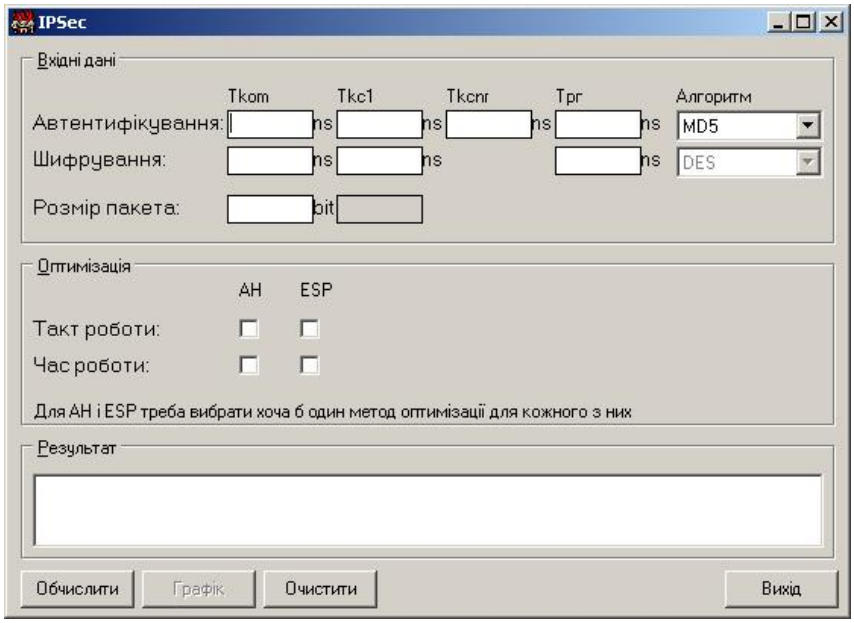

Рисунок 1 – Головне вікно програми пошуку параметрів оптимальної структури операційних пристроїв процесора IPSec

Результатом роботи програми є видача найкращих значень часових характеристик для параметрів структури операційних пристроїв хешування і шифрування. На основі проведених обчислень будуються графіки залежності часу оброблення пакетів даних комп'ютерних мереж від структур операційних пристроїв шифрування та хешування.

Список використаних джерел

1. Шнайер Б. Прикладная криптография, 2-е издание: протоколы, алгоритмы, исходные тексты на языке Си. - Под редакцией П.В. Семьянова. М., Триумф, 2002.
2. Т. Коркішко, Л. Коркішко, Р. Шевчук. Базові структури операційних пристроїв хешування для процесорів підтримки протоколу IPSEC // Комп'ютинг. – 2003. – Том 2. №1. – С. 41-47.
3. Шевчук Р., Манжула В., Адамів О. Оцінка технічних характеристик операційних пристроїв процесорів хешування // Вісник Тернопільського державного технічного університету. – Тернопіль, 2009. № 2. – С. 103 – 108.

УДК 681.511:3

ОЦІНКА СТІЙКОСТІ СТЕГАНОФОНІЧНИХ СИСТЕМ

Шевчук Р.П., Карпова О. В.
Тернопільський національний економічний університет

I. Постановка проблеми

Стеганофонічні системи – це системи в яких приховується факт передачі таємного повідомлення, а саме повідомлення інкапсулюється у стек мережевих протоколів та передається у реальному масштабі часу [1]. 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]. Структура та принципи роботи систем комп'ютерної стеганофонії аналогічні до стеганографічних систем, тому часто про ці галузі захисту даних порівнюють між собою.

Аналіз літератури [1] показує, що в стеганофонії чимало проблем поки що знаходяться на початковій стадії свого вирішення. Актуальним є наукове завдання аналізу підходів щодо оцінки стійкості стеганофонічних систем. Вирішення цього завдання дозволить запропонувати методи підвищення стійкості стеганофонічних систем.

II. Мета роботи

Метою дослідження є аналіз підходів щодо оцінки стійкості стеганофонічних систем.

III. Аналіз стійкості стеганофонічних систем та методи її підвищення

Ступінь захищеності стеганофонічних систем оцінюється їх стійкістю. Під стійкістю стегосистем розуміють їх здатність приховувати від кваліфікованого порушника факт таємної передачі повідомлень, можливість протистояти спробам порушника зруйнувати, спотворити, видалити таємні повідомлення, а також здатність підтвердити або спростувати достовірність інформації, яка передається [2-5].

Підходи щодо оцінки стійкості стеганофонічної системи будуть ідентичні аналогам у стеганографічних системах [6]:

- оцінка в теоретико-інформаційній моделі системи;
- оцінка в теоретико-складнісній моделі.

Для аналізу стійкості стеганофонічних систем до виявлення факту передачі таємного повідомлення розглянемо модель стегосистем з пасивним супротивником. В даній моделі стеганофонічної системи відомий імовірнісний розподіл пустих контейнерів (*Pc*) і імовірнісний розподіл стего (*Ps*).

Використаємо відносну ентропію $D(P_c||P_s)$ між розподілами *Pc* і *Ps* для оцінки стійкості стеганофонічної системи у випадку пасивного супротивника. Стеганофонічна система називається ε-стійкою проти пасивного порушника, якщо $D(P_c||P_s) \leq \varepsilon$. Якщо $\varepsilon = 0$, то така система є ідеальною [1].

В теоретико-інформаційній моделі стеганофонічна система вважається стійкою, якщо порушник не спроможний отримати ніякої інформації про вбудоване повідомлення, аналізуючи перехоплені стего при умові, що він знає статистичні характеристики пустих контейнерів [2]. В рамках цього визначення підраховується взаємна інформація *I(M;(S,C))* між прихованими повідомленнями *M* і множинами стего *S* і відповідним їм контейнерам *C*. В теоретико-інформаційній стійкій стеганофонічій системі повинна виконуватися рівність *I(M;(S,C))=0*. Взаємна інформація може бути визначена через безумовну і умовну ентропію:

$$I(M;(S,C)) = H(M) - H(M/(S,C)) = 0. \quad (1)$$

Це дає фундаментальну умову стійкості стеганофонічної системи вигляду

$$H(M/(S,C)) = H(M). \quad (2)$$

Визначення (2) означає, що невизначеність порушника відносно повідомлення *M* не повинна зменшуватися при знанні ним стего *S* і контейнера *C*, тобто *M* повинно бути незалежним від *S* і *C*.

В теоретико-складнісній моделі робиться припущення, що існує множина можливих контейнерів *N*, елементи якої $n \square N$ породжуються деяким поліноміальним алгоритмом. Таємне повідомлення $m \square M$ вибирається з множини можливих повідомлень $M = \{0,1\}^l$. Стеганофонічна система визначається трійкою $< G, E, D >$ поліноміальних алгоритмів. Алгоритм *G* є процесом генерації ключа, який у відповідь на вхідну стрічку з одиниць породжує псевдовипадковий стегоключ $k \in \{0,1\}$. Відповідно до принципу Керхгофа стійкість залежить від ключа, а його довжина є параметром таємності стегосистеми. Алгоритм *E* виконує вбудовування інформації, формуючи на основі $c \in C, m \epsilon M$ і k, стего $s \epsilon C$. Алгоритм *D* витягує з *s* з використанням ключа *k* повідомлення *m'*. У випадку, коли контейнер *s* дійсно містив вбудоване повідомлення, то $m' = m$. Для визначення присутності стеганофонічної системи порушник повинен вирішити наступну задачу: на основі контейнера $s \epsilon C$ визначити, чи існує ключ $k \epsilon \{0,1\}$, який породжується G і повідомлення $m \epsilon M$ такі, що *D(s,k) = m* [2].

Стеганофонічна система називається умовно стійкою, якщо у порушника немає можливості правильного визначення стего з імовірністю ~0,5. Поняття умовно стійкої стегосистеми більш слабке, ніж поняття стегосистеми, стійкої з інформаційно-теоретичної точки зору і включає її як частковий випадок.

Висновки

У роботі проведено аналіз підходів щодо оцінки стійкості стеганофонічних систем. На даний час жоден з підходів не може гарантувати абсолютну стійкість стеганофонічній системі. Чим більшою є кількість даних, які приховуються, тим більша імовірність того, що факт їх передачі буде виявлений.

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