ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ ЗАСОБІВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Павлюк Т. Р.
Кухарська Н. П., к. ф.-м. н., доцент
Львівський державний університет безпеки життєдіяльності

Інформація є одним з найбільш важливих і цінних продуктів, створюваних людиною. Саме тому сьогодні велике значення надається її захисту від несанкціонованого отримання і використання.

Здавна людству відомі два основних напрямки вирішення цих завдань: криптографія і стеганографія. На сучасному етапі сильним поштовхом до розвитку стеганографії послужило те, що в більшості країн на застосування криптографічних засобів накладаються певні обмеження: так, наприклад, вимагається передавати ключі від використовуваних систем шифрування державі. Також обов'язковими є реєстрація та ліцензування криптографічних систем незалежно від того чи є вони апаратними, чи програмними засобами. Стеганографія не підпадає під дію зазначених обмежень та, водночас, є ефективною.

Класичне завдання стеганографії полягає в організації каналу передачі секретного повідомлення у такий спосіб, щоб не тільки зміст повідомлення, але й сам факт його передавання був прихований від усіх, крім “законного” одержувача. Це завдання зазвичай вирішується шляхом вбудовування секретного повідомлення в деяке інше повідомлення (контейнер), зміст і факт передачі якого не має викликати жодних здогадок у неутаємничених осіб. Контейнером, наприклад, можуть бути файли, що містять цифрові фотографії, музику або відео. Перелічені типи файлів використовуються найчастіше. Тому що, з одного боку, вони надають досить багато можливостей, зокрема мають достатньо місця для розміщення прихованих повідомлень, а з іншого боку, їх пересилання каналами комп'ютерних мереж виглядає абсолютно звичною справою. Наприклад, навряд чи в когось викличе підозру серія світлин, що пересилається електронною поштою або така, що є викладеною на сайті в Інтернеті, оскільки, це виглядає доволі природньо: одна людина ділиться з іншою, скажімо, враженнями про свою туристичну мандрівку. При цьому важливо дотримуватися однієї умови: ніхто не повинен мати одночасний доступ до файлу, який містить приховане повідомлення, і до вихідного файлу-контейнеру. В іншому випадку, завдання виявлення прихованого повідомлення матиме тривіальний характер і зводитиметься до простого порівняння файлів.

Зауважимо, методи стеганографії застосовуються не тільки для прихованої передачі повідомлень, але і для захисту авторських немайнових та майнових прав на цифрові зображення, фотографії чи інші оцифровані твори мистецтва. Переваги, які дає представлення їх у цифровому вигляді, можуть виявитися настільки легко перекресленими, наскільки можливими є їх крадіжка чи модифікація. Тому сьогодні розробляються різні заходи захисту інформації: організаційного і технічного характеру. Один з найбільш ефективних технічних засобів захисту мультимедійної інформації полягає у впровадженні в інформаційний об'єкт невидимих міток – цифрових водяних знаків. Вони можуть містити багато корисної інформації: коли створений файл, хто володіє авторськими правами, як налагодити контакт з автором і т. п. Внесені дані можуть бути вагомими доказами для доведення факту нелегального копіювання. Цифрові водяні знаки часто відіграють вирішальне значення при вирішенні судами спорів, що стосуються авторства.

Перспективним напрямком досліджень у сфері захисту інформації, на нашу думку, є аналіз успішно здійснених атак та виявлених вразливостей в стеганосистемах з метою їх класифікації та з’ясування причин їх появи та існування. Метою наших досліджень є визначення подальших напрямків розвитку стеганографії та сфер її застосування. Для цього необхідно буде розв'язати цілий ряд завдань, а саме слід вивчити відомі стеганоалгоритми і виявити основні вразливості в їх реалізації. Дослідження і аналіз існуючих алгоритмів є однією з необхідних умов розробки безпечних систем. Спираючись на отримані результати, можна буде розробити нові більш стійкі стеганоалгоритми, які здійснюватимуть надійний захист даних.

ЛІТЕРАТУРА

1. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.
2. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 249 с.