УДК 004.891

В.М. ДЖУЛІЙ, Є.О. КОВРИГА
Хмельницький національний університет

АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ПРИХОВАНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ

В статті проведено аналіз існуючих програм впровадження інформації в звукові файли, виявлено їх переваги та недоліки. Розглянуті можливі області застосування стеганографії. Виявлені недоліки методів впровадження інформації в звукові файли.

Розглянуті методи впровадження інформації в файли формату MIDI не можуть застосовуватися для захисту авторських прав, зважаючи на відсутність секретного ключа, тому необхідно вирішити задачу захисту авторських прав і забезпечити секретність впровадження за допомогою ключа розподілу.

Ключові слова: стеганографія, контейнер, прихований канал, секретний ключ.

V.M. DZULIY, E A. KOWRYHA
Khmelnytsk national university

ANALYSIS METHOD AND MEANS FOR SECURE DATA TRANSMISSION

The paper analyzes existing programs apply the information to your audio files revealed their advantages and disadvantages. The possible fields of application of steganography. Identified deficiencies methods apply the information in audio files.

The methods of implementation of the information in MIDI file format can not be used for copyright protection in the absence of a secret key, so you need to solve the problem of copyright protection and to ensure secrecy implementation by key

Keywords: steganography, container, hidden channel, the secret key

Вступ. Мережева безпека стає все більш актуальною з огляду зростаючих обсягів даних, що пересилаються по локальних і глобальних мережах. Для захисту інформації від несанкціонованого доступу та використання необхідно забезпечити конфіденційність і цілісність даних. Захист інформації може бути забезпечено криптографією, стеганографією, або одночасно криптографією і стеганографією. При використанні криптографії інформація модифікується, перетворюється. В результаті перетворень приховується зміст повідомлення. Стеганографія, в свою чергу, приховує сам факт передачі або зберігання інформації. Це досягається шляхом впровадження інформації, що захищається, в різні мультимедійні об'єкти (контейнери), які не втрачають від цього своїх споживчих властивостей. Відносно обчислювальної техніки виділився окремий напрямок стеганографії - комп'ютерна стеганографія. Як контейнери тут використовуються файли різних форматів, мережеві пакети і т.д. З іншого боку, стеганографія стала доступна для більшості користувачів і може застосовуватися в протизаконних цілях, наприклад, для несанкціонованої передачі комерційних або державних секретів; переписки терористичних угруповань. Тому з'являється необхідність у розробці ефективних методів виявлення прихованих вкладень, в мультимедійних об'єктах, переданих в комп'ютерних мережах.

Стеганографічна система - це сукупність засобів і методів, за допомогою яких створюється прихований канал передачі інформації. Повідомленням може бути секретний текст, зображення, фотографія, мітка, водяний знак. Стеганографічний канал - канал передачі заповненого контейнера. Стегоключ - секретні дані, використовувані в процесі впровадження приховуваного повідомлення в контейнері. На рис. 1 представлена узагальнена модель стегосистеми і проілюстровані наведені визначення.

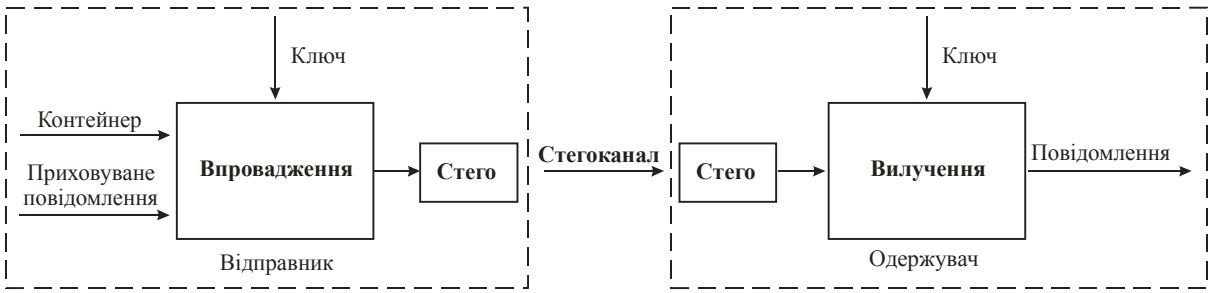

Рис. 1. Узагальнена модель стегосистеми

Відповідно до даної моделі, на стороні відправника приховуване повідомлення впроваджується в контейнер за спеціальним алгоритмом впровадження та ключем. Заповнений контейнер передається по відкритим каналам передачі даних одержувачу. На стороні одержувача із заповненого контейнера витягується вхідне повідомлення за алгоритмом витягування і ключем.

Комп'ютерна та цифрова стеганографія. Широке поширення мультимедійних технологій дало імпульс розвитку нових і вдосконаленню існуючих методів приховування інформації, а також сприяло виникненню більш складних методів організації прихованих каналів зв'язку, в основу яких були покладені особливості подання інформації в комп'ютерних файлах, пристроях, обчислювальних мережах і т.п. Комп'ютерна стеганографія застосовується для захисту ліцензійного програмного забезпечення, маскування мережевого трафіку, прихованого зберігання інформації. Основними положеннями організації прихованого каналу зв'язку з використанням комп'ютерної стеганографії є наступні: методи впровадження інформації повинні забезпечити автентичність та цілісність файлу; передбачається, що противнику повністю відомі

можливі методи впровадження інформації; методи впровадження інформації повинні зберігати основні властивості відкритого переданого контейнера; безпека методів впровадження грунтується на деякій невідомій противнику інформації - ключі; витяг вкладеного повідомлення повинен представляти собою складну обчислювальну задачу, навіть якщо факт приховування повідомлення став відомий противнику.

Методи комп'ютерної стеганографії розділяються на два класи: методи, засновані на надмірності інформації, (цифрова стеганографія); методи, засновані на використанні різних властивостей комп'ютерних форматів (форматна стеганографія).

До першого класу відносяться методи, які використовують молодші розряди цифрових відліків і методи, засновані на цифровій обробці сигналу. До другого класу відносяться методи видалення - ідентифікують заголовок файлу; методи впровадження інформації в невикористовувані області гнучких і жорстких дисків; методи впровадження інформації в текстові файли; методи, які використовують зарезервовані поля різних комп'ютерних форматів файлів.

З використанням цифрової стеганографії вирішують наступні завдання: вбудовування прихованої інформації; вбудовування цифрових водяних знаків; вбудовування ідентифікаційних номерів; вбудовування заголовків. Класифікація існуючих методів стеганографії представлена на рисунку 2.

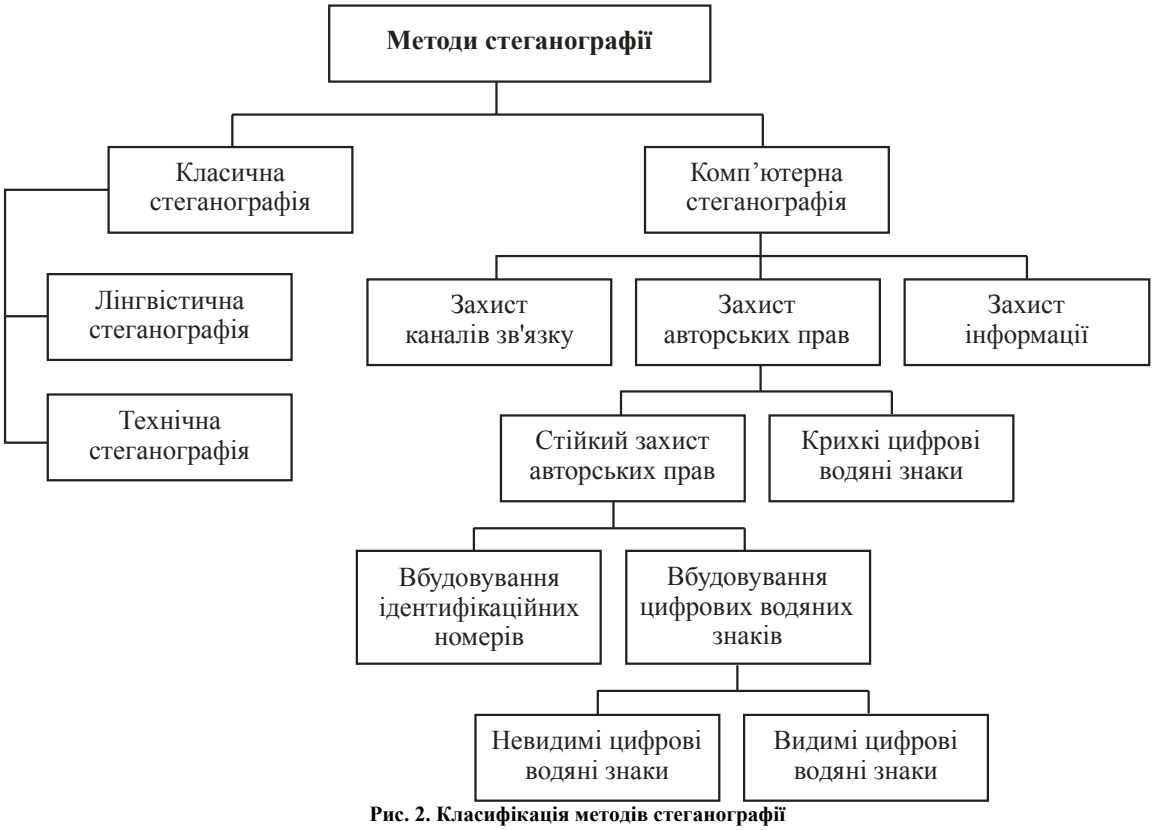

Рис. 2. Класифікація методів стеганографії

Цифрова стеганографія застосовується для захисту від копіювання і несанкціонованого використання, дозволяє захищати авторські права і інтелектуальну власність в області цифрової аудіо та відеоіндустрії. Для цього використовують вбудовування цифрових водяних знаків і ідентифікаційних номерів. Вбудовування невидимих заголовків застосовується для підпису медичних знімків та фотографій; нанесення легенди на карту, швидкого пошуку в базі даних по впровадженим в цифрові об'єкти ключовим словам, синхронізації відеопотоку зі звуком.

До методів організації прихованого каналу зв'язку засобами цифрової стеганографії пред'являються наступні вимоги: прозорість - відсутність помітних відмінностей між пустим контейнером і заповненим контейнером; стійкість до спотворень - впроваджена інформація повинна бути стійкою до різних перетворень, що відбуваються в процесі передачі інформації (вимога прозорості завжди конфліктує з вимогою стійкості до спотворень); стійкість до атак - впроваджена інформація може піддаватися взлому, видаленню або атакам (вимога стійкості до атак є головною вимогою пропонованою до будь-яких стеганографічних методів, однак досягти абсолютної стійкості впровадженої інформації до різного роду атак практично неможливо); можливість впровадження певного обсягу інформації - при істотному збільшенні обсягу впроваджуваної інформації знижується прозорість і стійкість до спотворень; секретність впровадження - у більшості випадків потрібно забезпечити секретність вбудованої інформації, її захист секретним ключем.

Методи впровадження інформації в звукові сигнали. Метод заміни найменшого значущого біта. Формат файла WAV містить в собі дискретний, квантований, звуковий сигнал або абсолютні значення амплітуди в кожній точці дискретизації. Чим більше розрядність двійкового числа, використовуваного для представлення відліку, тим точніше відображається значення амплітуди. Заміна молодших розрядів цифрових сигналів є найпростішим способом впровадження конфіденційних даних. Метод має прийнятну

стійкість до злому, дозволяє приховувати досить великий обсяг інформації в одному звуковому файлі, і якщо замінювати один останній біт, то спотворення звукового файлу будуть незначними. Наприклад, при довжині файлу 16 Мбайт і розмірі відліку 16 біт в ньому можна розмістити 1 Мбайт інформації. Для звукового файлу формату WAV з двома звуковими каналами (стерео) і розміром відліку 16 біт найменшим значущим бітом є кожен шістнадцятий біт в кожному звуковому каналі. Аналогічно для звукового файлу з одним звуковим каналом; (моно) і розміром відліку 8 біт найменшим значущим бітом є кожен восьмий біт.

Зміна останнього біта у відліку призводить до незначної зміни амплітуди сигналу. Ці зміни в амплітуді сигналу неможливо визначити на слух. Недоліком вказаного методу є низька стійкість до виявлення прихованої інформації статистичними методами і до різних перетворень. Для підвищення стійкості впровадженої інформації необхідне застосування методів нормалізації локальних статистик молодших біт (модифікація молодших біт сусідніх відліків, таким чином, щоб статистики порожнього і заповненого контейнера не відрізнялися) і розподілення впроваджуваного секретного повідомлення по всьому контейнеру.

Метод модифікації фази. Існують різні варіації методів впровадження інформації на основі фазового кодування. Суть методів модифікації фази полягає в зміні фази кожної частотної складової дискретного сигналу. Для цього вихідний сигнал розбивають на серію коротких сегментів, що містять однакову кількість елементів (відліків). Кількість елементів повинна бути більше ніж кількість біт в переданому повідомленні. До кожного сегмента застосовують дискретне перетворення Фур'є. В результаті для кожного сегмента створюються масиви фаз і амплітуд, кількість елементів масиву рівна кількості елементів в сегментах. Для збереження скритності повідомлення необхідно зберігати різницю фаз між сусідніми сегментами, так як слухова система людини більш чутлива до різниці фаз, ніж до абсолютних значень фази. Модифікацію фаз формують в масиві фаз першого сегмента. Вбудовування інформації здійснюють шляхом заміни вихідного значення фази на значення, рівне $-\pi/2$, якщо біт повідомлення дорівнює 0, і значення $\pi/2$, якщо біт повідомлення дорівнює 1. Щоб зберегти існуючу різницю фаз, необхідно отриманий масив фаз першого сегмента скласти з обчисленою раніше різницею між першим і другим масивом фаз, і так далі для кожного масиву фаз. Для відновлення звукового сигналу необхідно виконати зворотне дискретне перетворення Фур'є для масивів амплітуд і модифікованих масивів фаз. Недоліком даного методу є низька пропускна здатність.

Метод розширення спектра. У даному методі інформацію вбудовують в звуковий сигнал незначною зміною амплітуди сигналу. Метод розширення спектра застосовується в радіозв'язку для забезпечення високої завадостійкості сигналу в каналах з високим рівнем шуму й ускладнення перехоплення сигналу. Завадостійкість забезпечується тим, що енергія сигналу розподіляється по широкому діапазону частот. Дана обставина ускладнює виділення сигналу на фоні шуму і, що більш важливо, робить сигнал стійким до внесення шуму. Застосування даного методу в стеганографії робить впроваджену інформацію стійкою до несанкціонованого вилучення і спотворення. В разі застосування даного методу для приховування інформації в звуковому сигналі, дані множать на псевдовипадкову послідовність і на основний несучий сигнал, в результаті отримують розширену послідовність. Щоб зробити отриманий послідовністю шум низьким, його необхідно ослабити. Рівень ослаблення вибирається залежно від вимог непомітності змін до несучого сигналу. В звуковому сигналі спотворення непомітні при ослабленні послідовності до рівня однієї сотої. Ослаблений сигнал послідовності підсумовують з основним несучим сигналом. Для вилучення впровадженої інформації одержувачу повинен бути відомий немодифікований основний сигнал і псевдовипадкова послідовність, яка в даному випадку є ключем. Недоліком даного методу також є низька пропускна здатність.

Метод кодування з використанням ехо-сигналу. Метод впровадження інформації з використанням ехо-сигналу заснований на тому, що слухова система людини не може зафіксувати ехо-сигнал, якщо затримка між основним сигналом, і ехо-сигналом менше певного значення. Впровадження даних в звуковий сигнал виробляється шляхом підмішування до нього ехо-сигналу (рис. 3).

Рис. 3. Приклад ехо-кодування

Для вбудовування інформації в сигнал використовують дві часових затримки: одна для кодування нуля, інша для кодування одиниці. Щоб в звуковий сигнал можна було вбудувати декілька біт, його необхідно розбити на сегменти, що відповідають кількості біт в повідомленні. Кожен блок в цьому випадку розглядається, як окремий сигнал і використовується для кодування одного біта повідомлення. Для приховування інформації в звуковому сигналі необхідно створити одиничний і нульовий змішувані сигнали. Сума нульового змішуваного сигналу і одиничного змішуваного сигналу завжди має дорівнювати одиниці, щоб виключити різкі зміни в кінцевому сигналі. Недоліком методу є те, що для деяких звукових сигналів неможливо отримати достатню кількість правильно витягнутих біт впровадженого повідомлення.

Метод впровадження інформації варіацією різниці часу. Існує два підходи до впровадження інформації в MIDI-файли: використання подій MIDI; використання структури даних MIDI-файлу.

До першого підходу відноситься метод впровадження інформації в MIDI-файли шляхом варіації різниці часу між записаними в файл подіями, які не змінюють характеристики (налаштування) пристрою відтворення. Це відбувається, наприклад, коли поспіль слідують кілька однакових керуючих подій.

Для прихованої передачі інформації зазначеним методом використовується не тільки програмне регулювання гучності, а й інші керуючі події. Наприклад, здійснювати вимкнення неувімкненої ноти, підйом педалі, якщо вона не була натиснута, багаторазову установку стереобалансу на одне і те ж значення і т.д.

Недоліками даного методу прихованої передачі інформації є відсутність секретного ключа, який запобігав би можливості читання впровадженої інформації будь-яким користувачем. По суті, захист інформації утримується на секретності алгоритму, що суперечить правилу Керкхофа. Крім того, розглянутий метод має низьку стійкість до виявлення впровадженої інформації. Музикант, добре знайомий з форматом MIDI, легко виявить, що у файлі присутні «дивні» події. Звісно, що подібні події можна виявити автоматично спеціально розробленою програмою.

Метод впровадження інформації варіацією порядку запису подій. Впровадження інформації в MIDI-файл можна здійснити шляхом варіації порядку запису подій, що одночасно відбуваються. При використанні даного методу до файлу не додається нова інформація, і розмір файлу не змінюється. Даним методом зручно впроваджувати інформацію в одночасно виконувані ноти (акорди). Порядок запису нот в аркуші подій не має ніякого значення для відтворювальної апаратури, а варіація їх взаємного розташування при запису дозволяє кодувати переданий символ.

Програмні засоби прихованої передачі інформації. На основі проведеного аналізу існуючих програм були розглянуті наступні розробки: S-Tools 4.00, ArtMasker 1.06, StegHide 0.5.1, Invisible Secrets 4, Steganography 1.8.1. Слід зауважити, що всі зазначені програми в якості алгоритму впровадження інформації застосовують метод заміни найменшого значущого біта. S-Tools 4.00 – безкоштовна програма для приховування даних. Не вимагає інсталяції. Дані впроваджуються в графічні файли (формати BMP або GIF) або в звуковий файлі формату WAV. Крім цього, програма дозволяє попередньо зашифрувати дані алгоритмами IDEA, DES, Triple DES, MDC. Недоліком даної програми є відсутність розподілу інформації по декількох файлах. Впровадження ведеться по всій довжині фонограми, включаючи ділянки «повної тиші».

Ще однією безкоштовною розробкою є ArtMasker 1.06. Програма вимагає інсталяції. Даний програмний продукт не має користувальницького меню і відрізняється простотою у використанні. Програма дозволяє зашифрувати дані перед впровадженням. Користувач отримує інформацію про те, якого обсягу текст може бути впроваджений у вибраний файл. До недоліків програми можна віднести відсутність довідкового керівництва, автоматичне закриття програми після завершення кожної операції та відсутність перевірки структури файл-контейнерів.

StegHide 0.5.1 також відноситься до безкоштовних програм. Інтерфейс програми виконаний у вигляді командного рядка. Як контейнери використовує графічні або звукові файли формату WAV і AU. Впроваджувану інформацію програма дозволяє попередньо зашифрувати алгоритмом AES. Недоліками є відсутність ключа розподілу інформації в контейнері, вся секретність тримається на алгоритмі впровадження інформації та шифруванні.

Invisible Secrets 4 є комерційним програмним продуктом. Користувач вибирає файл з інформацією, файл-контейнер і вказує шлях для збереження результатів. Користувач може вибрати криптографічні алгоритми шифрування інформації та ввести ключ для дешифрування. До переваг Invisible Secrets 4 можна віднести простий і зрозумілий інтерфейс, високу продуктивність і великий вибір алгоритмів шифрування. До недоліків слід віднести високу вартість, відсутність розподілу інформації як всередині контейнера, так і по декількох контейнерах.

Steganography 1.8.1 - комерційна програма, дозволяє працювати сім днів на тестовому режимі. Програма дозволяє легко впроваджувати інформацію в файл-контейнер і також просто її витягти з файл-контейнера. Контейнером може бути графічний, виконуваний, звуковий файл формату WAV або MP3. Недоліком програми є те, що секретна інформація впроваджується в кінець файлу, тим самим, збільшуючи розмір файл-контейнера. Виявлення вкладення для фахівців не становить складності. Вся криптостійкість тримається, по суті, на алгоритмі шифрування, назву якого ніде не вказано.

Прихований канал передачі інформації. Вперше поняття прихованого каналу передачі інформації було введено Батлером Лемпсоном в 1973 році в роботі «The Note on the Confinement Problem». Він визначив прихований канал, як канал взагалі, не призначений для передачі інформації. Поняттям прихованого каналу в рамках стеганографії є визначення, наведене Кремерером. Прихований канал - це канал, який використовує об'єкти, які зазвичай не розглядаються як об'єкти даних для передачі інформації від відправника до одержувача.

У цифровій стеганографії прихований канал передачі інформації передбачає передачу контейнера по відкритих каналах зв'язку. Однак, на основі відкритого каналу передачі інформації організується прихований канал, що несе інформацію в самому контейнері.

Захист ключової інформації. Забезпечення секретності ключів є найважливішим завданням в галузі захисту інформації. Для забезпечення секретності ключів в мережах передачі даних застосовуються такі організаційні та технічні заходи: обмеження кола користувачів, допущених до роботи з ключами; регламентація розподілу, зберігання, знищення ключів; регламентація порядку зміни ключів; застосування технічних засобів захисту ключів від несанкціонованого доступу. Для розподілу ключів використовується принцип розподілу секрету. Розподілення секрету - це спосіб розподілу частки секретної інформації між декількома користувачами, при якому знання будь-якою особою будь-якої з часток, не дозволяє йому

відновити секрет простіше, ніж перебором значень секрету, а сукупність всіх часток дозволяє однозначно обчислити секрет. Найпростіша схема розподілу ключа x, що складається з n біт, між m користувачами полягає в розподілі між ними векторів $x_1,...,x_m$, кожен вектор також складається з n бітів, при яких $x = x_1 \oplus ... \oplus x_m$.

В симетричних криптосистемах для розсилки ключів використовують кур'єрську службу, надійний захищений канал зв'язку, або кілька паралельних каналів зв'язку і схему розподілу секрету. Розподіл ключів між користувачами є найважливішим завданням забезпечення захисту інформації. На сьогоднішній день застосовують такі протоколи розподілу ключів: передача ключа користувачеві; спільне вироблення ключа користувачами; попередній розподіл ключів між користувачами.

Секретність ключа при зберіганні може бути забезпечена такими способами: ключ зберігається поза комп'ютером, і кожен раз вводиться користувачем через клавіатуру; ключ записується на картку і вводиться в комп'ютер через зчитувальний пристрій; ключ розділяється на дві частини, одна частина зберігається в пам'яті комп'ютера, друга частина зберігається на картці; ключ зберігається в пам'яті комп'ютера в зашифрованому виді і перед використанням дешифрується, при цьому таємність ключа шифрування забезпечується вищевказаними способами.

Повідомлення, передане по мережах зв'язку, не має високої цінності, як при його зберіганні. Некоректну передачу повідомлення можна виправити, виконавши повторну передачу повідомлення, але некоректне дешифрування повідомлення може призвести до втрати самого повідомлення. Отже, в, інформаційній системі необхідно передбачити механізми захисту збережених зашифрованих повідомлень від внесення спотворень, шляхом створення резервних копій. В деяких випадках частини збереженого шифрованого повідомлення можуть зберігатися у відкритому виді. Якщо не забезпечено захист інформації, то у криптоаналітика є можливість визначення ключа шифрування. Одним із варіантів організації захищеного каналу зв'язку є застосування методів стеганографії. Шифрований ключ може зберігатися в пам'яті комп'ютера впровадженим в який-небудь мультимедійний об'єкт, наприклад, звуковий файл. В звуковий файл впровадження ключа здійснюється методами стеганографії. Захист відкритої інформації може бути також забезпечено методами стеганографії, які дозволяють приховувати інформацію. Передача ключів здійснюється звуковими файлами формату WAV. Ключ розділяється на декілька частин, і кожна частина ключа, впроваджується методами стеганографії в окремий звуковий файл формату WAV. Кожен звуковий файл із впровадженою частиною ключа передається: користувачам по відкритих каналах зв'язку.

Висновки. На основі проведеного аналізу наведено поняття прихованого каналу передачі інформації, а також класифікація методів і завдань прихованої передачі інформації.

Проведено огляд існуючих методів впровадження інформації в звукові файли. Наведено аналіз існуючих програм впровадження інформації в звукові файли, виявлено їх переваги та недоліки. Розглянуті можливі області застосування стеганографії, зокрема-стеганографія може бути використана для зберігання і розподілення ключів в мережах зв'язку. Виявлені недоліки методів впровадження інформації в звукові файли і їх програмні реалізації не дозволяють в повній мірі використовувати їх для безпечної передачі інформації. Для організації прихованого каналу зв'язку, розподілу і передачі ключової інформації найбільш адекватним є метод впровадження інформації LSB, на відміну від інших розглянутих методів, він має високу пропускну здатність. Однак для його застосування в реальних задачах необхідно вирішити задачу підвищення стійкості до злому і спотворень. Розглянуті методи впровадження інформації в файли формату MIDI не можуть застосовуватися для захисту авторських прав зважаючи на відсутність секретного ключа, тому необхідно вирішити задачу захисту авторських прав і забезпечити секретність впровадження за допомогою ключа розподілу.

Література

1. Грибунин В.Г. Цифровая стеганография. /В.Г.Грибунин, И.Н.,Оков И.В.,Туринцев // М.: СОЛОН-Пресс; 2002. - 261 с.

2. Конахович Т.Ф. Компьютерная стеганография / Т.Ф Конахович, А.Ю Пузыренко // Теория и практика. Киев: МК-Пресс, 2006. -288с.

3. Мамаев М. Технологии защиты информации:в Интернете/ Мамаев М., Петренко С. //: Специальный;справочник..СИб::Иитер 2002. -848 с.

Хайкин С. Нейронные сети. / Хайкин С. //Полный курс: пер. с англ. / 2-е изд. М.: Издательский дом «Вильяме», 2006. -1104 с.

References

1. Hrybunyn VG Tsyfrovaya steganography. /V.H.Hrybunyn, IN, shackles IV, Turyntsev // .: SOLON M-Press; 2002 - 261 p.

2. Konahovych TF Kompyuternaya steganography / T.F Konahovych, A.YU Puzыrenko // Theory and Practice. Kiev: MK-Press, 2006 -288s.

3. Mamaev M. Technologies of protection of information: on the Internet / M. Mamaev, S. Petrenko //: Spetsyalnыy; spravochnyk..SYb :: Yyter 2002 -848 p.

4. Haykyn S. neural network. / Haykyn S. // Polnыy course: Lane. with the English. / 2nd ed. M .: Yzdatelskyy home "Vylyame" 2006. -1104 p.

Рецензія/Peer review : 7.10.2014 р. Надрукована/Printed : 16.11.2014 р.