Список використаних джерел

1. Mazurczyk W., Lubacz J., Szczypiorski K., Hiding data in VoIP, December, 2008.
2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: СОЛОН-Пресс. – 2002. – 261 с.
3. Основы компьютерной стеганографии / А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин. – М.: Радио и связь, 2003. – 152 с.
4. Хорев А.А., Макаров Ю.К. К оценке эффективности защиты акустической (речевой) информации//Специальная техника, № 5, 2000, с. 46 – 56.
5. Хорошко В.А., Шелест М.Е. Введение в компьютерную стеганографию. – К., 2002. – 140 с.
6. Katzenbeisser S., Petitcolas F. Defining Security in Steganographic Systems.

УДК 004.056.5

МЕТОД ПРИХОВУВАННЯ СТЕГО У ТРАФІКУ IP-ТЕЛЕФОНІЇ

Шевчук Р.П., Міхайліді К.О.
Тернопільський національний економічний університет

Вперше принципи та визначення комп'ютерної стеганофонії були сформовані польськими спеціалістами з Варшавського університету технологій у 2008 році, які запропонували декілька методів приховування даних у трафіку IP-телефонії [1]. Молодість комп'ютерної стеганофонії породжує велике поле досліджень у цій галузі, які є надзвичайно актуальними, оскільки частка мовної інформації в IP-мережах на сьогоднішній день є найбільш прогресуючою.

Структура та принципи роботи систем комп'ютерної стеганофонії аналогічні до стеганографічних систем. Різниця між цими спорідненими галузями захисту даних полягає у середовищі формування даних та особливостях приховування даних у стегоконтейнері.

Метою роботи є розробка нового методу приховування даних у трафіку IP-телефонії.

Основою для побудови методу приховування даних у IP-телефонії став аналіз мережевих затримок, що виникають при передачі даних між абонентами IP-телефонії. У таблиці 1 показано середні затримки передачі мовного трафіку між кінцевими абонентами при різних алгоритмах стиснення мовного сигналу [2].

Таблиця 1

Назва алгоритму	Стандарт	Швидкість, біт/с	Довжина кадру, мс.	Середній час затримки (*Tcep*), мс
CS- ACELP	G.729	16000	10	74
CS- ACELP	G.729	8000	10	81
ACELP	G.723	5300	20	92

Аналіз таблиці 1, показує що середня затримка коливається в межах 70-100 мс., що дозволяє гарантувати хорошу якість передачі мовного сигналу.

На підставі аналізу стандарту H.323, у якому для забезпечення середньої якості (MOS 3,5-4.0) передачі мовних сигналів затримка не повинна перевищувати 350 мс., розроблено метод приховування даних у трафіку IP-телефонії, який можна представити наступними етапами:

1. Оцінюється середня затримка (*Tcep)* передачі одного пакету між абонентами А та В.
2. Порівнюються значення середньої затримки та значення максимально допустимої затримки у мережі. Якщо *Tcep < 350* то *K= 350/Tcep.*
3. Визначається кількість пакетів, які можна передати від А до В, без втрат якості мовного сигналу. Якщо *mod (K)>=1*, то прекодер стеганофонічої системи абонента А генерує *mod (K)* пакетів у які стегокодер інкапсулює таємне повідомлення. Кількість бітів, які інкапсулюються в пакет буде визначатись форматом стиснення, що використовується у IP-телефонії.
4. Стегокодер системи абонента А маркує одне з резервних полів згенерованих пакетів, для того щоб стегодекодер розпізнав таємне повідомлення та передав його у декодер абонента В.
5. Передача згенерованих пакетів від абонента А до В.

Ефективність представлено методу буде прямопропорційно залежати від мережевої затримки між абонентами IP-телефонії. Основною перевагою запропонованого методу є набагато більший

об’єм стего контейнера переданого за одиницю часу між абонентами IP-телефонії, у порівнянні з аналогами. Недоліком алгоритму є невисока ефективність роботи у:

- мережевих середовищах, у яких затримка передачі мовного трафіка близька до критичної межі;
- системах в яких стиснення мовного сигналу виконується кодеками із змінною швидкістю кодування.

Список використаних джерел

1. W. Mazurczyk, J. Lubacz, and K. Szczypiorski, Hiding Data in VoIP, In Proc. of: The 26th Army Science Conference, December 1-4, 2008, Orlando, FL, USA

2. Тимченко О.В., Колодій Р.С., Смолінський М.В. Оцінка якості IP телефонії. Збірник «Наукові праці ОНАЗ». - №3, 2004. С. 72-75.