УДК 004.056.55

Д.М. Драгоєв
Національний авіаційний університет, Київ

РОЛЬ МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ В ЖИТТІ ЛЮДИНИ

У сучасному суспільстві інформаційні технології пройшли довгий шлях і проникли в усі сфери життя людини. Нові технології дозволяють передавати інформацію з однієї точки земної кулі в іншу за лічені секунди. Крім особистого листування, електронні повідомлення використовуються для передачі інформації між державними органами, органами місцевого самоврядування, військовими частинами тощо. І всі ці повідомлення можна перехопити і використовувати в своїх корисливих цілях. А щоб зловмисники не дізналися інформацію, використовуються різні методи шифрування, які надаються сучасною криптографією. Криптографія - це наука про методи забезпечення конфіденційності (неможливості прочитати інформацію від сторонніх), цілісності даних (неможливості ненавмисної зміни інформації), аутентифікації (перевірки справжності авторства або інших властивостей об'єкта), а також неможливості заперечувати авторство. Ключовою метою криптографічного захисту інформації є забезпечення конфіденційності та захисту інформаційних даних комп'ютерних мереж в процесі їх передачі по мережі між користувачами системи.

Основним видом криптографічного перетворення інформації в комп'ютерних мережах є шифрування. Шифрування відноситься до процесу перетворення відкритої інформації в зашифровану інформацію (зашифрований текст) або до процесу перетворення зашифрованої інформації назад в відкриту інформацію. Процес перетворення відкритої інформації в закриту називається шифруванням, а процес перетворення закритої інформації в відкриту інформацію дешифруванням.

Ефективність шифрування для захисту інформації вимагає таємності ключа і криптографічної стійкості шифру.

Криптографічні методи можна розділити на два класи:

1) обробка інформації шляхом заміни і переміщення букв, які не змінюють обсяг даних (шифрування);

2) стиснення інформації шляхом заміни окремих поєднань літер,

слів чи словосполучень (кодування).

Можливі як апаратні, так і програмні методи шифрування при обміні інформацією між комп'ютерами через телекомунікаційну мережу, а також при роботі з локальними абонентами. Апаратне шифрування використовується для захисту текстової інформації при передачі на віддалені станції в телекомунікаційній мережі. Методи апаратного шифрування використовуються для передачі захищених даних по телекомунікаційної мережі. Програмні методи шифрування використовуються для зберігання інформації на магнітних носіях (дисках, стрічках). Це можуть бути дані з різних інформаційних і допоміжних систем, ACS, ASOD і інших методів програмного шифрування, які зводяться до повторного кодування, впорядкування і додаванню операцій по модулю 2 з використанням ключових слів.

У той же час слід використовувати разом кілька методів шифрування для захисту цілісності та конфіденційності даних. Комбіновані шифри застосовуються з послідовним використанням двох або навіть трьох різних шифрів.

Сьогодні криптографія є невід'ємною частиною всіх інформаційних систем: від електронної пошти до стільникового зв'язку, від доступу до Інтернету до електронних грошей. Криптографія забезпечує підзвітність, прозорість, точність та конфіденційність. Це запобігає спробам шахрайства в електронній комерції та забезпечує юридичну силу фінансових операцій. Криптографія допомагає ідентифікувати вас, але також надає анонімність. Захищає бандитів від зловживання сервером та конкуренції шляхом проникнення у ваші конфіденційні документи. І в майбутньому, оскільки бізнес та комунікації все більше прив'язуються до комп'ютерних мереж, криптографія буде необхідною.

ВИКОРИСТАНІ ДЖЕРЕЛА

1. Панасенко С.П., Захист інформації в комп'ютерних мережах // Журнал «Світ ПК» 2002./ – № 2.

2. Введення в криптографію / За заг. ред. В.В. Ященко - М., МЦНМО, 2000 – 272 с.

3. Шнайдер Б. Прикладна криптографія. М. – Світ. – 2004.