УДК 657(076)

ЭЛЕКТРОННАЯ ПОДПИСЬ В БУХГАЛТЕРСКОМ УЧЕТЕ: ПРОБЛЕМЫ, ПРЕИМУЩЕСТВА И ПЕРСПЕКТИВЫ

***Я.И. Варакса, А.В. Шаметько**, 2 курс*
*Научный руководитель – **А.И. Горбачева**, к.т.н., доцент*
Белорусский национальный технический университет

Электронная подпись, или правильнее электронная цифровая подпись (далее ЭЦП) — 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 ЭЦП.

28 декабря 2009 года принят Закон «Об электронном документе и электронной цифровой подписи», который вступит в силу в декабре 2010 года[1].

Ключевую роль играет успешная проверка ЭЦП. Эта процедура позволяет установить, во–первых, происхождение документа и его авторство, во–вторых – его целостность, т.е. тот факт, что после подписания никто не вносил в документ никаких изменений. Технически этого можно добиться, выработав в момент подписания некую контрольную характеристику. Существует алгоритм (на языке специалистов именуемый функцией хэширования, или хэш–функцией), который позволяет получать для любой последовательности двоичных кодов одну и только одну контрольную сумму, или дайджест. Любое исправление, внесенное в эту последовательность, приведет к тому, что при повторном подсчете получится совсем другая сумма. И наоборот, воспроизведение ранее зафиксированной суммы при новом подсчете означает, что с момента ее фиксации никакие изменения не производились. Алгоритм подсчета контрольной суммы в нашей стране закреплен СТБ 1176.1–99 «Информационная технология. Защита информации. Функция хэширования».

При выработке ЭЦП контрольная сумма шифруется определенным способом, при котором применяется пара из двух ключей. С помощью одного из них информация шифруется, с помощью другого – расшифровывается, но так, что обратно зашифровать ее этим ключом невозможно. Первый из этой пары ключей должен быть известен только отправителю, и тем самым неоспоримо доказывается его авторство. Поэтому он именуется личным ключом. Второй же ключ, открытый, служит для проверки подлинности сообщения. Заново подсчитав контрольную сумму переданного сообщения и сравнив ее с той, которая была приложена в зашифрованном виде и поддалась расшифровке этим ключом, мы можем убедиться, что сообщение создал владелец первого ключа и после этого в не был изменен ни один бит информации. Алгоритм выработки ЭЦП закреплен в СТБ 1176.2–99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи».

К сожалению, этот подход тоже не лишен «узких мест», вынуждающих учитывать сопутствующие обстоятельства. Прежде всего, адресат должен каким–то способом удостовериться, что примененная при выработке ЭЦП пара ключей действительно принадлежит тому, что указан в качестве автора документа. В ныне действующем законе предусматривается распространение официальной информации о том, кому принадлежит тот или иной открытый ключ, путем распечатывания его значения на бумажном документе (карточке открытого ключа) и заверения подписью и печатью владельца. Владелец должен лично вручить или разослать такие карточки всем, кому предполагает в дальнейшем отправлять электронные документы, и получить такие же карточки от других участников информационного взаимодействия. Очевидно, что такой подход эффективен только в системах с ограниченным числом участников – наподобие системы электронных межбанковских расчетов, ради которой он и разрабатывался [2]

Практика показала, что в системах с большим и неограниченным числом участников гораздо

удобнее подтверждать принадлежность открытого ключа путем выдачи его владельцу электронного сертификата, заверенного третьей стороной (неким удостоверяющим или регистрирующим центром). Имея такой сертификат, владелец может приложить его к электронному документу, отправляемому в адрес любого участника взаимодействия, не вступая с ним в предварительный контакт. Действующий закон в этом отношении слишком неконкретен – он допускает распространение открытого ключа путем его рассылки в электронном документе, но не уточняет, чьей ЭЦП этот документ должен быть заверен и как получатель может проверить эту подпись[3]

Правда, нерешенным пока остается вопрос о технической совместимости средств ЭЦП, применяемых в корпоративных системах. Ведь для успешной проверки ЭЦП мало знать, кому принадлежит применяемый открытый ключ. Нужно еще иметь программу, способную расшифровать с его помощью контрольную сумму конкретного документа, сравнить ее с заново подсчитанной и выдать подтверждение в доступной пользователю форме. К сожалению, универсальной программы такого рода пока не существует, а применяемые в корпоративных системах жестко ориентированы на определенные виды документов и на технические особенности этих систем. С принятием нового закона ситуация должна измениться, поскольку его ст. 24 предписывает, что «требования к технологии электронной цифровой подписи устанавливаются техническими нормативными правовыми актами». Это предполагает регламентацию на уровне стандарта, который будет разработан в ближайшее время.

Одним из «узких мест» подхода, основанного на применении ЭЦП, является то, что успешная ее проверка сама по себе недостаточна для признания документа подлинным. Приходится принимать в расчет правомочность применения личного ключа и срок его действия. Представим себе, например, ситуацию, когда уже уволенный сотрудник получил доступ к информационной системе организации и заверил своей ЭЦП какой–то исходящий документ. Очевидно, что этот документ не может иметь юридической силы, но как об этом узнать получателю?

Продолжая тему архивного хранения, нельзя не отметить еще одно «узкое место» технологии, основанной на ЭЦП. Она совершенно не рассчитана на документы, подлежащие хранению в течение десятков лет, а тем более постоянно. Во–первых, весьма маловероятно, что на компьютерах и под операционными системами столь далекого будущего можно будет запустить сегодняшнее средство ЭЦП, способное эту подпись проверить. Но даже если это и удастся, процедура не будет иметь смысла: за это время наверняка истечет срок стойкости криптоалгоритма, с помощью которого ЭЦП была выработана. Иначе говоря, за время порядка десятков лет теоретически можно подобрать ключ к любому шифру. А если это возможно в принципе, кто поручится, что такой взлом не имел место в каждом конкретном случае? Совпадение контрольной суммы с той, которая была зашифрована много лет назад, юридически ничего не доказывает.

Список использованных источников

1. Закон Республики Беларусь от 28.12.2009 N 113–З. Об электронном документе и электронной цифровой подписи /Национальный реестр правовых актов Республики Беларусь, 20.01.2010, N 15, 2/1665

2. Постановление Совета Министров Республики Беларусь от 20.07.2010 N 1086. Об утверждении Положения о порядке удостоверения формы внешнего представления электронного документа на бумажном носителе./ "Национальный реестр правовых актов Республики Беларусь", 02.08.2010, N 183, 5/32219

3. Носевич Вячеслав. Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи»: комментарий специалиста (2010)/ Архівы і справаводства. 2010. № 2 (68). С. 34–44.// Электронный ресурс. http://www.vln.by/node/144. Дата доступа: 01.02.2012.