ФОРМИРОВАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ НА ОСНОВЕ ОТПЕЧАТКА ПАЛЬЦА

А.В. Никитин

ЗАО «Диджитал Дизайн», Санкт-Петербург, Российская Федерация

Электронная подпись появилась в связи с развитием электронного способа оборота документов. Так как фальсификация подписи на основе обычного изображения не составляет труда, требовалось создать метод, позволяющий реализовать безопасную идентификацию субъекта, выполнившего подпись документа. Основным методом, который позволяет это сделать, является электронная цифровая подпись, которая основана на генерации открытого и закрытых ключей шифрования посредством использования определенной хэш-функции в зависимости от требуемого уровня защищенности подписи. С помощью закрытого ключа осуществляется подписание документа и, поэтому, данный ключ доступен исключительно субъекту, подписавшему документ. Открытый же ключ является общедоступным и используется субъектом, которому требуется проверить, что документ подписан нужной подписью.

В работе рассмотрены виды и алгоритмы электронной подписи, проведен анализ работы данных алгоритмов и исследованы особенности работы с ним. Также проведен анализ существующих методов биометрической идентификации и изучены способы применения биометрических данных для формирования на их основе электронной подписи.

Метод сканирования отпечатков пальцев прост в использовании и обеспечивает надежность. Основным преимуществом данного метода является стоимость реализации и небольшие размеры сканирующего устройства. Биометрическая система распознавания реализуется в аппаратной и программной части. В аппаратную часть входят сканеры, которые считывают биометрические особенности с физического объекта (папиллярные линии) и создают их цифровую модель. Программная часть использует полученную цифровую модель и сверяет ее с базой данных для распознавания субъекта. Основными параметрами оценки точности работы являются коэффициент ложного пропуска (FAR) и коэффициент ложного отказа (FRR). Таким

образом, имея уникальные модели физического признака субъекта можно реализовать генерацию уникальной подписи на ее основе.

В работе реализовано приложение, позволяющее подписывать документы формата PDF посредством использования электронной подписи на основе биометрических данных. Приложение реализовано с использованием библиотеки Bouncy Castle, содержащей провайдер для JCE и JCA (архитектура криптографии в Java и расширение криптографии соответственно). В использованной библиотеке также поддерживается сертификат X.509 и стандарт OpenPGP (протокол шифрования электронной почты).

В перспективе, имея единую базу данных с сохраненными в ней электронными моделями физических признаков субъектов, будет упрощен процесс подписания документов.