УДК 621.391

АНАЛІЗ СКРИТНОСТІ ТА СТІЙКОСТІ ДО ШУМУ В КАНАЛАХ ЗВ'ЯЗКУ МЕТОДІВ МЕРЕЖНОЇ СТЕГАНОГРАФІЇ

А.О. ЩЕРБАК, А.А. АСТРАХАНЦЕВ
Харківський національний університет радіоелектроніки
О.В. ЩЕРБАК
Харківський національний університет Повітряних Сил імені Івана Кожедуба
Г.Є. ЛЯШЕНКО
Харківський національний університет радіоелектроніки

Abstract *– In this paper, for the first time, the effectiveness of network steganography methods has been investigated using channel coding of data when they are transmitted over communication channels with interferences, and the method of mathematical modeling evaluates the stability of network steganography methods to the detection. The network steganography methods concealing data in such protocols as HTTP, TCP and ICMP were considered. Using the ICMP «Secure» mode of the developed method, the greatest throughput was achieved. To study the noise resistance of the methods before transmission by the communication channel, the packets were encoded using the 2 Binary 1 Quandary linear coding algorithm, after which additive white Gaussian noise was added to the stego object. The paper substantiates the possibility of using network steganography methods to protect biometric data from unauthorized access in the case of using remote biometric authentication. Based on the research results, it was determined that the network steganography method based on hiding data in TCP is more efficient when working via communication channels with noise. It makes possible to recover a message with small distortions at a dispersion value of 0.4. But according to a set of criteria for resistance to noise and detection probability, the best is the «Fast» mode of the network steganography method based on hiding data in ICMP.*

Анотація *– В роботі вперше досліджено ефективність методів мережної стеганографії за умови використання канального кодування даних при їх передачі каналом зв'язку з шумами та оцінено стійкість методів мережної стеганографії до виявлення. На основі результатів досліджень визначено, що метод мережної стеганографії з використанням протоколу TCP є більш ефективним за умови роботи каналами зв'язку з шумами, але за сукупністю критеріїв стійкість до шумів / прихованість найкращим є режим «Швидкий» методу мережної стеганографії з використанням протоколу ICMP.*

Аннотация *– В работе впервые исследована эффективность методов сетевой стеганографии при использовании канального кодирования данных при их передаче по каналу связи с шумами и оценена методом математического моделирования устойчивость методов сетевой стеганографии к выявлению. На основе результатов исследований определено, что метод сетевой стеганографии с использованием протокола TCP является более эффективным при работе по каналам связи с шумами, но по совокупности критериев устойчивость к шумам / скрытность лучшим является режим «Быстрый» метода сетевой стеганографии с использованием протокола ICMP.*

Вступ

Оскільки обмін інформацією, представленою в цифровому вигляді, стає все поширенішим, то проблема її захисту є як ніколи важливою. За допомогою різних технічних засобів зловмисники можуть отримувати несанкціонований доступ до захищених даних і модифікувати їх. Відповідно до цього, актуальною на цей час задачею є

захист біометричних даних від несанкціонованого доступу у разі використання віддаленої біометричної автентифікації. Віддалена автентифікація може бути використана, наприклад, в рішеннях Інтернету речей (Internet of Things, IoT), при здійсненні мобільних платежів і взаємному розпізнаванні користувачів.

Одне з найпоширеніших застосувань біометричної автентифікації – її використання при наданні віддаленого доступу телекомунікаційною мережею. В такому випадку використовується загальна клієнт-серверна модель, коли клієнтський термінал оснащується необхідним пристроєм, який вимірює біометричну характеристику і обчислює вектор біометричних ознак (біометричний шаблон). Біометрична система на етапі реєстрації записує зразок біометричної характеристики користувача за допомогою датчика – наприклад, сканується райдужна оболонка ока [1]. Потім з біометричної характеристики обчислюється вектор біометричних ознак. Система зберігає вектор у базі даних поряд з іншими ідентифікаторами, такими як ім'я або ідентифікаційний номер. Для автентифікації користувач пред'являє датчику ще один біометричний зразок. Пропонований користувачем біометричний зразок перетворюється модулем реєстрації в вектор біометричних ознак, який і обробляється в подальшому. Ознаки, витягнуті з нього, являють собою запит, який система порівнює з вектором заявленої особистості за допомогою алгоритму зіставлення. Він повертає рейтинг відповідності, що відображає ступінь схожості між шаблоном і запитом. Система приймає заяву, тільки якщо рейтинг відповідності перевищує заздалегідь заданий поріг.

Віддалена біометрична автентифікація може ґрунтуватись на протоколі EAP (Extensible Authentication Protocol), який представляє собою розширювану інфраструктуру, що використовується для вибору конкретного механізму автентифікації. На даний момент розроблено близько сорока різних методів, що використовують EAP. Дані методи визначені в Internet Engineering Task Force (IETF) Request for Comments (RFCs). EAP дозволяє використовувати сервер автентифікації, який може реалізовувати деякі або всі способи автентифікації.

Одним з етапів вирішення задачі автентифікації є приховання самого процесу передачі біометричних даних. Тому у даній роботі обґрунтовується можливість використання для цього методів мережної стеганографії з порівняльною оцінкою їх ефективності. За останні роки було отримано множину результатів, які спрямовані на створення нових методів мережної стеганографії. Так, в роботі [2] було розроблено метод мережної стеганографії, який не можна виявити. В роботі [3] запропоновано його застосування для встановлення прихованого зв'язку між зловмисником і активним шкідливим додатком на стороні зараженого терміналу. В свою чергу, в роботі [4] запропоновано новий метод мережної стеганографії – «метод опцій», та описано теоретичну основу на прикладі опцій «запис маршруту» та «тимчасовий штамп». Щодо досліджень впливу стеганографічних характеристик, у роботі [5] проводились дослідження важливості впливу такої характеристики як стеганографічна вартість на ймовірність виявлення методів мережної стеганографії.

Метою даної роботи є дослідження ефективності методів мережної стеганографії у разі проведення віддаленої автентифікації шляхом оцінювання прихованості вказаних методів та їх стійкості до шуму в каналах зв'язку [6].

I. Огляд реалізованих методів мережної стеганографії

В роботі досліджувались основні методи мережної стеганографії, що ґрунтуються на приховуванні даних, які передаються в заголовках протоколів. Дослідження та оцінка ефективності проводились для трьох методів, які використовують мережні фрагменти даних (Protocol Data Units, PDUs) протоколів Transmission Control Protocol (TCP), Hypertext Transfer Protocol (HTTP) та Internet Control Message Protocol (ICMP). Для дослідження зазначених методів було реалізовано спеціальний комплекс програм.

Перший метод мережної стеганографії (МС), який було досліджено, приховує дані у сегментах TCP. Тому надалі для посилання на нього буде використовуватись скорочення МС-TCP. В TCP-сегмент можна вбудовувати дані у такі поля, як:

– Window Size;

– TCP Option;

– Acknowledge (ACK) number.

У даній роботі для приховування даних у TCP-сегменті використовувалось поле Window Size, порядок модифікації якого був розглянутий у роботі [7]. Його зміст полягав у внесенні приховуваних даних в це поле, після чого TCP-сегмент передавався на сторону приймача, та вже на його стороні відбувалось відновлення прихованих даних. Через те що розмір даного поля складає 16 біт, то в один сегмент можна вбудувати 2 байти даних. Проте для більшої надійності було вирішено, що в одне поле варто вбудовувати один байт даних, що зазнав деяких перетворень. Спочатку програма бере по одному байту даних і конвертує у десятковий вигляд, після чого це число множиться на 150, і якщо отриманий результат множення менше десяти тисяч, це число знову помножується на 6, після чого результуюче число заноситься до поля Window Size. Дані множники були обрані з огляду на те, що один байт, який відновлюється з даних, може мати максимальне значення 255 у десятковій системі числення і, помножуючи це число на 150, результат не буде перевищувати максимально можливе значення поля Window Size – 65535. Описані раніше множники виступають секретними ключами, не знаючи яких, приймаюча сторона не зможе відновити приховане повідомлення зі стегоконтейнеру. Перед тим як передавати приховані дані, на стороні приймача необхідно почати перехоплення трафіка. На рис. 1 показано приклад того, як користувач задає файл (steg.txt), передачу якого необхідно приховати.

```
########## [Steganography] ##########
Write the path of the file for Steganography:'steg.txt'
Do you want send the packet with Steganography:'y'
```

Рис. 1. Передача прихованого повідомлення за допомогою методу МС-TCP

На стороні приймача програма відновлює значення поля Window Size і, виконуючи зворотні перетворення, отримує дані, що були передані у відкритому вигляді. На рис. 2 представлено приклад того, як відбувається відновлення прихованого повідомлення на приймальній стороні. Для маніпуляції полями TCP було використано Python Framework Scapy.

```
########## [Recovering Message] ##########
Enter the path of the packets to analyze: 'packets.txt'
Write the output file name: 'result.txt'
Writing into the file...
Closing files...
```

Рис. 2. Відновлення прихованого повідомлення за допомогою методу MC-TCP

Другий метод реалізує приховування даних у HTTP-заголовках, надалі він буде іменуватись як метод MC-HTTP. У цьому методі для прихованої передачі даних можуть бути використані різні характеристики HTTP-повідомлень. До них належать модифікації порядку заголовків, їх структури та змісту [8, 9]. Програмна модель, яка реалізує метод MC-HTTP, відповідає клієнт-серверній архітектурі: на стороні клієнта повідомлення перетворюється у двійковий формат і кодується як пробіли всередині HTTP-заголовків запитів. Нуль кодується як пробіл, а одиниця – подвійний пробіл. Перше місце після двокрапки в HTTP-заголовках не використовується для приховування даних. У разі подвійного пробілу це візуально дуже помітно. Крім того, для забезпечення більшої пропускної здатності пробіл(-и) також додається безпосередньо перед кінцем заголовка (\r\n), що важче помітити. На рис. 3 представлено перший з переданих HTTP-заголовок, що містить частину прихованого повідомлення «Security». Його було перехоплено за допомогою програми Wireshark.

```
GET /test/test.php?id=1 HTTP/1.1\r\n
dnt: 1 \r\n
accept-language: bg-BG,  bg;q=0.8, en;q=0.6,  de;q=0.7 \r\n
x-requested-with: XMLHttpRequest \r\n
connection: keep-alive  \r\n
cache-control: must-revalidate,  public, max-age=0  \r\n
upgrade-insecure-requests: 1  \r\n
referer: http://www.mysite.com/ \r\n
accept-charset: utf-8, iso-8859-1;q=0.5,  *;q=0.1 \r\n
host: 127.0.0.1  \r\n
accept-encoding: gzip, deflate,  sdch  \r\n
user-agent: Mozilla/5.0 (Windows NT 10.0;  Win64;  x64) AppleWebKit/537.36  (KHTML,  like  Gecko) Chrome/58.0.3029.110  Safari/537.36 \r\n
accept: text/html,  application/xhtml+xml, application/xml;q=0.9,  image/webp,  */*;q=0.8  \r\n
\r\n
```

Рис. 3. HTTP-заголовок з частиною прихованого повідомлення

На рис. 3 виділено місця, куди було приховано біти літери «S», що має в двійковому коді значення «01010011». Однією рискою відображено пробіл, двома – подвійний пробіл.

Третій досліджуваний метод – це метод мережної стеганографії на основі приховування даних у ICMP-заголовках (MC-ICMP). Для реалізації даного методу також була розроблена програма, яка має два шари, один з яких відповідає за графічний інтерфейс, криптографію та стиснення даних, а другий – за вбудовування інформації в ICMP-заголовки. Обидва шари – це окремі програми, які взаємодіють одна з одною

за допомогою inter-process communication (IPC) Unix. Як було згадано вище, програма використовує стиснення та шифрування інформації, яку необхідно приховано передати. Для стиснення використовувалась бібліотека zlib, а шифрувались дані за допомогою Advanced Encryption Standard (AES) 265 [10, 11]. Розроблена програма підтримує в рамках методу MC-ICMP два режими вбудовування даних. Перший режим – «Швидкий», він дає можливість приховати 60 байтів інформації в один стегоконтейнер. У даному режимі використовуються такі поля, як Identifier, Sequence number і поле даних. Другий режим – «Безпечний», він змінює лише два поля: Identifier і Sequence number. Тому другий режим має меншу пропускну здатність у порівнянні з режимом «Швидкий». Для двох режимів пакет було обрано розміром 64 байти.

Оскільки зазначені методи мають використовуватися для віддаленої біометричної автентифікації, велике значення у разі оцінювання їх ефективності набуває стійкість до шумів у відкритих каналах зв'язку.

II. Порівняння методів мережної стеганографії за стійкістю до шумів у каналах зв'язку

Першою характеристикою, за якою проводилося порівняння реалізованих методів, було обрано стійкість до шумів у каналах зв'язку. Перед передаванням каналом зв'язку пакети було закодовано за допомогою алгоритму лінійного кодування 2 Binary 1 Quandary (2B1Q) [12], що є одним з варіантів реалізації алгоритму амплітудно-імпульсної модуляції з чотирма рівнями вихідної напруги без повернення до нульового рівня (Non Return To Zero, NRZ). Для реалізації даного кодування весь пакет було перетворено у двійковий формат, після чого отримані дані було поділено на групи по два біти в кожній. Залежно від комбінації значень бітів кодової групи їй ставився у відповідність один з чотирьох рівнів кодової напруги. Отже, закодовані відповідно до алгоритму 2B1Q дані являли собою послідовність значень напруги, що змінюється стрибкоподібно. В табл. 1 наведено відповідність між кодовою групою та кодовою напругою.

Таблиця 1. Відповідність між кодовою групою та кодовою напругою в 2B1Q

Кодова група	Кодова напруга
00	-2,5 В
01	-0,833 В
10	+2,5 В
11	+0,833 В

У ході дослідження використовувався адитивний білий гаусів шум (Additive White Gaussian Noise, AWGN). Даний тип шуму характеризувався двома параметрами: середнім значенням μ і дисперсією σ^2. Він мав рівномірну потужність за всією смугою частот. Випадковий характер шуму у часовій області в окремих випадках

спричиняв передачу символу, який був спотворений таким чином, що приймач інтерпретував його як інший символ. Якщо в передані дані вносились помилки, цілісність системи могла порушуватись.

Для оцінки ефективності системи було використано коефіцієнт бітових помилок (Bit Error Ratio, BER). В табл. 2 представлено результати розрахунку коефіцієнту бітових помилок відносно одного контейнеру.

Таблиця 2. Результати розрахунку BER для реалізованих методів стеганографії

Дисперсія	BER для методу MC-HTTP	BER для методу MC-ICMP	BER для методу MC-TCP
0,1	0	0	0
0,2	0	0	0
0,3	0,003	0,004	0,0023
0,4	0,0034	0,016	0,0093
0,5	0,038	0,041	0,03

З табл. 2 видно, що метод MC-ICMP є менш стійким до шумів, так як забезпечував більші значення коефіцієнту бітових помилок у порівнянні з іншими методами. В методі MC-HTTP при значеннях дисперсії менш ніж 0,3 приховані данні відновлювались без змін. Проте при збільшенні значення дисперсії повідомлення не відновлювалось. В методі MC-ICMP повідомлення не відновлювалось при значенні дисперсії більш ніж 0,3, а в методі MC-TCP данні можна відновити з невеликими спотвореннями при значенні дисперсії 0,4. В результаті даного порівняння методів можна зробити висновок, що найбільш стійким до шуму виявився метод мережної стеганографії, що приховує дані у TCP-заголовках.

III. Дослідження стійкості до виявлення реалізованих методів мережної стеганографії

Для дослідження стійкості до виявлення реалізованих методів мережної стеганографії було проведено аналіз впливу передачі вбудованого прихованого повідомлення на характеристики трафіка в цілому. Трафік перехоплювався та аналізувався за допомогою програми Wireshark: при включеному браузері після початку перехоплення трафіка за хвилину часу було завантажено дві http-сторінки та дві https-сторінки. Також було використано клієнтську програму YateClient, за допомогою якої було виконано п'ятисекундний дзвінок за допомогою технології Voice over Internet Protocol (VoIP). Для забезпечення цих двох сервісів було використано протокол доменної системи імен (Domain Name System, DNS), протокол захисту транспортного рівня (Transport Layer Security, TLS), протокол встановлення сесії (Session Initiation Protocol, SIP) / протокол опису сеансу зв'язку (Session Description Protocol, SDP), SIP, протокол

датаграм користувача (User Datagram Protocol, UDP), протокол передачі даних у реальному часі (Real-time Transport Protocol, RTP), протокол управління передачею в реальному часі (Real-time Transport Control Protocol, RTCP).

На рис. 4 зображена гістограма, на якій представлено динаміку зміни характеристик трафіка при використанні методу MC-HTTP. Можна побачити, що у разі передачі невеликої кількості прихованих даних (24 байти) статистичні характеристики трафіка майже не змінилися, але при передачі більшої кількості даних, значно збільшується об'єм TCP і HTTP трафіка. Кількість TCP-сегментів зростає з тієї причини, що при надсиланні кожного нового HTTP-заголовку встановлюється нове з'єднання, при якому кожний раз відбувається початок сеансу TCP.

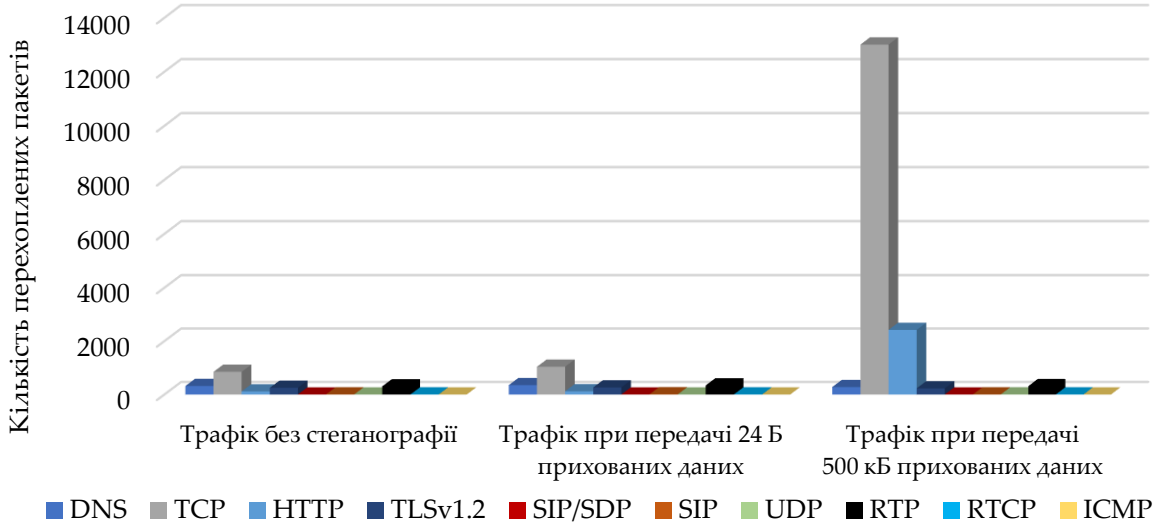

Рис. 4. Дослідження статистичних характеристик трафіка при використанні методу MC-HTTP

На рис. 5 представлено отримані результати аналізу характеристик трафіка, коли використовувався метод MC-TCP. Як і очікувалось, при невеликому розмірі прихованих даних, що передаються, об'єм TCP-трафіка збільшився незначно. В свою чергу, при зростанні об'єму прихованих даних (500 кБ) об'єм TCP-трафіка зростає майже в два рази, що робить даний метод мережної стеганографії досить помітним.

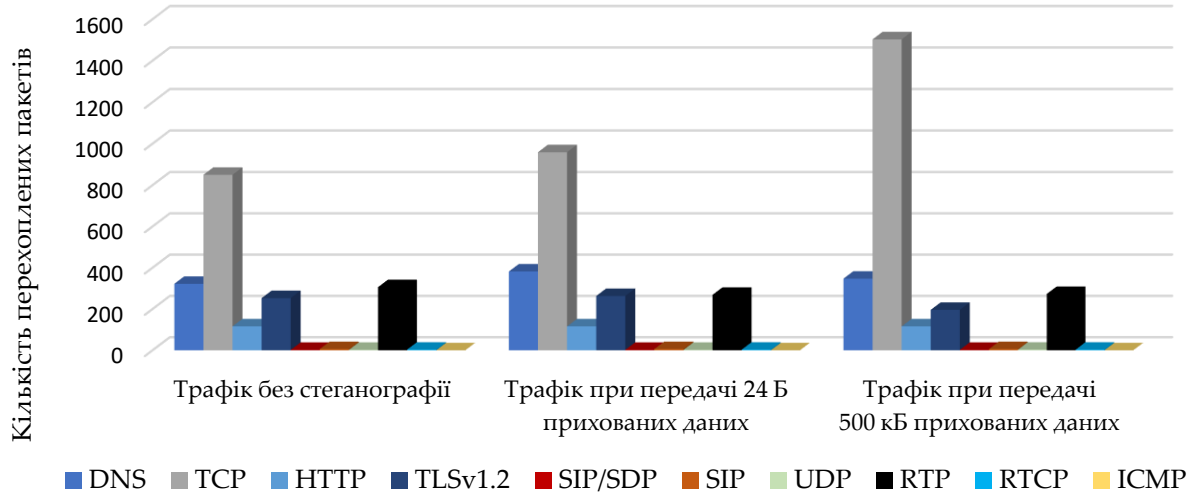

Рис. 5. Дослідження статистичних характеристик трафіка при використанні методу MC-TCP

Метод MC-ICMP досліджувався за умови вбудовування інформації у двох режимах. На рис. 6 та рис. 7 представлено статистичні характеристики трафіка, що були досліджені для режимів «Безпечний» і «Швидкий» відповідно.

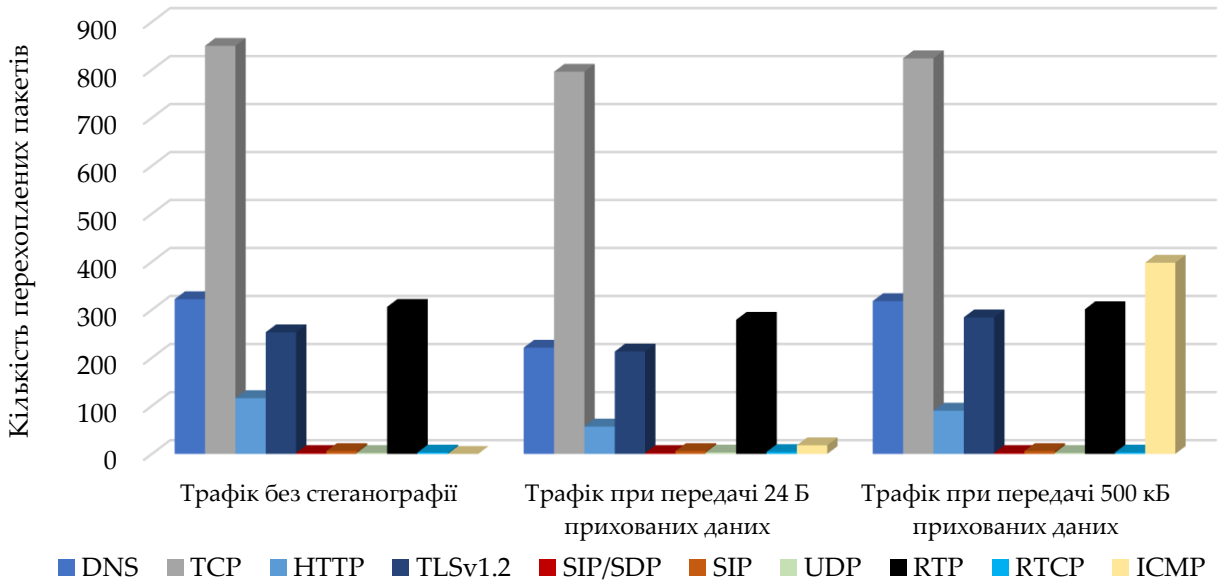

Рис. 6. Дослідження статистичних характеристик трафіка при використанні режиму «Безпечний» методу MC-ICMP

Результати показують, що кількість ICMP-пакетів значно зросла при передачі даних розміром 500 кБ в режимі «Безпечний», що не можна сказати про режим «Швидкий». У разі використання режиму «Швидкий» кількість нових ICMP-пакетів значно менша, що вказує на те, що, використовуючи даний метод для створення прихованого каналу передачі даних, можливість його виявлення значно менша.

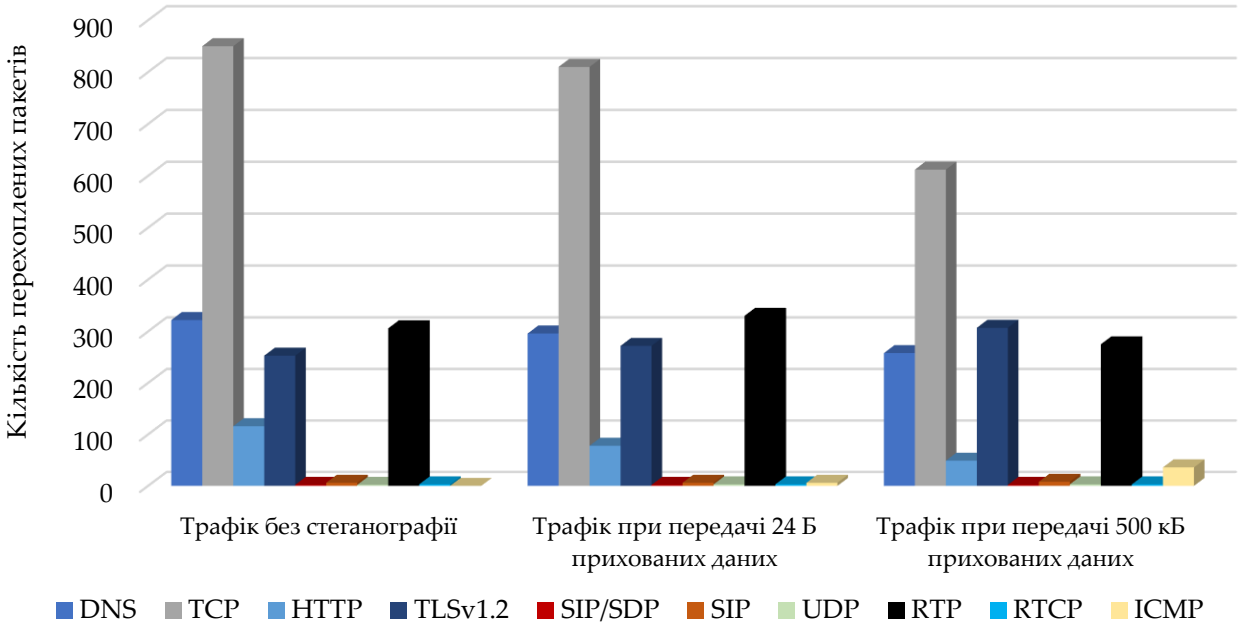

Рис. 7. Дослідження статистичних характеристик трафіка при використанні режиму «Швидкий» методу MC-ICMP

Висновки

У даній роботі було проведено програмну реалізацію та аналіз методів мережної стеганографії, що ґрунтуються на приховуванні даних, які передаються в заголовках протоколів TCP, HTTP та ICMP. Вперше досліджено ефективність зазначених методів мережної стеганографії за умови використання канального кодування даних при їх передачі каналами зв'язку з шумами та оцінено їх стійкість до виявлення, що складає наукову новизну вказаної роботи.

Результати дослідження показали, що найгіршим виявився метод MC-HTTP, який мав низьку стійкість до шуму, через те що при значенні дисперсії менше 0,3 приховане повідомлення не відновлювалось. Крім того, у разі застосування методів MC-HTTP та MC-TCP трафік різко збільшувався в декілька разів. У свою чергу, метод MC-TCP є найбільш ефективним за умови роботи каналами зв'язку з шумами: він дає можливість відновити приховане повідомлення з невеликими спотвореннями при значенні дисперсії 0,4. Проте даний метод мережної стеганографії значно програє режиму «Швидкий» методу MC-ICMP за критерієм прихованості. З огляду на специфіку застосування розглянутих методів мережної стеганографії для віддаленої автентифікації за сукупністю критеріїв стійкість до шумів / прихованість, рекомендується для використання режим «Швидкий» методу MC-ICMP.

Список літератури:

1. *Pacut A., Czajka A., Strzelczyk P.* Iris Biometrics for Secure Remote Access // Cyberspace Security and Defense: Research Issues. – 2004. – Vol. 196. – P. 259-278. – DOI: 10.1007/1-4020-3381-8.

2. *Frączek W., Szczypiorski K.* StegBlocks: Ensuring perfect undetectability of network steganography // Availability, Reliability and Security (ARES) 2015: Proceedings of the 10th International Conference. Toulouse, France, 24-27 August, 2015. – IEEE, 2015. – P. 436-441. – DOI: 10.1109/ARES.2015.22.

3. Bąk P., Bieniasz J., Krzemiński M., Szczypiorski K. Application of Perfectly Undetectable Network Steganography Method for Malware Hidden Communication // Frontiers of Signal Processing (ICFSP): Proceedings of the 4th International Conference. Poitiers, France, 24-27 September, 2018 – IEEE, 2018. – P. 34- 38. – DOI: 10.1109/ICFSP.2018.8552057.

4. *Рубан И.В., Смирнов А.А.* Возможности по использованию заголовков пакетов сетевого уровня базовой модели сетевого взаимодействия OSI/ISO в качестве стегоконтейнера // Системи озброєння і військова техніка. – 2014. – № 3(39). – С. 138-141.

5. *Mazurczyk W., Wendzel S., Villares I.A., Szczypiorski K.* On Importance of Steganographic Cost For Network Steganography // Security and Communication Networks. – 2016. – Vol. 9., No.8. – P. 781-790. – DOI: 10.1002/sec.1085.

6. *Конахович Г.Ф., Пузыренко А. Ю.* Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.

7. *Giffin J., Greenstadt R., Litwack P., Tibbetts R.* Covert Messaging through TCP Timestamps // Privacy Enhancing Technologies (PET): Proceedings of the 2nd international conference on Privacy enhancing technologies. San Francisco, CA, USA, 14-15 April, 2002 – P. 194 – 208. – DOI: 10.1007/3-540-36467-6_15.

8. *Blasco J., Hernandez-Castro J.C., de Fuentes J. M., Ramos B.* A Framework for Avoiding Steganography Usage over HTTP // Networks and Computer Applications. – 2012. – Vol. 35, Issue 1. – P. 491-501. – DOI: 10.1016/j.jnca.2011.10.003.

9. *Mazurczyk W., Wendzel S., Zander S., Houmansadr A., Szczypiorski K.* Information Hiding in Communication Networks: Fundamentals, Mechanisms, and Applications. IEEE Series on Information and Communication Networks Security, 1st Edition, Wiley, 2016. – 256 p. – DOI: 10.1002/9781119081715.

10. *Жданов О.Н., Золотарев В.В.* Методы и средства криптографической защиты информации: Учебное пособие. – Красноярск: СибГАУ, 2007. – 217 с.

11. *Панасенко С.П.* Алгоритмы шифрования. Специальный справочник. – СПб: БХВ-Петербург, 2009. – 576 с.

12. *Бортник Г.Г., Кичак В.М., Стальченко О.В.* Системи доступу: підручник. – Вінниця: ВНТУ, 2010. – 298 с.