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 и мире. Определено в соответствии с законодательством понятие электронной подписи, проведено сравнение понятий по действующему и прошлому 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. Проанализированы новеллы, введенные федеральным законом от 27.12.2019 № 476-ФЗ. Дана практика применения электронной подписи как в публично-правовых, так и в частноправовых отношениях. Сделаны выводы о том, что соответствующее российское законодательство развивается недостаточными темпами, не успевая за техническими новшествами в сфере электронного документооборота.

Ключевые слова: электронная подпись, электронный документооборот, цифровая экономика, виды электронных подписей, квалифицированная подпись, доверенная третья сторона, инфраструктура открытых ключей

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

MARK VITALYEVICH 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 and worldwide. It defines the concept of electronic signature in accordance with the legislation and compares the notions according to the current and past laws. The functions of electronic signatures, which underscore their value and necessity in their 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 electronic signatures, which makes it possible to identify the signer and the authenticity of a document, was pointed out. The novelties introduced by the federal law from 27.12.2019 № 476-FZ are analyzed. The practice of electronic signature application in both public and private legal relations is given. Conclusions are made that the relevant Russian legislation is developing at an insufficient pace, not keeping pace with technical innovations in the field of electronic document management.

Keywords: electronic signature, electronic document management, digital economy, types of electronic signatures, qualified signature, trusted third party, public key infrastructure

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, активно происходит развитие дистанционных сервисов для интернет-торговли, электронного документооборота. В связи с этим начали широко внедряться и применяться электронные подписи, 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 использования электронной подписи в Российской Федерации начал развиваться позже, так, первый федеральный закон, регламентирующий основу правового режима электронных подписей в Российской Федерации, вступил в силу только в 2002 г. (Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи»). При этом одной из первых стран мира, которая ввела в национальное законодательство понятие «электронная подпись» стали Соединённые Штаты 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 на практике, и демонстрировало особенности подходов в разных юрисдикциях.

Национальная программа «Цифровая экономика Российской Федерации» 2019 г.[1] и Стратегия развития электронной торговли в РФ 2017 г. (на период до 2025 г.)[2], которые предусматривают создание правовых условий для применения электронных документов и подписей во всех сферах российской экономики, включая 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 юридической значимостью.

Юридическая взаимосвязь наличия подписи какого-либо лица с использованием надежного метода для установления личности и указания намерения лица в отношении информации, содержащейся в электронном документе, обозначена в Типовых законах ЮНСИТРАЛ об электронной торговле 1996 г. и электронных подписях 2001 г. [Kim H., 2019: 4]. Похожий принцип использован также в законодательстве Евросоюза (Директиве ЕС 1999 г и заменяющем её Постановлении 2014 г. об электронной идентификации и

[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: https://minpromtorg.gov.ru/common/upload/docVersions/5a941a3a65222/actual/strat_torg.doc

доверительных услугах для электронных сделок). 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 Закона № 63-ФЗ «об электронной подписи» устанавливает признание зарубежных электронных подписей в РФ, созданных в соответствии с нормами иностранного и международного права.

С. Мейсон, признанный британский эксперт в области исследования правовой природы электронных подписей, справедливо выделяет [Mason S., 2016: 69-70] три модели развития законодательных подходов в сфере регулирования электронного документооборота и использования электронных подписей:

— «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) [Ловцов Д. А., 2016: 220] а также добавление дополнительного критерия надежности, 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 таких услуг чаще всего лицензируется.

Принципы российской модели электронной подписи 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 мнению российских исследователей, данный подход неоднозначен, поскольку он ни обеспечивает правовую определенность, 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 [Ou P., Tsai A., Kaiser N., 2016: 5]. 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 российского законодательства об электронной подписи.

1. Понятие и функции электронной подписи

1.1. Эволюция российского законодательства об электронной подписи

В России практика электронной подписи и ее 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 использования электронных подписей осуществляется Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи». В отличие от первого закона от 2002 г., данный закон теперь прямо предусматривает другие формы электронной подписи, что позволяет отнести российское законодательство об электронной подписи к двухуровневому подходу, более приближенному к европейскому законодательству.

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…» привнёс существенные изменения и дополнения в Закон № 63-ФЗ. Изменения направлены на усовершенствование системы выдачи квалифицированных сертификатов и технологии использования квалифицированной электронной подписи при участии в правоотношениях разных субъектов электронного документооборота (физических, юридических лиц, нотариусов, государственных служащих, индивидуальных предпринимателей и других категорий лиц). Для второго этапа характерно следующее: значительное ужесточены требования к порядку аккредитации и деятельности удостоверяющих центров (УЦ), расширение полномочий государственных органов по выпуску квалифицированных сертификатов ключей электронной подписи, заметные изменения в технологии подписания электронных документов квалифицированной подписью, в том числе введение в оборот машиночитаемых доверенностей, введение института третьей доверенной стороны и определение понятия метки доверенного времени, а также заложение фундамента для использования облачной электронной подписи и удалённой идентификации лиц-заявителей без необходимости их личной явки для выдачи сертификатов.

Закрепление в законодательстве возможности использования участниками электронного взаимодействия электронной подписи гарантирует её законность и недопустимость признания электронной подписи и (или) подписанного с её помощью электронного документа не имеющими юридической силы лишь исходя из того, что такая электронная подпись поставлена не собственноручно, а с использованием технических средств для автоматического создания и (или) автоматической проверки электронных подписей в информационной системе[3] (ч. 3 ст. 4 ФЗ «Об электронной подписи»).

1.2. Определение и функции электронной подписи

Первоначальный закон № 1-ФЗ от 10.01.2002 г. 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

[3] Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 11.06.2021) «Об электронной подписи» // СЗ РФ. 11.04.2011. № 15. Ст. 2036.

подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе»[4].

В последующем законе слово «цифровая» из дефиниции было исключено. Так, в соответствии с п. 1 ст. 2 закон № 63-ФЗ «Об электронной подписи» 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»[5]. Таким образом, закон устанавливает условия признания электронных документов, подписанных ЭП, равнозначными документам на бумажном носителе с собственноручной подписью[6] (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 «подписью» электронную подпись можно считать лишь условно. Объясняется это тем, что она 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 [Танимов О. В., 2005: 8]. В свою очередь полагаем, что применение самого слова «подпись» в данном случае условно, и криптографическое заверение аутентичности информации является ближайшим по надёжности аналогом собственноручной подписи документов в цифровом мире.

Отметим, что в обеих дефинициях содержится указание на определение при помощи электронной подписи конкретного лица-подписанта. При этом мы считаем данное положение спорным. Конкретнее, электронная подпись не даёт возможность определить со стопроцентной точностью лицо, фактически поставившее электронную подпись в документ [Иванов Н. А., 2006: 11]. Получается, что нет гарантированной уверенности, лишь по факту наличия в документе электронной подписи, установить, что конкретный документ подписан именно владельцем электронной подписи, а не кем-то другим. Соответственно, это даёт пространство для некоторых злоупотреблений и даже правонарушений (при несанкционированном использовании).

Согласно доктринальным мнениям, электронной подписью может быть воспроизведение записи голоса, отправленного либо полученного через Интернет, результат сканирования сетчатки глаза, отпечатка пальца, считанный биометрическими устройствами, рукописная подпись, отсканированная графически, персональный идентификационный номер (PIN) [Kim H., 2019: 3] или даже сообщение электронной почты, в котором человек напечатает свое имя. 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,

---

[4] 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.

[5] Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 11.06.2021) «Об электронной подписи» // СЗ РФ. 11.04.2011. № 15. Ст. 2036.

[6] Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 11.06.2021) «Об электронной подписи» // СЗ РФ. 11.04.2011. № 15. Ст. 2036.

Шестакова Е. В. или Гурьянова Н. В., 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 содержится информация, позволяющая установить подписанта документа, техническая информация, а также криптографические данные. Она также может содержать дату и время подписания, сведения для дополнительных механизмов проверки подписи (которая может производиться как офлайн, так и онлайн [Kazmierczyk Z., Turner I. J., 2021: 1]), расширенную информацию о подписавшем, его полномочиях и отношении к подписываемым данным, комментарии, файлы, графическое изображение собственноручной подписи и другие функционально востребованные данные. В новых поправках к законодательству об электронной подписи, отдельное место уделено регламентации механизма использования метки доверенного времени — достоверной закодированной информации о дате и времени подписания электронного документа электронной подписью. 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.

Заметим, что российское законодательство исходит из концепции всеобщего признания электронных документов, подписанных электронными подписями, которые позволяют достоверно идентифицировать подписавшего, в то же время не отрицая другие виды электронных подписей. Эта концепция лежит в основе международного и зарубежного регулирования электронных подписей.

Что касается 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 [Mason S., 2016: 69]: 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 быть связанной с передаваемыми данными таким образом, что при их случайной или намеренной модификации такая подпись становится недействительной. Данное требование получило

отражение в законодательстве некоторых европейских стран, где понятие «электронная подпись» охватывает все традиционные виды использования собственноручной подписи для обеспечения идентификации подписавшего и установления связи конкретного лица с содержанием документа. Одним из способов защиты владельца электронной подписи является закрепление на законодательном уровне обязательности процедуры удостоверителя заявителя на оформление электронной подписи путем видеофиксации со сроком централизованного хранения записи до окончания срока действия сертификата ключа такой подписи. К сожалению, в действующем законе «Об электронной подписи» подобные формы защиты отсутствуют, что может использоваться злоумышленниками для несанкционированного оформления и использования электронной подписи в противоправных 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 «Об электронной подписи» в качестве видов электронной подписи законодательством предусмотрены простая, усиленная неквалифицированная и квалифицированная электронная подпись.

Законодатель установил, что участники электронного взаимодействия вправе использовать электронную подпись любого вида по своему усмотрению, если требование об использовании определённого вида электронной подписи в соответствии с целями ее использования не предусмотрено федеральными законами или принимаемыми в соответствии с ними нормативными правовыми актами либо соглашением между участниками электронного взаимодействия. Также участники электронного взаимодействия вправе самостоятельно определять любую информационную технологию и (или) технические средства, позволяющие выполнить требования законодательства применительно к использованию конкретных видов электронных подписей [Пешкова Х. В. и др., 2020: 207]. 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

Простая электронная подпись применяется чаще всего для подписания писем или спецификаций, подтверждается с использованием паролей, кодов и иных средств, чаще всего используется в системах корпоративного электронного документооборота. Простые подписи — это комбинации логинов/паролей или кодов и других инструментов, которые позволяют идентифицировать автора документа, но не дают возможность проверить внесение изменений в документ после его подписания. Этот вид подписи может использоваться физические лица при предоставлении в электронной форме услуг муниципальных и государственных учреждений.

Информация в электронной форме, подписанная квалифицированной электронной подписью, признается электронным документом, равнозначным подписанному собственноручной подписью бумажному документу, и может применяться в любых правоотношениях в соответствии с законодательством РФ, кроме случая, если законами или другими нормативными правовыми актами установлено требование о необходимости составления документа исключительно на бумажном носителе[7] (ч. 1 ст. 6 закона № 63-ФЗ «Об электронной подписи»). Также отметим, что документы, требующие наличия печати, не могут быть подписаны простой электронной подписью.

В соответствии с пунктом 2 ст. 6 № 63-ФЗ «Об электронной подписи» 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 Санкт-Петербургской биржи[8] предусматривает, что проверка неквалифицированной электронной подписи осуществляется путем сопоставления информации, содержащейся в полученном электронном документе, подписанном неквалифицированной электронной подписью, и информации, содержащейся в документе на момент его подписания неквалифицированной ЭП. 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

Российским законодательством предусмотрено, что усиленная неквалифицированная подпись (УНЭП) создаётся в процессе криптографической обработки информации и использования закрытого ключа. Усиленная неквалифицированная подпись не только идентифицирует отправителя, но и подтверждает, что после подписания документ не подвергался изменениям. Документ с неквалифицированной электронной подписью может в некоторых случаях быть приравнен к бумажному документу, подписанному собственноручно. 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). Усиленная неквалифицированная подпись создается с использованием криптографических средств, что позволяет не только определить автора документа, но и проверить его на внесение изменений. Для создания таких подписей можно пользоваться сертификатом центра без аккредитации или вовсе обойтись без него, если между сторонами есть соглашение об использовании такой электронной подписи в качестве аналога личной подписи соответствующего лица.

---

[7] Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 11.06.2021) «Об электронной подписи» // СЗ РФ. 11.04.2011. № 15. Ст. 2036.

[8] Соглашение об использовании электронной подписи Публичного акционерного общества «Санкт-Петербургская биржа» // URL: https://spbexchange.ru/ru/otc_market/repository/files/Soglashenie_ob_ispolzovanii_EP.docx

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 [Kirillova E. A. et al., 2019: 294]. По мнению экспертов, вывод о том, что электронные документы, подлежащие проверке налоговой службы, можно удостоверять неквалифицированной подписью, ошибочен. Цифровые документы, заверенные такой подписью, будут равнозначны бумажным только при соблюдении всех условий пункта 2 статьи 6 Федерального закона № 63-ФЗ.

Отличие усиленной квалифицированной электронной подписи от усиленной неквалифицированной состоит в различной степени защищенности 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

Усиленная квалифицированная электронная подпись (УКЭП) аналогична неквалифицированной, но для ее создания и проверки используется криптозащита, сертифицированная ФСБ России. Усиленная квалифицированная подпись имеет сертификат от аккредитованного удостоверяющего центра. Квалифицированные подписи заменяют бумажные документы во всех случаях, за исключением тех, когда закон допускает только собственноручную, «живую» подпись. Важно отметить, что закон № 63-ФЗ признаёт сертификаты ключей подписей, выданные в соответствии с предшествующим законом 2002 г., квалифицированными сертификатами.

Определение удостоверяющего центра, содержащееся в законе № 63-ФЗ: «юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также другие функции, предусмотренные настоящим Федеральным законом». Заметим, что в Законе № 63-ФЗ появляется понятие аккредитованного удостоверяющего центра, которого не было в существовавшем ранее законодательстве. Вероятно, 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 устанавливает личность обратившегося за ней. Если это представитель юридического лица, центр проверяет также и его полномочия. В дальнейшем УЦ обеспечивает конфиденциальность ключей электронной подписи. При получении соответствующего обращения он вправе осуществить проверку электронной подписи (п. п. 1, 9 ч. 1, п. 4 ч. 2 ст. 13 Закона об электронной подписи). Федеральный закон № 476-ФЗ от 27.12.2019 г. 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[9].

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 [Chong K. W. et al., 2021: 1]. Под облачной подписью понимается то, что теперь 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 указанного ключа электронной подписи и предоставление по его требованию истории использования 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 убытки, причинённые в случае компрометации и (или) несанкционированного использования хранимых ключей электронной подписи.

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 Федерального закона от 27.12.2019 № 476-ФЗ) Идентификация будет проведена через ЕСИА (Единую систему идентификации и аутентификации) или при помощи ЕБС (Единой биометрической системы)[10]. 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

[9] Митина А. Новые правила в регулировании рынка электронной подписи // 19.07.2021. URL: https://cryptoarm.ru/news/rynok-ecp/

[10] Якушкина О. Перспективы развития облачной подписи // 05.10.2020. URL: https://cryptoarm.ru/news/oblachnoy-podpisi/

конфиденциальность ключей подписи, в том числе обязаны не допускать несанкционированного использования своих ключей, а также не использовать ключ при наличии оснований полагать, что его конфиденциальность нарушена [Дарькина М. М., 2020: 30].

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

В плане разграничения понятий закон 63-ФЗ внёс большую ясность в понятийный аппарат, заложенный законом № 1-ФЗ. Так, в законе 1-ФЗ присутствовала определённая путаница с термином «сертификат ключа подписи», связанная с тем, что понятие применялось к владельцу как закрытого ключа, так и открытого[11]. В законе 63-ФЗ эта проблема решается путём различения ключа электронной подписи и ключа проверки электронной подписи. Кроме того, были введены отдельные понятия сертификата ключа электронной подписи, принадлежащего её владельцу, и сертификата ключа проверки ЭП, выданного 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…».

Кроме того, Правительство РФ еще 30.08.2012 утвердило изменения в Регламент об электронном документообороте в органах государственной власти [Дарькина М. М., 2020: 29] — государственным органам было разрешено вносить документы в Правительство в электронном виде с использованием цифровой подписи.

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[12]. В проекте используются сервисы единой цифровой платформы для создания и выдачи электронной подписи, предоставляемые ПАО «Ростелеком» и ПАО «Банк ВТБ». 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

[11] 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.

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

подписывать с помощью «Госключа», будет расширен, в том числе планируется его использование для онлайн-подписания договоров купли-продажи автомобиля 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 федеральным законом № 476-ФЗ от 27.12.2019 г. 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 юридического лица без доверенности, необходимо получить квалифицированную электронную подпись 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[13].

3.2. Практика применения электронной подписи в частноправовой сфере

Российскими судами уже рассматривался вопрос о том, может ли физическое лицо оформить усиленную электронную подпись 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 содержалась информация о том, что лицо имеет право действовать от имени организации. Например, Нижегородский областной суд в 2018 г. (дело № 33-5337/2018[14]) в лице судебной коллегии по гражданским делам рассматривал ситуацию, связанную с тем, что одной усиленной квалифицированной электронной подписью, выданной на юридическое лицо, были подписаны договор займа, который был предоставлен юридическому лицу, и договор поручительства, оформленный с физическим лицом, которым являлся генеральный директор этого же ООО. В апелляционной жалобе, поданной представителем физического лица, было отмечено, что для признания контракта заключенным посредством обмена электронными письмами необходимо было заключить соглашение между участниками электронного взаимодействия на использование электронной подписи и обмена электронными сообщениями. Суд при оценке доказательств не учел, 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 отметил, что на основании пункта 1 статьи 2 и статьи 18 Закона № 63-ФЗ электронная подпись служит средством идентификации лица, подписавшего информацию. Сертификат ключа проверки

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

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

электронной подписи ООО был выдан на имя данного физического лица. Договор поручительства от имени физического лица был подписан сертификатом, выданным на его имя, то есть он был подтвержден электронной подписью, которая доказывает его подлинность и подтверждает авторство подписи гражданина.

Как видим, суд сделал вывод о том, что раз УКЭП юридического лица выдана на конкретное физическое лицо и его данные включены в сертификат ключа проверки подписи, то это физическое лицо имеет право использоваться им для подписания документов в собственных интересах. 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, в части сотрудников юридического лица. Что касается представителя, имеющего право действовать без доверенности, то вопрос остаётся открытым.

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. То есть электронная подпись иностранного или международного стандарта, выпущенная за рубежом, будет иметь в Российской Федерации юридическую силу, если её действительность 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 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 — 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[15]. Задача доверенной третьей стороны с правовой точки зрения заключается в проведении проверки электронных подписей в электронных документах в фиксированный момент времени, а также документальном подтверждении результатов такой проверки. В настоящее время привлечение доверенной стороны является добровольным. Деятельность доверенной третьей стороны может осуществляться

[15] 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.

юридическими лицами после получения соответствующей аккредитации в Минкомсвязи России. Отметим, что вмешательство доверенной третьей стороны влечет за собой образование инфраструктуры, контролирующей ее функционирование, устанавливающей технологические и регуляторные требования, и известной как Public Key Infrastructure (PKI) [Laborde C.M., 2010: 41].

Заключение

В условиях активной цифровизации общества и формирования цифровой экономики наблюдается недостаточность и неэффективность традиционных правовых механизмов регулирования современных цифровых технологий, включая механизмы электронной идентификации. Большинство исследователей цифрового права приходят к выводу, что законодательное регулирование в России строится на основе анализа зарубежного опыта, но без учета 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 внедрения. Помимо этого, высокая безопасность цифровых подписей, обусловленная математическими моделями, одновременно влечет сложности для каждодневного и удобного использования подписей бизнесом и гражданами, даже в Евросоюзе с его отлаженными правовыми механизмами [Krawczyk P., 2010: 17]. 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, закрепленного 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 [Kussainova A. K. et al., 2020: 312], следовательно, они могут использовать уже накопленный опыт России для совершенствования своего собственного законодательства.

Данные 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 [под общ. ред. Минбалеева А. В., 2019: 198]. 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.

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

4. 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.

5. 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.

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

7. Chong K. W. et al. (2021). A Study of Factors Affecting Intention to Adopt a Cloud-Based Digital Signature Service. Information, vol. 10, no. 7. 15 p.

8. Kazmierczyk Z., Turner I. J. (2021). Self-identification of electronically scanned signatures (ESS) and digitally constructed signatures (DCS). Forensic Science Research, 4 p.

9. Kim H. (2019). Globalization and regulatory change: The interplay of laws and technologies in E-commerce in Southeast Asia. Computer Law & Security Review, vol. 35, no. 5, 20 p.

10. Kussainova A. K. et al. (2020). Legal Issues for Electronic Documents Workflow Regulation. The Law, State and Telecommunications Review, vol. 12, no. 1, p. 293-318.

11. Kirillova E. A. et al. (2019). Legal status of smart contracts: features, role, significance. Jurídicas CUC, vol. 15, no. 1, p. 285-300.

12. Krawczyk P. (2010). When the EU qualified electronic signature becomes an information services preventer. Digital Evidence and Electronic Signature Law Review, vol. 7, p. 7-18.

13. Laborde, C. M. (2010). Electronic Signatures in International Contracts. Frankfurt am Main: Peter Lang, 247 p.

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

15. Ou P., Tsai A., Kaiser N. (2016). The e-signature in Taiwan: consent, integrity and accessibility. Digital Evidence and Electronic Signature Law Review, no. 13, p. 148-153.

References

1. Chong K. W. et al. (2021). A Study of Factors Affecting Intention to Adopt a Cloud-Based Digital Signature Service. Information, 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. P. 28-35.

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

4. Kazmierczyk Z., Turner I. J. (2021). Self-identification of electronically scanned signatures (ESS) and digitally constructed signatures (DCS). Forensic Science Research, 4 p.

5. Kim H. (2019). Globalization and regulatory change: The interplay of laws and technologies in E-commerce in Southeast Asia. Computer Law & Security Review, vol. 35, no. 5, 20 p.

6. Kussainova A. K. et al. (2020). Legal Issues for Electronic Documents Workflow Regulation. The Law, State and Telecommunications Review, vol. 12, no. 1, p. 293-318.

7. Kirillova E. A. et al. (2019). Legal status of smart contracts: features, role, significance. Jurídicas CUC, vol. 15, no. 1, p. 285-300.

8. Krawczyk P. (2010). When the EU qualified electronic signature becomes an information services preventer. Digital Evidence and Electronic Signature Law Review, vol. 7, p. 7-18.

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

10. Lovcov D. A. Sistemologiya pravovogo regulirovaniya informacionnyh otnoshenij v infosfere: Monografiya. M.: RGUP, 2016. 316 p.

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

12. Ou P., Tsai A., Kaiser N. (2016). The e-signature in Taiwan: consent, integrity and accessibility. Digital Evidence and Electronic Signature Law Review, no. 13, p. 148-153.

13. 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 ConsultantPlus. 2020. 229 p.

14. 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.

15. Tanimov O. V. Elektronnyj dokument i elektronnaya cifrovaya podpis' kak yuridicheskie fikcii // Informacionnoe pravo. 2005. № 3. P. 7-9.