Тункина А. А., РГППУ

ЭЛЕКТРОННАЯ ПОДПИСЬ КАК РЕКВИЗИТ ЭЛЕКТРОННОГО ДОКУМЕНТА

В связи со стремительным развитием науки и техники в современном мире широкое распространение получило применение электронных документов. Одной из проблем их использования – это придание такому документу юридической силы. Решение этой проблемы специалисты видят в применении электронной подписи. Согласно Федеральному закону № 63–ФЗ электронная подпись – «информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию»[1].

Федеральный закон № 63–ФЗ, принятый в 2011 г., выделяет следующие виды электронной подписи:

– простые подписи. Они создаются с помощью кодов, паролей и других инструментов, которые позволяют идентифицировать автора документа, но не позволяют проверить его на предмет наличия изменений с момента подписания;

– усиленные неквалифицированные подписи. Созданные с использованием криптографических средств, они позволяет определить не только автора документа, но проверить его на наличие изменений. Для создания таких подписей может использоваться сертификат неаккредитованного центра, можно также вообще обойтись без сертификата, если технические средства позволяют выполнить требования закона;

– усиленные квалифицированные подписи. Являясь разновидностью усиленных подписей, они имеет сертификаты от аккредитованного центра и создана с помощью подтвержденных ФСБ средств.

Каждому пользователю электронной подписи, участвующему в обмене электронными документами, генерируются уникальные открытый и закрытый (секретный) криптографические ключи. Ключевым элементом в применении электронной подписи является секретный ключ, с помощью него производится шифрование электронных документов и формируется сама электронная подпись. Секретный ключ выдается пользователю на отдельном носителе, которым может быть флэш-карта, смарт-карта или touch memory. Хранить его нужно в секрете от других пользователей сети.

---

[1] Об электронной подписи: Федер. закон от 6 апреля 2011 г. N 63-ФЗ // Рос. газ. 2011. 8 апреля.

Для проверки подлинности электронной подписи используют открытый ключ. В удостоверяющем центре находится дубликат открытого ключа, создана библиотека сертификатов открытых ключей. Удостоверяющий центр обеспечивает регистрацию и надежное хранение открытых ключей во избежание внесения искажений или попыток подделки[1].

Подделать электронную подпись невозможно – это требует огромного количества вычислений, которые не могут быть реализованы при современном уровне математики и вычислительной техники за приемлемое время, т. е. пока информация, содержащаяся в подписанном документе, сохраняет актуальность. Дополнительная защита от подделки обеспечивается сертификацией удостоверяющим центром открытого ключа подписи.

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 подписи, не утратил силу (действует) на момент проверки или на момент подписания электронного документа при наличии доказательств, определяющих момент подписания; подтверждена подлинность электронной подписи в электронном документе; электронная подпись используется в соответствии со сведениями, указанными в сертификате ключа подписи[2].

Электронная подпись предназначена для защиты от подделки электронных документов, для идентификации лица, подписавшего документ, либо защиты документа от изменения и просмотра третьими лицами. Использование электронной подписи позволяет: значительно сократить время, затрачиваемое на оформление сделки и обмен документацией; усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов; гарантировать достоверность документации; минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена[3].

Таким образом, электронная подпись – это программно-криптографическое средство, которое обеспечивает: проверку целостности документов; конфиденциальность документов; установление лица, отправившего документ.

---

[1] ГОСТ Р 34.10–2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М., 2001. С. 7–9.

[2] Электронная подпись. URL: http://www.tadviser.ru/index.php.

[3] Там же.