УДК 681.39

ЗАХИСТ ПРОГРАМ НА ОСНОВІ УЩІЛЬНЕННЯ ДАНИХ

Алєксєєва Т.М.
Науковий керівник – ст. викл. Каплун В.А.

Сучасні інформаційні технології потребують організації високого рівня захисту комп'ютерної інформації і програм зокрема.

Автори тез пропонують методи захисту програм від несанкціонованого використання за допомогою прив'язки до деяких заздалегідь визначених характеристик комп'ютера та подальшого ущільнення вхідного файлу з програмою, представленого у вигляді послідовності додатних чисел. Суть методу захисту полягає в тому, що виконуваний модуль програми, яка підлягає захисту, розглядається як послідовність байтів і становить вхідне повідомлення F_{obj}. Ця послідовність доповнюється ключем F_{key}. Ключем може бути як генероване певним чином випадкове число, так і деяка ключова фраза (наприклад, пароль) або послідовність символів, отриманих як параметри складових комп'ютерної системи (серійні номера пристроїв, дати та версії виготовлення моделей, швидкісні характеристики, параметри файлової системи та ін.), а також результати проміжних обчислень методів ущільнення даних.

У результуючій послідовності початковим елементом буде ключова інформація, яка є необхідною для однозначного відновлення виконуваного модуля програми. Отримане повідомлення представляється у вигляді послідовності додатних цілих чисел певної розрядності, незалежно від їх фактичного вмісту. Потім здійснюється ущільнення шляхом обчислення відхилень від сусідніх чисел послідовності. Після такої модифікації дану програму неможливо запустити на виконання. Для відновлення функціональних властивостей захищеної програми необхідно використати ключову інформацію і здійснити процес, зворотний обчисленню відхилень.

При зберіганні результуючої послідовності ключ відокремлюється від неї та може зберігатися на зовнішньому носії, бути прихованим у будь-якому файлі, генеруватись наново або знову отримуватись з параметрів комп'ютерної системи (в залежності від того, як він був початково створений). Отже, легальна версія програми може коректно відновитись і правильно функціонувати лише при наявності ключа.

Запропонований метод захисту може бути посилений додатковими криптографічними методами, використанням антидампінгових засобів. Також передбачається можливість самознищення програми після зняття захисту.