Защита информации в современном документообороте

Стахно Р. Е.[1], Гончар А. А.[2]

[1]Стахно Роман Евгеньевич / Stahno Roman Evgenyevich - кандидат технических наук;
[2]Гончар Артем Александрович / Gonchar Artem Aleksandrovich - кандидат военных наук,
кафедра математики и информатики,
Санкт-Петербургский университет МВД России, г. Санкт-Петербург

Аннотация: *в статье рассмотрено применение электронной подписи в документообороте органами государственной власти, организациями, юридическими и физическими лицами. Определение подлинности электронной подписи.*

Ключевые слова: *информационная безопасность, электронная подпись, определение подлинности электронной подписи, обеспечение конфиденциальности информации.*

Потребности современного электронного документооборота привели к возникновению нетрадиционных задач защиты информации, одной из которых является аутентификация электронной информации в условиях, когда обменивающиеся информацией стороны не доверяют друг другу. Эта проблема связана с созданием систем электронной подписи.

Электронная подпись необходима для защиты от подделок и сохранения целостности электронного документа, защиты авторских прав (подтверждение авторских прав) и является неотъемлемым атрибутом любого электронного документа. Электронная подпись делается в виде специально закодированной строки при помощи новейших технических средств [1, с. 2].

Электронная подпись состоит из трех частей:

- сертификат;
- закрытый ключ;
- открытый ключ.

Виды электронной подписи:

1. Простая электронная подпись. Она формирует информацию о лице, поставившем эту подпись посредством простых кодов и паролей.
2. Усиленная электронная подпись. Она, в свою очередь, имеет подвиды:

- Неквалифицированная подпись. Здесь для формирования информации о подписанте используется криптографический алгоритм с использованием ключа электронной подписи. Также с ее помощью можно определить подписанта, определить, что в документ были внесены изменения, а также для ее создания применяются средства электронной подписи.
- Квалифицированная подпись. В нее входят все те же признаки, что и в неквалифицированную, но она выдается только в аккредитованных ФСБ РФ удостоверяющих центрах.

Вопросы электронных подписей регламентирует Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ.

Электронная подпись представляет собой последовательность символов, полученных в результате криптографического преобразования электронных данных. Электронная подпись добавляется к блоку данных и позволяет получателю блока проверить источник и целостность данных и защититься от подделки. Электронная подпись используется в качестве аналога собственноручной подписи (см. Рис. 1).

Электронная подпись в электронном документе равнозначна собственноручной подписи в документе на бумажном носителе при одновременном соблюдении следующих условий:

- 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. Сертификат ключа подписи - это документ на бумажном носителе или электронный документ с электронной подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной подписи и идентификации владельца сертификата ключа подписи;
- подтверждена подлинность электронной подписи в электронном документе. Подтверждение подлинности электронной подписи в электронном документе - положительный результат проверки соответствующим сертифицированным средством электронной подписи с использованием сертификата ключа подписи принадлежности электронной подписи в электронном документе владельцу сертификата ключа, подписи и отсутствия искажений в подписанном данной электронной цифровой подписью электронном документе;
- электронная подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

Технология электронной подписи широко используется в системах электронного документооборота различного назначения: государственного, коммерческого, внешнего и внутреннего обмена,

организационно-распорядительного, кадрового, законотворческого, торгово-промышленного и прочего. Это продиктовано главным свойством электронной подписи – она может быть использована в качестве аналога собственноручной подписи и/или печати на бумажном документе, в соответствии с нормативными правовыми актами или соглашением сторон может заверяться электронной подписью уполномоченного лица.

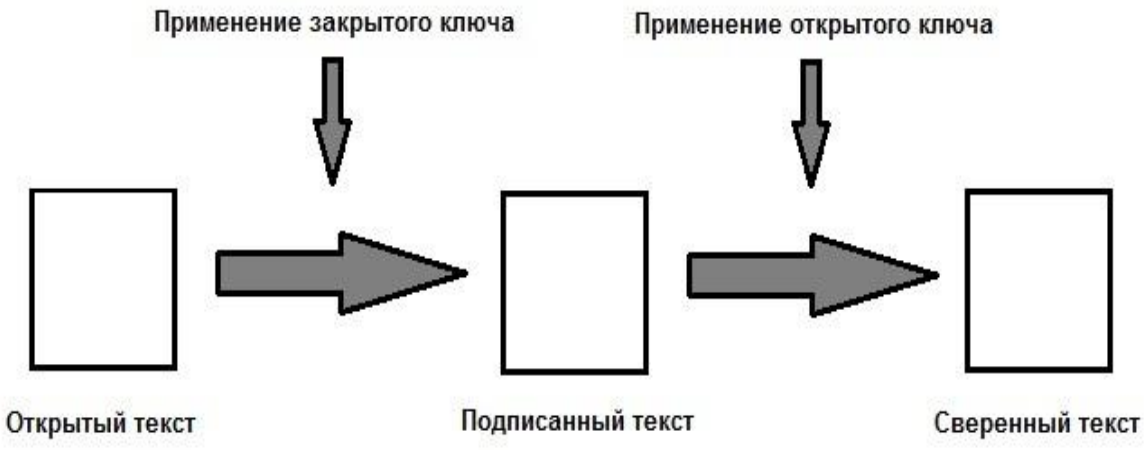

Рис. 1. Схема применения электронной подписи

В случаях, установленных законами и иными нормативными правовыми актами РФ или соглашением сторон, электронная подпись в электронном документе, сертификат которой содержит необходимые при осуществлении данных отношений сведения о правомочиях его владельца, признается равнозначной собственноручной подписи лица в документе на бумажном носителе, заверенном печатью.

Электронная подпись, как и другие реквизиты документа, выполняющие удостоверительную функцию, является средством, обеспечивающим конфиденциальность информации [3, с. 6].

Механизм выполнения собственноручной (физической) подписи непосредственно обусловлен психофизиологическими характеристиками организма человека, в силу чего эта подпись неразрывно связана с биологической личностью подписывающего.

Собственноручная подпись позволяет установить (идентифицировать) конкретного человека по признакам почерка.

Электронная подпись, являясь криптографическим средством, не может рассматриваться в качестве свойства, присущего непосредственно владельцу электронной подписи как биологической личности. Между электронной подписью и человеком, ее поставившим существует взаимосвязь не биологического, а социального характера. Возникновение, существование и прекращение данной связи обусловлено совокупностью различных правовых, организационных и технических факторов.

Для проверки формирования квалифицированной электронной подписи применяются сертифицированные средства безопасности. Срок действия ключа электронной подписи (секретного ключа), сформированного с помощью средства электронной подписи, не должен превышать срока, указанного в эксплуатационной документации.

Если следовать этим правилам, то вероятность компрометации ключа электронной подписи (а, следовательно, и подделки электронной подписи), будет ничтожна мала.

Отождествление человека по собственноручной подписи и подтверждение на этой основе подлинности документа, которой он заверен, достигается путем проведения судебно-почерковедческой экспертизы, решающей данную идентификационную задачу.

Определение подлинности электронной подписи свидетельствует только о знании лицом, ее поставившим, закрытого ключа электронной подписи. Для того чтобы установить, действительно ли владелец сертификата ключа заверил документ, надо выяснить помимо подлинности электронной подписи и указанные выше факторы.

Задача установления факта удостоверения электронного документа владельцем сертификата ключа подписи решается в результате процессуальной деятельности по доказыванию в ходе судебного разбирательства [2, с. 22].

Литература

1. Федеральный закон от 06.04.2011 N 63-ФЗ (ред. от 28.06.2014) «Об электронной подписи» (с изм. и доп., вступ. в силу с 01.07.2015) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru.
2. Федеральный законот 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс]. Режим доступа: http://www.consultant.ru.
3. Гражданский кодекс РФ регулирует использование электронных документов и электронной подписи при совершении сделок и заключении договоров (ст. 160, 434, 847 ГК РФ) [Электронный ресурс]. Режим доступа: http://www.consultant.ru.