# АНАЛІЗ ВІДЕОДАНИХ ЯК СТЕГАНОГРАФІЧНОГО КОНТЕЙНЕРА ДЛЯ ПРОВЕДЕННЯ АТАК

Літвін О.О., Наконечний М.В., В'юхін Д.О.
Харківський Національний університет радіоелектроніки, Харків, Україна

Стеганографія відеофайлів також як і стеганографія зображень стає одним із ключових інструментів у сучасних кібератаках, оскільки дозволяє зловмисникам ефективно приховувати шкідливий код або конфіденційну інформацію, мінімізуючи ймовірність виявлення [1].

**Метою доповіді** є аналіз можливості використання відео як стеганографічного контейнера для проведення різноманітних атак.

Використовуючи методи стеганографії, хакери можуть передавати віруси, трояни чи інші шкідливі програми без явних ознак у вигляді традиційних підозрілих файлів [2]. Це дозволяє їм обминати системи безпеки, такі як антивірусне програмне забезпечення, і здійснювати атаки, не привертаючи уваги. Враховуючи ці загрози, розробка високотехнологічних методів для виявлення прихованих шкідливих кодів у відеофайлах є надзвичайно важливою для боротьби з кіберзлочинністю та захисту інформаційних систем.

Було проведено дослідження методів аналізу стеганографії у відео даних. Основними є методи: статистичний аналіз, спектральний аналіз, методи машинного навчання, зворотний аналіз.

Виходячи з отриманих даних найбільш перспективним є гібридний метод, що поєднує машинне навчання та спектральний аналіз. Машинне навчання ефективно виявляє приховані закономірності, а спектральний аналіз дозволяє виявляти зміни в частотній ділянці, характерні для стеганографії. Таке поєднання підвищує точність та надійність виявлення прихованої інформації, особливо у стислих відеоформатах.

Розглянуті деякі методи захисту сучасних систем від атак з використанням відеофайлів.

Захист від атак через відеофайли потребує багаторівневого підходу, що включає: технологічні обмеження (sandbox, контроль MIME); інструменти для аналізу прихованих даних; безперервне оновлення ПЗ, аналітику й моніторинг поведінки файлів.

**Список літератури**

1. Гриньов, Р.С., Сєвєрінов, О.В. (2019). Аналіз небезпеки впровадження вірусного програмного забезпечення в зображення // Комп'ютерні та інформаційні системи і технології.

2. Гриньов, Р., & Сєвєрінов, О. (2019). Метод подолання засобів захисту з використанням вразливостей графічних файлів формату BMP. Радіотехніка, 3(198), 192–202.