

Содержание:

image not found or type unknown



Введение

В 2002 г. Постановлением Правительства РФ от 28 января 2002 г. № 65 была утверждена Федеральная целевая программа «Электронная Россия (2002 - 2010 годы)». Данная Программа стала важным шагом на пути развития электронного документооборота и электронной торговли в России. Принятие названной Программы стало возможным благодаря формированию законодательной базы в сфере электронного документооборота. И прежде всего следует отметить принятие Федерального закона от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи» (далее – Федеральный закон). Этот Федеральный закон, по оценкам специалистов, дает значительный стимул развитию всего высокотехнологического бизнеса в России.

Информационные технологии, бурное развитие которых началось в 90-е годы, коренным образом изменили нашу жизнь. Темпы информатизации российского общества одни из самых высоких в мире. Уже сегодня большая часть оборота информации и документов осуществляется в электронном виде. Технология же электронной подписи способна еще более расширить возможности электронного документооборота, распространить его на все сферы общественной жизни. Технологии электронной цифровой подписи постепенно завоевывают признание во всем мире. Вместе с тем развитие возможностей электронной коммерции благоприятным образом скажется в целом на рынке российских информационных технологий, т.к. все проекты электронной коммерции, такие как Интернет-торговля, Интернет-банкинг, Интернет-провайдинг, являются крупными потребителями прикладного программного обеспечения, а его разработка создаст целую отрасль специализированных программно-технологических предприятий в России.

Все сказанное характеризует актуальность темы работы.

Цель контрольной работы: изучение электронной цифровой подписи как инструмента для придания юридической силы электронным документам.

Исходя из поставленной цели, можно выделить следующий круг задач:

1. Рассмотреть правовое регулирование отношений в области использования электронной цифровой подписи.
2. Раскрыть понятие и сущность электронной цифровой подписи как основного реквизита электронного документа. Условия использования электронной цифровой подписи.
3. Охарактеризовать электронный документ.
4. Рассмотреть особенности использования электронной цифровой подписи.

При работе над данной темой и решении поставленных задач использовались: нормативно-правовые источники, регулирующие использование электронную цифровую подпись, учебные пособия.

1. Правовое регулирование отношений в области использования электронной цифровой подписи

Правовое регулирование отношений в области использования электронной цифровой подписи осуществляется в соответствии с настоящим Федеральным законом, Гражданским кодексом Российской Федерации (далее - ГК РФ), Федеральным законом «Об информации, информационных технологиях и защите информации», Федеральным законом «О связи», другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, а также осуществляется соглашением сторон.

До принятия настоящего Федерального закона правовой базой для применения электронной цифровой подписи (далее - ЭЦП) являлись п. 2 ст. 160, ст. 434 ГК РФ. Статья 434 ГК РФ предоставляет сторонам возможность заключать договоры путем телетайпной, телефонной, электронной связи, позволяющей достоверно установить, что документ исходит от стороны по договору. При этом п. 2 ст. 160 ГК говорит, что использование ЭЦП при заключении сделок допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон.

Согласно п. 3. ФЗ «Об информации, информационных технологиях и защите информации», электронное сообщение, подписанное электронной цифровой

подписью или иным аналогом собственноручной подписи, признается электронным документом, равнозначным документу, подписанному собственноручной подписью, в случаях, если федеральными законами или иными нормативными правовыми актами не устанавливается или не подразумевается требование о составлении такого документа на бумажном носителе.

Законодатель не говорит и о том, какая категория документов может подтверждаться ЭЦП, а следовательно, полагаем, что речь может идти о любых документах, хранимых, обрабатываемых и передаваемых с помощью информационных и телекоммуникационных систем, за исключением тех, которые в соответствии с законодательством могут существовать только в бумажном виде. Так, в частности, согласно ст. 4 Федерального закона от 11 марта 1997 г. № 48-ФЗ «О переводном и простом векселе» простой и переводной векселя могут быть составлены только на бумаге.

Отдельные положения, касающиеся применения ЭЦП, содержатся в Федеральном законе от 10 января 2003 г. № 20-ФЗ «О Государственной автоматизированной системе Российской Федерации «Выборы». В частности, в ст. 12 данного Закона говорится, что электронные документы, подготовленные с использованием ГАС «Выборы», приобретают юридическую силу после их подписания электронной цифровой подписью соответствующих должностных лиц, а протокол, сводная таблица о голосовании и иные сводные документы, подготовленные в электронном виде, приобретают юридическую силу только после «обязательной проверки с помощью открытых ключей электронной цифровой подписи подлинности всех исходных электронных документов, на основе которых готовится сводный электронный документ».

В соответствии с п. 3 ст. 75 Арбитражного процессуального кодекса Российской Федерации документы, подписанные с помощью ЭЦП, могут представляться в качестве письменных доказательств в арбитражном процессе. Аналогичная позиция была изложена в раздел IV письма Высшего Арбитражного Суда РФ от 19 августа 1994 г. № С1-7/ОП-587 «Об отдельных рекомендациях, принятых на совещаниях по судебно-арбитражной практике».

Итак, Федеральный закон состоит из 5 глав, 21 статьи.

В главе I «Общие положения» (ст. ст. 1 - 3) определяется сфера правового регулирования, указывается состав законодательства в области использования электронной цифровой подписи, а также раскрываются основные понятия,

используемые в Федеральном законе.

В главе II «Условия использования электронной цифровой подписи» (ст. ст. 4 - 7) закреплены условия, при соблюдении которых признается равнозначность электронной цифровой подписи и собственноручной подписи, условия использования средств электронной цифровой подписи, содержание и порядок хранения сертификата ключа подписи - документа, позволяющего подтверждать подлинность электронной цифровой подписи и ее принадлежность конкретному лицу.

Глава III «Удостоверяющие центры» (ст. ст. 8 - 15) регламентирует статус и деятельность организаций, обеспечивающих функционирование технологии электронной цифровой подписи, принципы взаимодействия между удостоверяющим центром и уполномоченным федеральным органом исполнительной власти. В этой же главе определяются основные права и обязанности удостоверяющих центров и владельцев сертификатов ключа, указываются основания для приостановления, аннулирования сертификата ключа подписи, последствия прекращения деятельности удостоверяющего центра.

В главе IV «Особенности использования электронной цифровой подписи» (ст. ст. 16 - 19) предусмотрены особенности использования электронной цифровой подписи в сфере государственного управления, в корпоративных информационных системах (с ограниченным кругом участников), а также условия признания иностранных сертификатов электронной цифровой подписи и случаи, когда электронная цифровая подпись может замещать не только собственноручную подпись, но и печать.

Глава V (ст. ст. 20 и 21) устанавливает заключительные и переходные положения, связанные с введением в действие Федерального закона.

Федеральный закон основывается на следующих принципах.

1. Цифровая подпись не может быть дискриминирована по сравнению с собственноручной подписью только по тому основанию, что она имеет электронную форму. Если соблюдены все указанные в Федеральном законе требования, предъявляемые к электронной подписи, то она порождает те же правовые последствия, что и собственноручная. Более того, обе подписи могут быть равным образом использованы в качестве доказательства в суде.

2. Осуществление государственного контроля за обращением продуктов и услуг, связанных с электронной цифровой подписью, который проявляется прежде всего в том, что физические и юридические лица могут использовать только сертифицированные средства электронной цифровой подписи, а деятельность удостоверяющих центров подлежит лицензированию.
3. Федеральный закон устанавливает минимальные и достаточные требования, предъявляемые как к самой электронной цифровой подписи, так и к удостоверяющим центрам.
4. Правовым признанием пользуется электронная цифровая подпись, полученная с помощью использования технологий асимметричной криптографии.
5. Широкая сфера применения электронной цифровой подписи. Электронная цифровая подпись может использоваться субъектами публичных отношений для идентификации отправителя и (или) в частноправовой сфере для подписания договоров. При этом Федеральный закон не касается вопросов заключения и действительности договоров, которые относятся к предмету регулирования Гражданского кодекса.
6. Признание иностранного сертификата ключа подписи, что, несомненно, способствует не только развитию внутреннего рынка, но и международной электронной коммерции.

2. Понятие и сущность электронной цифровой подписи как основного реквизита электронного документа

Развитие систем электронного документооборота, электронных платежей, электронной почты, распространение информационных систем с большим числом пользователей поставили задачу нахождения инструмента взаимодействия с помощью электронных средств, при котором пользователи, в т.ч. незнакомые друг с другом, могли бы достоверно передавать друг другу информацию, точно определять источник той или иной информации, полученной ими по электронным каналам, а сам источник информации не мог бы отрицать свое авторство. Таким инструментом стали реквизиты, идентифицирующие электронный документ, которые в значительной степени и определяют его юридическую силу. Существует

множество различных способов идентифицировать информацию, зафиксированную в электронном документе, которые различаются по степени достоверности.

Так, С. Бернет и С. Пейн считают, что электронная подпись «...это любой знак или процедура, реализованные электронными средствами, то есть выполненные или принятые участвующей стороной с намерением связать запись с обязательством или удостоверить подлинность записи». В соответствии с приведенным определением электронной подписью может являться выходной сигнал сложного биометрического устройства, такого как система компьютерного распознавания отпечатков пальцев или простой ввод имени в конце электронного сообщения, т.е. в соответствии с данным определением для электронной подписи технология ее создания электронными средствами не имеет значения.

Н.И. Соловяненко также указывает на то, что связанные с электронным документом символы, коды, пароли и т.д. могут рассматриваться как электронная подпись, если они «исполнены или приняты сторонами по взаимному соглашению и с явным намерением подтвердить подлинность написанного». При этом Н.И. Соловяненко справедливо полагает, что доверие к электронной подписи обеспечивается посредством следующей общей схемы:

во-первых, реализуется принятый международной практикой принцип функционального эквивалента, который предполагает, что во всех случаях, когда правовая система государства требует наличия подписи, таковым требованиям удовлетворяет электронная подпись;

во-вторых, между контрагентами заключается соглашение, оговаривающее возможность и условия использования электронной подписи в предпринимательской деятельности. «Стороны договариваются о том, что электронные подписи, сопровождающие передаваемый документ, достаточны для удостоверения того, что документ создан надлежащей стороной».

Цифровая подпись, по мнению С. Бернета и С. Пейна, может быть определена как «заданное преобразование записи с помощью несимметричной криптосистемы и хэш-функции так, что лицо, располагающее исходной записью и открытым ключом автора сообщения, может точно определить, осуществлялось ли преобразование с помощью секретного ключа, соответствующего открытому ключу автора и была ли исходная запись изменена после того, как было выполнено ее преобразование» . Тот смысл, который вкладывают С. Бернет и С. Пейн в термин «цифровая подпись» в значительной степени соответствует определению электронной цифровой

подписи, сформулированному в п. 3 ФЗ «Об электронной цифровой подписи»: «Электронная цифровая подпись - 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», - что позволяет сделать вывод, что термины «электронная цифровая подпись» и «цифровая подпись» должны рассматриваться как синонимы.

Однако существует и иная точка зрения. Е.В. Ильиных и М.Н. Козлова указывают на необходимость разграничения таких смежных категорий, как «электронная цифровая подпись», «цифровая подпись» и «аналоги собственноручной подписи». К аналогам собственноручной подписи кроме ЭЦП относят пароли, PIN-коды, факсимильное изображение и т.д. Цифровая подпись является также более общим понятием по отношению к электронной цифровой подписи. ЭЦП следует считать такую цифровую подпись, которая создана с использованием системы сертификатов и удостоверяющих центров.

Итак, электронная цифровая подпись (цифровая подпись) создается с помощью криптографической системы с открытым ключом, тогда как электронная подпись генерируется любым компьютерным методом, включая криптосистемы с открытым ключом. Электронные цифровые подписи (цифровые подписи) привязаны к определенной технологии, электронные подписи - более широкое понятие и от технологии не зависят.

Российскому законодательству известны и другие определения электронной цифровой подписи, приведем лишь некоторые из них.

Электронная цифровая подпись (ЭЦП) - вид аналога собственноручной подписи, являющийся средством защиты информации, обеспечивающим возможность контроля целостности и подтверждения подлинности электронных документов (далее - ЭД). ЭЦП позволяет подтвердить ее принадлежность зарегистрированному владельцу. ЭЦП является неотъемлемой частью ЭД (пакета ЭД).

Электронная цифровая подпись (ЭЦП) - последовательность символов, полученная в результате криптографического преобразования исходной информации, которая позволяет подтверждать целостность и неизменность этой информации, а также ее авторство.

Электронная цифровая подпись основана на асимметричных криптографических алгоритмах. Особенностью таких алгоритмов является то, что для шифрования информации используется один ключ, а для ее расшифровки - другой, специальным образом полученный из первого. При этом первый ключ является секретным - закрытым ключом, он известен только лицу, подписывающему документ: «...закрытый ключ электронной цифровой подписи - уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи...». Вторым ключом - несекретным - открытым ключом, он может быть известен любому получателю документа: «Открытый ключ электронной цифровой подписи - уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе...» (ст. 3 Федерального закона).

По мнению А. Гарибян, ЭЦП обладает двумя основными свойствами: 1) воспроизводима только одним лицом, а подлинность ее может быть удостоверена многими; 2) она неразрывно связана с конкретным документом и только с ним.

Определение ЭЦП, закрепленное в ФЗ «Об электронной цифровой подписи», не ставит задачи идентификации автора электронного документа. Речь идет об идентификации владельца сертификата ключа подписи, а это представляется вполне возможным.

В сочетании с положениями ст. 4 ФЗ «Об электронной цифровой подписи», устанавливающей условия признания равнозначности ЭЦП в электронном документе и собственноручной подписи в документе на бумажном носителе, а именно:

- сертификат ключа подписи, относящийся к этой электронной цифровой подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания;
- подтверждена подлинность электронной цифровой подписи в электронном документе;

- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи, - презумпция авторства в значительной степени гарантировала бы юридическую силу электронного документа, заверенного ЭЦП.

Таким образом, стабильный юридически значимый электронный документооборот субъектов предпринимательской деятельности нуждается, прежде всего, не в разрозненных ведомственных нормативных актах, а в законе, детально регламентирующем порядок использования ЭЦП в электронном документе.

На основании вышеизложенного можно сделать следующие выводы.

1. Наиболее важным реквизитом электронного документа является электронная подпись.
2. Электронная подпись, основанная на асимметричных криптографических алгоритмах, - электронная цифровая подпись, на сегодняшний день является самым надежным с технической точки зрения способом идентификации информации электронного документа. Однако использование технологии открытых ключей нуждается в детальной правовой регламентации.

Каждая подпись уникальна для подписанных данных и используемых ключей. Когда один человек подписывает два сообщения одним и тем же ключом, подписи будут различными. Более того, когда два человека с различными ключами подписывают одни и те же данные, их подписи будут различными.

3. Электронный документ

В связи с возрастающим хранением и использованием информации все чаще используется понятие электронного документа. Действующее законодательство дает понятия обычного и электронного документа (далее - ЭД). Документированная информация (документ) представляет собой зафиксированную на материальном носителе информацию с реквизитами, позволяющими ее идентифицировать. Электронный документ совершенно отличается от той последовательности символов, которые в нем представлены.

В соответствии со ст. 3 Федерального закона, электронный документ - документ, в котором информация представлена в электронно-цифровой форме. Составление электронного документа состоит не в последовательном написании на бумажный

носитель букв, а в нанесении совокупности невзаимосвязанных между собой математических символов.

Для электронного документа характерны все признаки, присущие юридической фикции: универсальность; нормативное закрепление фикции в нормах права; неопровержимость юридической фикции; заведомая условность; особое целевое назначение в механизме правового регулирования общественных отношений; способность фикций вызывать друг друга.

Следует отметить, что использование электронных документов началось еще до появления глобальной сети Интернет, однако ее появление стало мощным толчком к развитию безбумажных технологий в предпринимательской деятельности.

В настоящее время хозяйствующие субъекты применяют электронный документооборот, базирующийся как на информационной среде Интернета, так и на иных электронных формах, электронных средствах. При этом, с точки зрения правового регулирования используемые средства коммуникации не влияют на юридическую значимость формируемых электронных документов.

С внедрением новых информационных технологий вместо бумаги в качестве материальных носителей стали использоваться электронные носители - магнитные и оптические диски, электрические колебания, электромагнитные волны. В связи с этим происходит постепенный процесс вытеснения бумажного документа и замены его формой электронного документа. К сожалению, в отличие от информации, зафиксированной на бумажном носителе, информация на электронном носителе может быть легко изменена без желания ее автора в результате несанкционированного доступа к ней постороннего лица, причем без всяких следов такого вмешательства. Применение электронного документа вызывает свои сложности, которых можно избежать при использовании бумажных документов. Поэтому возникает вопрос о том, насколько оправданно и целесообразно применение электронного документа в российской практике. Иными словами, сможет ли электронный документ конкурировать с бумажным, вытеснить его, ведь при применении электронных документов неизбежны дополнительные материальные затраты. Вообще при использовании систем электронного документооборота (далее - ЭДО) возникают различные проблемы. К таким проблемам можно отнести следующие: проверка подлинности электронного документа; возможность использования электронных документов в качестве доказательств в арбитражных судах; распределение риска убытков, которые могут возникнуть в процессе функционирования систем ЭДО; взаимоотношения

юридических лиц, использующих ЭДО, с аудиторскими фирмами, налоговыми и другими государственными органами, куда необходимо представлять отчетность о своей деятельности; международно-правовые проблемы, которые могут возникнуть, когда, например, два участника, ЭДО и провайдер, находятся в разных странах; стандартизация; защита прав субъектов авторского и патентного права; защита информации в системах ЭДО. Проверка подлинности электронного документа является одной из основных проблем его применения. Для решения этой проблемы и применяется ЭЦП.

В результате сказанного хотелось бы подчеркнуть следующее:

- электронный документ и электронная цифровая подпись представляют собой технико-юридический прием - фикцию, являющуюся одной из основ регулирования общественных отношений с применением информационных технологий в сфере электронного документооборота.

4. Особенности использования электронной цифровой подписи

Статья 16 Федерального закон предусматривает широкое использование электронной цифровой подписи среди государственных органов власти - федерального уровня, субъектов Федерации, органов местного самоуправления, а также организаций, участвующих в документообороте с такими органами. При этом электронная цифровая подпись закрепляется за конкретным физическим лицом, уполномоченным государственным органом или организацией. Таким образом, владельцем электронной цифровой подписи является не орган или организация, а его должностное лицо. В практической деятельности это может привести к возможному злоупотреблению владельцем своими полномочиями, например, лицо может продолжать скреплять электронные документы своей электронной цифровой подписью и после того, как оно лишилось своего должностного положения.

Федеральным органом исполнительной власти, являющимся по существу удостоверяющим центром по отношению к уполномоченным лицам федеральных государственных органов, является Федеральное агентство по информационным технологиям. Оно ведет специальный реестр сертификатов ключей подписей, выдает пользователям сертификаты, подтверждающие подлинность электронных

цифровых подписей тех или иных должностных лиц, включенных в реестр. Федеральное агентство по информационным технологиям осуществляет данную деятельность в соответствии с правилами, установленными в отношении деятельности удостоверяющих центров

Использование электронного документооборота, в том числе и электронной цифровой подписи, в отношениях между двумя или несколькими договорившимися хозяйствующими субъектами имело свое место значительно раньше принятия данного Федерального закона. Например, взаимодействие банка с клиентом по электронной системе «банк-клиент», которая успешно продолжает применяться во многих банках и в настоящее время (ст. 17 Федерального закона).

Порядок использования ЭЦП в отношениях между коммерческими банками, Центральным банком РФ ввиду особого статуса последнего регулируется нормативно-правовыми актами ЦБ РФ и договорами об обмене электронными документами, утвержденными в качестве приложений к актам.

Корпоративная информационная система представляет собой информационную систему, состоящую из ограниченного круга лиц - ее участников. Количество и круг лиц определяются владельцем такой системы либо соглашением между ее участниками.

Федеральный закон предоставляет корпоративным системам относительную автономность. Так, если корпоративная система не взаимодействует с участниками информационной системы общего пользования, то вопросы внутреннего функционирования и взаимодействия между участниками решаются ею самостоятельно на основании внутренних нормативных актов. Если корпоративная система взаимодействует с любой из систем общего пользования, например предоставляет услуги удостоверяющего центра корпоративной информационной системы, то она автоматически должна соответствовать требованиям, предъявляемым Федеральным законом к информационным системам общего пользования.

К внутренним вопросам корпоративной системы относится определение порядка использования электронных цифровых подписей, что регулируется внутренними нормативными актами. Внутренними актами корпоративной информационной системы признаются соглашения участников данной системы либо решения владельца системы, которые являются обязательными для остальных ее участников (клиентов).

Данные нормативные акты определяют содержание информации в сертификатах ключей подписей, порядок ведения реестра сертификатов, порядок хранения аннулированных сертификатов, случаи утраты юридической силы данными сертификатами. Также соглашением участников может быть определен тот участник, на которого возлагаются функции удостоверяющего центра.

Содержание документа на бумажном носителе, заверенного печатью и преобразованного в электронный документ, может быть подписано электронной цифровой подписью и будет иметь равную юридическую силу, но при условии, что такое преобразование осуществлено согласно имеющемуся соглашению между сторонами либо в соответствии с нормативным правовым актом (ст. 19 Федерального закона).

Данная возможность использования электронной цифровой подписи в качестве эквивалента не только собственноручной подписи, но и печати значительно расширяет возможности организаций в гражданско-правовых отношениях.

Надо отметить, что Гражданский кодекс РФ не предусматривает обязательного скрепления договора печатью, а относит это к дополнительному требованию, которое может устанавливаться по соглашению сторон, законом или иными нормативными правовыми актами. Но хотя скрепление печатью договоров и иных документов организаций не является обязательным, ряд подзаконных нормативных актов налоговых органов прямо указывает на такую необходимость. Кроме того, Гражданский кодекс РФ предписывает на доверенность, выданную от имени юридического лица, помимо подписи руководителя прикладывать и печать данной организации. Федеральный закон признает равнозначность для владельца электронной цифровой подписи как его собственноручной подписи, так и собственноручной подписи, заверенной печатью. Это положение предоставляет возможность использования электронной цифровой подписи не только организациям в своей хозяйственной деятельности, но и физическим лицам, чья подпись на бумажном носителе заверена печатью, например нотариусам. Удостоверяющий центр берет на себя ответственность за подтверждение подлинности и аутентичности документа, подписанного электронной цифровой подписью именно владельцем сертификата ключа подписи.

Можно говорить, что удостоверяющий центр выполняет согласно Закону об ЭЦП функцию нотариусов в электронном документообороте.

Заключение

Итак, развитие и широкое применение информационных и коммуникационных технологий является глобальной тенденцией мирового развития и научно-технической революции последних десятилетий.

Сегодня субъекты предпринимательской деятельности взаимодействуют посредством электронного документооборота как между собой, так и с конечными потребителями и органами власти.

Задача реформирования российского законодательства в связи с переходом к активному использованию электронного документооборота поставлена на государственном уровне. Правовой основой регулирования электронной цифровой подписи как инструмента для придания юридической силы электронным документам является Федеральный закон «Об электронной цифровой подписи».

Принципиально важным для стабилизации и безопасности электронного документооборота является, с одной стороны, прямое закрепление в нормах права презумпции авторства, в соответствии с которой электронная цифровая подпись в электронном документе признается созданной владельцем сертификата ее открытого ключа, если владелец сертификата ключа подписи не докажет обратное, с другой стороны, установление обязанности удостоверяющих центров непосредственно проверить соответствие данных, изложенных в заявлении на изготовление сертификата ключа электронной цифровой подписи, предоставленным документам.

Особое внимание в работе уделено исследованию правового регулирования использования такого электронного аналога собственноручной подписи, как электронная цифровая подпись (ЭЦП). Это объясняется предпринятой в действующих нормах права попыткой законодательного закрепления равенства собственноручной и электронной цифровой подписи при условии соблюдения требований закона

ЭЦП позволяет подтвердить ее принадлежность зарегистрированному владельцу. ЭЦП является неотъемлемой частью электронного документа.

ЭЦП обладает двумя основными свойствами: 1) воспроизводима только одним лицом, а подлинность ее может быть удостоверена многими; 2) она неразрывно связана с конкретным документом и только с ним.

Рассматривая правовой режим электронного документа, отмечено соответствие его правовых признаков закрепленным в действующем законодательстве признакам документа в традиционном понимании, электронный документ - это документ на новом техническом уровне, а следовательно, на него должен быть распространен правовой режим документа вообще.