ПРОГРАММНО-АППАРАТНЫЕ АСПЕКТЫ РЕАЛИЗАЦИИ ЦИФРОВОЙ ПОДПИСИ

В.А. Липницкий, А.А. Полещук

Электронная цифровая подпись (ЭЦП) — это реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП. Значение реквизита получается в результате криптографического преобразования информации с использованием закрытого ключа.

Цифровая подпись предназначена также для аутентификации лица, подписавшего электронный документ.

Обычно цифровая подпись базируется на определенной системе шифрования данных. Одной из наиболее популярных систем шифрования данных является криптосистема Ривеста, Шамира, Адлемана (RSA). Именно эта криптосистема взята за основу в данной работе. Одним из этапов формирования цифровой подписи является хеширование больших сообщений. В данной работе использован наиболее распространенный стандарт хеширования MD5.

В докладе рассматривается вариант аппаратной реализации цифровой подписи файлов на основе микроконтроллера AVR с возможностью хранения файлов на устройстве хранения информации формата SD/microSD.