УДК 004.415.24

Ігор Олександрович Дука,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Володимир Якович Пєвнєв,
кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Способи виявлення таємних комунікацій кіберзлочинців

Міжнародними експертами з кібербезпеки Cybersecurity Ventures підраховано, що в 2019 році в світі кібератаки відбуваються кожні 14 секунд [1]. До 2020 року у світі також продовжиться зростання кількості випадків шахрайства з використанням технологій соціальної інженерії – за підсумками 2018 року фахівцями BNP paribas вже відзначено зростання цього виду злочинів на 6%.

Зі збільшенням числа кібератак зростає і заподіяний ними збиток. Якщо в 2018 році збитки компаній різних секторів економіки склали 1,5 трлн доларів, то в 2019 році, за прогнозом BNP paribas, вони досягнуть вже 2,5 трлн. До 2022 року, за прогнозом Всесвітнього економічного форуму, сума планетарного збитку від кібератак може зрости до 8 трлн доларів [1].

Для того, щоб дії хакерів були скоординованими і точними необхідно добре налагоджений і безпечний канал зв'язку. Спілкування між хакерами проходить на форумах із обмеженим або закритим доступом, доступ до них має невелика кількість людей, усі повинні мати високу позитивну репутацію, що підтверджує надійність хакера [2]. Якщо необхідно залишити повідомлення у відкритому доступі, для цього правопорушники публікують відео, аудіо, фотографії в соціальних мережах, відкритих віртуальних дисках, в цих матеріалах приховується таємне повідомлення. Для приховування інформації в графічних зображеннях

використовуються алгоритми: LSB, метод приховування інформації: в коефіцієнтах дискретного косинусного перетворення, молодших біт палітри, в службових полях формату, в коефіцієнтах спектральних перетворень файлу, широкосмуговий.

В продовж 2017 року, за приблизним підрахунком InfoTrends було зроблено 1,2 трильйона фотографій [3] на смартфонах, фотоапаратах, тощо. Реальна кількість цих фотографій значно більша, такий об'єм інформації спец. службам неможливо перевірити, тому стеження проводиться тільки за суб'єктами, котрі привертають увагу.

Проаналізуємо методи виявлення факту наявності прихованого повідомлення в графічних зображеннях [4]:

- візуальні методи – базуються на здатності людини візуально аналізувати і виявляти істотні відмінності в порівнювальних зображеннях;

- метод візуального аналізу бітових зрізів. Основна ідея методу полягає в порівнянні зображення в цілому з зображеннями його бітових зрізів;

- статистичні методи – базуються на понятті «природного» контейнера. Суть методів полягає в оцінюванні ймовірності існування стеганографічного вкладення з невідомої стеганографічні системи на основі критерію оцінки близькості досліджуваного контейнера до «природного»;

- метод оцінки числа переходів значень молодших біт в сусідніх елементах зображення. У методі використовується знання, що між молодшими бітами сусідніх елементів і між ними та іншими бітами природних контейнерів є кореляційні зв'язки;

- метод оцінки частот появи k-бітових серій в потоці незалежних бітових елементів контейнера. Метод дозволяє оцінити рівномірність розподілу елементів у досліджуваній послідовності на основі аналізу частоти появи нулів і одиниць, і серій, що складаються з k біт;

- метод аналізу гістограм, побудованих за частотами елементів зображення. Метод дозволяє оцінити рівномірність розподілу елементів зображення, а також визначити частоту появи конкретного елемента;

- метод перевірки розподілу елементів на монотонність. Метод дозволяє оцінити рівномірність розподілу елементів зображення за результатами аналізу довжин ділянок не зростання і не спадання елементів послідовності;

Боротьба із стегоконтейнерами – є актуальною проблемою для спец. служб з точки зору складності, бо перевірити графічні зображення дуже важко, задача доказу того, що файл є контейнером секретного повідомлення – не так просто. Складність в тому, що для добре відомих алгоритмів і його варіацій існують методи атак, на відміну до рідких або зовсім невідомих, що використовують не очевидні конструкції, або принципи. Одного методу доказу наявності стегоконтейнера недостатньо для комплексної перевірки, бо для кожного типу файлів необхідна модифікація – пов'язано із алгоритмом формування зображення.

У представленій доповіді розглядаються можливі варіанти пошуку і відстеження прихованої інформації в графічних зображеннях із використанням приведених методів.

Список бібліографічних посилань

1. Потери организаций от киберпреступности // TADVISER : сайт. 29.08.2019. URL: http://www.tadviser.ru/index.php/Статья:Потери_организаций_от_киберпреступности (дата звернення: 25.10.2019).
2. Эксперты рассказали, как хакеры взаимодействуют друг с другом // Федеральное агентство новостей : сайт. 29.04.2019. URL: https://riafan.ru/1174326-eksperty-rasskazali-kak-khakery-vzaimodeistvuyut-drug-s-drugom (дата звернення: 25.10.2019).
3. Here's How Many Digital Photos Will Be Taken in 2017. URL: https://focus.mylio.com/tech-today/heres-how-many-digital-photos-will-be-taken-in-2017-repost-oct (дата звернення 25.10.2019).
4. Швидченко И. В. Методы стеганоанализа для графических файлов. *Штучний інтелект.* 2010. № 4. С. 697–705. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/58671/81-Shvidchenko.pdf?sequence=1 (дата звернення: 25.10.2019).

Одержано 29.10.2019