ЗАЩИТА ИНФОРМАЦИИ

УДК 622.691.4.01

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ, СОДЕРЖАЩЕЙСЯ В НОРМАТИВНО-ТЕХНИЧЕСКИХ ДОКУМЕНТАХ ГАЗОВОЙ ПРОМЫШЛЕННОСТИ

В.Г. Лим, Б.Т. Кабулов

Рассматриваются вопросы использования электронной цифровой подписи (ЭЦП) для подтверждения достоверности и юридической силы электронныхформ нормативно-технических документов газовой промышленности в случае централизованной однонаправленной передачи информационных сообщений (электронных НТД) от одного распространителя (издателя) ко многим получателям.

Ключевые слова: *криптографические методы, электронно-цифровая подпись, верификация, закрытый ключ, открытый ключ.*

Keywords*: cryptographic methods, electronic digital signature, verification, secured key, open key.*

В связи с широким распространением в отраслях газовой промышленности электронных форм нормативно-технических документов (НТД) особо актуальной стала проблема установления их подлинности, авторства, принадлежности к определенному издателю. Для решения этой проблемы было предложено использовать ЭЦП, которая позволила бы подтверждать достоверность и юридическую силу электронного документа аналогично тому, как рукописная подпись и печать подтверждают достоверность и юридическую силу документа на бумажном носителе. Если электронный НТД распространяется официальным издателем, для подтверждения его подлинности может быть использована ЭЦП издателя. В настоящей работе рассматривается вариант централизованной однонаправленной передачи информационных сообщений (электронных НТД) от одного распространителя (издателя) ко многим получателям.

С целью обеспечения функциональной эквивалентности ЭЦП рукописной подписи необходимо, чтобы ЭЦП представляла собой строку символов, однозначно связанную как с распространителем НТД, так и с содержанием документа. Кроме того, электронная подпись так же, как и рукописная, должна быть защищена от подделки. Для исключения возможности подделки текста документа ЭЦП должна быть однозначно связана с этим текстом и, соответственно, быть для каждого документа уникальной, а для исключения возможности подделки самой электронной подписи она должна быть защищена криптографическими средствами.

Применение ЭЦП должно обеспечить защиту распространителя (пользователь А) и получателя НТД (пользователь В) от таких действий, как [1]:

- отказ (ренегатство) – распространитель впоследствии отказывается от переданного документа;
- фальсификация – получатель подделывает документ;
- изменение – получатель вносит изменения в документ;
- маскировка – нарушитель маскируется под одного из пользователей.
- повтор – нарушитель повторно направляет ранее переданный документ.

Для верификации документа М (пользователь А → пользователю В) необходимо следующее.

1. Распространитель (пользователь А) должен внести в М подпись, содержащую дополнительную информацию, зависящую от М, от известной только распространителю закрытой информации k_A и, в общем случае, от получателя документа.

2. Необходимо, чтобы правильную подпись М: SIG{k_A, М, идентификатор В} в документе для пользователя В нельзя было составить без k_A.

3. Для предупреждения использования предыдущей проверенной на достоверность информации процедура составления подписи должна зависеть от времени.

4. Пользователь В должен иметь возможность удостовериться, что SIG{k_A, М, идентификатор В} есть правильная подпись документа М пользователем А.

Рассмотрим эти пункты подробнее.

1. Подпись – это вид пароля, зависящий от распространителя, получателя информации и содержания передаваемого документа. Такая подпись может быть получена в результате некоторого криптографического преобразования документа М.

2. Закрываемым элементом k_A в преобразовании

<М, Идентификатор В> → SIG{k_A, М, идентификатор В}

является ключ криптопреобразования.

Во всех практических криптографических системах kA принадлежит конечному множеству ключей К. Исчерпывающая проверка всех ключей, задаваемых соответствующими парами

<М, идентификатор В> ↔ SIG{k_A, М, идентификатор В},

должна привести к определению ключа k_A злоумышленником. Если множество К достаточно велико и ключ k определен методом случайного выбора, то полная проверка ключей практически невозможна. Вместе с тем определение SIG{kA, М, идентификатор В} без k_A, с вычислительной точки зрения, эквивалентно поиску ключа.

3. Подпись должна меняться от документа к документу для предупреждения ее повторного использования. Цифровая подпись отличается от рукописной, которая обычно не зависит от времени составления и данных. Цифровая и рукописная подписи идентичны в том смысле, что они характерны только для данного владельца.

4. Хотя получатель информации не может составить правильную подпись, он должен уметь удостоверять ее подлинность. Установление подлинности подписи – это процесс, посредством которого каждая сторона устанавливает подлинность другой. Обязательным условием этого процесса является сохранение тайны. Для того чтобы в системе обработки данных получатель мог установить подлинность распространителя, необходимо выполнение следующих условий.

1. Распространитель (пользователь А) должен обеспечить получателя (пользователя В) удостоверяющей информацией AUTH{kA, М, идентификатор В}, зависящей от секретной информации kA, известной только пользователю А.

2. Необходимо, чтобы удостоверяющую информацию AUTH{kA, М, идентификатор В} от пользователя А пользователю В можно было дать только при наличии ключа kA.

3. Пользователь В должен располагать процедурой проверки того, что AUTH{kA, М, идентификатор В} действительно подтверждает личность пользователя А.

4. Для предупреждения использования предыдущей проверенной на достоверность информации процесс установления подлинности должен иметь некоторую зависимость от времени.

Отметим, что установление подлинности и верификация распространяемого документа имеют сходные элементы: цифровая подпись является удостоверением подлинности информации с добавлением требования об ее зависимости от содержания документа.

В качестве ЭЦП, удовлетворяющей приведенным требованиям, можно в простейшем случае использовать криптограмму, получаемую в результате шифрования текста вместе с

реквизитами распространителя (фамилией ответственного лица) и датой. Действительно, такая ЭЦП в случае успешного ее дешифрования позволяет не только однозначно определить распространителя (поскольку только ему должен быть известен секретный ключ шифрования), но и проверить достоверность и целостность документа (путем сопоставления открыто полученного и дешифрованного вариантов текста). Однако такая ЭЦП не очень удобна, так как, во-первых, имеет большой объем, а во-вторых, предполагает предварительный обмен секретными ключами между распространителем и получателем. Если первый фактор не столь критичен при современном состоянии информационно-коммуникационных технологий, то второй практически исключает возможность оперативной работы (обмен секретными ключами представляет собой сложную процедуру, особенно при наличии значительного числа получателей при распространении НТД) и сводит на нет все преимущества электронного документооборота.

Решение проблемы распространения секретных ключей предложили Уитфилд Диффи (Whitfield Diffie) и Мартин Е. Хеллман (Martin E. Hellman) [2]. Они заложили основы криптографии с открытым ключом [3]. Сходное понятие, открытое Ральфом Мерклем (Ralph Merkle), описано в [4]. Вскоре последовала его первая практическая реализация – RSA [5], предложенная Рональдом Райвестом (Ronald Rivest), Эди Шамиром (Adi Shamir) и Леонардом Эйдлеманом (Leonard Adleman).

Основная идея систем с открытым ключом – использовать для шифрования и расшифровки разные ключи, причем один из них должен быть секретным, а второй может быть сделан общедоступным. В таком случае отпадает необходимость в обмене секретными ключами. При осуществлении коммуникации по каналу связи передается только открытый ключ, что делает возможным использование для этой цели обычного канала и устраняет потребность в специальном защищенном канале для передачи ключа. Если сделать общедоступным ключ расшифрования, то на базе полученной системы можно построить систему аутентификации распространяемых документов.

Для уменьшения размера ЭЦП (чтобы не шифровать, как описано выше, весь документ) было предложено использовать специальные необратимые криптографические функции (хэш-функции) H, которые позволяют преобразовать документ M произвольной длины в строку H(M) фиксированного размера (иногда называемую дайджестом сообщения или сверткой). H(M) имеет обычно размер 128, 160, 256 или 512 бит. При этом криптографическое преобразование выполняется таким образом, что практически невозможно подогнать документ $M' \neq M$ к заданному хэш-значению H(M). В результате, шифруя дайджест, сформированный из подписываемого файла, получаем короткую цифровую подпись, уникальную для каждого документа.

Цифровая подпись документа обычно создается в следующей последовательности (см. рис.). Для документа M вычисляется значение хэш-функции H(M). Получившаяся строка далее зашифровывается секретным ключом K1 подписывающегося с использованием того или иного асимметричного алгоритма. Зашифрованный набор бит и представляет собой ЭЦП. К этой ЭЦП обычно прикладывается открытый ключ K2 подписывающего, парный секретному. Получатель НТД сначала решает для себя, доверяет ли он тому, что открытый ключ принадлежит именно этому распространителю (с помощью сети центров сертификации, образующих инфраструктуру открытых ключей, или на основе априорного знания), и затем дешифрует ЭЦП с помощью ключа K2. В результате дешифровки ЭЦП получается значение хэш-функции H(M), вычисленное распространителем НТД. Далее получатель самостоятельно вычисляет значение H'(M) той же хэш-функции H для полученного от распространителя документа. Если дешифрованное и вычисленное значения хэш-функции совпали, то целостность документа считается подтвержденной.

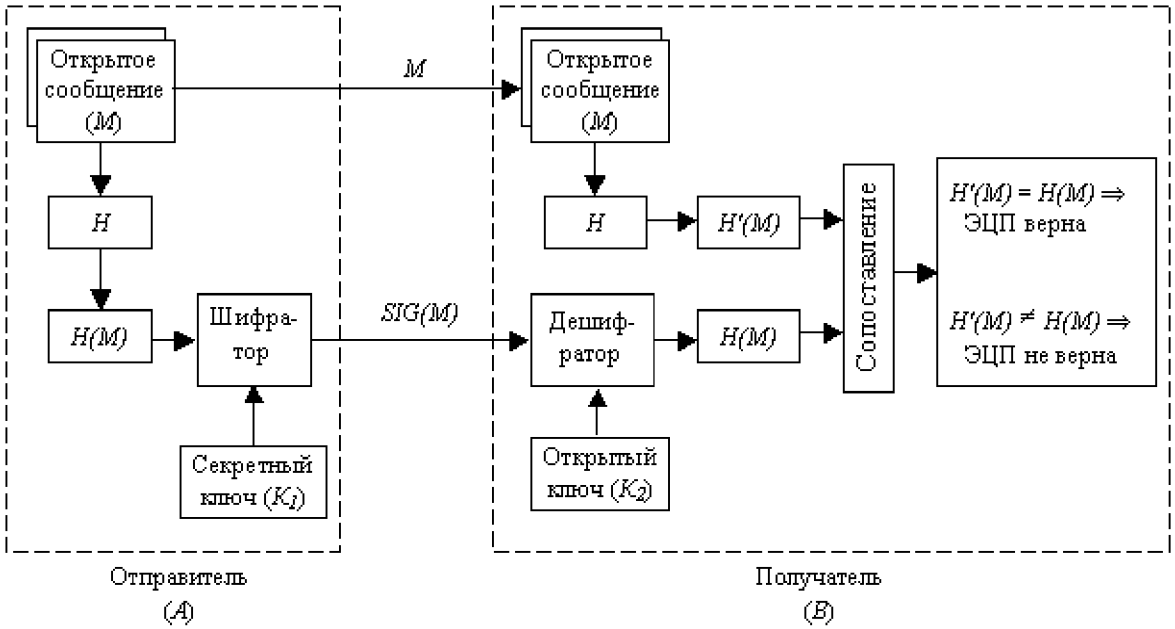

Рис. Схема формирования и верификации ЭЦП

Таким образом, функция хэширования позволяет обнаруживать модификацию документа. Теоретически возможно, что два различных документа будут сжаты в одну и ту же свертку (так называемая ситуация «столкновения», или коллизии). Поэтому для обеспечения стойкости функции хэширования необходимо предусмотреть способ избегания коллизий. Полностью коллизий избежать нельзя, так как мощность множества аргументов хэш-функции неограниченно больше мощности множества ее значений. Однако вероятность коллизии должна быть низкой.

Для того чтобы функция хэширования H могла быть должным образом использована в процессе аутентификации, H должна обладать следующими свойствами [1].

1. H может быть применена к аргументу любого размера.
2. Выходное значение H имеет фиксированный размер.
3. H(x) достаточно просто вычислить для любого x. Скорость вычисления хэш-функции должна быть такой, чтобы скорость выработки и проверки ЭЦП при использовании хэш-функции была значительно больше, чем при использовании текста самого документа.
4. Для любого y с вычислительной точки зрения невозможно найти x, такое что H(x) = y.
5. Для любого фиксированного x, с вычислительной точки зрения, невозможно найти $x' \neq x$, такое что H(x') = H(x).

Свойство 5 гарантирует, что не может быть найден другой документ, дающий ту же свертку. Это предотвращает подделку и также позволяет использовать H в качестве криптографической контрольной суммы для проверки целостности.

Электронные нормативно-технические документы газовой промышленности зачастую распространяются в составе баз данных НТД, управляемых информационно-поисковыми системами. Для реализации защиты НТД представляется целесообразным встраивать алгоритмы верификации ЭЦП в состав программного обеспечения информационно-поисковых систем для оперативной проверки подлинности НТД при их открытии и просмотре.

Таким образом, использование криптографических методов позволяет решить актуальную задачу установления подлинности электронных нормативно-технических документов при их распространении в системах обработки информации.

Библиографический список

1. ***Баричев, С. Г.*** Основы современной криптографии / С. Г. Баричев, Р. Е. Серов. – М. : Горячая линия – Телеком, 2002. – 175 с.

2. ***Саломаа, А.*** Криптография с открытым ключом / А. Саломаа. – М. : Мир, 1996. – 318 с.

3. ***Diffie, W.*** New directions in cryptography / W. Diffie, M. Hellman // IEEE Transactions on Information Theory IT-22. – 1976. – P. 644–645.

4. ***Merkle, R.*** Hiding information and signatures in trapdoor knapsacks / R. Merkle, M. Hellman // IEEE Transactions on Information Theory IT-24. – 1978. – P. 525–530.

5. ***Rivest, R.*** A method for obtaining digital signatures and public-key cryptosystems / R. Rivest, A. Shamir, L. Adleman // ACM Communications 21. – 1978. – P. 120–126.