НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА

ЗБІРНИК МАТЕРІАЛІВ

76-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

ТОМ 1

14 травня – 23 травня 2024 р.

УДК 004.49

Т.М. Фесенко, к.т.н., доцент
М.Ю. Дамян, студент
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

СТЕГАНОГРАФІЯ У ХАКЕРСТВІ

Стрімкий розвиток цифрових технологій та засобів електронних комунікацій постійно стимулює створення різноманітних методів захисту інформації. Відомо, що для гарантованого захисту вмісту повідомлення існує два різних по суті підходи.

Перший, це блокування несанкціонованого доступу до інформації шляхом шифрування повідомлення. Для цієї мети використовуються криптографічні методи захисту. Другий підхід полягає в тому, що повідомлення, яке передається, намагаються приховати так, щоб його неможливо було знайти. Для приховування факту існування інформації застосовуються стеганографічні методи захисту.

Стеганографія – це метод завдяки якому можна сховати інформацію всередині файлу або в повідомленні. При цьому, стеганографію часто порівнюють з криптографією. Проте головна відмінність між ними полягає в тому, що дані не приховуються під час передачі і не потребують ключа для розшифрування. Суть стеганографії полягає в тому, щоб відправник не знав, що було отримано прихований цифровий об’єкт, і що цей об’єкт знаходиться у звичайному файловому повідомленні.

Окремої уваги заслуговують методи комп’ютерної стеганографії. Зазначені методи є самостійним науковим напрямом інформаційної безпеки, що вивчають проблему створення прихованих інформаційних компонентів у відкритому інформаційному середовищі.

Варто зазначити, що нині, стеганографія є одним із найпопулярніших методів кібератак та шахрайства. Адже без додаткових перевірок важко визначити чи у файлі присутній вірус чи ні. Але, при цьому з впевненістю можливо стверджувати, що стеганографія може використовуватися не тільки у зловмисних цілях, а і для обходу цензури, нанесення цифрових водяних знаків та передачі особливо важливої інформації.

Беручи до уваги вищесказане та аналізуючи відкриті джерела, можна з впевненістю сказати що зловмисники зазвичай прикріплюють наступну інформацію:

- вихідний код хакерського програмного забезпечення;
- список скомпрометованих серверів;
- плани майбутніх атак;
- координації та канал зв’язку.

Аналізуючи види сучасної стеганографії необхідно зазначити, що вони поділяються на два види, а саме:

1. Технічну стеганографію, де здійснюється шифрування текстових повідомлень. Даний вид стеганографії застосовує наступні методи приховування повідомлень:

- *Невидиме посилання* – метод, що використовує невидиме чорнило для приховування текстових повідомлень;

- *Мікрокрапки* – метод, за допомогою якого можна приховати до однієї сторінки в одній точці;

- *Комп'ютерні методи* – використовують додаткову (зловмисну) інформацію в текстах, зображеннях, звуках, відео тощо.

2. Лінгвістичну стеганографію – метод приховування повідомлення в носії у якийсь винахідливий спосіб. Цю техніку також класифікують як семаграма або відкритий код.

Семаграми – техніка, що використовує символи та різні знаки для приховування даних або повідомлень. Вона поділяється на:

- *Візуальні семаграми* – реалізуються шляхом використання малюнків, веб-сайту або інших "нешкідливих" об'єктів для передачі повідомлення;

- *Текстові семаграми* – приховування текстового повідомлення шляхом перетворення зовнішнього вигляду самого носія текстового повідомлення (зміна розмірів і стилів шрифту, додавання додаткових пробілів у документі тощо).

Отже, аналіз стеганографічних і криптографічних технологій показує, що в найближчому майбутньому досить ймовірно їхнє поєднання та взаємна інтеграція. В подальшому зазначена обставина забезпечить новий істотний підйом рівня захисту інформації та кібербезпеки під час її збереження і передавання загальнодоступними каналами зв'язку.

Література

1. Живило Є.О., Шевченко Д.Г., Черноног О.О. Типологія систем кібербезпеки в інформаційно-телекомунікаційних системах військового (спеціального) призначення. Наукову фахове видання "Сучасні інформаційні технології у сфері безпеки та оборони", випуск 3 (42)/2021- С. 37-46. DOI: https://doi.org/10.33099/2311-7249/2021-42-3-37-44;

2. Global Cyber Insurance Market (2019-2025). URL: https://www.researchandmarkets.com/reports/4871728/global-cyber-insurancemarket-2019-2025.

3. Onyshchenko, S., Zhyvylo, Y., Cherviak, A., Bilko, S. (2023). Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. Eastern-European Journal of Enterprise Technologies, 5 (13 (125)), 65–76. doi: https://doi.org/10.15587/1729-4061.2023.288175.