2. Кіберзлочинність: проблеми боротьби і прогнози [Електронний ресурс]. – Режим доступу: http://anticyber.com.ua/article_detail.php?id=140

3. Прохоренко В. Кіберзлочинність для України стає актуальним поняттям – НБУ. - // Економічна правда від 26 лютого, 2013року.- 10 с.

Криптографічні методи захисту інформації: види та вимоги до них

Гладковський Е.О.
слухач 2-го курсу магістратури факультету № 1
Одеського державного університету внутрішніх справ

Ісмайлов К.Ю.
кандидат юридичних наук,
завідувач кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

Збереження інформації в таємниці турбує людей ще з стародавніх часів, коли з появою писемності з'явилася і небезпека прочитання її небажаними особами. З розвитком новітніх комп'ютерних технологій та формування інформаційного суспільства, глобалізації всесвітньої мережі Інтернет, набуває ще більшого значення проблема захисту персональних даних фізичних, юридичних осіб, а також державних установ.

В даний час більшість засобів захисту інформації базується на використанні криптографічних шифрів і процедур шифрування-розшифрування. Ці процеси відбуваються в рамках певної криптосистеми, яка диктує правила і визначає параметри шифрування і дешифрування.

Вивченню методу криптографічного шифрування присвячені праці таких науковців: В.В. Ященко, І.Н. Войцехівська, О.В. Гомонай, О.В. Вербіцький, В.О. Хорошко, М.С. Шелест, Ю.Є. Яремчук та ін.

Перш ніж переходити до детального розгляду криптографічного захисту інформації, необхідно розглянути, що саме входить в це поняття, отже: криптографічний захист - це вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо [1].

Доцент Адигеєв М.Г., розглядає криптографію, як науку про способи перетворення інформації з метою її захисту від незаконних користувачів [2, с. 4].

Професор Войцехівська І.Н. надає найбільш розгорнуте поняття криптографія (від грец. κρυπτός - таємний, прихований та γράφω - пишу) - спеціальна історична дисципліна про шифрування (та розшифровування) записів за спец. технологіями з метою зробити їх зміст зрозумілим тільки для обмеженого кола осіб [3].

Проаналізувавши сучасні засоби криптографічного захисту інформації можна здійснити таку видову класифікацію:

– 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 [4].

Отже, метою застосування криптографічних методів є захист інформаційної системи від цілеспрямованих руйнівних впливів (атак) з боку противника. Способи захисту істотно залежать від ситуації: по-перше від якого роду загрози необхідно захищатися; по-друге якими можливостями володіє противник.

Шифрування дозволяє захистити інформацію шляхом її перетворення в незрозумілий текст (шифр-текст) з можливістю подальшого розшифрування (дешифрування). Зашифровувати можна і звичайні тексти, і комп'ютерні файли. Так, шифрування поділяється на симетричне та асиметричне [3].

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, який генерується 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, що в свою чергу негативно відображається на оперативності передачі даних.

Для сучасних криптографічних систем захисту інформації є загальні вимоги, а саме:

- зашифроване повідомлення повинно піддаватися читанню тільки при наявності ключа;
- кількість операцій, необхідних для визначення ключа шифрування за фрагментом шифрованого повідомлення і відповідного йому відкритого тексту, повинна бути не менша загальної кількості можливих ключів;
- кількість операцій, необхідних для розшифровування інформації шляхом перебору всіх можливих ключів, повинна мати строгу нижню оцінку і виходити за межі можливостей сучасних комп'ютерів (з урахуванням можливості використання мережних обчислень та прогнозу зростання потужності обчислювальних засобів);
- знання алгоритму шифрування не повинно впливати на надійність криптографічного захисту;
- незначна зміна ключа повинна приводити до істотної зміни вигляду зашифрованого повідомлення;
- структурні елементи алгоритму шифрування повинні бути незмінними;
- довжина шифрованого тексту повинна бути близькою довжині вихідного тексту;
- не повинно бути простих і легко встановлюваних залежностей між ключами, послідовно використовуваними в процесі шифрування;
- алгоритм повинен допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна вести до якісного погіршення алгоритму шифрування [5, с. 54].

Отже розглянувши поняття, види та характеристики криптографічного методу захисту інформації можна дійти висновків

- що доцільним є використання асиметричних методів шифрування даних. Хоча несиметрична криптографія є досить повільною у порівнянні зі швидкими і перевіреними часом і практикою симетричних алгоритмів, все ж таки використання несиметричної криптографії радикально спрощує процедуру розподілу ключів між учасниками інформаційних відносин.
- є ряд недоліків, які притаманні криптографічним системам, а саме: якщо інформація була криптографічно зашифрована, то у випадку збоїв у жорсткому диску, така інформація буде втрачена, оскільки практично не буде підлягати відновленню та розшифруванню
- для кращого захисту слід використовувати криптографічно стійку функцію зміни станів отже, можна зробити висновок, що в додатках, що пред'являють підвищені вимоги до безпеки конфіденційної інформації, не слід використовувати шифратори «з довільним доступом», так як принцип їх побудови суперечить даним вимогам
- для шифрування з метою передачі інформації в інформаційних мережах доцільно застосовувати асиметричні методи, а для шифрування з метою зберігання інформації – симетричні.

Література:

1. Про Положення про порядок здійснення криптографічного захисту ін- формації в Україні: Указ Президента України від 22.05.1998 № 505/98. [Електронний ресурс]. – Режим доступу:http://zakon3.rada.gov.ua/laws/show/505/98.

2. Адигеев М.Г. Введение в криптографию. Часть 1. Основные понятия, задачи и методы криптографии. - Ростов-на-Дону: Ростовский гос. ун-т, 2002. - 35 с.

3. Войцехівська І.Н. Криптографія // Енциклопедія історії України: Т. 5: Кон - Кю / Редкол.: В.А. Смолій (голова) та ін. НАН України. Інститут історії України. - К.: В-во «Наукова думка», 2008. - 568 с. [Електронний ресурс]. - Режим доступу: http://www.history.org.ua/?termin=Kriptografiya.

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

5. Хорошко В.О., Азаров О.Д., Шелест М.С., Яремчук Ю.Є. Основи комп'ютерної стеганографії. Навчальний посібник. - Вінниця: ВДТУ, 2003. - 143 с.

Слідчий огляд в справах про комп'ютерні злочини

Білоусов А.С.
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу та криміналістики
Інституту права ім. В. Сташиса Класичного приватного університету
м. Запоріжжя

Слідчий огляд є, як правило, невідкладною слідчою дією, що полягає у безпосередньому сприйнятті, дослідженні, оцінці й фіксації слідчим обстановки місця події, слідів та об'єктів, які мають відношення для справи, їх ознак, властивостей, станів та взаємозв'язків, з метою з'ясування сутності події, що сталася, механізму злочину та його обставин, які мають значення для встановлення істини по справі. Слідчий огляд являє собою цілеспрямовану діяльність процесуальної особи, що має бути належним чином організована і спланована. Планування й організація слідчої діяльності виступають як тактичні прийоми [1, с.151].

Загальні та окремі тактичні вимоги щодо проведення слідчого огляду наповнюються істотними особливостями в разі огляду комп'ютерних об'єктів. Основна складність в разі розслідування злочинів, що вчинені з використанням комп'ютерних об'єктів, полягає в тому, що дії з огляду на властивості комп'ютерних об'єктів не охоплюються традиційним розумінням слідчого огляду. Відмінною особливістю огляду таких комп'ютерних об'єктів як системні блоки електронно-обчислювальних машин, комп'ютерні програми, інформація, що міститься на магнітних носіях тощо є те , що їх не можна оглянути і сприйняти безпосередньо всіма учасниками огляду, як це передбачено завданнями проведення слідчого огляду. Для сприйняття властивостей окремих комп'ютерних об'єктів потрібно здійснити доступ до них шляхом використання спеціальних технічних пристроїв з відповідним програмним забезпеченням. При цьому слідчий в присутності понятих не просто спостерігає за комп'ютерним об'єктом, а повинен сам або за допомогою спеціаліста ввести в автоматизовану систему певні команди, і лише після цього буде отримана інформація, яка й розкриє та зробить доступною для сприйняття властивість комп'ютерних об'єктів.

Підготовка до огляду місця події з наявними на ньому комп'ютерними об'єктами поділяється на два етапи. Перший етап охоплює підготовку слідчого до виїзду на місце події і розпочинається відразу після отримання ним інформації про подію з ознаками комп'ютерного злочину. Вже на цьому етапі варто звернутися по допомогу до спеціаліста в галузі комп'ютерної техніки, бажано, щоб цей же спеціаліст надавав би допомогу під час огляду. Не зайвою буде допомога і оперативних сил та засобів.

До виїзду на місце події треба уточнити місце знаходження засобів електронно-обчислювальної техніки, комп'ютерної інформації, що використовувалися під час вчинення злочину, або на яких збереглися сліди злочину і віддати розпорядження відповідним посадовим особам підприємства, установи щодо забезпечення охорони місця події, звернувши особливу увагу на охорону комп'ютерних об'єктів та вжиття можливих заходів щодо запобігання внесення змін в обстановку й знищення слідів. Визначивши місце, де знаходяться засоби комп'ютерної техніки та носії комп'ютерної інформації, варто встановити їх власника чи користувачів, уточнити місце їх перебування на час планованого проведення огляду і з'ясувати можливість процесуального вилучення в разі потреби комп'ютерної техніки та носіїв такої інформації. Також не зайвим буде з'ясувати питання щодо режиму роботи об'єкта, де буде проводитися слідча дія, кількісний та персональний склад осіб, допущених до операційної системи, а в разі встановлення на ділянках з обробки інформації режиму обмеженого доступу до неї, підібрати понятих та інших учасників слідчої дії з урахуванням цих обставин.

Після прибуття на місце події слідчий повинен визначитися з конкретним місцем проведення слідчої дії, обсягами роботи, яку належить виконати, достатністю задіяних для цього сил і засобів. Особливістю огляду за справами про комп'ютерні злочини є те, що відразу після прибуття до місця події слідчий повинен здійснити заходи щодо недопущення до засобів обчислювальної техніки, які є на місці події всіх осіб, що працюють на об'єкті. Щоправда, на тих об'єктах, де безперервна робота обчислювальної техніки забезпечує роботу всього технологічного процесу або його окремих складових, заборонити здійснення операцій по керуванню комп'ютерними процесами не можна. І тому, слідчий до початку огляду повинен зафіксувати технічні параметри комп'ютерної техніки на кожному робочому місці та попередити виконавців про невтручання в інформаційні процеси, якщо це не пов'язано з