электронному документу или же ссылки на такую доверенность. Ранее предполагалось, что с 1 января 2022 года сотрудники и уполномоченные лица организаций должны будут применять новый формат подписания документов: использовать личную электронную подпись физлица и прикладывать к ней соответствующую МЧД. Однако в связи с неготовностью как законодательной базы, так и пользователей (граждан и бизнеса) к использованию новой системы, введение обязательного использования МЧД было сначала отложено до 1 января 2023 г., а по последним данным — может быть отложено до 1 сентября 2023 г[32].

3.3. Трансграничное использование электронных подписей

Актуальной проблемой для современной цифровой экономики остаётся трансграничный обмен заверенными ЭП документами и взаимное признание ЭП разными странами. В связи с разнообразием применяемых криптографических методов, а также разницы правовых моделей ЭП российское юридическое лицо должно принимать во внимание все необходимые законодательные требования правовых систем как России, так и страны нахождения его контрагента. В силу п. 1 ст. 7 Закона № 63-ФЗ электронные подписи, созданные в соответствии с нормами права иностранного государства и международными стандартами, в Российской Федерации признаются электронными подписями того вида, признакам которого они соответствуют. Исходя из этого, электронная подпись иностранного или международного стандарта, выпущенная в другой стране, будет иметь в Российской Федерации юридическую силу, если её валидность будет подтверждена доверенной третьей стороной или аккредитованным удостоверяющим центром. К примеру, ввоз и вывоз из России устройств с наличием криптографии (шифрования), ограничен согласно Решению Коллегии

[32] Проект Федерального закона «О внесении изменений в статьи 17.2 и 17.4 Федерального закона "Об электронной подписи"…» (подготовлен Минцифры России) (дата обращения: 26.07.2022).

Евразийской экономической комиссии от 21.04.2015 г. № 30 «О мерах нетарифного регулирования». В связи с этим напрямую применять УКЭП российского стандарта иностранный контрагент не сможет. Решить эту проблему можно, используя неквалифицированную ЭП (заключив соглашение о признании и проверке ЭП), либо же воспользоваться услугами доверенной третьей стороны, что и предлагает новый Закон № 476-ФЗ.

Доверенная третья сторона (ДТС) — это «юридическое лицо, осуществляющее деятельность по проверке электронной подписи в электронных документах в конкретный момент времени в отношении лица, подписавшего электронный документ, для обеспечения доверия при обмене данными и электронными документами и иные функции, предусмотренные законодательством»[33]. Иными словами, задача ДТС состоит в проведении проверки ЭП в электронных документах в заданный момент времени, а также юридически значимом подтверждении результатов данной проверки. В настоящее время привлечение ДТС является добровольным. Деятельность доверенной третьей стороны может осуществляться заинтересованными организациями после соответствующей аккредитации в Минкомсвязи России. Отметим, что вмешательство доверенной третьей стороны влечёт за собой образование инфраструктуры, контролирующей её функционирование, устанавливающей технологические и регуляторные требования, и известной как Public Key Infrastructure (PKI)[34].

Заключение

В условиях последовательной цифровизации общества и развития цифровой экономики проявляется недостаточная эффективность существующих правовых механизмов регулирования цифровых технологий, включая механизмы электронной идентификации. Большинство исследователей информационного права приходят к выводу, что законодательное регулирование в России строится на основе анализа зарубежного опыта, но без учёта национальной специфики и сложившихся взаимоотношений сторон электронного документооборота. Несмотря на заметный достигнутый в последние годы прогресс, законодательство, регламентирующее аспекты выдачи и использования электронной подписи в России, развивается недостаточными темпами, и всё же не успевает за техническими новшествами и практикой

[33] Федеральный закон от 27.12.2019 № 476-ФЗ «О внесении изменений в Федеральный закон "Об электронной подписи"…» (ред. от 30.12.2021) // СЗ РФ. 2019. № 52 (ч. I), ст. 7794.

[34] *Laborde C. M.* Electronic Signatures in International Contracts. Frankfurt am Main: Peter Lang, 2010. P. 41.

внедрения. Помимо этого, высокая безопасность цифровых подписей, обусловленная математическими моделями, одновременно влечёт сложности для каждодневного и удобного использования подписей бизнесом и гражданами, даже в Евросоюзе с его отлаженными правовыми механизмами[35]. Насколько электронные средства связи упрощают и ускоряют коммуникацию, настолько же инфраструктура открытых ключей (PKI) избыточна сложна для основных целей её использования.

Анализируя российский опыт в области правового регулирования электронного документооборота и электронных подписей, необходимо подчеркнуть, что одним из способов преодоления отставания от ведущих стран является активное использование накопленного опыта, закреплённого не только в законах этих стран, но и в подзаконных актах и стандартах. Более того, и другие страны СНГ испытывают тот же спектр проблем, что объясняется однотипной советской законодательно базой[36], следовательно, они могут использовать уже накопленный опыт России для совершенствования своего собственного законодательства.

Между тем, укрепление доверия к электронной среде и применяемым техническим средствам является основополагающим для устойчивого экономического и социального развития. Имеющиеся проблемы предлагается разрешать путём применения института саморегулирования в сфере цифровых технологий. Такие предложения уже находят свой отклик во вступивших в силу нормах о доверенной третьей стороне как новых участниках электронного взаимодействия[37]. Всё это, определённо, вносит вклад в формирование цифровой среды доверия в России.

Список литературы

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

2. *Иванов Н. А.* Об электронных документах и электронной цифровой подписи. // Информационное право. — 2006. — № 3. — С. 11-12.

[35] *Krawczyk P.* When the EU qualified electronic signature becomes an information services preventer. // Digital Evidence and Electronic Signature Law Review. 2010. Vol. 7. P. 17.

[36] *Kussainova A. K. et al.* Legal Issues for Electronic Documents Workflow Regulation. // The Law, State and Telecommunications Review. 2020. Vol. 12. No. 1. P. 312.

[37] Правовое регулирование цифровых технологий в России и за рубежом…: монография / под общ. ред. д.ю.н., доц. А. В. Минбалеева. Саратов: Амирит, 2019. С. 198.

3. *Ловцов Д. А.* Системология правового регулирования информационных отношений в инфосфере: монография. — М.: РГУП, 2016. — 316 с.

4. *Митина А.* Новые правила в регулировании рынка электронной подписи. // 19.07.2021. URL: https://cryptoarm.ru/news/rynok-ecp/ (дата обращения: 10.08.2022).

5. *Пешкова (Белогорцева) Х. В. и др.* Комментарий к Федеральному закону от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (постатейный). // СПС КонсультантПлюс. — 2020. — 229 с.

6. Правовое регулирование цифровых технологий в России и за рубежом. Роль и место правового регулирования и саморегулирования в развитии цифровых технологий: монография / под общ. ред. д.ю.н., доц. А. В. Минбалеева. — Саратов: Амирит, 2019. — 207 с.

7. Соглашение об использовании электронной подписи ПАО «СПБ Биржа» // URL: https://spbexchange.ru/ru/otc_market/repository/documents/sogl_epodp/soglashenie_ob_ispolzovanii_ep291221.pdf.

8. Стратегия развития электронной торговли в Российской Федерации на период до 2025 года. Проект. Минпромторг России. 2017 г. // URL: http://minpromtorg.gov.ru/common/upload/content/strat_torg.doc (дата обращения: 21.08.2022).

9. *Танимов О. В.* Электронный документ и электронная цифровая подпись как юридические фикции. // Информационное право. — 2005. — № 3. — С. 7-9.

10. *Туркин Р. Э.* Электронная подпись: опыт комплексного изучения. // 29.03.2013. — URL: https://zakon.ru/blog/2013/3/29/elektronnaya_podpis_opyt_kompleksnogo_izucheniya (дата обращения: 14.08.2022).

11. *Якушкина О.* Перспективы развития облачной подписи. // 05.10.2020. URL: https://cryptoarm.ru/news/oblachnoy-podpisi/ (дата обращения: 10.08.2022).

12. *Chong K. W. et al.* A Study of Factors Affecting Intention to Adopt a Cloud-Based Digital Signature Service. // Information. — 2021. — Vol. 10. — No. 7. — 15 p.

13. *Kazmierczyk Z., Turner I. J.* Self-identification of electronically scanned signatures (ESS) and digitally constructed signatures (DCS). // Forensic Science Research. — 2022. — Vol. 7. — No. 2. — Pp. 261-264.

14. *Kim H.* Globalization and regulatory change: The interplay of laws and technologies in E-commerce in Southeast Asia. // Computer Law & Security Review. — 2019. — Vol. 35. — No. 5. — 20 p.

15. *Kussainova A. K. et al.* Legal Issues for Electronic Documents Workflow Regulation. // The Law, State and Telecommunications Review. — 2020. — Vol. 12. — No. 1. — Pp. 293-318.

16. *Kirillova E. A. et al.* Legal status of smart contracts: features, role, significance. // Jurídicas CUC. — 2019.— Vol. 15. — No. 1. — Pp. 285-300.

17. *Krawczyk P.* When the EU qualified electronic signature becomes an information services preventer. // Digital Evidence and Electronic Signature Law Review. — 2010. — Vol. 7. — Pp. 7-18.

18. *Laborde C. M.* Electronic Signatures in International Contracts. — Frankfurt am Main: Peter Lang, 2010. — 247 p.

19. *Mason S.* Electronic Signatures in Law (4th edition). — London: University of London Press, 2016. — 476 p.

20. *Ou P., Tsai A., Kaiser N.* The e-signature in Taiwan: consent, integrity and accessibility. // Digital Evidence and Electronic Signature Law Review. — 2016. — No. 13. — Pp. 148-153.

References

1. *Chong K. W. et al.* A Study of Factors Affecting Intention to Adopt a Cloud-Based Digital Signature Service. // Information. — 2021. — Vol. 10. — No. 7. — 15 p.

2. *Dar'kina M. M.* Praktika ispol'zovaniya elektronnoj cifrovoj podpisi v predprinimatel'skoj deyatel'nosti. // Pravo i cifrovaya ekonomika. — 2020. — № 3. — Pp. 28-35.

3. *Ivanov N. A.* Ob elektronnyh dokumentah i elektronnoj cifrovoj podpisi. // Informacionnoe pravo. — 2006. — № 3. — Pp. 11-12.

4. *Kazmierczyk Z., Turner I. J.* Self-identification of electronically scanned signatures (ESS) and digitally constructed signatures (DCS). // Forensic Science Research. — 2022. — Vol. 7. — No. 2. — Pp. 261-264.

5. *Kim H.* Globalization and regulatory change: The interplay of laws and technologies in E-commerce in Southeast Asia. // Computer Law & Security Review. — 2019. — Vol. 35. — No. 5. — 20 p.

6. *Kirillova E. A. et al.* Legal status of smart contracts: features, role, significance. // Jurídicas CUC. — 2019.— Vol. 15. — No. 1. — Pp. 285-300.

7. *Krawczyk P.* When the EU qualified electronic signature becomes an information services preventer. // Digital Evidence and Electronic Signature Law Review. — 2010. — Vol. 7. — Pp. 7-18.

8. *Kussainova A. K. et al.* Legal Issues for Electronic Documents Workflow Regulation. // The Law, State and Telecommunications Review. — 2020. — Vol. 12. — No. 1. — Pp. 293-318.

9. *Laborde C. M.* Electronic Signatures in International Contracts. — Frankfurt am Main: Peter Lang, 2010. — 247 p.

10. *Lovtsov D. A.* Sistemologiya pravovogo regulirovaniya informacionnyh otnoshenij v infosfere: monografiya. — M.: RGUP, 2016. — 316 s.

11. *Mason S.* Electronic Signatures in Law (4th edition). — London: University of London Press, 2016. — 476 p.

12. *Mitina A.* Novye pravila v regulirovanii rynka elektronnoj podpisi. // 19.07.2021. URL: https://cryptoarm.ru/news/rynok-ecp/ (date of access: 10.08.2022).

13. *Ou P., Tsai A., Kaiser N.* The e-signature in Taiwan: consent, integrity and accessibility. // Digital Evidence and Electronic Signature Law Review. — 2016. — No. 13. — Pp. 148-153.

14. *Peshkova (Belogorceva) H. V. i dr.* Kommentarij k Federal'nomu zakonu ot 27 iyulya 2010 g. № 210-FZ «Ob organizacii predostavleniya gosudarstvennyh i municipal'nyh uslug» (postatejnyj). // SPS Konsul'tantPlyus. — 2020. — 229 p.

15. Pravovoe regulirovanie cifrovyh tekhnologij v Rossii i za rubezhom. Rol' i mesto pravovogo regulirovaniya i samoregulirovaniya v razvitii cifrovyh tekhnologij: monografiya / pod obshch. red. d.yu.n., doc. A. V. Minbaleeva. — Saratov: Amirit, 2019. — 207 p.

16. Soglashenie ob ispol'zovanii elektronnoj podpisi PAO «SPB Birzha» // URL: https://spbexchange.ru/ru/otc_market/repository/documents/sogl_epodp/soglashenie_ob_ispolzovanii_ep291221.pdf (date of access: 28.07.2022).

17. Strategiya razvitiya elektronnoj torgovli v Rossijskoj Federacii na period do 2025 goda. Proekt. Minpromtorg Rossii. 2017 g. // URL: http://minpromtorg.gov.ru/common/upload/content/strat_torg.doc (date of access: 21.08.2022).

18. *Tanimov O. V.* Elektronnyj dokument i elektronnaya cifrovaya podpis' kak yuridicheskie fikcii. // Informacionnoe pravo. — 2005. — № 3. — Pp. 7-9.

19. *Turkin R. E.* Elektronnaya podpis': opyt kompleksnogo izucheniya. // 29.03.2013. — URL: https://zakon.ru/blog/2013/3/29/elektronnaya_podpis_opyt_kompleksnogo_izucheniya (date of access: 14.08.2022).

20. *Yakushkina O.* Perspektivy razvitiya oblachnoj podpisi. // 05.10.2020. URL: https://cryptoarm.ru/news/oblachnou-podpisi/ (date of access: 10.08.2022).