Особливості застосування електронного цифрового підпису

АрхиповаЄ.О.

При використанні систем документообігу, незалежно від того, відкритою чи таємною є інформація, що циркулює в них, обов'язковим є забезпечення можливості встановлення наступних фактів:

1) ідентичності отриманого повідомлення тому, що було відправлено, тобто перевірка цілісності отриманої інформації: якщо на шляху від відправника до отримувача документ зазнав будь-яких змін, то цей факт (факт порушення цілісності) має бути зафіксований;
2) підтвердження того, що отримане повідомлення надіслане саме відправником, а не якою-небудь іншою особою, що лише використала його прізвище, тобто проведення автентифікації відправника.

При використанні паперового документообігу встановлення цих фактів здійснюється шляхом візуальної перевірки відсутності в отриманому документі підробок (підчисток, замаскованих виправлень тощо), зовнішніх пошкоджень упаковки документів та наявності підпису уповноваженої особи, завіреного відбитком печатки. Така перевірка повторюється для кожного документа, що надходить або циркулює в організації, та виконується співробітниками установи чи організації власноруч, отжемає суб'єктивний характер.

В системах електронного документообігу перевірка цих фактів здійснюється програмним шляхом, що стає можливим завдяки використанню електронного цифрового підпису (ЕЦП), який отримують в результаті криптографічного перетворення набору електронних даних та який додається до цього набору або логічно з ним поєднується [1].

Для накладення ЕЦП перш за все необхідно представити вихідну інформацію в електронній формі. Це здійснюється шляхом кодування повідомлення за допомогою стандартного машинного бінарного коду, після чого отримуємо послідовність бінарних символів, що записується у вигляді нулів та одиниць. Порядок слідування бінарних символів, довжина (обсяг коду) залежать від змісту та форми конкретного повідомлення. Незважаючи на

уявнускладність опису процедури кодування, фактично вона реалізується досить просто та швидко: шляхом набору документу з клавіатури комп'ютера. Тобто під час друкування тексту на комп'ютері ми формуємо електронний документ, візуальна форма якого спостерігається на екрані комп'ютера.

Першим кроком, який стосується безпосередньо процедури вироблення ЕЦП, є операція хешування електронного документу. Метою хешування є «стискання» вихідної бітової послідовності довільної довжини до повідомлення фіксованої довжини з певної кількості бітів, тобто створення хеш-образу вихідного повідомлення. Зауважимо, що якщо традиційна архівація дозволяє відтворити вихідне повідомлення у повному обсязі, то за хеш-образом цього зробити не можна.

Процедура створення хеш-образу має відповідати наступним вимогам:

- хеш-образ повинен мати однакову, чітко визначену довжину для вихідного тексту будь-якого розміру (зазвичай його довжина становить 128 чи більше біт);
- процедура хешування має бути незворотною, тобто повинна бути виключена можливість відтворити повний текст з хеш-образу;
- два тексти, в яких наявна найменша різниця (зокрема, змінена чи видалена хоч одна буква), повинні мати різні хеш-образи, що забезпечує фіксацію підробки/порушення цілісності документів, що передаються;
- має бути виключена можливість випадкового генерування однакових хеш-образів для будь-яких різних документів, що вже створені або будуть створені у майбутньому.

Наступний крок – це безпосереднє формування ЕЦП, що в найпростішому випадку виконується шляхом шифрування тільки хеш-образу, а у більш відповідальних ситуаціях – ще й додаткової інформації (наприклад, ідентифікаційних кодів відправника та отримувача, фіксація часу формування ЕЦП тощо).

Слід зазначити, що визначальним елементом вироблення ЕЦП та його

перевірки є спосіб, у який виконується шифрування. Справа в тому, що замість відомого з давніх часів симетричного алгоритму шифрування, що передбачає використання однакових ключів як для шифрування, так і для розшифрування, при роботі з ЕЦП застосовується асиметричний крипто алгоритм, суть якого полягає у використанні двох різних ключів. Тоді як відкритий (публічний) ключ, що використовується для розшифрування, доступний всім, то закритий (таємний, особистий) – відомий лише відправнику. Відправник, розрахувавши хеш-образ за відомим виключно йому алгоритмом із застосуванням свого таємного ключа, зашифровує хеш-образ та, додавши до нього вихідне повідомлення, відправляє документ листом через систему відкритого зв'язку. Отримувач приймає повідомлення та формуєхеш-образ для отриманого тексту за допомогою власного відкритого ключа та відомого йому алгоритму розшифрування. Отриманий ним хеш-образ порівнюється з хеш-образом сформованим та надісланим відправником листа. У разі їх співпадіння отримувач може бути певним, що отриманий документ не був модифікований без відома власника.

Розшифрування отриманого повідомлення, хешування та співставлення двох хеш-образів складають перевірку ЕЦП. Позитивний результат перевірки, окрім підтвердження ідентичності надісланого та отриманого текстів, свідчить також про автентичність відправника, бо лише відправник міг зашифрувати текст таємним ключем, який складає пару до відкритого ключа отримувача.

Останнє є дуже важливим з точки зору можливості забезпечення реалізації «антисаботажної функції», суть якої полягає в тому, що відправник, використавши відомий лише йому закритий ключ, не може відмовитися від авторства щодо даного документу. Таким чином, ЕЦП дозволяє встановити чіткі межі відповідальності за створення та виконання документів, а також гарантує цілісність документа та автентичність його відправника.

Список літератури

1) Закон України «Про електронний цифровий підпис» [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/852-15