УДК 343.98

Т.В. Ахраменко

ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ: ПОНЯТИЕ, СУЩНОСТЬ, ОСОБЕННОСТИ НАЗНАЧЕНИЯ ЭКСПЕРТИЗЫ

Широкое распространение электронного документооборота и его определенные специфические признаки предопределяют необходимость поиска средств решения задач идентификации автора и определения целостности электронных документов.

Техническим средством, которое способно решить указанные задачи при использовании электронных документов, юридическим гарантом, который обеспечивает реализацию и защиту прав участников электронного документооборота и придает юридическую силу электронным документам, является электронная цифровая подпись.

Впервые понятие электронной подписи было предложено в 1981 г. учеными Стенфордского университета (США) – программистом У. Диффи и профессором М. Хеллманом. Уже в следующем году американские ученые Р. Ривест и Л.М. Адлеман в сотрудничестве с израильтянином А. Шамиром создали алгоритм шифрования, названный по первым буквам их фамилий – RSA. Алгоритм основывался на математическом принципе разложения натуральных чисел на простые множители и мог использоваться для простейшего шифрования пересылаемых документов. С развитием криптографии и компьютерных технологий стали появляться вероятностные схемы цифровых подписей, например схема Рабина, а затем и первые хэш-алгоритмы. К 1984 г. ученые под руководством Р. Ривеста строго сформулировали основные принципы безопасности, применяемые к цифровым подписям.

В соответствии со ст. 1 Закона Республики Беларусь «Об электронном документе и электронной цифровой подписи» электронная цифровая подпись – это последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности.

Электронная цифровая подпись предназначена для удостоверения информации, составляющей общую часть электронного документа (осуществляется путем применения сертифицированных средств электронной цифровой подписи с использованием личных ключей лиц, подписывающих электронный документ); подтверждения целостности и подлинности электронного документа (осуществляется путем применения сертифицированных средств электронной цифровой подписи с использованием открытых ключей лиц, подписавших электронный документ).

Электронная цифровая подпись является аналогом собственноручной подписи, также может применяться как аналог оттиска печати или штампа.

Суть электронной цифровой подписи заключается в персонификации всех возможных лиц, за которыми закрепляются персональные идентификационные номера, и криптографической привязке цифровых данных, подписанных этим лицом, таким образом, что любое, даже незначительное изменение содержимого файла документа с электронной цифровой подписью четко проявляется как нарушение аутентичности данного электронного документа.

Электронной цифровой подписью можно заверить текст или его часть. В этом случае электронная цифровая подпись представляет собой набор символов, включаемых в текст. Подписанный таким образом текст вместе с подписью может быть распечатан на бумаге, сохранен на электронном носителе, передан по компьютерной сети.

Если цифровой подписью подписывается файл целиком (причем это может быть файл, содержащий как текст, так и графику), то электронная цифровая подпись обычно формируется в виде отдельного файла (файла электронной цифровой подписи), который прилагается к подписанному файлу.

Несмотря на высокую степень защиты электронной цифровой подписи от подделки, система электронных цифровых подписей находится под действием постоянных преступных посягательств. Если имеются данные о несоответствии электронного документа оригиналу, назначают экспертизу электронной цифровой подписи.

Экспертиза электронной цифровой подписи – сравнительно новый вид исследования, проводящийся в рамках компьютерно-технической экспертизы. Огромные потоки электронного документооборота наравне со значительно увеличившимися скоростями торговых, банковских и прочих экономических взаимодействий ставят экспертизу электронной цифровой подписи в разряд наиболее важных исследований.

Экспертизу электронной цифровой подписи проводят в следующих случаях: если есть основание полагать, что лицо, удостоверившее документ, пользуется поддельной электронной цифровой подписью; при подозрении на подделку ключа проверки электронной цифровой подписи; если имеются основания считать, что документ был изменен в процессе пересылки, то есть были внесены поправки после того, как документ был заверен электронной цифровой подписью; в любых других случаях, когда требуется надлежащая проверка документации.

Для проведения экспертизы в распоряжение эксперта предоставляются корневые сертификаты электронной цифровой подписи, выданные соответствующей организацией; спорные электронные документы, подлинность которых ставится под сомнение; ключ проверки электронной цифровой подписи.

Таким образом, применение электронной цифровой подписи позволяет не только надежно идентифицировать автора электронного документа, но и предотвратить как случайное, так и умышленное искажение информации.

УДК 343.9

О.С. Бочарова

МНОГООБРАЗИЕ ДОКУМЕНТОВ КАК ОСНОВАНИЕ ДЛЯ РАСШИРЕНИЯ ПРЕДЕЛОВ КОМПЕТЕНЦИИ ЭКСПЕРТА ПО СУДЕБНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЕ ДОКУМЕНТОВ

В настоящее время в теории и практике судебной экспертизы, процессуальном законодательстве используются понятия «компетенция эксперта», «пределы компетенции эксперта», «вопросы, входящие в компетенцию эксперта», предполагающие наличие у эксперта комплекса специальных знаний (познаний). Иначе говоря, компетентность лица в той или иной области знаний является одним из оснований для привлечения его в качестве судебного эксперта, а вопросы, поставленные перед экспертом, и