

ОБ АНАЛОГАХ СОБСТВЕННОРУЧНОЙ ПОДПИСИ

Н. А. Иванов, старший преподаватель кафедры правовой информатики Омского юридического института, кандидат юридических наук

Для того чтобы официальный документ обладал юридической силой, он должен быть подписан автором документа или уполномоченным должным образом лицом. Если документ является многосторонним, т. е. составленным от имени двух и более сторон, то он должен быть завизирован каждой из сторон.

Отсутствие подписи на официальном документе (или одной из подписей на многостороннем документе) автоматически приводит к признанию его недействительным и не обладающим юридической силой.

Статьей 160 Гражданского кодекса РФ помимо исполнения рукописной подписи допускается использование «факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи либо иного аналога собственноручной подписи». Заложив данную фразу в законодательный акт, авторы кодекса допустили несколько серьезных ошибок.

Во-первых, собственноручная рукописная подпись является уникальной биометрической характеристикой лица, подписывающего документ. Факсимильное воспроизведение подписи с помощью средств механического или иного копирования является ничем иным как нанесением изображения подписи. Изображение подписи, нанесенное каким-либо способом в документе, никоим образом не может быть напрямую связано с биометрическими характеристиками лица, подпись от имени которого являлась прообразом для нанесения ее изображения.

Во-вторых, говоря о документах, полученных по телекоммуникационным каналам связи, нужно также четко представлять, что речь идет уже не об оригиналах документов, а о копиях документов, и что по копии документа лишь в очень ограниченном количестве случаев можно установить способ или технологию нанесения подписи на оригинале документа.

В-третьих, можно допустить признание юридической силы копий документов, полученных по телекоммуникационным каналам связи, в которых имеется изображение подписи, но при этом необ-

ходимо помнить, что нанесение изображения подписи «с помощью средств механического или иного копирования» является одним из основных способов технической подделки подписей.

Для предотвращения фактов использования поддельных документов в официальном документообороте нормативными актами¹ отдельных министерств и ведомств напрямую запрещено нанесение на документы каким-либо способом изображения подписи в официальных документах, доверенностях, платежных документах и иных документах, имеющих финансовые последствия. Специальными нормативными актами установлены ограничения на документы (а вернее, копии документов), полученные по телекоммуникационным каналам связи. Так, Федеральная служба России по надзору за страховой деятельностью установила, что документы (бухгалтерские и статистические отчеты, документы на лицензирование, запросы и т. п.), поступившие по факсимильной связи, не имеют юридической силы.

С учетом вышеизложенного полагаем, что п. 2 ст. 160 ГК РФ следовало бы сформулировать следующим образом: «В случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон, копии документов с имеющимися в них изображениями подписей признаются обладающими юридической силой при наличии у каждой из сторон идентичного экземпляра оригинала документа, подписанного собственноручной подписью». При этом следует оговориться, что данная формулировка относится только к традиционным документам, изготовленным на бумажных или аналогичных им носителях.

Проблема уменьшения сроков создания документов и ускорения процессов передачи документов была решена путем создания так называемых «документов на машинных носителях» или «электронных документов» (ЭД).

В ГОСТе Р 51141-98 «документ на машинном носителе» определялся как «документ, созданный

¹ См.: Об использовании факсимиле подписи: письмо МНС РФ от 1 апреля 2004 г. № 18-0-09/000042; О порядке оформления карточки с образцами подписей и оттиска печати: указание ЦБР от 21 июня 2003 г. № 1297-У.

с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной»². В Федеральном законе «Об электронно-цифровой подписи»³ и ГОСТе Р 52069.0-2003⁴ электронный документ определялся как «документ, в котором информация представлена в электронно-цифровой форме».

Вне зависимости от способа создания электронных документов, также как и при использовании традиционных документов на бумажных носителях, требуется, учитывая специфическую форму ЭД, каким-либо способом осуществить процедуру его удостоверения (подписания, визирования) автором документа, или сторонами, от имени которых он составлен.

Существуют различные системы удостоверения ЭД. Например, в США согласно Закону «Об электронных подписях в мировой и национальной торговле» (Electronic Signatures in Global and National Commerce Act) удостоверение ЭД в системе электронной торговли может производиться любым «звуком, символом или процессом», который послан с помощью электронного средства обмена и указывает на согласие человека к взаимодействию. Звук, символ или процесс может представлять собой воспроизведение записи голоса, отправленного и полученного через Интернет, сканирование сетчатки глаза, отпечаток пальца, который послан с помощью электроники, рукописную подпись, отсканированную графически, или изображение подписи, внедренное в ЭД посредством использования планшетного дигитайзера, частный номер (типа PIN). Фактически подпись может быть нечто столь же простое, как щелчок на кнопку «да» («Yes»).

В России основным средством удостоверения автора официального электронного документа является «электронная цифровая подпись»⁵ (ЭЦП), которая согласно ФЗ «Об электронно-цифровой подписи» является реквизитом электронного документа, «предназначенным для защиты данного электронного документа от подделки», целей идентификации автора ЭД («владельца сертификата ключа подписи»), а также для установления «отсутствия искажения информации в электронном документе».

Законодатель, определяя ЭЦП как аналог собственноручной подписи, недостаточно четко представлял себе ее функции и принципы использова-

ния, поскольку при практическом использовании ЭЦП возникает ряд проблем. Во-первых, получив ЭД, подписанный ЭЦП, вы никоим образом не можете идентифицировать лицо, «подписавшее» электронный документ с помощью существующей технологии. А во-вторых, ЭЦП может воспользоваться не уполномоченное на это лицо. В этом случае, как отмечала Н. Н. Лебедева, кто бы ни подписал электронный документ, «он будет считаться подлинным, если до момента подписания документа лицо, официально владеющее закрытым ключом ЭЦП, не уведомило всех участников системы электронного документооборота о необходимости аннулирования ЭЦП в связи с ее выходом из-под контроля»⁶. В этом случае ситуация очень напоминает вариант несанкционированного использования традиционной печати. И так же, как и в случае с традиционными печатями, одним из наиболее важных вопросов обеспечения безопасности документооборота является обеспечение защиты и сохранности закрытого ключа ЭЦП.

Исключить возможность несанкционированного использования ЭЦП, а также обеспечить ее жесткую привязку только к ее владельцу можно только в том случае, когда использование закрытого ключа ЭЦП будет «завязано» на индивидуальные биометрические характеристики ее владельца. В качестве таких биометрических характеристик могут выступать папиллярный узор пальца, рисунок радужной оболочки глаза. И лишь реализовав данный процесс, можно говорить о том, что электронная цифровая подпись действительно является аналогом собственноручной подписи, жестко связанной с одной из уникальных биометрических характеристик ее владельца.

В современных условиях реализовать применение ЭЦП с использованием биометрических показателей пользователя средств компьютерной техники не составляет большого труда. Так, например, на рынке портативных мобильных устройств для хранения данных появился флэш-накопитель Sijpdrjve Fjngel, оборудованный сенсором для считывания отпечатков пальцев. Новинка емкостью 256 Мбайт и стоимостью менее \$60 снабжена интерфейсом USB и позволяет пользователю самому устанавливать уровень необходимой защиты, вводя параметры как одного, так и нескольких пальцев.

² См.: Делопроизводство и архивное дело. Термины и определения: Государственный стандарт РФ ГОСТ Р 51141-98.

³ См.: Об электронной цифровой подписи: федер. закон от 10 января 2002 г. № 1-ФЗ.

⁴ См.: Защита информации. Система стандартов. Основные положения: Государственный стандарт РФ ГОСТ Р 52069.0-2003.

⁵ См.: Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения: ГОСТ 6.10.4-84.

⁶ Лебедева Н. Н. Право. Личность. Интернет. - М.: Волтерс Клувер, 2004 - С. 126.