



## Введение

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 позволяющей идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажений информации в электронном документе. Электронная цифровая 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;
- подтверждена подлинностью электронной цифровой подписи в электронном документе;
- электронная цифровая подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи.

При этом электронный документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи.

## 1. Основные положения

Общая суть электронной подписи заключается в следующем. С помощью криптографической хэш-функции вычисляется относительно короткая строка символов фиксированной длины (хэш). Затем этот хэш шифруется закрытым ключом владельца - результатом является подпись документа. Подпись прикладывается к документу, таким образом получается подписанный документ. Лицо, желающее установить подлинность документа, расшифровывает подпись открытым ключом владельца, а также вычисляет хэш документа. Документ

считается подлинным, если вычисленный по документу хэш совпадает с расшифрованным из подписи, в противном случае документ является подделанным.

При ведении деловой переписки, при заключении контрактов подпись ответственного лица является неременным атрибутом документа, преследующим несколько целей:

- гарантирование истинности письма путем сличения подписи с имеющимся образцом;
- гарантирование авторства документа (с юридической точки зрения).

Выполнение данных требований основывается на следующих свойствах подписи:

- подпись аутентична, то есть с ее помощью получателю документа можно доказать, что она принадлежит подписывающему;
- подпись неподделываема; то есть служит доказательством, что только тот человек, чей автограф стоит на документе, мог подписать данный документ, и никто иной;
- подпись непереносима, то есть является частью документа и поэтому перенести ее на другой документ невозможно;
- документ с подписью является неизменяемым;
- подпись неоспорима;
- любое лицо, владеющее образцом подписи может удостовериться, что документ подписан владельцем подписи.

Развитие современных средств безбумажного документооборота, средств электронных платежей немыслимо без развития средств доказательства подлинности и целостности документа. Таким средством является электронно-цифровая подпись (ЭЦП), которая сохранила основные свойства обычной подписи.

## **Заключение**

Цифровая подпись обеспечивает:

- Удостоверение источника документа. В зависимости от деталей определения «документа» могут быть подписаны такие поля как автор, внесённые изменения, метка времени и т. д.
- Защиту от изменений документа. При любом случайном или преднамеренном изменении документа (или подписи) изменится хэш, следовательно подпись станет недействительной.