
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. 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.

Область применения электронно цифровой подписи

В связи с тем, что электронно цифровая подпись позволяет защитить электронный документ от изменений, проверить его целостность и делает невозможным отказ от авторства, но дает возможность это авторство доказать, в настоящее время сфера применения ЭЦП достаточно широка. Среди целей, для которых применяются электронные цифровые подписи, можно выделить следующие: обеспечение для электронных документов юридической значимости с помощью электронной подписи; передача обязательной бухгалтерской и налоговой отчетности в электронном виде в налоговые инспекции; обмен электронными документами между организациями и их структурными подразделениями; декларирование товаров и услуг для целей таможенного оформления; авторизация для получения доступа к специализированным информационным ресурсам; передача данных в органы статистики и отделения Пенсионного фонда;

предоставление отчетности в контролирующие органы; участие в электронных торгах; защита сообщений электронной почты и др.

Получение ЭЦП

Перед тем как практически начать применять ЭЦП в своей работе, надо создать файлы сертификата и закрытого ключа. Сертификат будет использоваться для проверки подлинности данных подписанных ЭЦП любым человеком, использующим эти данные. А закрытый ключ нужен человеку для формирования ЭЦП подписываемых им данных. При создании сертификатов и ключей используется специальные криптографические программы, которые в принципе есть в составе операционной системы любого компьютера. Однако, доверять полученному таким образом сертификатам могут только люди,

работающие на этом компьютере. Для того чтобы создать и в дальнейшем использовать сертификат, которому будут доверять все, кто будет проверять подлинность ЭЦП, нужна определенная организация, которая обеспечит нормативную, организационную и правовую основу использования выпущенных ею сертификатов. Такой организацией является Удостоверяющий Центр. Электронная цифровая подпись аналогична подписи человека, а для того чтобы убедиться в подлинности документов, подписываемых человеком, любая организация отправляет его сначала к нотариусу, который проверив дееспособность человека удостоверяет его собственноручную подпись на самых различных документах. Конечно, организация, установив соответствующее программное обеспечение, может организовать собственный Удостоверяющий центр, но при этом следует иметь ввиду, что ЭЦП, наносимые работниками организации, не смогут иметь юридическое значение за пределами этой организации. Поэтому точно так же, как и при обращении к нотариусам, следует пользоваться услугами внешних аттестованных удостоверяющих центров. Подписав договор с Удостоверяющим Центром организация может получать от него сертификаты для своих работников, которые будут пользоваться ЭЦП. В процессе создания сертификата каждому из таких работников будет сгенерирован закрытый ключ. Процедура создания ключей может выполняться по-разному. Ключи могут создаваться в Удостоверяющем центре и передаваться пользователям вместе с сертификатом. Ключи могут создаваться и на рабочем месте пользователя в организации, а открытая часть ключа пересылаться в Удостоверяющий центр для последующего изготовления сертификата. И ключ, и сертификат хранятся в файлах. Для того, чтобы никто, кроме владельца подписи, не мог воспользоваться закрытым ключом, его обычно

записывают на съемный носитель ключа. Его также как банковскую карточку для дополнительной защиты снабжают PIN кодом. И точно также как при операциях с картой, перед тем как воспользоваться ключом для создания ЭЦП надо ввести правильное

5

значение PIN кода. Именно надежное сохранение пользователем своего закрытого ключа гарантирует невозможность подделки злоумышленником документа и цифровой подписи от имени заверяющего документ подписанта. Сертификат содержит всю необходимую информацию для проверки ЭЦП. Данные сертификата открыты и публичны. Поэтому обычно сертификаты хранятся в хранилище операционной системы (в каждом компьютере, в общем сетевом хранилище, в базе данных и т.п.). Конечно, все сертификаты всегда хранятся и в Удостоверяющем центре, точно так же, как и нотариус хранит всю необходимую информацию о человеке, выполнившем у него нотариальное действие. Получение работником организации закрытого ключа, обеспечение его сохранности и действия с ним обычно регламентируется приказом по организации с утверждением инструктивных материалов. В них регламентируется порядок выпуска сертификатов, применение ключей для подписания документов, получение, замену, сдачу закрытого ключа работниками, и действия выполняемые при компрометации ключа. Последние аналогичны действиям выполняемым при потере банковской карты.

Заключение

Электронная цифровая подпись — это эффективное средство защиты информации от модификации, искажений, позволяющее при этом однозначно идентифицировать отправителя сообщения и перенести свойства реальной подписи под документом в область электронного документа. Электронная цифровая подпись является наиболее перспективным и широко используемым в мире способом защиты электронных документов от подделки и обеспечивает высокую достоверность сообщения.

6

Список литературы

1.Федеральный закон «Об электронной цифровой подписи» от 10 января

2002года

2.«Некоторые вопросы правового обеспечения использования ЭЦП» БеззубцевО.А.

3.Современные криптографические методы защиты информации - системы с открытым ключом