

СТЕГАНОГРАФІЧНИЙ ЗАХИСТ ДАНИХ З ВИКОРИСТАННЯМ ФАЙЛІВ ЗОБРАЖЕНЬ

Вінницький національний технічний університет

Анотація

Розглянуто особливості стеганографічного захисту даних. Розроблено програмний засіб «BiKod» для операційної системи Windows.

Ключові слова: захист даних, стеганографічний метод, приховування даних.

Abstract

Features of steganographic data protection are considered. Developed the software tool "BiKod" for the Windows operating system.

Keywords: data protection, shorthand method, data hiding.

Вступ

Захист інформації в наш час є однією з важливих сфер життєдіяльності, як певної організації, так і країни в цілому. Збереження таємності певних інформаційних повідомлень чи безпечного зберігання технологій є одним з ключових завдань. Проте дане завдання часто є непростим, тому що інформацію потрібно не тільки шифрувати, а й приховати сам факт шифрування для більшої надійності.

Термін "безпека" розуміють як стан захищеності життєво важливих інтересів особи, суспільства, держави від внутрішніх та зовнішніх загроз. Але його зміст у науковому розумінні ще повною мірою не визначений. Сьогодні точиться дискусія навколо цього питання, зокрема навколо оцінки критеріїв безпеки, характеристик вірогідних небезпек та їх структури або принципів побудови системи забезпечення національної безпеки [1].

Водночас спеціалісти відчують певний дефіцит у спеціальній літературі з питань правового висвітлення сучасних проблем інформаційного права. Незважаючи на вихід у світ окремих вдалих видань і наукових статей, висвітлені ці проблеми лише загальною. Крім того, у сучасній науковій і навчальній літературі нерідко і не завжди правильно відображені проблеми правового забезпечення інформаційних процесів або недостатньо фактичного матеріалу.

Цифрова стеганографія — напрям класичної стеганографії, заснований на приховуванні або впровадженні додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі спотворення цих об'єктів. Але, як правило, дані об'єкти є мультимедіа-об'єктами (зображення, відео, аудіо, текстури 3D-об'єктів) та внесення спотворень, які знаходяться нижче межі чутливості середньостатистичної людини, не призводить до помітних змін цих об'єктів [2].

Крім того, в оцифрованих об'єктах, тобто таких, що спочатку мають аналогову природу, завжди присутній шум квантування; також, при відтворенні цих об'єктів з'являється додатковий аналоговий шум і нелінійні спотворення апаратури, все це сприяє більшій непомітності прихованої інформації.

Метою роботи є створення алгоритму та програмного забезпечення приховування даних у файлах зображень для використання, навіть прости користувачем, без наявної підготовки та набутих знань в аспекті шифрування даних. Дані умови розширюють кількість можливих користувачів в разі.

Об'єктом дослідження є стеганографічні методи захисту даних.

Предметом дослідження є програмне забезпечення для захисту даних від несанкціонованого доступу стеганографічним методом [3].

Головною задачею є розробка програмного забезпечення для захисту файлів стеганографічним методом.

Розробка програмного засобу «BiKod»

Програмний продукт «BiKod» призначений для приховування даних у файлах зображень в форматі .bmp, .gif, .png та інших форматах, які не передбачають використання алгоритмів ущільнення зображень з втратами. В процесі приховування даних у файлах зображень виконується також їх шифрування. Криптографічний алгоритм передбачає розсіювання даних по довжині файлового контейнера та їх гамування. Функціонал програми має потрібний набір функцій для виконання

процесу приховування або вилучення даних з файлу-контейнера. Програмний продукт не потребує додаткових засобів чи втручання в процес приховування, всі процеси виконуються в фоновому стані та не заважають діяльності інших програм.

Сьогодні існує декілька аналогів зі схожим функціоналом, які мають принципові відмінності. Розглянемо деякі з них.

Головним конкурентом є «АхСрут», який додає захист паролем до файлів. Створений для Windows, «АхСрут» простий у використанні. Шифрування виконується за допомогою 128-бітного шифрування AES. Зашифровані файли матимуть розширення .АХХ. Після інтеграції з Windows, все, що вам потрібно зробити, щоб зашифрувати файл або папку, це клацнути правою кнопкою миші та вибрати «Шифрувати». Підтримується кілька мов і доступний для завантаження безкоштовно. [4]. Головними недоліками є те, що даний програмний продукт виконує лише шифрування даних і не містить засобів приховування даних.

Програмний засіб «Folder Lock» є ще одним аналогом розробки [5]. Додаток має досить обмежений функціонал і потребує лише пароль для відкриття файлу. Тобто робить лише видимість, що забезпечує захист, а насправді лише обмежує доступ до файлу.

Головним недоліком додатку «Elite Keylogger» є досить складна реєстрація та авторизація, що займає багато часу, для нормального функціонування вам потрібно підтвердження по номеру телефона та доступ до Інтернет-мережі [6].

Таким чином, проаналізувавши недоліки конкурентів та потреби споживачів, було створено власний алгоритм шифрування та приховування даних, що становить основу програми - «ViKod». Програма має нескладний та інтуїтивно-зрозумілий інтерфейс. Модель роботи додатку «ViKod» наведено на рисунку 1.

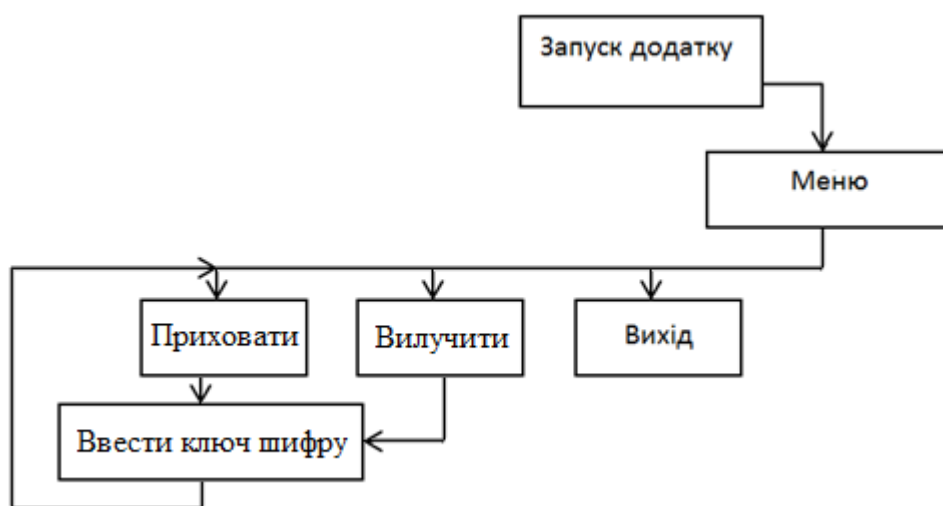


Рисунок 1 – Модель роботи програми «ViKod»

Функціонал програмного засобу «ViKod» має доволі прості функції з погляду користувача: панель вибору можливості приховування, вилучення файлу з контейнера та вихід з програми.

Висновок

Програмний продукт «ViKod» призначений для приховування даних у файлах зображень в форматі .bmp, .gif, .png та інших форматах, які не передбачають використання алгоритмів ущільнення зображень з втратами. В процесі приховування даних у файлах зображень виконується також їх шифрування. Криптографічний алгоритм передбачає розсіювання даних по довжині файлу-контейнера та їх гамування. Програму розроблено під операційну систему Windows. Функціонал програми «ViKod» включає:

- приховування файлу в контейнері;
- вилучення файлу з контейнера.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Gribunin V. G. DIGITAL STEGANOGRAPHY / Cruz Zapata Belen., 2016. – 43 с. – Packt Publishing.
2. Sierra K. Shorthand/ Veksman R.A., Kazhdan J.K., Porto T.S., 2009. – O'Reilly, – 254 с.
3. Complete Guide to the C # 8.0 Programming Language and .NET Core 3 Platform [Електронний ресурс] // Complete Guide to the C #. – 2018. – Режим доступу до ресурсу: <https://metanit.com/sharp/tutorial>.
4. AxCrypt [Електронний ресурс] // Stack Exchange Inc. – 2018. – Режим доступу до ресурсу: <https://axcrypt.ru.downloadastro.com/>
5. Folder Lock [Електронний ресурс] – Режим доступу до ресурсу: https://folder_lock.ru.downloadastro.com/
6. Elite Keylogger [Електронний ресурс] – Режим доступу до ресурсу: https://elite_keylogger.ru.downloadastro.com/

Білоконь Владислав Васильович, студент групи ІПІ-20м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Україна, olgerddragon@gmail.com.
Науковий керівник: **Майданюк Володимир Павлович**, кандидат технічних наук, доцент кафедри програмного забезпечення, Вінницький національний технічний університет, Вінниця, e-mail: maidaniuk2000@gmail.com

Bilokon Vladislav, student of group IPI-16b, Faculty for Information Technologies and Computer Engineering, Vinnytsia National Technical University, Ukraine, , olgerddragon@gmail.com.
Supervisor: **Maidanyuk Volodymyr Pavlovych**, Candidate of Technical Sciences, Associate Professor of Software, Vinnytsia National Technical University, Vinnytsia, e-mail: maidaniuk2000@gmail.com