# *РОЛЬ СТЕГАНОГРАФІЇ У СУЧАСНОМУ ЗАХИСТІ ІНФОРМАЦІЇ*

***Мальцева Наталія, Полотай Орест***

кафедра безпеки інформаційних технологій Національного університету «Львівська політехніка»,

кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

*У роботі наведено практичне використання стеганографії, роль даного напряму в захисті інформації, приведено результати виконаного дослідження із приховування файлів у стегоконтейнері.*

***Ключові слова**: стеганографія, секретний ключ, стегоконтейнер, приховування інформації.*

*This work presents the practical use of steganography, the purpose and objectives of this area in the information security and also contains results of the research based on hiding files in the stegocontainer.*

***Key words:** steganography, secret key, stegocontainer, information hiding.*

В першу чергу, визначимо поняття стеганографії. Стеганографія — наука, предметом якої є приховування факту присутності секретної інформації. Саме в цьому і полягає відмінність даної науки від не менш поширеного напрямку захисту інформації — криптографії, при використанні якого читання вмісту повідомлення стає неможливим.

Сучасну стеганографію прийнято розділяти на класичну, комп'ютерну і цифрову [1, ст. 65], також виділяють мережеву. Класична пов`язана із приховуванням текстових даних, використовуючи властивості самого тексту або ж навколишнього середовища. З іншого боку — комп'ютерна і цифрова стеганографія, які розглядають методи приховування будь-якої електронної інформації (текст, звуковий файл, зображення, відео, програма) з використанням можливостей інформаційних систем. Мережева стеганографія використовує можливості протоколу передачі даних транспортного рівню – TCP.

В нашій роботі зосередимось на можливостях цифрової стеганографії, спираючись на розповсюдженність цифрового середовища і розвиток кібернетичного простору [2, ст. 97]. Підґрунтям розвитку стеганографії в останньому десятиріччі можна вважати величезні об'єми графічної інформації, що поширюються у мережі. Тим часом, кожен цифровий об'єкт потенційно може містити приховані дані.

Отже, розглянемо напрями цифрової стеганографії [3]:

- вбудовування інформації з метою її прихованої передачі або ж прихованого зберігання;
- вбудовування цифрових водяних знаків для захисту авторських прав;
- вбудовування ідентифікаційних номерів з метою відстежування наступних дії з даними або контентом і також підтвердження достовірності переданої інформації.

Серед актуальних та практичних застосувань стеганографії слід виділити: можливість вкладення більш таємного файлу у менш таємний, який у свою чергу вкладений у файл-контейнер; шифрування прихованого файлу за допомогою одного з криптографічних алгоритмів (наприклад, потрійний DES, MDC або IDEA); можливість приховування аудіофайлу в іншому звуковому файлі. Тож, стеганографія реалізує захист даних у два кроки: приховує факт наявності даних, а при їх виявленні вимагає проведення автентифікації – введення секретного ключа.

Для досліження ми обрали стеганографічний програмний засіб S-Tools. В ході роботи було виконано приховування у файлі-контейнері різнотипних файлів: аудіофайлу (із

розширенням .wav), виконуваної програми (.exe), зображення (.bmp), текстового файлу (.txt). Після того ми переглянули оригінальне зображення та модифіковане у двійковому вигляді і визначили, що приховані файли рівномірно розподіляються по бітах файлу-контейнеру з метою приховування самого факту існування таємної інформації.

Під час виконання цього завдання було встановлено, що у файлі зображення (1920×1080 пікселів) обсягом 6 220 854 байт можна приховати 777 584 байт інформації, що становить більше 10% об'єму початкового файлу. Співвідношення між розміром файлу із зображенням і розміром файлу, який можна приховати, залежить від конкретного випадку, однак при правильному виборі файлу-контейнера, факт використання стеганографічних засобів (не знаючи секретний ключ) встановити і довести практично неможливо. Якщо ж скористатись компресією зображення і приховувати не сам файл, а його архів, то у зображенні меншого розміру можна приховати зображення більшого розміру.

Ми зробили висновок, що для більшої надійності приховування слід використовувати зображення з великою кількістю півтонів та відтінків і не рекомендується – зображення з великими зонами одного кольору.

У випадку аудіофайлу наведемо елементарні розрахунки: нехай перетворення аналогового сигналу у цифровий відбувається із частотою дискретизації 44,1 кГц. Це дозволяє кожну секунду зберігати 44100 біт інформації для монофонічного сигналу та 88200 біт – відповідно для стереофонічного. Отже, у звуці, який триває всього 1 секунду, можна вмістити текст обсягом більш ніж 10 Кбайт. При цьому, в результаті приховування отримується аудіофайл без помітних для слуху втручань, що містить інший закодований прихований файл

Ми переконались, що при застосуванні стеганографії програми використовують певні алгоритми, які приховують секретні дані серед вмісту контейнера: біти початкового файлу у випадкових позиціях замінюються на біти приховуваного файлу. Таким чином, розмір початкового файлу і файлу-контейнеру (що містить вкладену інформацію) є однаковим, навіть за умови приховуванні різної кількості файлів або різного обсягу даних.

Таким чином, для людини не є можливим визначити, чи були використані засоби стеганографії під час створення певного файлу. Для цього необхідне застосування спеціалізованого програмного забезпечення, проте з причини низької швидкодії воно не може бути використане в промислових об'ємах, а антивірусні програми не виявляють файли-контейнери.

## Література


1. Мельник С. МЕТОДИ ЦИФРОВОЇ СТЕГАНОГРАФІЇ: СТАН ТА НАПРЯМИ РОЗВИТКУ // С. Мельник, В. Кащук. // Information Security of the Person, Society and State. – 2013. – №3. – С. 65–70;

2. Шелест М. КОМП'ЮТЕРНА СТЕГАНОГРАФІЯ ТА ЇЇ МОЖЛИВОСТІ // М. Шелест, В. Андреев. // Сучасна спеціальна техніка. – 2011. – №24. – С. 97–104;

3. Конахович Г., Прогонов Д., Пузиренко О. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних [підручник]. — К. : «Центр навчальної літератури», 2018. — 558 с.