Содержание:

Введение

Сегодня сложно найти специалиста в области информатизации или телекоммуникаций, который бы не знал, что такое электронная цифровая подпись (ЭЦП). Однако мало кто осознает, что само по себе использование этой технологии только создает предпосылки для организации юридически значимого электронного документооборота. Точно так же как технология производства бумаги или авторучек - это лишь возможность организовать традиционный бумажный документооборот. Что необходимо предпринять, чтобы обмен электронными документами с ЭЦП стал столь же привычным, как и документами на бумажном носителе? 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 электронной документ с электронной цифровой подписью имеет юридическое значение при осуществлении отношений, указанных в сертификате ключа подписи. В скором будущем заключение договора будет возможно в электронной форме, который будет иметь такую же юридическую силу, как и письменный документ. Для этого он должен иметь механизм электронной цифровой подписи, подтверждаемый сертификатом. Владелец сертификата ключа подписи владеет закрытым ключом электронной цифровой подписи, что позволяет ему с помощью

средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы). Для того, чтобы электронный документ могли открыть и другие пользователи, разработана система открытого ключа электронной подписи. Для того, чтобы иметь возможность скреплять электронный документ механизмом электронной цифровой подписи, необходимо обратиться в удостоверяющий центр за получением сертификата ключа подписи. Сертификат ключа подписи должен быть внесен удостоверяющим центром в реестр сертификатов ключей подписей не позднее даты начала действия сертификата ключа подписи. Первый в России такой удостоверяющий центр запущен в сентябре 2002 г. Российским НИИ развития общих сетей (РосНИИРОС). Удостоверяющий центр по закону должен подтверждать подлинность открытого ключа электронной цифровой подписи.

Основная часть

Хэш-функция защищаемого электронного документа представляет собой уникальное число, получаемое из исходного документа путем его преобразования с помощью сложного, но известного алгоритма (хэш-функции). Хэш-функция чувствительна к всевозможным искажениям исходного электронного документа, то есть изменение (искажение) хотя бы одного знака в исходном документе приводит в среднем к искажению половины знаков хэш-значения. Кроме того, она устроена таким образом, что, во-первых, по хэш-значению документа нельзя восстановить исходный электронный документ, а во-вторых, практически невозможно отыскать два различных электронных документа, которые обладали бы одним и тем же хэш-значением. Схема формирования электронной цифровой подписи под электронным документом его создателем (отправителем) предусматривает вычисление хэш-функции этого документа и шифрование этого значения посредством секретного ключа отправителя. Результатом шифрования и является значение ЭЦП как реквизит электронного документа, которое пересылается получателю вместе с этим документом. Таким образом, электронная цифровая подпись жестко увязывает содержание документа и секретный ключ для формирования ЭЦП и делает невозможным изменение документа без нарушения подлинности данной подписи. Функции ЭЦП: Поскольку электронная цифровая подпись - средство защиты информации, предоставляющее возможность контроля целостности и подтверждения подлинности электронного документа, то ЭЦП должна обеспечивать выполнение следующих основных функций: подтверждать, что подписывающее лицо сознательно подписало электронный документ;

подтверждать, что документ подписало именно подписывающее лицо и только оно; ЭЦП должна существенно зависеть от подписываемого документа, в том числе от имеющихся в нем отметок времени; подписывающее лицо не должно иметь возможности отказаться впоследствии от факта подписи электронного документа. 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. В результате этого 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 непременным атрибутом документа, преследующим несколько целей: гарантирование истинности письма путем сличения подписи с имеющимся образцом и 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; 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 удостоверится, что документ подписан владельцем подписи.