УДК 004[681.518]
ПЕТРО СЕРГІЙОВИЧ КЛІМУШИН
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Комплексний захист інформації ґрунтується на використанні правових, фізичних, організаційних та програмно-апаратних засобів захисту інформації, до яких належить криптографічний захист інформації. Цей вид захисту інформації реалізується шляхом перетворення інформації з використанням ключів на основі математичних методів. Є дві мети використання криптографічних методів – приховування інформації шляхом її шифрування та підтвердження юридичної значимості документів з використанням електронного підпису.

Криптографічні методи вирішують два завдання – забезпечення конфіденційності інформації шляхом позбавлення зловмисника можливості видобути інформацію з каналу зв’язку та забезпечення цілісності інформації шляхом недопущення зміни інформації та внесення в неї неправдивого змісту [1].

Аналіз літературних джерел дає підстави стверджувати, що у процесі використання криптографічних засобів захисту інформації є певні недоліки, які знижують ефективність їх функціонування.

Метою досліджень є надання пропозицій з ефективного використання криптографічних методів і засобів у діяльності органів внутрішніх справ.

Шифрування дозволяє захистити інформацію шляхом її перетворення шифртекст з можливістю подальшого дешифрування. Зашифровувати можна і звичайні тексти, і комп’ютерні файли. Шифрування поділяється на симетричне та асиметричне. В симетричному шифруванні використовується один таємний ключ і для шифрування, і для дешифрування. В асиметричному шифруванні

для шифрування використовується відкритий ключ, а для дешифрування – інший, таємний особистий ключ.

Недоліком симетричного шифрування є необхідність передачі ключа особі, що спричиняє загрозу розкриття та дешифрування інформації зловмисниками. Перевагою симетричного шифрування є його більша швидкість, ніж асиметричного, бо під час асиметричного шифрування використовують довші ключі, що збільшує час шифрування.

Симетричні алгоритми шифрування можна розділити на потокові та блочні. Потокові алгоритми шифрування послідовно обробляють текст повідомлення, блочні алгоритми, в свою чергу, працюють з блоками фіксованого розміру.

В сучасних криптосистемах, використовуються комбінації симетричних та асиметричних алгоритмів, для того, аби отримати переваги обох схем. Асиметричні алгоритми використовуються для розповсюдження ключів швидших симетричних алгоритмів.

Для уникнення підміни чи модифікації повідомлення відправник передає отримувачу контрольну суму, яка є унікальною для кожного повідомлення. Для передачі контрольної суми її включають до електронного підпису.

Усунути основні недоліки, властиві як симетричним, так і асиметричним методам криптографічного захисту інформації, дозволяє їх комбіноване використання. У сучасних реальних криптосистемах шифрування даних здійснюється за допомогою «швидких» симетричних блокових алгоритмів, а завданням «повільних» асиметричних алгоритмів стає шифрування ключа сеансу. В цьому випадку зберігаються переваги високої секретності (асиметричні) та швидкості роботи (симетричні).

Електронний підпис дозволяє підтвердити авторство документа та гарантувати цілісність інформації та відсутність спроб її перекручення. Електронний підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа. Підпис повинен залежати від

часу, щоб не можна було використати старі повідомлення; цим електронний підпис відрізняється від рукописного підпису.

Електронний підпис дозволяє захистити інформацію від таких злочинних дій: *відмова від авторства* (автор документа відмовляється від авторства); *фальсифікація* (отримувач документа підробляє його); *зміна* (отримувач документа вносить у нього зміни); *маскування* (користувач маскується під іншого користувача) [1].

Документ складається з тексту, електронного підпису та сертифіката користувача, який містить дані користувача, його ідентифікаційне ім’я та відкритий ключ дешифрування для перевірки підпису адресатом документа [2].

Важливою характеристикою методів шифрування є їх криптографічна стійкість, тобто стійкість до дешифрування без ключа, яка визначається як кількість обчислювальних та інших ресурсів для такого дешифрування.

Порядок здійснення криптографічного захисту інформації з обмеженим доступом використовуються криптосистеми і засоби криптографічного захисту допущені до експлуатації Державної службою спеціального зв’язку та захисту інформації України, які мають сертифікат відповідності.

Таким чином, для шифрування з метою передачі інформації в інформаційних мережах доцільно застосовувати асиметричні методи, а для шифрування з метою зберігання інформації – симетричні. Що ж стосується програм для шифрування інформації, то для захисту інформації, яка використовується органами внутрішніх справ, допустимим є використання лише програмних засобів криптографічного захисту інформації, які сертифіковані в Україні.

Список використаних джерел:

1. Зачек О. І. Криптографічний захист інформації у діяльності органів внутрішніх справ. Науковий вісник Львівського державного університету внутрішніх справ. серія юридична. 2014. Вип. 2. С. 91–99.

2. Клімушин П. С. Стратегії та механізми електронного урядування в інформаційному суспільстві. Монографія. Харків. Вид-во ХарРІ НАДУ «Магістр», 2016. 524с.