УДК 004.056

ЗАСІБ СТЕГАНОГРАФІЧНОЇ ПЕРЕДАЧІ ДАНИХ ПО ПРОТОКОЛУ RTP

О. П. Войтович к.т.н., доц.; Р. Є. Ніколюк
Вінницький національний технічний університет
o_p_v@list.ru

Інформація, що передається по каналах зв’язку вимагає захисту від нелегального копіювання, крадіжок, зміни тощо. Тема приховання інформації від зловмисників завжди є актуальною, а тому стеганографічні методи захисту залишаються у моді. У зв'язку із зростанням популярності IP-телефонії, за допомогою якої передається великий обсяг даних за різноманітними протоколами, вона все більше привертає увагу наукового співтовариства як ідеальний носій для стеганографічного приховування даних.

Аналіз літературних джерел показав наявність ряду методів приховування інформації у VoIP-потік (рис.1).

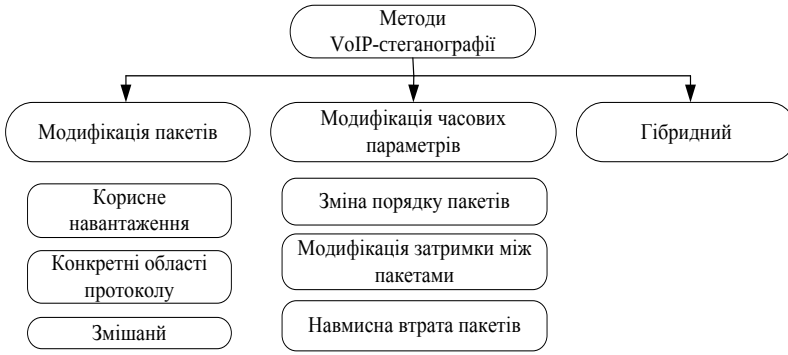

Рисунок 1 – Методи приховування інформації у VoIP

Одним з протоколів, який може бути використаний для стеганографічних цілей – це протокол RTP (Real-Time Transport Protocol), що використовується для формування та передавання пакетів з медіа-даними. Формат пакету RPT показаний на рис. 2.

+ Біти	0-1	2	3	4-7	8	9-15	16-31
0	Ver.	P	X	CC	M	PT	Порядковий номер
32	Мітка часу						
64	SSRC-идентификатор						
96	... CSRC-идентификатори ...						
96+(CC×32)	Додатковий заголовок (необов'язковий), містить довжину блоку даних — «AHL»						
96+(CC×32) + (X×(AHL+16))	Дані						

Рисунок 2 – Формат кадру протоколу RTP

Аналіз особливостей пакету RTP показав, що приховану інформацію можна вбудовувати у додатковий опційний заголовок, який починається з 96 біта. Загальний розмір цього заголовку залежить від значення поля CC (число CSRC містить код кількості csrc-ідентифікаторів, які записані в пакеті «4 біта»). Розрахунок показав, що величина заголовку може змінюватись від 32-480 біт.

Раніше запропонований алгоритм мав певні недоліки, зокрема певні часові затримки, що виникали під час вбудовування даних у медіа-потік, а також недостатня захищеність прихованої інформації від стегоаналізу. Запропоновано покращений алгоритм для розбиття повідомлення, що дозволяє частково зменшити ці недоліки.

Вибір розміру вбудовуваних даних відбувається залежно від кількості та розміру повідомлень, які використовуються як стегоконтейнер. Такий підхід дозволить не заповнювати поле додаткового заголовку повністю, а отже, підвищиться швидкодія, а зловмисник не зможе зробити висновок про наявність стегоповідомлення за розміром поля.