УДК 303.7
Кузнєцов Т.В.[1], Зайко Т. А.[2]
[1]студ. гр. КНТ-117 НУ «Запорізька Політехніка»
[2] канд. техн. наук, доц. НУ «Запорізька Політехніка»

РОЗРОБКА І РЕАЛІЗАЦІЯ ВБУДОВАНОГО ЗАХИСТУ ПРОГРАМ

Комерційні програми зазвичай захищають від несанкціонованого тиражування. Наявність доступу тільки до носія інформації з дистрибутивом (набором інсталяційних файлів) програмного продукту не повинна давати можливості встановити працездатну копію програми. Тобто даних дистрибутива, який можна скопіювати або непомітно взяти на декілька днів, не повинно вистачати для створення працездатної копії програми. Подібні обмеження можуть бути реалізовані різними способами. Наприклад, дуже багато комерційних програм при інсталяції вимагають ввести серійний номер, надрукований на коробці або вказаний в одному з документів, що додаються до програмного продукту (у Microsoft – в сертифікаті автентичності) [1].

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: моральноетичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначимо, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту [2].

Криптографічний захист (шифрування) інформації – це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. На відміну від тайнопису, який приховує сам факт передавання повідомлення, зашифровані повідомлення передаються відкрито, приховується їхній зміст.

Методи криптографії поділяють на дві групи – підставлення (заміни) і переставлення. Підстановчий метод передбачає, що кожна літера та цифра повідомлення замінюється за певним правилом на інший символ. Зокрема, для визначення порядку підставлення може використовуватись певне слово або фраза – ключ. У загальному випадку, у криптографії ключ – це послідовність бітів, що використовуються для шифрування та розшифрування даних .

Розглядаючи програмні засоби захисту, доцільно спинитись на стеганографічних методах. Слово «стеганографія» означає приховане письмо, яке не дає можливості сторонній особі взнати про його існування. Одна з перших згадок про застосування тайнопису датується V століттям до н. е.

Сучасним прикладом є випадок роздрукування на ЕОМ контрактів з малопомітними викривленнями обрисів окремих символів тексту – так вносилась шифрована інформація про умови складання контракту.

Комп'ютерна стеганографія базується на двох принципах. По-перше, аудіо- і відеофайли, а також файли з оцифрованими зображеннями можна деякою мірою змінити без втрати функціональності. По-друге, можливості людини розрізняти дрібні зміни кольору або звуку обмежені. Найчастіше стеганографія використовується для створення цифрових водяних знаків. На відміну від звичайних їх можна нанести і відшукати тільки за допомогою спеціального програмного забезпечення – цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки можуть забезпечити автентичність або недоторканість документа, ідентифікувати автора або власника, перевірити права дистриб'ютора або користувача, навіть якщо файл був оброблений або спотворений.

Криптографічні алгоритми використовуються як для шифрування повідомлень, так і для створення електронних (цифрових) підписів (ЦП) – сукупностей даних, які дають змогу підтвердити цілісність електронного документа та ідентифікувати особу, що його підписала. Звичайно терміни «електронний підпис» і «цифровий підпис» застосовуються як синоніми, але перший з них має ширше значення, оскільки позначає будь-який підпис в електронній формі («оцифрований» не означає «цифровий»). Отже, електронні підписи не обов'язково базуються на криптографічних методах і можуть бути створені, наприклад, за допомогою засобів біометрії[3].

Таким чином, можна зробити висновок, що використання принципів вбудованого захисту інформації для захисту програм від хакерів у сфері розробки ПЗ є одним з найефективнішим та активно запровадженим рішеням.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Шевчук Р.П. Опорний конспект лекцій з дисципліни „Методи та засоби захисту програмного забезпечення”, для студентів напрямку „Комп’ютерні науки” / Р.П. Шевчук. – Тернопіль, 2007. – 50 с.

2. Мандиа К. Защита от вторжений. Расследование компьютерных пре ступлений / К. Мандиа, К. Просис.– М., 2005. – 496 с.

3. Луцкер А. Авторское право в цифровых технологиях и СМИ / А. Луцкер. – М., 2005. – 416 с.