УДК 004.056.55

О. І. Зачек

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ У ДІЯЛЬНОСТІ ОРГАНІВ ВНУТРІШНІХ СПРАВ

Розглянуто криптографічні методи та засоби захисту інформації, які є одним з елементів комплексної системи захисту інформації. Висвітлено види шифрування, а також сутність електронних підписів. Наведено правові підстави застосування криптографічних методів захисту інформації. Представлено програмні засоби іноземних та українських розробників, що призначені для криптографічного захисту інформації. Надано пропозиції з ефективного використання криптографічних методів і засобів у діяльності органів внутрішніх справ.

Ключові слова: *комплексний захист інформації, криптографічні методи захисту інформації, правова основа криптографічного захисту інформації, програмні засоби криптографічного захисту інформації.*

Постановка проблеми. Кримінально-пошукова та інша криміналістична інформація виконує неабияку роль у боротьбі зі злочинністю. Ця інформація збирається та зберігається в інформаційних системах ОВС. Значна роль у цьому належить підрозділам інформаційно-аналітичного забезпечення МВС. Інформація, яка збирається і обробляється цими підрозділами, цікава не лише ОВС, але і злочинцям, які також здійснюють розвідувальні і контрозвідувальні заходи, спрямовані на нейтралізацію зусиль ОВС у боротьбі зі злочинністю. Сучасні інформаційні технології надають їм таку можливість. Також значна частина інформації циркулює між підрозділами ОВС із використанням засобів зв'язку. Ця інформація також становить значний інтерес для злочинців. Тому великого значення набуває проблема захисту цієї інформації з використанням криптографічних методів і засобів на їх основі, а наукові дослідження в цьому напрямі є актуальними.

Комплексний захист інформації ґрунтується на використанні правових, фізичних, організаційних та програмно-апаратних засобів захисту інформації, до яких належить криптографічний захист інформації.

Стан дослідження. Проблемам створення і функціонування засобів криптографічного захисту інформації присвячено достатньо публікацій у відкритих, і в закритих літературних джерелах, зокрема таких учених, як А. П. Алферов, А. В. Бабаш, С. Г. Баричев, В. С. Блінцов, О. В. Вербіцький, Ю. Л. Гальчевський, В. О. Голубєв, І. Д. Горбенко, В. О. Горобцов, Т. О. Гріненко, В. П. Захаров, А. Ю. Зубов, Б. А. Кор-

мич, А. С. Кузьмин, А. В. Персиков, В. В. Поповський, Р. Е. Сєров, А. А. Терехов, А. В. Черемушкін, Г. П. Шанкін. Важливість наукового здобутку та внеску у теорію і практику інформаційної безпеки цих учених складно переоцінити.

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

Метою статті є надання пропозицій з ефективного використання криптографічних методів і засобів у діяльності органів внутрішніх справ. Завданнями дослідження є розгляд криптографічних методів та засобів захисту інформації, а також правових підстав їх використання.

Виклад основних положень. Одним із елементів комплексної системи захисту інформації є 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 значимості документів з використанням електронного цифрового підпису.

Іншими словами, на думку В. В. Поповського, 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, с. 12].

Є два розділи науки, які стосуються криптографічних методів: криптографія та криптоаналіз, які разом утворюють криптологію. Криптографія вивчає математичні перетворення, що дозволяють зашифровувати інформацію. Криптоаналіз вивчає методи дешифрування без знання таємного ключа [1, с. 12].

Засоби криптографічного захисту інформації поділяються на:

– засоби, які реалізують криптографічні алгоритми перетворення інформації;

– засоби, системи та комплекси захисту від нав'язування неправдивої інформації, що використовують криптографічні алгоритми перетворення інформації;

– засоби, системи і комплекси, призначені для виготовлення та розподілу ключів для засобів криптографічного захисту інформації;

– системи та комплекси, що входять до складу комплексів захисту інформації від несанкціонованого доступу, та використовують криптографічні алгоритми перетворення інформації [2].

Засоби криптографічного захисту інформації разом з ключовою та іншими видами документації, які забезпечують необхідний рівень захисту інформації, утворюють криптографічну систему [2].

Шифрування дозволяє захистити інформацію шляхом її перетворення в незрозумілий текст (шифртекст) з можливістю подальшого розшифрування (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 загальнодоступний ключ, а для дешифрування – інший, таємний, які генеруються за допомогою генераторів псевдовипадкових чисел. Асиметричне шифрування ще називають шифруванням із відкритим ключем. Недоліком симетричного шифрування є необхідність передачі ключа особі, якій адресований текст, що спричиняє загрозу його 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.

Спосіб кодування тексту під час шифрування заснований на алгоритмі, а закодований текст можна дешифрувати лише за допомогою ключа. Для надсилання повідомлень різним адресатам може бути використаний один алгоритм із різними ключами. Секретність визначається ключем, а не алгоритмом, оскільки більшість алгоритмів є відомими широкому колу фахівців. Унаслідок підвищення продуктивності комп'ютерної техніки зростає імовірність добирання ключів шляхом перебору комбінацій, тому доводиться використовувати дедалі довші ключі, а це збільшує час на шифрування [3, с. 57].

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 [1, с. 12].

З метою криптографічного захисту інформації в комп'ютерній мережі необхідно створювати спеціальну службу, яка здійснює генерацію ключів і розподіляє їх між користувачами мережі.

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 [3, с. 58].

Для створення електронних підписів здійснюється шифрування контрольної суми та додаткової інформації за допомогою особистого ключа відправника. Щоб уникнути перехоплення та повторного використання, до підпису включений порядковий номер.

Електронний підпис дозволяє підтвердити авторство документа та гарантувати цілісність інформації та відсутність спроб її перекручення. 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 [3, с. 69].

Електронний підпис дозволяє захистити інформацію від таких злочинних дій [4, с. 88]:

– «відмова від авторства», коли автор документа відмовляється від авторства;

– «фальсифікація», коли отримувач документа підробляє його;

– «зміна», коли отримувач документа вносить у нього зміни;

– «маскування», коли користувач маскується під іншого користувача.

Для підтвердження повідомлення необхідне виконання таких умов:

– відправник повинен внести в повідомлення підпис, що містить додаткову інформацію, яка залежить від повідомлення та від одержувача повідомлення, але відома лише відправнику;

– правильний підпис не можна скласти без додаткової інформації;

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

– отримувач повинен мати змогу переконатись, що підпис належить відправнику і є правильним щодо цього повідомлення.

Відтак можна зробити висновок, що електронний підпис – це вид паролю, який залежить від відправника, одержувача та змісту повідомлення [4, с. 89].

Згідно із Законом України «Про електронні документи та електронний документообіг» електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу і накладанням електронного підпису завершується створення електронного документа [5].

Правовий статус електронного цифрового підпису визначає Закон України «Про електронний цифровий підпис», згідно з яким елек-

тронний цифровий підпис – це вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа [6].

Порядок здійснення криптографічного захисту інформації з обмеженим доступом, розголошення якої завдає (може завдати) шкоди державі, суспільству або особі, в Україні визначається «Положенням про порядок здійснення криптографічного захисту інформації в Україні». Згідно з цим Положенням, для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави, використовуються криптосистеми і засоби криптографічного захисту, допущені до експлуатації. Для криптографічного захисту конфіденційної інформації використовуються криптосистеми і засоби криптографічного захисту, які мають сертифікат відповідності [7].

Є велика кількість програмних продуктів, що призначені для криптографічного захисту інформації, і іноземних розробників, і українських.

Однією з кращих програм для шифрування інформації вважається «BestCrypt» від фінської компанії «Jetico». Вона дозволяє створювати зашифрований контейнер для збереження інформації на будь-яких типах носіїв і розрахована для роботи і під Windows, і під Linux. У програмі на вибір можна використовувати один із найбільш сильних алгоритмів, що реалізовані з 256-бітним ключем: Rijndael (AES), російський федеральний стандарт ГОСТ 28147-89, Blowfish та Twofish. У новіших версіях алгоритм Blowfish може використовувати 448-бітний ключ [8].

Також відомою є програма «Private Disk» від молдавської компанії «Dekart». Вона дозволяє створювати зашифрований віртуальний диск для збереження інформації. Шифрування здійснюється алгоритмом AES 256. Під час роботи з інформацією файли на віртуальному диску не відрізняються за своїми властивостями від незашифрованих, доки користувач не закриє доступ. Віртуальний диск захищений від вірусів, троянських і шпигунських програм за допомогою вбудованого в програму брандмауера Disk Firewall [9].

Є система криптографічного захисту інформації «Карма» від української компанії «NetCom Technology». Вона призначена для за-

безпечення використання електронного цифрового підпису та шифрування, зокрема в юридично значущому електронному документообігу. Особливістю цієї системи є можливість додавати до складу електронного цифрового підпису зображення власноручного підпису. Внаслідок цього електронний документ виглядатиме як паперовий [10].

ТОВ «СКЗ «Криптософт» пропонує програмний комплекс криптографічного захисту інформації «Криптосервер» для роботи під MS Windows XP, MS Windows 7. Цей комплекс забезпечує захист даних, які передаються незахищеними загальнодоступними (Internet) або відкритими (наприклад орендовані канали, MPLS) каналами. Захист здійснюється за допомогою шифрування даних на основі вітчизняних алгоритмів шифрування. Максимальний гриф обмеження доступу інформації, що захищається цим комплексом, – «конфіденційно» [11].

На сайті Державної служби спеціального зв'язку та захисту інформації України наведено перелік сертифікованих в Україні засобів криптографічного захисту інформації українських розробників. До них належать:

– програмний виріб «NovaLib», розробник ТОВ «Науково-виробничий центр «Безпека інформаційних технологій і систем»;

– програмний виріб «Шифр», розробник ЗАТ «Сайфер»;

– виріб програмний «Шифр+», розробник ЗАТ «Сайфер»;

– програмне забезпечення апаратно-програмних засобів електронного цифрового підпису «Основа», розробник ТОВ «Експотрейд»;

– засіб апаратно-програмний криптографічного захисту інформації «Старт», розробник ТОВ «Науково-виробничий центр «Безпека інформаційних технологій і систем» [12].

Нашим авторським колективом було розроблено та запатентовано два засоби для криптографічного захисту інформації, що можуть бути використані для забезпечення захисту інформації під час телефонних переговорів без змін фізичних параметрів лінії зв'язку. Це шифрувальна телефонна гарнітура, яка дозволяє забезпечити захист інформації під час телефонних переговорів із використанням засобів стільникового зв'язку [13], та шифрувальний телефонний апарат, що дозволяє здійснити захист інформації під час телефонних переговорів із використанням стаціонарного телефонного зв'язку [14].

Висновки. Розглянувши методи шифрування інформації, можна зробити висновок, що 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. У своїй діяльності працівники органів внутрішніх справ дедалі частіше опиняються у ситуації, коли підозрювані здійснюють шифрування інформації за допомогою програм криптографічного захисту типу BestCrypt чи Private Disk. У випадку використання 256-бітних ключів вони забезпечують доволі надійний захист інформації, зламати який не завжди можливо навіть із використанням найсучасніших засобів обчислювальної техніки. Тому можна порекомендувати ввести адміністративну відповідальність за використання несертифікованих в Україні програм фізичними та юридичними особами, та ввести вимогу до розробників програм під час сертифікації надавати правоохоронним органам засоби для дешифрування за рішенням суду інформації, зашифрованої з використанням їхніх програм.

1. Поповский В. В. Основы криптографической защиты информации в телекоммуникационных системах. – Ч. 1 / В. В. Поповский, А. В. Персиков. – Х.: Компания СМИТ, 2010. – 352 с.

2. Горобцов В. О. Криптографічний захист інформації. Юридический словарь / В. О. Горобцов // zakony.com.ua від 11.02.2014. [Електронний ресурс]. – Режим доступу: http://www.zakony.com.ua

3. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинами: монографія / В. О. Голубєв. – Запоріжжя: ГУ «ЗІДМУ», 2003. – 250 с.

4. Баричев С. Г. Основы современной криптографии / С. Г. Баричев, Р. Е. Серов. – 2006. – 152 с. [Електронний ресурс]. – Режим доступу: http://padabum.com/php?id=2667

5. Про електронні документи та електронний документообіг: Закон України від 22.05.2003 № 851-IV. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/851-15

6. Про електронний цифровий підпис: Закон України від 22.05.2003 № 852-IV. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/852-15

7. Про Положення про порядок здійснення криптографічного захисту інформації в Україні: Указ Президента України від 22.05.1998 № 505/98. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/505/98

8. Басыров Роберт. Обзор BestCrypt – программы для криптографической защиты данных от 11.07.2007 / Роберт Басыров. [Електронний ресурс]. – Режим доступу: http://www.ixbt.com/soft/bestcrypt.shtml

9. Private Disk лучшая программа для шифрования файлов. [Електронний ресурс]. – Режим доступу: http://www.private-disk.net/ru

10. Система «КАРМА». Універсальна система для криптографічного захисту інформації. [Електронний ресурс]. – Режим доступу: http://www.eos.com.ua/eos/ua/products/carma

11. Комплекс програмний КЗІ «Криптосервер». [Електронний ресурс]. – Режим доступу: http://cryptosoft-ua.com/kataloh/8-kompleks-prohramnyi-kzi-kryptoserver

12. Перелік сертифікованих засобів криптографічного захисту інформації. [Електронний ресурс]. – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article

13. Дмитрик Ю. І. Патент України на корисну модель № 71446 «Шифрувальна телефонна гарнітура» / Ю. І. Дмитрик, О. І. Зачек, В. Д. Смичок // Видано згідно із заявкою № u 2012 00477 від 16.01.2012 р. – 4 с.

14. Захаров В. П. Патент України на корисну модель № 82310 «Шифрувальний телефонний апарат» / В. П. Захаров, О. І. Зачек, Ю. І. Дмитрик, А. Т. Рудий, В. Д. Смичок // Видано згідно із заявкою № u 2013 02307 від 25.02.2013 р. – 4 с.

Зачек О. И. Криптографическая защита информации в деятельности органов внутренних дел

Рассмотрены криптографические методы и средства защиты информации, которые являются одним из элементов комплексной системы защиты информации. Рассмотрены виды шифрования, а также смысл электронных подписей. Приведены правовые основания использования криптографических методов защиты информации. Представлены программные средства иностранных и украинских разработчиков, предназначенные для криптографической защиты информации. Даны предложения по эффективному использованию криптографических средств и методов в деятельности органов внутренних дел.

Ключевые слова: *комплексная защита информации, криптографические методы защиты информации, правовое основание криптографической защиты информации, программные средства криптографической защиты информации.*

Zachek O. I. Cryptographic protection of information in activity of the bodies of internal affairs

The article deals with cryptographic methods and data protection, which is one element of comprehensive information security systems and are used to hide information by encrypting it, and to confirm the relevance of documents using a digital signature. Kinds of encryption are considered – symmetric, which should be used for the purpose of storing information, and asymmetric, which should be used to transfer information in information networks. An important characteristic of encryption methods is their cryptographic resistance, which is resistance to decrypt without the key. We also considered the nature of electronic signatures, summarized that this kind of password, which depends on the sender, recipient and message content. The legal grounds for the use of cryptographic methods of information se-

curity are presented. The software tools for cryptographic security by foreign and Ukrainian developers are submitted, in particular, given a list of certified in Ukraine tools for cryptographic information protection from Ukrainian developers. It is concluded that for the protection of information that is used by the bodies of internal affairs, only software tools of cryptographic information protection, that were certified in Ukraine, are acceptable to use. Attention is paid to the repeated instances when the suspects carried out information encryption using encryption software BestCrypt or Private Disk. These programs provide enough reliable data protection when using a 256-bit key, which is not always possible to hack even with the use of advanced computer technology. We recommend that to enter administrative responsibility for the use of non-certified programs in Ukraine to encrypt information by individuals and legal entities. Another recommendation is to require application developers during certification to provide law enforcement agencies the means to decrypt by court order information encrypted using their programs.

Key words: *complex information protection, cryptographic methods of information protection, the legal basis of cryptographic protection of information, software cryptographic protection of information.*

Стаття надійшла 03 березня 2014 р.

УДК 342.9.(477)

О. М. Ілюшик

КЛАСИФІКАЦІЯ АДМІНІСТРАТИВНИХ ДОГОВОРІВ, ЩО ВИКОРИСТОВУЮТЬСЯ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Досліджено питання щодо класифікації адміністративних договорів, що регламентують особливості діяльності органів публічної влади у правоохоронній сфері, зокрема їхню взаємодію. Проаналізовано наукові підходи щодо класифікації адміністративних договорів, зокрема адміністративних договорів, що використовуються в правоохоронній сфері. Наголошено на тому, що для розробки практичних рекомендацій щодо покращення застосування адміністративних договорів у діяльності правоохоронних органів, з урахуванням особливостей кожного виду адміністративного договору, істотне значення має їх класифікація.

Ключові слова: *адміністративний договір, класифікація адміністративних договорів, правоохоронний орган, компетенція, координаційний адміністративний договір, субординаційний адміністративний договір.*

Постановка проблеми. Адміністративний договір, як один із найбільш ефективних і демократичних засобів регулювання діяльно-