Секція 1

ДОСЛІДЖЕННЯ ІСНУЮЧИХ МЕТОДІВ СТЕГОАНАЛІЗУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Дука І. О
Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ»
Науковий керівник Пєвнєв В.Я.

Актуальність. Завдання захисту цінної інформації від несанкціонованого доступу вирішувалося в усі часи історії людства. Серед методів захисту виділяється стеганографічний, через можливість зберігати та передавати інформацію у всіх перед очима, тобто стеганографія приховує сам факт передачі. За допомогою стеганографії можливо одночасно забезпечити конфіденційність і цілісність інформації [1]. Використання комп'ютерів дозволило зробити якісний стрибок у розвитку стеганографії. Її використання передбачає наявність контейнера - файлу, в якому розміщується інформація, що передається. В даний час це можуть бути текстові, графічні, аудіо- та відеофайли.

Методи стеганографії можуть бути як корисними так і небезпечними. Це залежить від того, хто користується та для чого. Коли мова йде про таємну комунікацію між хакерами, терористами, продавцями наркотичних речовин, вірусна програма для передачі конфіденційною інформації – ці приклади демонструють небезпечні дії, але важливо відмітити й корисні, наприклад цифрові водяні знаки на зображеннях та у фреймах фільму чи відео, - допомагають боротися із піратством та крадіжкою інтелектуальної власності[2]. Але частково стеганографію використовують із недобрим наміром. Одночасно з розвитком стеганографії розвивається й стегоаналіз.

Метою роботи є дослідження існуючих стеганографічних методів та методи стегоаналізу цифрових контейнерів.

Основні положення. В доповіді освітлюються особливості методів стеганографії та стегоаналізу. З аналізу наявних методів стегоаналізу випливає, що їх можна умовно поділити на дві основні групи. Перша група призначена для роботи з відомими стеганографічними алгоритмами; друга - для всіх інших алгоритмів стеганографії [3]. Методи обох груп побудовані з урахуванням припущення про недоступність початкового порожнього контейнера, який було використано для розміщення інформації в досліджуваний

стегоконтейнер.

У доповіді наведено аналіз існуючих методів стегоаналізу. Метод візуального аналізу є найпростішим способом аналізу графічних файлів, оскільки для цього досить просто поглянути на перехоплене зображення. Статистичні методи базуються на понятті «природного» контейнера. Суть методів полягає в оцінюванні ймовірності існування стеганографічного вкладення зі стегосистеми, яка є невідомою, на основі критерію оцінювання близькості досліджуваного контейнера до «природного». До переваг цієї групи методів належить необмежена сфера застосування, що є досить істотним як під час перевірки гіпотези про наявність стеганографічного вкладення з невідомої стегосистеми, так і під час розроблення схемних методів стегоаналізу. Основним недоліком методів цього класу є саме припущення про існування "природного" контейнера.

Висновок. Основним висновком по поданій роботі можна вважати те, що незважаючи на актуальність розробки систем стегоаналізу, в інтернеті мало інформації про можливі алгоритми їх застосування з теоретичної точки зору та практичної реалізації.

Список літератури

1. Пєвнєв В. Я. Моделі загроз і забезпечення цілісності інформації. *Системи та технології*. 2018. №2 (56/1). С. 79–94.

2. Цифровая стеганография как продвинутая техника уклонения от обнаружения вредоносных программ. URL: https://ichi.pro/ru/cifrovaa-steganografia-kak-prodvinutaa-tehnika-uklonenia-ot-obnaruzenia-vredonosnyh-programm-218817175139967

3. Кустов В. Н., Параскевопуло А. Ю. Простые тайны стегоанализа *Защита информации*. INSIDE. 2005. № 4. С. 72-78.

Відомості про авторів

Дука Ігор Олександрович, магістрант кафедри комп’ютерних систем, мереж і кібербезпеки, м.т. 066-420-15-30, i.o.duka@student.csn.khai.edu

Пєвнєв Володимир Яковлевич, доцент кафедри комп'ютерних систем, мереж і кібербезпеки, д.т.н., доцент, v.pevnev@csn.khai.edu