УДК 004.772

В. І. Чистов, К. С. Васюта

АНАЛІЗ МЕТОДІВ СТЕГАНОГРАФІЧНОЇ ПЕРЕДАЧІ ДАНИХ В ІНФОРМАЦІЙНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків

Анотація. Для маскування факту передачі інформації в інформаційно-телекомунікаційних мережах, останнім часом широко застосовуються методи мережевої стеганографії, які засновані на використанні структурних властивостей протоколів моделі OSI (Open System Interconnection - мережевої взаємодії відкритих систем). Це дозволяє приховано передавати, на основі фонового трафіку, важливі дані без істотного зниження швидкості передачі даних в базовому (відкритому) каналі. При адекватному виборі властивості (групи властивостей) протоколу (протоколів) моделі OSI, методи мережевої стеганографії не дозволяють стеганоаналітіку виявити факт наявності прихованої передачі даних. Стосовно до мережевої стеганографії, процес виявлення прихованої передачі даних заснований на аналізі протокольних характеристик використовуваних протоколів моделі OSI на предмет відповідності стандартам. При використанні протоколів канального та мережевого рівнів моделі OSI, як технологічної основи для організації прихованого каналу передачі даних, приховування здійснюється за рахунок розміщення даних, факт передачі яких повинен бути прихований, в видимих полях заголовків відповідних протоколів, тобто у відкритому вигляді. У зв'язку із тим, що технологія IP-шифрування охоплює лише корисне навантаження протоколів мережевого рівня, то доцільним є використання протоколів транспортного рівня моделі OSI. На даному рівні найпоширенішим є протокол TCP, при цьому він стандартизований і використовується протиборчими сторонами, в тому числі й у військовій сфері. В роботі проведено аналіз сучасного стану прихованої передачі даних в інформаційній телекомунікаційній мережі загального користування та методів стеганографічної передачі даних в інформаційно-телекомунікаційних мережах. Також проаналізовано мережеві протоколи, які використовуються в інформаційних телекомунікаційних мережах розкрито поняття "мережева стеганографія", основним завданням якої є приховування самого факту передачі повідомлення в каналах передачі даних.

Ключові слова: інформаційно-телекомунікаційні мережі, мережева стеганографія, протокол, дейтаграма, стек TCP/IP.

Abstract. Recently, network steganography methods based on the use of structural properties of OSI (Open System Interconnection) protocols have been widely used to mask the fact of information transmission in information and telecommunication networks. This allows to covertly transmit important data based on background traffic, without significantly reducing the data rate in the base (open) channel. With the correct choice of properties (groups of properties) of the protocol (protocols) of the OSI model, the methods of network steganography do not allow the steganoanalyst to detect the fact of hidden data transmission. In network steganography, the process of detecting hidden data transmission is based on the analysis of the protocol characteristics of the used protocols of the OSI model for compliance with standards.
When using protocols of channel and network levels of the OSI model, as a technological basis for organizing a hidden data transmission channel, concealment is carried out by placing data, the fact of transmission of which must be hidden, in the visible fields of the headers of the corresponding protocols, i.e. in open form. Due to the fact that the IP encryption technology covers only the payload of network layer protocols, it is advisable to use transport layer protocols of the OSI model. At this level, the TCP protocol is the most common, and it is standardized and used by opposing parties, including the military. The paper analyzes the current state of hidden data transmission in public information telecommunications networks and methods of steganographic data transmission in information and telecommunications networks. The network protocols used in information telecommunication networks were also analyzed, the concept of "network steganography" was revealed, the main task of which is to hide the very fact of message transmission in data transmission channels.

Key words: information and telecommunication networks, network steganography, protocol, datagram, TCP/IP stack.
DOI: https://doi.org/10.31649/1999-9941-2022-54-2-61-67.

Вступ

Останнім часом, методи прихованої передачі даних в інформаційно-телекомунікаційних мережах (ІТКМ), що використовують особливості протоколів моделі OSI, набули широкої популярності. Всі протоколи моделі OSI виконані у вигляді стандартів RFC (Request For Comments) і носять рекомендаційний характер, не примушуючи до реалізації протоколів у всіх тонкощах, але основний акцент ставиться на обов'язковій наявності можливості сумісного використання усіх розроблених версій.

Множину таких методів об'єднує в собі "мережева стеганографія", основним завданням якої є приховування самого факту передачі повідомлення, що підсилює систему захисту інформації ще одним рівнем.

Мережева стеганографія − напрям комп'ютерної стеганографії, об'єктом вивчення якої, є виявлення властивостей (особливостей) протоколів моделі OSI, придатних для організації прихованих каналів передачі даних.

WLAN (Wireless Local Area Networks) стеганографія ґрунтується на методах, які використовуються для передачі стеганограмм в бездротових мережах. Практичний приклад WLAN стеганографії − це система Hidden Communication System for Corrupted Networks (HICCUPS) [2]. Основою цих методів є недоліки, властиві бездротовим мережам. Ці недоліки іноді викликають викривлення енергетичних характеристик сигналів. В результаті цих викривлень час від часу з'являються "некоректні" пакети, контрольна сума яких не збігається з заявленою. Для реалізації такого роду методів, необхідно володіти актуальною статистикою активності в мережі в використовуємому середовищі, для запобігання виникненню аномальної активності в цій самій мережі.

Lost Audio Packets Steganography стеганографія або LACK стеганографія являє собою маскування повідомлень під час розмов із застосуванням IP-телефонії. Прикладом є застосування пакетів що затри-

муються (навмисно пошкоджуються, ігноруються) приймачем або прикладною програмою, але не додатком для стеганографії [3].

У зв'язку із тим, що найпоширенішим в інтернеті є стек протоколів TCP/IP, то доречним є побудова стеганографічних каналів на його базі.

Під мережевою стеганографіэю на мережевому рівні моделі OSI (далі IP - стеганографія), розуміється група методів мережевої стеганографії, в яких основою стегоконтейнеру є невикористані (зарезервовані) місця в заголовках і полях даних IP - дейтаграм.

Відповідно моделі OSI і принципам стеганографічної передачі даних, необхідно проаналізувати можливість використання методів IP-стеганографії для досягнення мети дослідження.

Актуальність

Актуальність роботи обумовлена необхідністю забезпечення надійного прихованого обміну інформації в умовах можливих атак на стеганографічні системи передачі даних.

Мета

Аналіз сучасного стану прихованої передачі даних в інформаційній телекомунікаційній мережі загального користування та методів стеганографічної передачі даних в інформаційних телекомунікаційних мережах.

Задачі

1. Аналіз сучасного стану прихованої передачі даних в інформаційній телекомунікаційній мережі загального користування.
2. Аналіз мережевих протоколів, які використовувалися в інформаційних телекомунікаційних мережах.
3. Аналіз методів стеганографічної передачі даних в інформаційних телекомунікаційних мережах.
4. Аналіз методів побудови мережевих стеганографічних каналів та можливих атак на стеганографічні системи передачі даних.

Розв'язання задач

Призначенням мережевого рівня моделі OSI є організація зв'язку станцій, що з'єднані з різними логічними каналами та/або роз'єднані другими логічними каналами. Функцією даного рівня в першу є вибір оптимальної черговості каналів між станціями у процесі передачі пакету (протокольного блоку даних на рівні мережі). Історино склалося, що перші мережеві протоколи розроблялися з метою використання їх в глобальних мережах (ГМ). Це можна обгрунтувати великою кількістю вузлів в ГМ – однією з найсуттєвіших проблем в роботі є досягнення ефективної маршрутизації. Одночасно з'явився термін стратегій передачі – данограма віртуальних каналів. Данограмна транспортна мережа – це мережа що передає незалежні пакети даних − данограми. Принцип роботи такої мережі схожий на роботу звичайної пошти – листи ніяк не пов'язані один з одним і можуть загубитися.

Перед тим, як почати передачу даних в мережі віртуальних каналів між процесами налагоджується віртуальний канал, який функціонує впродовж усього сеансу зв'язку. Роботу мережі віртуальних каналів можна порівняти з роботою міської телефонної мережі. Насамперед налагоджується канал зв'язку, послідовність інформації, яка передається, зберігається. Данограмна транспортна мережа відправляє пакети набагато швидше за мережу віртуальних каналів, але не забезпечує гарантії того, що пакет дійде до адресата (черговість надходження пакетів випадкова; є ймовірність втрати певних пакетів та перенасиення буферів). Мережа віртуальних каналів повільніша, але дає гарантія того, що пакет дійде до адресату (зберігається черговість надходження пакетів; відбувається припинення надходження пакетів від джерела якщо вузол перенасичений).

Одним із прикладів використання полів заголовків протоколу IP є метод, заснований на модифікації полів "identification" і "fragmentoffset" [4] – [7] при встановленому прапорі "DF" (do not fragment − НЕ фрагментувати). Якщо встановлений прапор DF, модуль IP не стане фрагментувати дейтаграмму. Замість цього дейтаграма відкидається і по протоколу ICMP генерується повідомлення про помилку – "необхідна фрагментація, але встановлений прапор заборони фрагментації", яке посилається відправнику пакета. Якщо IP-дейтаграмма була фрагментована, то кожен фрагмент стає окремим пакетом зі своїм власним IP-заголовком. Такі пакети маршрутизуються незалежно і, як наслідок, фрагменти дейтаграми можуть приходити в точку призначення з порушенням їх черговості. Однак в IP-заголовках фрагментів міститься вся необхідна інформації для їх правильного складання в пункті призначення.

Фрагментація в IP виконується незалежно від транспортного рівня моделі OSI. Не дивлячись на таку прозорість, фрагментація може привести до небажаних наслідків, які позначаються на рівнях вище IP.

Справа в тому, що через втрату одного фрагмента потрібно передати повторно всю дейтаграмму, а оскільки в самому протоколі IP не передбачені таймаут і повторна передача, то ці функції повинні бути покладені на вищі рівні. Протокол TCP здійснює повторну передачу з таймаут, а UDP – ні [8]. Якщо виявиться, що втрачено певну частину сегмента TCP, то з таймаут буде повторено передачу всього сегменту TCP. Повторна передача окремого фрагмента IP-дейтаграми неможлива в принципі. Дійсно, якщо

фрагментацію зробив не хост-джерело дейтаграми, а один з проміжних маршрутизаторів, то джерело не може знати, яким саме чином було виконано розбиття на фрагменти. Вже з однієї цієї причини бажано вживати заходів для запобігання фрагментації. Фрагментація пакетів в IP є штатною ситуацією, тому використання раніше зазначених полів заголовків IP-пакетів як стегоконтейнер є цілком доцільним методом для організації прихованого каналу зв'язку. При правильному виборі розміру пакету можна домогтися виконання наступної умови:

$$L \le PMTU, \tag{1}$$

де L – довжина пакету;
MTU – maximum transmission unit (максимальний розмір корисного блоку даних);
$PMTU$ – MTU траси від джерела до кінцевого адресата пакета.

$$PMTU = \min MTU_i, \tag{2}$$

де $\min MTU_i$ – мінімальне значення MTU серед інтерфейсів маршруту, по якому пройде пакет.

При виконанні умови (1) необхідність фрагментації пакетів на інтерфейсах маршруту відсутня. Це означає, що поля “identification”, “flags”, “fragmentoffset” оброблятися проміжними маршрутизаторами не будуть. В такому випадку, при використанні цих полів як стегоконтейнер, інформація вбудована в нього буде передана без змін. Ємність такого стегоконтейнер може становити до 32 біт.

Використання даного методу для досягнення мети дослідження недоцільно, так як порушується стандартні вимоги до протоколу IP, а приховувані дані розташовуються в заголовках IP-пакетів в явному вигляді.

На сучасному етапі метод “DF”, є єдиним описаним методом мережевий стеганографії, застосовуваний на мережевому рівні моделі OSI. Але слід зазначити, що можуть існувати й інші поля заголовка IP-дейтаграми, які можливо використовувати для організації прихованих каналів обміну інформацією в інформаційно-телекомунікаційних мережах (ІТКМ). До таких поліф відносяться опції IPv4, розмір яких може досягати 40 байт (рис. 1).

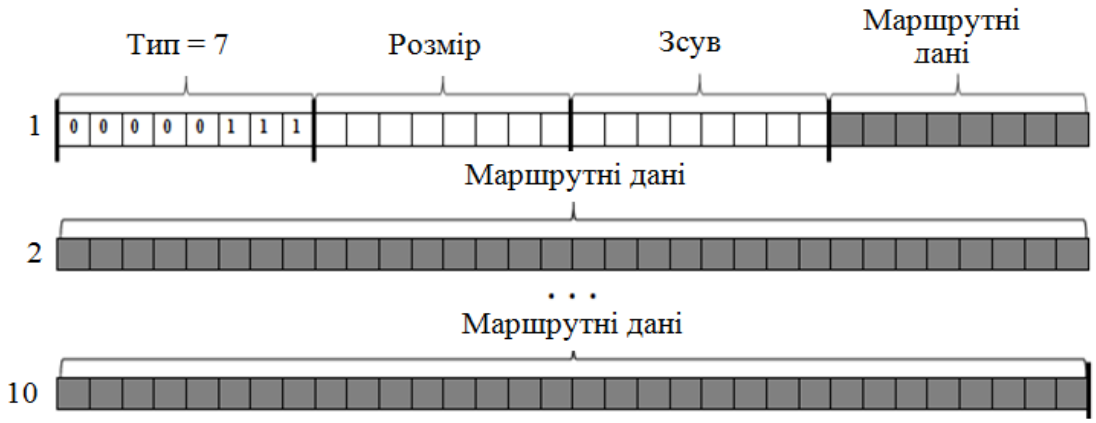

Рисунок 1 – Вид поля опції “Запис маршруту”

До опцій, які можна використовувати з метою прихованої передачі даних можна віднести наступні: “запис маршруту”, “часовий штамп”, “маршрутизація від джерела”. Спільною рисою перерахованих опцій є виділення достатнього (до 40 октетів) місця в заголовку IP-пакету для їх реалізації. Поле опцій є необов'язковим, а їх підтримка повинна реалізуватися у всіх модулях IP (на хостах і шлюзах). Використання опцій визначається для окремої дейтаграми, а не для реалізації модуля. Теоретична основа “методу опцій” описана на прикладі опцій “запис маршруту” і “часовий штамп”. При використанні в якості стегоконтейнера поля для запису проміжних вузлових пристроїв (опція “запис маршруту” або Record Route (RR)), можливо досягти розміру контейнера до 37 байт. Опція RR призначена для запису в заголовок дейтаграми IP-адрес вихідних інтерфейсів маршрутизаторів, що пересилали дану дейтаграмму. При використанні даної опції представляється можливим записати до 9 IP-адрес. Це пов'язано із тим, що в IP-дейтаграми відведено до 40 байтів для опису опцій, 3 з яких - заголовок опції RR.

Опція починається з поля типу опції, за яким слід поле довжини, що враховує Type = 7 повний розмір опції (тип, розмір, зсув, маршрутні дані). Третій октет містить покажчик на октет, з якого починається наступна область запису маршруту. Зсув відраховується від початку опції, тому значення покажчика

не може бути менше 4. Хост, що відправляє дейтаграму, повинен забезпечити достатній простір (розмір опції) для запису адрес на шляху до одержувача. У вихідній дейтаграмі поля адрес повинні мати нульові значення.

Якщо поле маршрутних даних вже заповнено (значення покажчика перевищує розмір опцій), дейтаграмма пересилається без подальшого запису маршруту. Якщо простір, що залишився для запису маршрутних даних недостатньо для включення адреси, дейтаграма розглядається як помилкова та відкидається. У таких випадках відправник дейтаграм може бути переданий ICMP повідомлення про помилку в параметрах. Тому, якщо на передаючій стороні записати приховану інформацію в поля, призначені для запису IP-адрес вихідних інтерфейсів, а для полів “зсув” та “розмір” буде виконано умова (1), то ця дейтаграма буде доставлена без змін.

$$L_p < L_1, \tag{3}$$

де L_p – октет маршрутних даних, починаючи з якого буде оброблятися наступний параметр, який застосовується в опорній опції;

L_1 – значення розміру опції (в октетах), з урахуванням полів типу та розміру опції, а також октету покажчика та власне опції.

Для реалізації описаного способу, необхідно мати встановлене програмне забезпечення на стороні відправника та одержувача інформації, що приховується. Ситуація при якій поточний маршрутизатор не зможе записати необхідну в опції інформацію, є штатною для протоколу IP [9]. Подібний підхід можливо застосувати й до решти опцій IP − SR (source route − маршрутизація від джерела), TS (time stamp − часовий штамп), при виконанні умови (3). Для запису, необхідних даних для опцій “маршрутизація від джерела” і “запис маршруту” відводиться 37 байт, а для опції “часовий штамп” − 36 байт в кожній IP-дейтаграмі, що є ємністю такого стегоконтейнеру. Менша ємність стегоконтейнера, при використанні в якості опорної, опції “часовий штамп” (рис. 2), обумовлена тим, що в четвертому октеті поля опції зберігається інформація, необхідна для виконання призначення опції.

Поле “надлишок” показує кількість маршрутизаторів, які не змогли виконати необхідну операцію. Поле “прапор” може набувати таких значень:

- 0 − проміжні маршрутизатори повинні записувати тільки часові мітки, які зберігаються в послідовності 32-бітових слів;
- 1 − перед кожною позначкою поміщається IP-адреса, яка реєструє мітку модуля;
- 3 − поля адрес вказуються заздалегідь і модуль IP поміщає часову мітку тільки в тому випадку, коли адреса цього модуля вказана наступною у списку адрес опції.

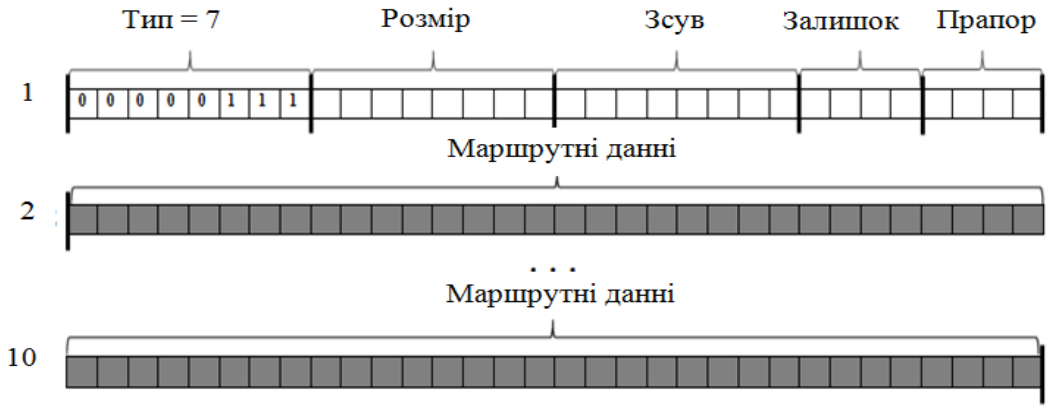

Рисунок 2 – Вид поля опції “Часовий штамп”

Використання даного методу для досягнення мети дослідження недоцільно з огляду на те, що приховувані дані розташовуються в полі опцій заголовків IP-пакетів в явному вигляді.

Під мережевою стеганографією на транспортному рівні моделі OSI (далі TCP − стеганографія), розуміється група методів мережевої стеганографії, в яких основою стегоконтейнер є технологічні особливості протоколів транспортного рівня моделі OSI.

Одним з представників методів TCP − стеганографії, є метод на основі управління довжиною поля корисного навантаження протоколу TCP.

Суть методу DL (DataLength) полягає в тому, що секретний текст представляють у вигляді послідовності біт, яку передають одержувачу частинами. Це пов'язано з тим, ємність такого стегоконтейнера

обмежена і в разі необхідності передачі великої кількості інформації, що приховується, її необхідно розбивати на порції. Стегоконтейнером є довжина поля даних кожного інформаційного TCP-сегмента, представлена в двійковій формі обчислення. В [10] задекларовано, що у випадку хендшейку, на початку TCP-сесії, сторони заздалегідь не домовляються про допустиме максимальне значеннях MSS (Maximum Segment Size − максимальний розмір сегменту), то його значення приймається за замовчуванням рівним 536 байтам. В роботі [11] автор пропонує приховано передавати інформацію, представлену у вигляді тексту, де кожній букві відповідає двійкова послідовність з прийнятною таблицею кодування. Для даного методу це може бути кодування windows-1251 (таблиця CP1251). Це кодування є 8-розрядною. Довжина поля даних TCP-сегмента наступна:

$$DL = MSS - L_4 = 536 - 20 = 516, \tag{4}$$

де L_4 − довжина заголовку TCP-сегмента без опцій.

В цьому випадку, кількість розрядів двійкового значення довжини відкритого тексту (ДВТ) відповідає

$$L_{OT} = L_m - 1, \tag{5}$$

де $L_m = \log_2(DL) \approx 9,07$, при округленні до найближчого більшого відповідає 10 розрядів.

TCP-дамп процесу передачі даних, заснованому на методі DL, зображений на рис.3. У методі закладена необхідність отримання підтверджень про доставку кожного сегмента до відправки наступного. Для цього використовується прапор PUSH (прапор проштовхування даних).

TCP: 50240 > scp-config [SYN] Seq=0 Win=32792 Len=0 MSS=16369 TSV=528243 TSER=0 WS=6
TCP: scp-config > 50240 [SYN, ACK] Seq=0 ACK=1 Win=32768 Len=0 MSS=16369 TSV=528243 TSER=528243
TCP: 50240 > scp-config [ACK] Seq=1 Ack=1 Win=32832 Len=0 TSV=528243 TSER=528243
TCP: 50240 > scp-config [PSH, ACK] Seq=1 Ack=1 Win=32832 Len=**116** TSV=529497 TSER=528243
TCP: scp-config > 50240 [ACK] Seq=1 ACK=117 Win=32768 Len=0 TSV=529497 TSER=529497
TCP: 50240 > scp-config [PSH, ACK] Seq=117 Ack=1 Win=32832 Len=**101** TSV=529523 TSER=528497

Рисунок 3 – TCP-дамп при передачі даних по методу DL

Для досягнення більшої стійкості до виділення прихованої інформації автор використовує криптографію. А саме, використання шифрування самого приховуваного тексту, розсіювання приховуваного тексту в двійкових значеннях довжини полів даних TCP-сегментів, задіяння секретної маски, що представляє собою двійкову послідовність, поодиноке значення яких відповідає інформаційним, а нульові – сегментам, що камуфлюють. Даний метод має можливість передавати будь-які дані, які можливо уявити 8 розрядами в двійковій системі числення. Це може бути: текст, зображення, аудіозапис, відеозапис.

В [5] запропоновано метод, який дозволяє передавати приховувані дані всередині пакетів TCP, що відправляються нібито для виправлення невдало переданих даних. Цей алгоритм отримав назву RSTEG (Retransmission Steganography − стеганографія в повторній передачі).

Описаний метод прихованої передачі даних для досягнення мети дослідження непридатний, тому що порушуються стандартні вимоги до протоколу TCP, в частині оптимального використання канальних ресурсів, і знижується більш ніж в два рази швидкість передачі даних в базовому віртуальному каналі передачі даних.

Також, викликає інтерес метод TCP-стеганографії заснований на управлінні ретрансляції фрагментів протоколу TCP − RSTEG.

Одержувач приймає початковий пакет і відправляє повідомлення про успішний прийом. Замість того, щоб передати наступний пакет, відправник ігнорує повідомлення про успішний прийом і відправляє

пакет з прихованим змістом, але цей пакет має такий же ідентифікатор, що і попередній, а системи аналізу мережевого трафіку вже не перевіряють повторний пакет.

Для всіх систем мережевого захисту новий пакет з секретним вмістом не відрізняється від початкового пакету, в якому не містилося нічого підозрілого. Коли повторно переданий пакет досягає приймаючої сторони, з нього витягується прихована інформація.

Висновки

В даній роботі основну увагу приділено аналізу сучасного стану прихованої передачі даних в інформаційній телекомунікаційній мережі загального користування та методів стеганографічної передачі даних в інформаційно-телекомунікаційних мережах.

Проведено аналіз мережевих протоколів, які використовуються в інформаційних телекомунікаційних мережах розкрито поняття "мережева стеганографія", основним завданням якої є приховування самого факту передачі повідомлення в каналах передачі даних.

Окремого розгляду вимагають питання дослідження можливих атак на стеганографічні системи (СГС) передачі даних та розробки пропозицій щодо покращення показників ефективності щодо прихованості управління при передачі даних в інформаційній телекомунікаційній мережі, що і буде напрямком подальших досліджень.

Список літератури

[1] W. Mazurczyk, K. Szczypiorski, "Steganography of VoIP Streams," Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications. [Online]. Available: http://arxiv.org/pdf/0805.2938v1/. Accessed on: May 14, 2022.

[2] K. Szczypiorski, "HICCUPS: Hidden Communication System for Corrupted Networks," Warsaw University of Technology, Institute of Telecommunications. [Online]. Available: https://goo.gl/ZU9tDM. Accessed on: May 4, 2022.

[3] D. Kundur, K. Ahsan, "Practical Internet Steganography: Data Hiding in IP," Proc. Texas Wksp. Securit of Information Systems, Apr. 2003. [Online]. Available: http://arxiv.org/pdf/1207.0917.pdf. Accessed on: October 10, 2021.

[4] E. Cauich, R. Gómez Cárdenas, R. Watanabe, "Data Hiding in Identification and Offset IP Fields," in *Proceedings of 5th International School and Symposium of Advanced Distributed Systems (ISSADS)*, jan. 2005, pp. 118-125. [Online]. Available: https://goo.gl/2bjjXZ. Accessed on: October 29, 2021.

[5] Theodore G. Handel, Maxwell T. Sandford II, *Hiding data in the OSI network model*. [Online]. Available: https://goo.gl/hz8X1m. Accessed on: September 20, 2021.

[6] О. Ю. Пескова, Г. Ю. Халабурда, "*Применение сетевой стеганографии для защиты данных, которые передаются по открытым каналам Интернет*," *Объединённая конференция "Интернет и современное общество"*. [Електроний ресурс]. Режим доступу: https://goo.gl/qtC7D3. Дата звернення: Серп. 19.2021.

[7] Е. О. Саватєєв, "*Построение стеганографической системы на базе протокола IPv4*". [Електроний ресурс]. Режим доступу: https://goo.gl/wUogUB. Дата звернення: Серп. 30.2021.

[8] "Internet protocol – DARPA Internet Program Protocol Specification". RFC-768. User Datagram Protocol, 28 August 1980. [Online]. Available: https://tools.ietf.org/html/rfc768. Accessed on: October 22, 2021.

[9] "Internetprotocol – DARPA Internet Program Protocol Specification" RFC-791 USC / Information Sciences Institute, September 1981 [Online]. Available: http://www.rfc-base.org/txt/rfc-791.txt. Accessed on: October 21, 2021.

[10] "Internet protocol – DARPA Internet Program Protocol Specification" RFC-793 USC / Transmission control protocol, September 1981 [Online]. Available: https://tools.ietf.org/html/rfc793. Accessed on: October 21, 2021.

[11] В. П. Орлов, "Методы скрытой передачи информации в телекомуникационных сетях," дис. канд. техн. наук: 05.12.13. Самара, 2012.

Стаття надійшла: 20.05.2022.

References

[1] W. Mazurczyk, K. Szczypiorski, "Steganography of VoIP Streams," Warsaw University of Technology, Faculty of Electronics and Information Technology, Institute of Telecommunications. [Online]. Available: http://arxiv.org/pdf/0805.2938v1/. Accessed on: May 14, 2022.

[2] K. Szczypiorski, "HICCUPS: Hidden Communication System for Corrupted Networks," Warsaw University of Technology, Institute of Telecommunications. [Online]. Available: https://goo.gl/ZU9tDM. Accessed on: May 4, 2022.

[3] D. Kundur, K. Ahsan, "Practical Internet Steganography: Data Hiding in IP," Proc. Texas Wksp. Securit of Information Systems, Apr. 2003. [Online]. Available: http://arxiv.org/pdf/1207.0917.pdf. Accessed on: October 10, 2021.

[4] E. Cauich, R. Gómez Cárdenas, R. Watanabe, "Data Hiding in Identification and Offset IP Fields," in *Proceedings of 5th International School and Symposium of Advanced Distributed Systems (ISSADS)*, jan. 2005, pp. 118-125. [Online]. Available: https://goo.gl/2bjjXZ. Accessed on: October 29, 2021.
[5] Theodore G. Handel, Maxwell T. Sandford II, *Hiding data in the OSI network model*. [Online]. Available: https://goo.gl/hz8X1m. Accessed on: September 20, 2021.
[6] O. Y. Peskova, G. Y. Halaburda, "Primenenie setevoj steganografii dlya zashchity dannyh, kotorye peredayutsya po otkrytym kanalam Internet," *Conference " Internet i sovremennoe obshchestvo"*. [Online]. Available: https://goo.gl/qtC7D3. Accessed on: Aug. 19.2021 [in Russian].
[7] E. O. Savateev, "Postroenie steganograficheskoj sistemy na baze protokola IPv4," [Online]. Available: https://goo.gl/wUogUB. Accessed on: Aug. 30.2021 [in Russian].
[8] "Internet protocol – DARPA Internet Program Protocol Specification". RFC-768. User Datagram Protocol, 28 August 1980. [Online]. Available: https://tools.ietf.org/html/rfc768. Accessed on: October 22, 2021.
[9] "Internetprotocol – DARPA Internet Program Protocol Specification" RFC-791 USC / Information Sciences Institute, September 1981 [Online]. Available: http://www.rfc-base.org/txt/rfc-791.txt. Accessed on: October 21, 2021.
[10] "Internet protocol – DARPA Internet Program Protocol Specification" RFC-793 USC / Transmission control protocol, September 1981 [Online]. Available: https://tools.ietf.org/html/rfc793. Accessed on: October 21, 2021.
[11] V. P. Orlov, "Metody skrytoj peredachi informacii v telekomunikacionnyh setyah", cand. of technical sciences thesis: 05.12.13. Samara, 2012 [in Russian].

Відомості про авторів

Чистов Валерій Ігорович – ад'юнкт науково-організаційного відділу Харківського національного університету Повітряних Сил імені Івана Кожедуба.

Васюта Костянтин Станіславович – доктор технічних наук, професор, заступник начальника Харківського національного університету Повітряних Сил імені Івана Кожедуба з навчальної роботи.

V. I. Chystov, K. S. Vasiuta

ANALYSIS OF THE CURRENT STATE OF HIDDEN DATA TRANSMISSION IN THE PUBLIC INFORMATION TELECOMMUNICATIONS NETWORK

Ivan Kozhedub Kharkiv National University of the Air Force, Kharkiv