Самый обычный вопрос, который задаётся человеком, впервые столкнувшимся с необходимостью использования цифровой подписи, звучит примерно так: ***«А зачем мне вообще электронная цифровая подпись? И нужна ли?»***

Электронная цифровая подпись (ЭЦП)— 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, а также обеспечивает неотказуемость подписавшегося.

Схема электронной подписи обычно включает в себя:
1) *Алгоритм генерации ключевых пар пользователя;*
2) *Функцию вычисления подписи;*
3) *Функцию проверки подписи.*

Функция проверки подписи проверяет, соответствует ли данная подпись данному документу и открытому ключу пользователя. Открытый ключ пользователя доступен всем, так что любой может проверить подпись под данным документом.

Алгоритмы ***ЭЦП*** делятся на два больших класса: *обычные цифровые подписи и цифровые подписи с восстановлением документа*.

-Обычные цифровые подписи необходимо пристыковывать к подписываемому документу ***(ECDSA, ГОСТ Р 34.10-2001, ДСТУ 4145-2002)****;*

-Цифровые подписи с восстановлением документа содержат в себе подписываемый документ: в процессе проверки подписи автоматически вычисляется и тело документа ***(RSA)****.*

Цифровая подпись обеспечивает:

1) Удостоверение источника документа. В зависимости от деталей определения документа могут быть подписаны такие поля, как «автор», «внесённые изменения», «метка времени» и т. д.

2) Защиту от изменений документа. При любом случайном или преднамеренном изменении документа (или подписи) изменится хэш, следовательно, подпись станет недействительной.
3) Невозможность отказа от авторства. Так как создать корректную подпись можно лишь, зная закрытый ключ, а он известен только владельцу, то владелец не может отказаться от своей подписи под документом. ***4)*** Предприятиям и коммерческим организациям сдачу финансовой отчетности в государственные учреждения в электронном виде;
5) Организацию юридически значимого электронного документооборота;

Возможны следующие угрозы ***цифровой подписи****:*

1) Злоумышленник может попытаться подделать подпись для выбранного им документа.
2) Злоумышленник может попытаться подобрать документ к данной подписи, чтобы подпись к нему подходила. Однако в подавляющем большинстве случаев такой документ может быть только один. ***3)*** Документы редко оформляют в виде Plain Text — файла, чаще всего в формате DOC или HTML.

Порядок получения ЭЦП для юридических и физических лиц немного различается. Но, в общем, **алгоритм получения ЭЦП** можно описать так:

1. *Определиться, для чего нужна подпись: в зависимости от сферы применения она может различаться. Основные сферы использования мы описали выше.*
2. *Заполнить заявку в удостоверяющем центре.*
3. *Подготовить и отправить комплект документов.*
4. *Оплатить.*

В России юридически значимый сертификат электронной подписи выдаёт удостоверяющий центр. Правовые условия использования электронной цифровой подписи в электронных документах регламентирует **ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 10.01.2002 N 1-ФЗ *«ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ»***

В Законе РФ от 10.01.2002 № 1-ФЗ *«ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ»* прописаны условия использования электронной цифровой подписи, особенности ее использования в сферах государственного управления и в корпоративной информационной системе. Благодаря электронной цифровой подписи теперь, в частности, многие российские компании осуществляют свою торгово-закупочную деятельность в Интернете, через «Системы электронной торговли», обмениваясь с контрагентами необходимыми документами в

электронном виде, подписанными ЭЦП. Это значительно упрощает и ускоряет проведение конкурсных торговых процедур.