УДК 004.932

ЗАХИСТ ТА ПЕРЕДАЧА ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ СТЕГАНОГРАФІЧНИХ МЕТОДІВ

***В.С. ЯГ'Я*[1*], *Л.Б. КАЩЕЄВ*[2]**

[1] *магістрант кафедри САІТ, НТУ «ХПІ», Харків, УКРАЇНА*
[2] *доцент кафедри САІТ, доцент, канд. техн. наук, НТУ «ХПІ», Харків, УКРАЇНА*
[*] *email: holeriaya@gmail.com*

Завдання надійного захисту інформації від несанкціонованого доступу – актуальне питання, що вирішувалося в усі часи історії людства та не є вирішеним до наших днів.

У зв'язку з розвитком і поширенням технологій, які дозволяють обробляти та відтворювати різні типи сигналів (так звані мультимедійні технології) за допомогою комп'ютера, питання захисту інформації, представленої в цифровому вигляді, є надзвичайно актуальним.

Переваги подання та передачі даних у такому вигляді можуть бути перекреслені з легкістю, з якою можливі їх викрадення та модифікація. Тому постало питання розробки засобів захисту інформації організаційного, методологічного й технічного характеру, серед них – методи криптографії та стеганографії [1].

Відомо, що для гарантованого захисту вмісту повідомлення існує два різних підходи. Перший – блокування несанкціонованого доступу до інформації шляхом шифрування повідомлення. Для цієї мети використовуються криптографічні методи захисту. У криптограмах, як правило, відсутні структура і закономірності, які властиві відкритим текстам. Тому, при проведенні моніторингу мереж телекомунікації, вони легко автоматично виділяються з інформаційного потоку.

Другий підхід полягає в тому, що повідомлення яке передається приховують таким чином, щоб його неможливо було помітити. Для приховування факту існування інформації застосовуються стеганографічні методи захисту, які значно знижують ймовірність її виявлення.

На відміну від криптографічного захисту, коли в «зловмисника» існує можливість знайти, перехопити та зробити спробу дешифрувати криптограму, стеганографічні методи дозволяють вмонтувати інформацію в невинні на вигляд послання так, щоб не можна було навіть запідозрити існування підтексту [2].

Звичайно, навряд чи стеганографія призначена для того, щоб замінити шифрування даних, швидше вона створює додатковий рівень безпеки. Реалізації саме стеганографічного підходу в передачі прихованої інформації присвячена дана робота.

У відповідності до поставленої мети в роботі досліджені питання: розгляд основних принципів стеганографії для доведення доцільності їх використання;

аналіз методів цифрової стеганографії і вибір контейнера для приховування даних; вибір програмних засобів для вирішення поставлених завдань; розробка та тестування програмних модулів для виконання приховування даних.

У якості «контейнера» зручно використовувати цифрове зображення. Елементам візуального середовища (цифровим зображенням і відео) властива значна надлишковість різної природи:

- кодова надлишковість;
- міжпіксельна надлишковість;
- психовізуальна залежність, зумовлена сприйманням органом зору людини зображення не в точності «піксель за пікселем», а з різною чутливістю.

Для програмної реалізації скористаємося методом заміни молодших біт (LSB-метод), який ґрунтується на тому, що молодші розряди графічних, аудіо- і відеоформатів несуть мало інформації і їх зміна фактично не позначається на якості переданого зображення. Це дає можливість замінювати надлишкову частину зображення бітами секретного повідомлення.

Вилучення же прихованого повідомлення відбувається за зворотним алгоритмом. Основною перевагою цього методу є простота реалізації та можливість таємної передачі великого обсягу інформації. Головним недоліком методу можна назвати нестійкість до більшості відомих перетворень зображень, наприклад, стискання із втратами, масштабування, повертання на певний кут тощо.

Аналізуючи отримані результати, можна зробити висновок, що найбільш перспективними за інформаційною ємністю є контейнери у вигляді файлів зображень у форматі .bmp. Завдяки використаному методу заміни молодших біт, що не змінює візуальну якість зображення, майже неможливо виявити факту впливу на зображення. А розробка додатку в середовищі програмування Microsoft Visual Studio за допомогою мови програмування C#, є оптимальною для створення інтуїтивно зрозумілого та «дружнього» до користувача інтерфейсу.

Список літератури:

1. Вікіпедія – Вільна енциклопедія. [Електронний ресурс]: Стеганографія. – Режим доступу: http://ru.wikipedia.org/wiki

2. *Горпенюк, А. Я.* Дослідження та порівняльний аналіз стеганографічних методів для впровадження даних у цифрові файли / *Горпенюк, А. Я., Стороженко, А.О. //* [Електронний ресурс]: – Режим доступу: http://lib.lp.edu.ua/bitstream/ntb/21464/1/32-176-179.pdf

3. Бюро науково-технічної інформації [Електронний ресурс]: Комп'ютерна стеганографія вчора, сьогодні, завтра. – Режим доступу: http://www.bnti.ru/showart.asp?aid=330&lvl=03.07.06