

ДО ПИТАННЯ ПРИХОВУВАННЯ ДАНИХ У ВІДЕОІНФОРМАЦІЇ

к.е.н., доц. М.І. Главчев, студент О.Ю. Нечитайло, Національний технічний університет "ХПІ", м. Харків

Основною перевагою стеганографії у порівнянні з криптографією, є можливість приховування самого факту передачі повідомлення. Разом з прихованою інформацією використовується стегоключ для вбудовування даних у файл та їх подальшого читання. Базові принципи, яким повинні відповідати стеганографічні методи, наступні:

- збереження цілісності й аутентичності файлу;
- збереження стеганографічним перетворенням основних властивостей файлу, що відкрито передається, при внесенні у нього секретного повідомлення й інформації ключа;
- видобування секретної інформації повинно представляти собою складну задачу.

Основні методи стеганографічних перетворень можна класифікувати за наступними групами:

1. Методи використання спеціальних властивостей комп'ютерних форматів даних. До таких методів відносять: запис інформації у місцях магнітних дисків, що переважно не використовуються, генерацію текстів і акростиха, шифрування приховуємого повідомлення, при цьому з результату видаляють ідентифікуючий заголовок, залишаючи лише шифровані дані.

2. Методи використання надлишковості аудіо та візуальної інформації. Ці методи припускають, що молодші розряди цифрових відліків містять дуже мало корисної інформації. Заповнення тих розрядів додатковою інформацією практично не впливає на якість сприйняття, що й дає можливість приховування конфіденційної інформації. В якості контейнера можуть служити практично будь-які файли: аудіо, відео, картинки й т.п. Внесення змін до них не призводить до помітних спотворень початкового файлу.

Для передачі інформаційних повідомлень через глобальні мережі найкращими є методи, що відносяться до другої групи вищенаведеної класифікації. Методи з цієї групи позитивно характеризуються можливістю прихованої передачі великого обсягу інформації, проте існує можливість знищення повідомлення, що передається, та спотворення переданих даних.

Початковий етап досліджень направлений на з'ясування потенційних можливостей приховування інформації у форматі відеоряду та властивих цьому проблем.