УДК 004.353
Максимець О. – ст. гр. СНм-52
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ МЕТОДІВ СТЕГАНОГРАФІЇ У ФАЙЛАХ ФОРМАТУ PORTABLE EXECUTABLE

Науковий керівник: к.т.н., доц. Козак Р. О.

Maksymets O.
Ternopil Ivan Pul'uj National Technical University

ANALYSIS OF STEGANOGRAPHIC TECHNIQUES IN PORTABLE EXECUTABLE FILES

Supervisor: Assoc. Prof. PhD Kozak R. O.

Ключові слова: захист інформації, стеганографія, виконуваний файл.
Keywords: information security, steganography, executable file.

На сьогоднішній день використання неліцензійного програмного забезпечення завдає значних економічних збитків компаніям, що його виробляють. Для запобігання такого використання існують різні програмні і апаратні засоби і методи захисту. Необхідно подбати про те, щоб механізм захисту не міг виявити власник копії. Для цього зазвичай вдаються до методів стеганографії.

Очевидно, що зараз найпопулярнішою операційною системою (для робочих станцій) є Microsoft Windows, тому в рамках дослідження будуть розглядатися методи приховування інформації у файлах формату Portable Executable.

Серед існуючих методів впровадження стеганографії у виконувані файли виділено такі:

1. Метод базується на тому, що можна переставляти місцями дві суміжні операції присвоювання, результат роботи яких не залежить від послідовності виконання. Така перестановка змінює порядок обчислень, але не спотворює результат. Якщо операції йдуть в лексикографічному порядку, то захований біт дорівнює 1, інакше 0. Головним завданням буде пошук таких операцій, які можна поміняти місцями.

2. Метод базується на можливості перестановки процедур всередині програми. Якщо в програмі переставити процедуру з одного місця на інше і виправити всі внутрішні і зовнішні посилання, які повинні помінятися внаслідок переміщення, то працездатність програми не буде порушено і з'явиться можливість закодувати приховані біти інформації.

3. Метод базується на можливості перестановки адрес в таблицях імпорту, що викликають функції Windows API. Адреси імпортованих функцій API операційної системи лежать всередині масиву. Заповнення цього масиву відбувається операційною системою на стадії запуску програми. Програма завантажує кілька бібліотек, в кожній бібліотеці знаходиться безліч імпортованих функцій. Потрібно згрупувати адреси функцій по бібліотеках. Відповідно, перестановки можливі тільки всередині цих груп.

Ці методи можна одночасно застосовувати до файлу для приховування інформації.