УДК 004.056:003.26

АНАЛІЗ ТА ПОРІВНЯЛЬНІ ДОСЛІДЖЕННЯ МЕТОДІВ МЕРЕЖНОЇ СТЕГАНОГРАФІЇ

О.О. КУЗНЄЦОВ, В.А. ТИМЧЕНКО, Б.С. ДУБРОВНИЙ

Розглядаються можливості стеганографічних методів захисту інформації, побудова яких заснована на використанні особливостей функціонування мережного стеку протоколів передачі даних сімейства TCP/IP (Transmission Control Protocol / Internet Protocol). Досліджуються різні методи мережної стеганографії, які засновані: на кодуванні вмісту інформаційних пакетів; на маніпуляціях потоку переданих пакетів; гібридні методи. Обґрунтовуються перспективні напрямки подальших досліджень із вдосконалення методів мережної стеганографії для їх використання з метою приховування факту існування скритої передачі інформації.

Ключові слова: мережна стеганографія, протоколи сімейства TCP/IP.

ВСТУП

У сучасному світі надзвичайно велику роль у виробничій, торгівельній, сервісній та інших сферах економіки та у житті людини відіграє інформація. Тому для забезпечення доступності, цілісності та конфіденційності інформації широко використовуються різноманітні криптографічні та стеганографічні методи захисту інформації [1, 2].

Нагадаємо, що криптографія – це наука, що вивчає методи та засоби для приховування значення змісту даних, що передаються [1, 2]. Стеганографія має на меті ті ж цілі, однак приховує при цьому сам факт існування таємного повідомлення в даних. Хоча методи стеганографії використовуються вже тривалий час, але завдяки розвитку комп'ютерної техніки і телекомунікаційних технологій, отримав стрімкий розвиток новий вид прихованої передачі даних – цифрова стеганографія [2], а з розвитком і вдосконаленням технологій передачі інформації комп'ютерними мережами, з'являються нові різноманітні методи непомітної передачі інформації – мережна стеганографія [3].

У мережній стеганографії роль носія виконує переданий по мережі пакет або сукупність пакетів даних [3, 4]. Це відкриває великі перспективи для тих, хто хоче непомітно передавати повідомлення через будь-які кордони і створює небезпеку для установ, що займаються захистом інформації від несанкціонованого витоку інформації. У загальному вигляді, мережна стеганографія є сімейством методів з модифікації даних у заголовках мережних протоколів і у полях корисного навантаження пакетів, зміни структури передачі пакетів та гібридних методів у тому чи іншому мережному протоколі [4].

Основні параметри мережної стеганографії – це пропускна здатність прихованого каналу, ймовірність виявлення і стеганографічна стійкість [4]. Пропускна здатність – обсяг секретних даних, який може бути відправлений за одиницю часу. Ймовірність виявлення визначається за можливістю виявлення стеганографії на певному носії. Найбільш популярний спосіб виявлення прихованого повідомлення – це аналіз статистичних властивостей отриманих даних і порівняння їх з типовими значеннями для цього носія. Стеганографічна стійкість характеризує ступінь зміни носія після впливу на нього стеганометоду.

Метою даної статті є аналіз методів прихованої передачі інформації з використанням мережної стеганографії, які є перспективними на сьогодні.

1. ПРОТОКОЛИ СІМЕЙСТВА TCP/IP

Термін «мережна стеганографія» уперше ввів Кжиштоф Джипйорскі (Krzysztof Szczypiorski) у 2003 році [3]. Хоча цей метод стеганографії з'явився відносно недавно, він має таку саму структуру стеганосистеми як і класична або цифрова стеганографія. Особливістю є те, що як контейнер, в якому приховано передається конфіденційне повідомлення, виступають певні комунікаційні компоненти: правило змін довжини пакетів або процедура перепопиту помилкових даних; службові поля пакетів даних, прапорці та ін. [3–11]. Розглянемо особливості побудови найбільш поширених мережних протоколів TCP/IP, які можуть бути застосовані для реалізації стеганографічних методів захисту інформації.

Стек сімейства протоколів TCP/IP є відкритим комунікаційним протоколом. Відкритість означає, що він забезпечує зв'язок у будь-яких комбінаціях пристроїв незалежно від того, наскільки вони різняться на фізичному рівні [6].

Переваги TCP/IP. Протокол TCP/IP забезпечує можливість міжплатформових мережних взаємодій. Наприклад, мережа під управлінням Windows може містити робочі станції Unix, і навіть інші мережі нижчого порядку. TCP/IP володіє такими характеристиками [6]:

– ефективні засоби відновлення після збоїв;

– можливість додавання нових мереж без переривання поточної роботи;

– стійкість до помилок;

– незалежність від платформи реалізації;

– низькі непродуктивні витрати на пересилання службових даних.

Протоколи TCP і IP спільно управляють потоками даних (як вхідними, так і вихідними)

у мережі. Але, якщо протокол IP тільки передає пакети, не звертаючи уваги на результат, TCP повинен простежити за тим, щоб пакети прибули в належне місце. Зокрема, TCP відповідає за виконання таких завдань [6]:

– відкриття та закриття сеансу;
– управління пакетами;
– управління потоком даних;
– виявлення та обробка помилок.

Розглянемо структуру заголовка IP версії 4, яку наведено на рис. 1 (на рис. 2 наведено структуру заголовка IP версії 6).

Поле версії. Визначає поточну версію IP, реалізовану мережною станцією.

Тип служби. Складається з таких полів: пріоритет, затримка, пропускна здатність і надійність [7].

Загальна довжина. Довжина дейтаграми (не пакета), виміряна в байтах (довжина цього поля становить 16 біт, отже, область даних IP-дейтаграми може мати довжину 65535 байт).

Поле ідентифікації. Показує, які фрагменти належать одній і тій самій дейтаграмі, щоб їх не переплутати. Приймаючий IP-рівень використовує це поле і IP-адреса джерела, щоб визначити, які фрагменти належать одній дейтаграмі [7].

Прапорці. Показує, чи мають ще надійти фрагменти або дані для поточної дейтаграми більше не передаватимуться (останній фрагмент), а також фрагментувати чи ні дейтаграму (біт відмови від фрагментації) [7].

Зсув фрагмента. Це поле використовується приймачем для зворотного збирання фрагментованою дейтаграмою.

Час життя. Визначає інтервал часу, протягом якого дейтаграмі дозволено перебувати у мережі.

На рис. 3 показано поля заголовка TCP у тому вигляді, у якому вони інкапсулюються в заголовок IP-дейтаграми [7]:

Порт-джерело. Номер порту передавальної станції.

Порт-приймач. Номер порту приймаючої станції.

Порядковий номер. Значення, присвоєне дейтаграмі TCP, визначає номер стартового байту пакета, якщо тільки не встановлений біт SYN. Якщо ж цей біт встановлений, то порядковий номер є початковим порядковим номером (ISN) і перший байт даних дорівнює ISN + 1.

Номер підтвердження. Значення, надіслане цільовою станцією станції відправника, яке підтверджує прийом переданого раніше пакета (пакетів).

Зсув даних. Визначає довжину заголовка TCP (тобто кількість 32-бітових слів у заголовку TCP).

Резерв. Зарезервовано для майбутнього використання.

Біти управління [7]:

URG – індикатор міцності, застосовується при посиланні повідомлення цільового вузла, що очікує прийом екстреної інформації.

ACK – якщо даний біт встановлений, отже, пакет містить підтвердження надісланої раніше дейтаграми.

PSH – функція виштовхування, негайне відсилання даних після зчитування сегмента (даних цього пакета).

RST – обрив з'єднання з метою відмови на запит з'єднання.

SYN – служить для ініціалізації та установки порядкового значення.

FIN – означає, що в ініціатора з'єднання даних більше немає.

Рис. 1

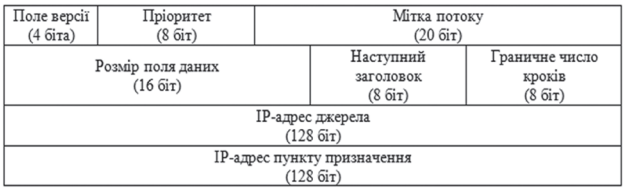

Рис. 2

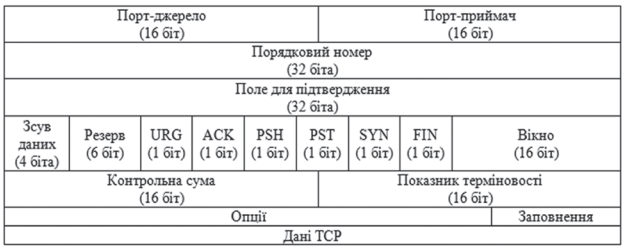

Рис. 3

Вікно. Кількість октет даних, починаючи з октету, зазначеного у полі підтверджень, які відправник сегмента може прийняти.

Контрольна сума. Значення, призначене для виявлення помилок.

Показник термінових даних. Задає порядковий номер байта, наступного за рядковими даними.

Опції. Поле змінної довжини, дозволяє використати такі опції TCP: кінець списку опцій, немає операції і максимальний розмір сегменту.

Розглянемо методи мережної стеганографії, які реалізуються з використанням особливостей функціонування протоколів TCP/IP, обґрунтуємо їх використання для приховування факту існування скритої передачі інформації.

2. АНАЛІЗ МЕТОДІВ TCP/IP СТЕГАНОГРАФІЇ

Методи мережної стеганографії можна розділити на три групи [4]:

– методи, що змінюють вміст інформаційних пакетів;

– методи, які засновані на маніпуляціях над потоком переданих пакетів;

– гібридні методи (об'єднання методів двох попередніх груп).

Типові методи мережної стеганографії включають зміну властивостей одного з мережних протоколів. Крім того, може використовуватися взаємозв'язок між двома або більше різними протоколами з метою більш надійного приховування факту передачі таємного повідомлення [8, 9].

Розглянемо більш докладно наведені методи мережної стеганографії, проведемо дослідження їх можливостей щодо прихованої передачі інформаційних повідомлень.

2.1. Методи модифікації вмісту інформаційних пакетів. Це найпростіша група методів, сутність яких полягає в записі інформаційного повідомлення у різні поля пакетів даних. Наприклад, у роботах [10] розглянуто *методи зміни даних у полях заголовків мережного протоколу*. Приклад подібного методу, заснований на модифікації полів заголовків протоколу IP, наведено на рис. 1 та на рис. 2. У даному методі розглядається модифікація заголовка IPv4 не використовуваних полів для створення прихованого каналу. Оскільки поле «Ідентифікатор» в IP заголовку може містити 16 біт інформації, в полі «Прапорці» доступний 1 біт, а в полі «Номер послідовності» в TCP заголовку доступний обсяг інформації в 32 біта можна зробити висновок, що загальна пропускна здатність стеганографії дорівнює 49 бітам. Але слід зазначити, що в даному методі ми використовуємо поле «Ідентифікатор» для передачі зашифрованого ключа в стеганограмі, який служить для вилучення секретної інформації з поля «Номер послідовності», а біт в полі «Прапорці» використовується як мітка.

Методи модифікації полів заголовків IP і TCP володіють певними особливостями, які виділяють їх на тлі інших методів [10]:

– як носії стеганограми використовуються найпоширеніші й стандартні протоколи;

– у сумі дають пропускну здатність 49 біт за 1 пакет;

– реалізуються на будь-якій операційній системі, реалізація не вимагає довгих налаштувань і підготовок;

– зміни в пакеті не вплинуть на його поведінку в мережі, у випадку, якщо він не буде фрагментований.

Розглянемо алгоритм вбудовування інформації в поле «Ідентифікатор» (див. рис. 4), де X (0 або 1) біти представляють ідентифікатор пакета IP і C (0 або 1) біти є секретним символом для вбудовування.

Алгоритм вбудовування. На вхід подаємо вибрані пакети та конфіденційну інформацію. Для початку прочитаємо символ впровадженого файла (наприклад, secret.txt), після зчитування перетворюємо символ в еквівалентне значення ASCII. Отриманий пакет на вході, зчитуємо значення 16-розрядного поля ідентифікації, скинувши молодші 8-розрядів (Tem = {Поле ID} AND {Маска 65280}) та додаємо секретний 8-бітний ASCII ({New IP ID} = Tem + Ch). Після закінчення повертаємося до пакета для ін'єкції з {New IP ID} області. На виході отримуємо стегано-пакет [10].

Рис. 4

Алгоритм виймання (див. рис. 5). На вході отримуємо стегано-пакет, з якого зчитуємо 16 біт інформації із поля ідентифікації при цьому скинемо найбільш значущі 8 біт інформації. Отримане значення перетворюємо на символ який еквівалентний в ASCII. Отриманий символ, збережемо у файл (recsecret.txt). У даному випадку стегано-ключ – це правило виймання інформації або інвертована маска вбудовування [10].

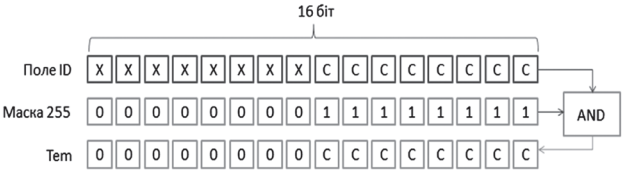

Рис. 5

До переваг методів зміни даних у полях заголовків мережного протоколу слід віднести [9]: простоту реалізації; високу стеганографічну пропускну здатність; не потрібно ніякої синхронізації між відправником та отримувачем. Як недоліки слід зазначити такі: погіршення якості роботи протоколу; легкість виявлення.

Іншим прикладом методів модифікації вмісту інформаційних пакетів є методи, що безпосередньо *змінюють власні дані пакетів* [4].

У цьому випадку застосовуються різні алгоритми цифрових водяних знаків, мовних кодеків та інших стеганографічних технік приховування даних [2].

Наприклад, до цієї групи можна віднести метод, який заснований на зміні розміру пакетів переданих даних. Особливість цього методу полягає у вбудовуванні інформації у розмір пакета даних, тобто саме розмір пакета міститиме інформацію про конфіденційне повідомлення.

Алгоритм методу «Розмір пакетів переданих даних» є наступним.

На комп'ютері відправника вводиться стеганограма. Відправник відсилає перший пакет, який містить у собі «стегано-ключ».

На основі «стегано-ключа» формується словник по одному і тому ж алгоритму на комп'ютері-відправника та комп'ютері-отримувача.

Починається передача файлів. Розмір кожного пакета відповідає букві або символу конфіденційного повідомлення. Пропускна здатність цього методу дорівнюватиме одній букві (символу) за 1 пакет.

До очевидних переваг таких методів слід віднести такі особливості: методи не потребують ніякої додаткової синхронізації між відправником та отримувачем інформаційного повідомлення; простота реалізації; інформаційне повідомлення важче виявити, ніж у випадку використання методів, які змінюють дані у полях заголовків протоколу. Як недоліки слід зазначити низьку стеганографічну пропускну здатність. Крім того, слід відмітити також потенційне погіршення якості отриманих даних користувача.

У роботах [4, 9, 11] розглянуто також *методи змішаних технік*, які побудовані через об'єднання двох попередніх методів. Прикладом реалізації цього методу є алгоритм HICCUPS (Hidden Communication system for CorrUPted networkS), який детально описується у роботах [9, 11]. До їх переваг слід віднести відсутність вимог щодо додаткової синхронізації між відправником та отримувачем, складність виявлення вбудованих повідомлень, високу стеганографічну пропускну здатність. Як недоліки слід зазначити високу складність практичної реалізації та підвищення рівня втрат мережних ресурсів.

2.2. Методи маніпуляції над потоками переданих пакетів. До цієї групи можна віднести метод затримки пакетів. Принцип функціонування методу затримки пакетів виглядає наступним чином (див. рис. 6) [3].

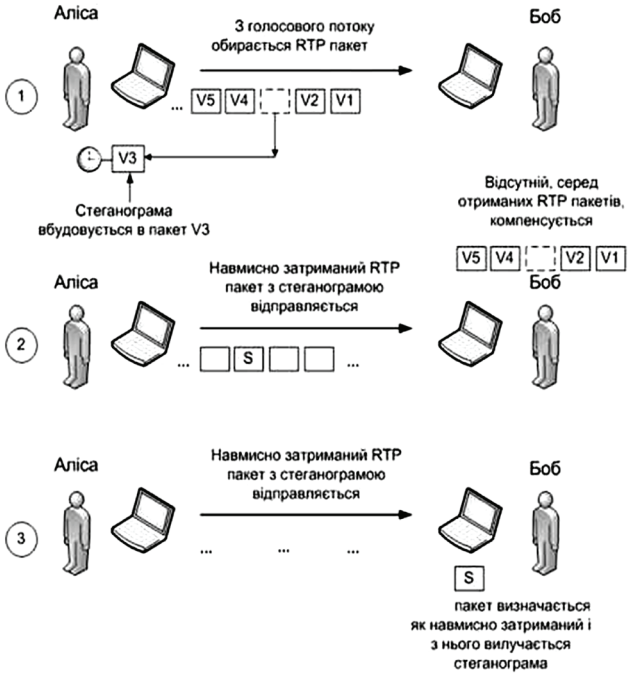

Рис. 6

Відправник (Аліса) обирає один з пакетів потоку і його корисне навантаження замінюється бітами секретного повідомлення – стеганограмою, яка вбудовується в пакет V3 (1). Потім обраний пакет навмисне затримується (2). Щоразу, коли надмірно затриманий пакет досягає отримувача, незнайомого з стеганографічною процедурою, він відкидається. Однак, якщо одержувач (Боб) знає про прихований зв'язок, то замість видалення отриманих пакетів, витягує приховану інформацію [3]. RTP – транспортний протокол, який належить до сімейства стека протоколів TCP/IP.

Як переваги даного методу слід відзначити простоту реалізації та важкість виявлення стеганоканалу. Як недоліки слід зазначити такі: дуже низька стеганографічна пропускна здатність; потрібна синхронізація між відправником й отримувачем та збільшення затримки передачі.

2.3. Гібридні методи. Метод RSTEG [9] (один із гібридних методів) заснований на механізмі повторної посилки пакетів, суть якої полягає у тому, що: коли відправник посилає пакет, то одержувач не відповідає пакетом з прапорцем підтвердження, і таким чином має спрацювати механізм повторної висилки пакетів і повторно посилається пакет зі стеганограмою всередині, на який також не приходить підтвердження. При наступному спрацьовуванні даного механізму надсилається оригінальний пакет без прихованих вкладень, на який приходить пакет з підтвердженням про вдалий отриманий (див. рис. 7). Перевагами даного методу є простота реалізації; важкість виявлення стеганоканалу; висока стеганографічна пропускна здатність; не потрібно ніякої синхронізації між відправником та отримувачем. Недоліками цього методу є потенційне погіршення якості даних користувача та підвищення рівня втрат у мережі.

Рис. 7

Результати проведеного аналізу відомих методів мережної стеганографії узагальнено у табл. 1, в якій наведено ранжування різних підходів до побудови захищених каналів скритої передачі повідомлень. Як показники ранжування використовувалися: складність практичної реалізації (у порядку ускладнення); надійність методів стеганозахисту (за спаданням); пропускна здатність (за спаданням).

Таблиця 1

Порівняльна характеристика методів

№	Методи	Реалізація	Надійність методів	Пропускна здатність
1	Методи, що змінюють тільки заголовки пакетів	1	5	4
2	Методи, що змінюють тільки передані дані	2	3	3
3	Методи, засновані на маніпуляціях над потоком переданих пакетів (сортування пакетів)	3	4	5
4	Методи, що включають одночасну модифікацію пакетних даних і маніпуляцію над потоком	4	1	1
5	Змішані методи, що використовують і заголовки пакетів, і дані	5	2	2

ВИСНОВКИ

Проведені дослідження показали, що методи мережної стеганографії останнім часом інтенсивно розвиваються та вдосконалюються. Це зумовлено стрімким поширенням мережних технологій та розповсюдженням сучасних інформаційно-телекомунікаційних засобів. Зокрема останніми роками відбулася справжня «революція мобільних пристроїв», коли майже кожна фізична особа експлуатує високопродуктивні «гаджети», які здатні надавати різні інформаційні послуги, в тому числі і за допомогою доступу до мережних обчислювальних та комунікаційних ресурсів. Таке стрімке поширення сучасних інфокомунікаційних технологій створює всі передумови для виникнення принципово нових технологій захисту інформації, зокрема методів скритної передачі конфіденційних повідомлень. Фактично, людство стоїть на порозі створення надтехнології прихованої передачі даних, коли застосовуючи відкриті канали зв'язку, зокрема засоби і технології глобальних мереж, можна миттєво та скритно організувати передачу потрібної інформації між будь-якими фізичними або юридичними особами, що розташовані у будь-якій точці земної кулі. При цьому приховується не тільки смисловий вміст переданих даних, але і сам факт існування скритої передачі інформації.

В цій роботі проведено аналіз найпростіших методів мережної стеганографії. І навіть такі методи виявили високі показники ефективності. У табл. 1 наведено порівняння досліджених методів за їх основними характеристиками та можливістю практичної реалізації. Позиція кожного методу в даній таблиці показує, на скільки його характеристики перевершують або поступаються іншим. На основі даних із таблиці можна зробити висновок про пряму залежність основних характеристик один від одного та перспективні шляхи щодо їх подальшого розвитку та вдосконалення. Проведені дослідження можуть бути використані як основа для розробки нових методів стеганографії або для захисту інформації від витоків по прихованих каналх, створених за допомогою розглянутих методів мережної стеганографії.

Література

[1] *Горбенко І.Д., Горбенко Ю.І.* Прикладна Криптологія. – Харків. Форт. – 2012. – С. 867.

[2] *Конахович Г.Ф., Пузеренко О.Ю.* Комп'ютерна стеганографія. Теорія і практика. – Київ. МК-Пресс. – 2006. – С. 288.

[3] *Коркач И.В., Пирогова Ю.И.* Использование технологий IP-телефонии для скрытой передачи информации. – [Електронний ресурс]. – Режим доступу: http://tzi.ua/ ru/vikoristannya_tehnologj_ip-telefon_ dlya_prihovano_ peredach_nformac.html

[4] *Пескова О.Ю., Халабурда Ю.Г.* Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет. - [Електронний ресурс] – Режим доступу: http://ojs.ifmo.ru/index.php/IMS/article/ view/132/132

[4] *Генне О.В.* Основні положення стеганографії [Електронний ресурс] – Режим доступу: http://easy-code.com.ua/2010/11/osnovni-polozhennya-stenografii/

[4] *Паркер Т., Сиян К.* TCP/IP. Для профессионалов. 3-е изд. – СПб.: Питер, 2004. – С. 859

[4] *Ногл М.* TCP/IP. Иллюстрированный учебник – М.: ДМК Пресс. – 480 с.

[4] *Thurston R.* Steganography developers turn their attention to hiding information in VoIP. [Електронний ресурс] – Режим доступу: http://www.scmagazineuk.com/ steganography-developers-turn-their-attention-to-hiding-information-in-voip/article/112102/

[4] *Sekhar A.* International Journal of Advanced Research in Computer and Communication Engineering. Vol. 4, Special Issue 1, June 2015 [Електронний ресурс] – Режим доступу: http://www.ijarcce.com/upload/2015/ si/icrtcc-15/IJARCCE%2017.pdf

[4] *Ziyad Tariq Mustafa, Authman Waleed Khalid.* Diyala journal for pure sciences. Packet Steganography Using IP ID. [Електронний ресурс]. – Режим доступу: http://www.sciencesmag.uodiyala.edu.iq/uploads/Volume%2010/Issue%204/English/1-10%20E.pdf

[4] *K. Szczypiorski,* HICCUPS: Hidden Communication System for Cor- rupted Networks, In Proc. of The Tenth International MultiConference on Advanced Computer Systems ACS–2003. – P. 31–40.

Надійшла до редколегії 10.11.2015

Кузнецов Олександр Олександрович, доктор технічних наук, професор, професор кадедри БІКС ХНУ ім. В.Н. Каразіна. Наукові інтереси: криптографія, теорія обробки і передачі даних, стеганографічні методи захисту інформації.

Тимченко Владислав Анатолійович, студент факультету комп'ютерних наук ХНУ ім. В.Н. Каразіна. Наукові інтереси: криптографія, стеганографія, теорія обробки і передачі даних.

Дубровний Богдан Сергійович, студент факультету комп'ютерних наук ХНУ ім. В.Н. Каразіна. Наукові інтереси: адміністрування баз даних, криптографія, стеганографія.

УДК 004.056:003.26

Анализ и сравнительные исследования методов сетевой стеганографии / А.А. Кузнецов, В.А. Тимченко, Б.С. Дубровный // Прикладная радиоэлектроника: научн.-техн. журнал. – 2015. – Том 14. – № 4. – С. 384–389.

Рассматриваются возможности стеганографических методов защиты информации, создание которых основано на использовании особенностей функционирования сетевого стека протоколов передачи семейства TCP/IP (Transmission Control Protocol / Internet Protocol). Исследуются разные методы сетевой стеганографии: на кодировании содержания информационных пакетов; на манипуляциях потока переданных пакетов; гибридные методы. Обосновываются перспективные направления дальнейших исследований по улучшению методов сетевой стеганографии для их использования с целью скрытия факта наличия скрытой передачи информации.

Ключевые слова: сетевая стеганография, семейство протоколов TCP/IP.

Табл.: 2. Рис.: 8. Библиогр.: 11 назв.

UDC 004.056:003.26

Analysis and comparative research of network steganography methods / Kuznetsov A.A., Tymchenko V.A., Dubrovny B.S. // Applied Radio Electronics: Sci. Journ. – 2015. – Vol. 14. – № 4. – P. 384–389.

The paper reviews capabilities of steganography methods, the construction of which is based on using of peculiarities of functioning the transmission protocols network stack of TCP/IP family. Different methods of network steganography are studied, namely: those based on content encoding of information packets, on manipulations of a stream of packets transmitted as well as hybrid ones. Perspective ways of further research with improving methods of network steganography to be used to conceal the existence of secret information transfer are substantiated.

Keywords: network steganography, TCP/IP protocols family.

Tab.: 2. Fig.: 8. Ref.: 11 items.