УДК 519.816 **О.В. Барабаш, Н.В. Лукова-Чуйко, А.П. Мусієнко, А.О. Смірнов**

МЕТОД ПРИХОВАНОЇ ПЕРЕДАЧІ ДАНИХ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ІЗ ЗАСТОСУВАННЯМ СТЕГАНОГРАФІЇ

У роботі розроблений та детально проаналізований метод прихованої передачі даних в інформаційній системі на основі генерації початкових номерів послідовності протоколу TCP. Описана можливість функціональної декомпозиції повного циклу передачі одного повідомлення на три етапи: формування стегоконтейнерів і відправки повідомлення, передача стегоконтейнерів в загальнодоступній глобальній мережі, прийом стегоконтейнерів і відновлення повідомлення. Зроблено висновок про те, що для стороннього спостерігача функціонування стеганографічної системи, що розробляється, не внесе тимчасових затримок у функціонування протоколу TCP.

***Ключові слова*:** інформаційна система, протокол TCP, стегоконтейнер, стеганографічна система.

Вступ

Аналіз відомих методів побудови мережевих стеганографічних каналів передачі даних [1, 2] показав, що технічна можливість використання особливостей протоколів моделі OSI в цілях потайної передачі даних існує у багатьох випадках.

Найбільш ефективними методами, являються методи, які ґрунтуються на протоколах моделі OSI від транспортного рівня і вище [2], що обумовлюється високою ресурсоємкістю їх стегоаналіза.

При розробці методу стеганографічної передачі даних основними вимогами стали:

– висока скритність процесу передачі повідомлень;

– достовірність доставки переданих повідомлень;

– достатня стеганографічна надмірність використовуваного базового каналу передачі даних;

– простота реалізації методу.

Таким вимогам відповідає протокол транспортного рівня – TCP [3] (Transmission Control Protocol – протокол управління передачею). Достовірність доставки повідомлень досягається за рахунок процедури трьох етапного встановлення з'єднання і квитування факту доставки фрагментів.

Аналіз останніх досліджень і публікацій

У основу розробленого методу покладений механізм генерації початкового номера послідовності(ISN - Initial Sequence Number) кожного TCP- з'єднання і кореляції байтів переданих (відкритих) даних і байтів повідомлення.

Згідно [3], генерація початкового номера послідовності, при встановленні TCP-з'єднання, ґрунтується на поточному (можливо, фіктивному) 32-бітовому значенні часу, в якому молодший біт інкремінується кожних 4 мікросекунди. Насправді, значення ISN обчислюється в різних операційних системах по-різному. Але в загальному випадку це значення являється, свого роду, тимчасовим штампом і відповідає значенню функції, аргументом якої, у тому числі, являється поточне значення машинного часу комп'ютера, тобто ISN = F(t).

Таким чином, значення ННП, для стороннього спостерігача, при першому спостереженні, є випадковим. При аналізі достатньої вибірки значень F(t), стає можливим вичислити закономірність(апроксимувати функцію).

У заголовку TCP- фрагмента, значення ННП записується в полі довжиною 32 біта (рис. 1).

Дані, які переносяться TCP- фрагментом, представляються у вигляді послідовності байтів, які мають "наскрізну" нумерацію. Номер першого байта даних, що передається відповідає(ISN+1).

© О.В. Барабаш, Н.В. Лукова-Чуйко, А.П. Мусієнко, А.О. Смірнов, 2017

Рис. 1. Формат заголовка протоколу TCP

На мал. 2 зображений фрагмент Ethernet- фрейма, представлений в 16-річній формі числення. Інтервал з нульового по 54-тий байт включно займають заголовки канального, мережевого і транспортного рівнів БЕММВ. Заголовок протоколу транспортного рівня (в даному випадку TCP) виділений сірим кольором і розпочинається з 55-го байта, якщо за початок відліку брати перший байт фрейма Ethernet.

0000	00	30	48	14	72	c9	14	da	e9	61	6d	71	08	00	45	00
0010	05	dc	2d	e4	40	00	80	06	40	94	c0	a8	02	ef	c0	a8
0020	02	64	d3	4d	01	bd	42	6a	a7	16	96	6e	9d	ef	50	10
0030	3e	be	e3	df	00	00	00	00	41	04	ff	53	4d	42	2f	00
0040	00	00	00	18	07	c8	00	00	11	9e	55	78	e9	34	00	8d
0050	00	00	06	08	ff	fe	00	10	80	1a	0e	ff	00	de	de	0d
0060	10	00	00	00	00	ff	ff	ff	ff	00	00	00	00	00	00	c4
0070	40	40	00	00	00	00	00	c5	40	ee	cf	ee	e8	f1	ea	20
0080	e8	20	ee	f6	e5	ed	ea	e0	20	e0	ed	ee	ec	e0	ed	e8

Рис. 2. Фрагмент Ethernet- фрейма

Дані для прикладного застосування(файл у форматі *.txt) передаються в кодуванні CP1251. Початку, безпосередньо, тексту (виділений чорним кольором на рис. 2) відповідає 123 байт від початку фрейма. Йому передують 68 байт службових даних для прикладного застосування.

Для потайної передачі, наприклад, слова "залп", використовуючи як стегоконтейнера поле "номер послідовності" і "дані" TCP- фрагмента необхідно:

– пронумерувати байти «поля даних» починаючи з нульового значення;

– поставити у відповідність кожну букву слова «залп» з номером байта в полі даних;

– згідно з дотриманням букв в секретному слові, заповнити відповідними значеннями номерів 32-розрядне слово;

– записати значення отриманого слова в полі "номер послідовності";

– передати отриманий фрагмент одержувачеві;

– на приймальній стороні витягнути стего в зворотній послідовності.

На мал. 2 чорним кольором виділений фрагмент текстових даних, у відповідність порядковим номерам байтів якого, поставлені букви приховуваного повідомлення «залп»: «з» - 8710 - 5716 - 0001 01002, «а» - 7710 - 4D16 - 0101 01112, «л» - 9310 - 5D16 - 0101 11012, «п» - 6710 - 4316 - 0100 00112.

© О.В. Барабаш, Н.В. Лукова-Чуйко, А.П. Мусієнко, А.О. Смірнов, 2017

Відповідно до логіки роботи описуваного методу, далі необхідно згенерувати потрібний номер ISN. У стеку протоколів TCP/IP заповнення заголовків і полів даних робиться в порядку «від старшого до молодшого». Потрібний початковий номер послідовності має вигляд 00010100010101110101110101000011$_2$= 4126982710.

Звідси витікає, що при оголошенні такого ISN, перший байт TCP даних, що переноситься матиме номер (341269827+1) $_{10}$. Подальше функціонування протоколу TCP відповідає варіанту, реалізованому в операційній системі.

Мета статті

Метою статті є розроблення методу прихованої передачі даних в інформаційній системі на основі генерації початкових номерів послідовності протоколу TCP та виконання детального аналізу процесу прихованої передачі даних в інформаційній системі по отриманому методу на основі дослідження властивостей вдосконаленої моделі обслуговування TCP- з'єднань.

Основна частина

Розширений опис розробленого методу прихованої передачі даних представлений на основі дослідження властивостей моделі обслуговування TCP-з'єднань для прихованої передачі даних в інформаційних системах. Такий підхід дозволяє вивчити процес функціонування СГС і врахувати усі технологічні особливості при розробці програмної реалізації методу прихованої передачі даних.

З метою детальнішого вивчення властивостей стеганографічної системи (СГС), математичне моделювання розділене на дві частини:

– моделювання процесу формування і відправки стегоконтейнерів;

– моделювання процесу отримання стегоконтейнерів і витягання повідомлень.

Для вірного розуміння описової частини математичного моделювання роботи СГС по розробленому стеганографічному методу, необхідно прийняти ряд визначень.

Під стегоконтейнером в роботі розуміється модернізоване з метою потайної передачі даних TCP- з'єднання в цілому.

Під повідомленням розуміються дані, що скрить передаються по стегоканалу.

Під стего розуміється частина повідомлення, що передається в одному стегоконтейнері. Під покриваючим об'єктом розуміється текст, що передається в межах відкритого каналу передачі даних.

Під інформативним значенням розуміється значення, яке відповідає номеру символу в опорному тексті, який використовувався при кодуванні і належить інтервалу $0 \le n \le 127$ де $n-$номер в порядку дотримання символу опорного тексту, що відповідає символу повідомлення.

Під неінформативним значенням розуміється значення, яке використовувалося при кодуванні в якості «маркера», за умови відсутності поточного символу повідомлення в черговому блоці з 128 символів опорного тексту, або при доповненні чергового блоку, необхідних для обчислення потрібного номера ISN, до чотирьох значень.

В якості інструменту при математичному моделюванні був вибраний апарат мереж Петрі [4, 5]. Це пов'язано з тим, що процес передачі даних в ІС є динамічним, а мережі Петрі є потужним апаратом для моделювання систем в динаміці і отримання важливої інформації про їх структуру.

Такий підхід до моделювання в теорії мереж Петрі обумовлює властивість інтенсивності мережі, яка і дозволила застосувати цей апарат для вирішення поставленого завдання.

Виходячи з властивості інтенсивності мереж Петрі, завжди існує можливість досягнення безлічі розміток $M = \{M_0, M_1, M_2, ..., M_n\}$ з нульової (початкової) розмітки, де n – кількість досяжних розміток.

© О.В. Барабаш, Н.В. Лукова-Чуйко, А.П. Мусієнко, А.О. Смірнов, 2017

На таких графах використовуються два типи вершин: позиції і переходи. При цьому однотипні вершини не можуть бути інцидентними. Позиції відповідають подіям, що відбуваються в процесі функціонування модельованої системи, а переходи – умовам настання відповідної події.

В цілому, граф мережі Петрі в початковій розмітці для моделювання стеганографічної системи представлений на рис. 3.

У розробленій мережі Петрі є присутніми конфліктні ситуації, які внесені навмисно і відображають умови спрацьовування у фіксований момент часу одного з вихідних для позиції переходів.

Модельованим процесом є прихована передача даних. Граф мережі Петрі, представлений на рис. 3, є трудомістким для аналізу. З цієї причини він був розділений на два підграфи: формування і відправка стегоконтейнерів і прийом СГК і витягання повідомлення. Таким чином, описова частина моделювання стеганографічної системи розділена на опис двох підмоделей.

У моделі обслуговування ТСР- з'єднань при формуванні і відправці стегоконтейнерів, конфлікт полягає у визначенні порядку спрацьовування пари переходів t_2 і t_5 і четвірки t_9, t_{10}, t_{11}, t_{12} .

У моделі обслуговування ТСР- з'єднань при прийом СГК і витягання повідомлення, конфлікт полягає у визначенні порядку спрацьовування пари переходів t_{15} і t_{16} і четвірки t_{20}, t_{21}, t_{22}, t_{24}. Порядок спрацьовування цих переходів описаний далі, але в загальному випадку може спрацювати тільки одна з представлених груп.

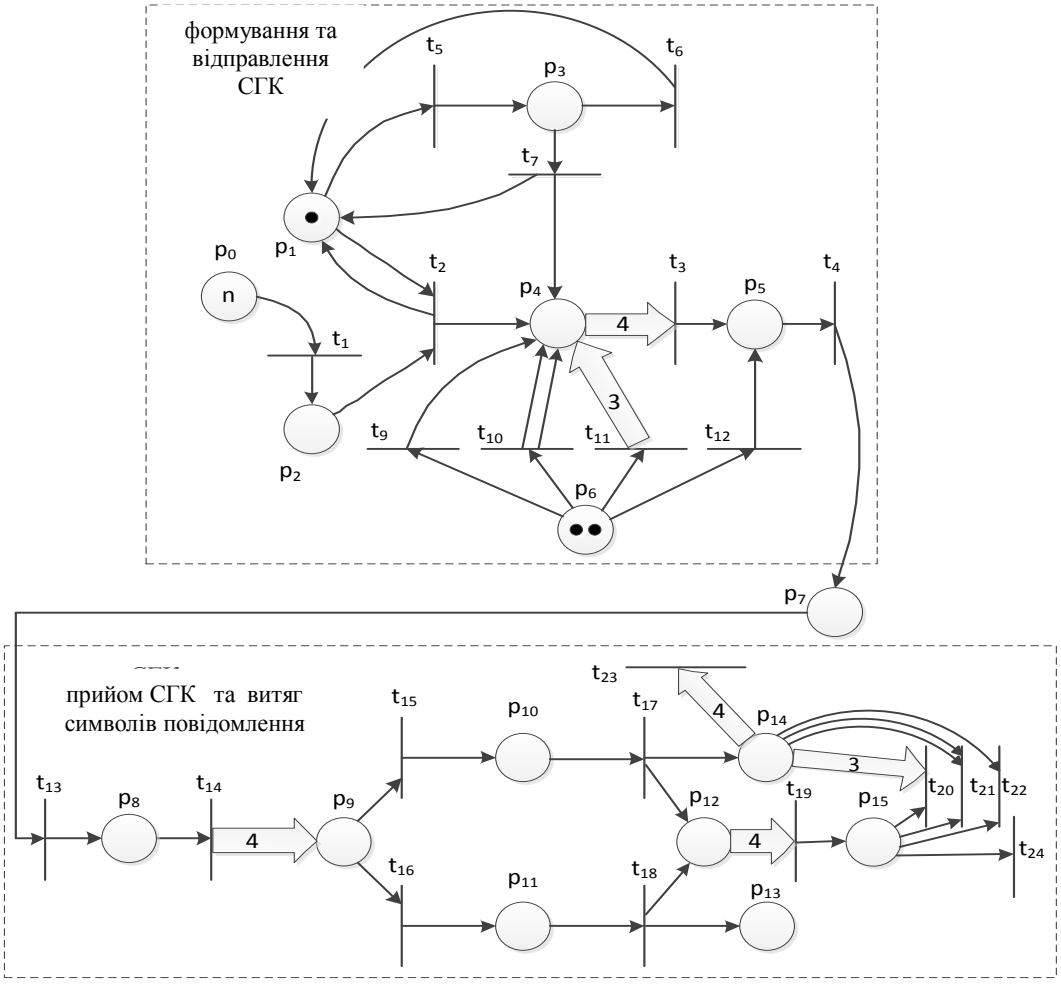

Рис. 3. Граф мережі Петрі в початковій розмітці
для моделювання стеганографічної системи

© О.В. Барабаш, Н.В. Лукова-Чуйко, А.П. Мусієнко, А.О. Смірнов, 2017

Згідно [4], мережа Петрі складається з чотирьох елементів: безліч позицій P безліч переходів T вхідній функції I і вихідній функції O. Тобто мережу Петрі можна задати вектором (1). Такий вектор називається структурою мережі Петрі:

$$C = (P, T, I, O). \quad (1)$$

Позиція p_6 (рис. 4) відповідає транспортуванню, формованих стеганографічною системою, TCP- фрагментів у віртуальному каналі зв'язку за правилами стандартного протоколу TCP.

На рис. 4 зображений граф мережі Петрі в початковій розмітці, який характеризує функціонування стеганографічної системи при формуванні і відправці стегоконтейнерів.

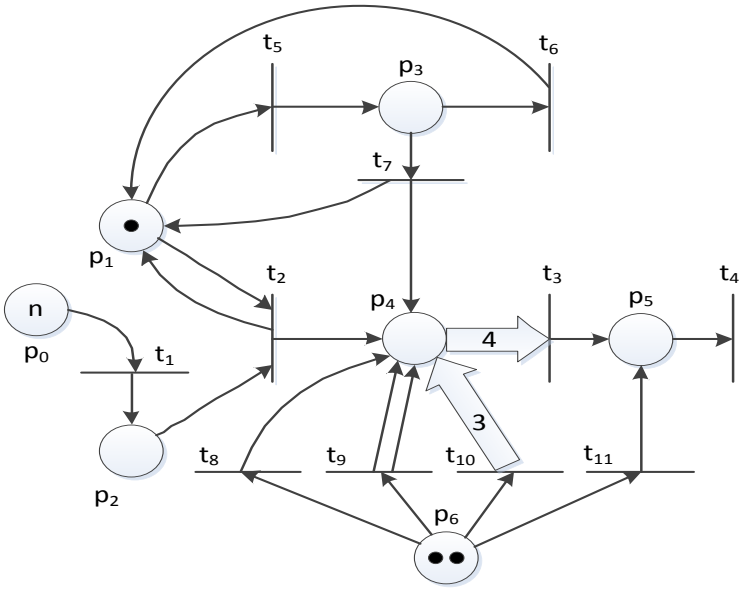

Рис. 4. Граф мережі Петрі в початковій розмітці $M_0 = \{n,1,0,0,0,0,2\}$.
СГС готова до передачі *n* символів повідомлення

Кожному елементу з безлічі позицій $P = (p_1, p_2, ..., p_6)$ мережі C_1 відповідає одно з можливих станів СГС при передачі повідомлень по мережевому стеганографічному каналу: p_0 – на вхід СГС поступило n символів повідомлення. Кількість фішок в цій позиції відповідає кількості символів в повідомленні (n- безпечна позиція); p_1 – отриманий черговий символ з безлічі символів, що містяться в опорному тексті. У початковій розмітці містить одну фішку; p_2 – отриманий черговий символ з безлічі символів, що містяться в повідомленні. У початковій розмітці не містить фішок; p_3 – поточний символ опорного тексту не відповідає поточному символу повідомлення, або не знайдений при повному переборі в актуальному блоці з 128 символів опорного тексту; p_4– чергове 8-розрядне значення поступило в регістр зрушення. Залежно від того, який з переходів спрацював ($t_2, t_7, t_9, t_{10}, t_{11}$), може бути інформативним або неінформативним. У початковій розмітці не містить фішок; p_5 – вичислено необхідне значення ННП для TCP - з'єднання. У початковій розмітці не містить фішок. Міра цієї позиції. Це відповідає накопиченню чотирьох байтів номера ISN; p_6 – передача останнього символу повідомлення. При цьому вводиться додаткове обмеження, яке полягає в тому, що з позиції p_6 може спрацювати тільки той перехід, для якого позиція p_4 являється вихідний з кратністю $k = 4 - n$, де n – кількість фішок в позиції p_4 у актуальній розмітці мережі. Якщо $n = 0$, то спрацювати може тільки перехід t_{12}.

© О.В. Барабаш, Н.В. Лукова-Чуйко, А.П. Мусієнко, А.О. Смірнов, 2017

Кожному елементу з безлічі переходів T мережі C_1 відповідає одно з можливих умов переходу СГС з вхідного(вхідних) у вихідний (вихідні) стан: t_1 – отриманий черговий символ повідомлення для порівняння з множиною символів опорного тексту. Цей перехід спрацьовує один раз, з початкової розмітки, і поміщає в позицію p_2 одну фішку; t_2 – поточний символ повідомлення і опорного тексту відповідають. При спрацьовуванні, цей перехід поміщає в позицію p_4 одну фішку, що відповідає вступу в регістр зрушення інформативного значення; t_3 – якщо позиція p_4 містить чотири фішки, то при спрацьовуванні, цей перехід поміщає в позицію p_5 одну і витягає з p_4 усі фішки. Це відповідає тому, що чотири значення, розміщені в регістрі зрушення, перетворяться в 32-розрядний ННП; t_4 – цей перехід витягає з позиції p_5 одну фішку. Це відповідає відправці чергового стегоконтейнера; t_5 – спрацьовує, якщо поточний символ опорного тексту не відповідає поточному символу повідомлення і поміщає в позицію p_3 одну фішку; t_6 – витягає з позиції p_6 і поміщає в позицію p_1 одну фішку. Спрацьовує, якщо вибраний наступний символ опорного тексту для порівняння з поточним символом повідомлення; t_7 – витягає з позиції p_3 одну фішку і поміщає в позиції p_5 і p_4 по одній фішці. Така подія відображає випадок, коли номер (в порядку дотримання) чергового символу опорного тексту досяг значення (2^7-1). При цьому, в регістр зрушення поступає випадково згенероване значення в межах від 2^7 до (2^8-1), а для порівняння поступає перший символ з наступного 128- символьного блоку опорного тексту; t_8, t_9, t_{10} – витягають з позиції p_6 одну і поміщають в позицію p_4 (k_4-m) фішок, де k_4 - міра позиції p_4 $m-$фактична кількість фішок в позиції p_4. Відображає випадок, коли необхідно доповнити 32-розрядний регістр зрушення одним, двома, трьома 8-розрядним значеннями відповідно, випадково згенерованими в межах від 2^7 до (2^8-1). Цей перехід спрацьовує, коли в позиціях p_0 і p_2 відсутні фішки; t_{11} – спрацьовує тільки після спрацьовування переходів t_8 (t_9 чи t_{10}). Цей перехід витягає з позиції p_6 і поміщає в позицію p_5 одну фішку. Спрацьовування цього переходу відповідає відправці стегоконтейнера, який інформує одержувача про те, що повідомлення передане повністю.

Функції інцидентності мережі Петрі $\Phi(p,t)$ і $\Phi(t,p)$ визначають кількість дуг ведучих з позиції в перехід і з переходу в позицію відповідно.

Для початку виконання зображеного на рис. 4 графи мережі Петрі, потрібне спрацьовування переходу t_1. Це відповідає вступу першого символу повідомлення для порівняння з першим символом вибраного опорного тексту.

$$\Phi(p,t)=\begin{vmatrix}1&0&0&0&0&0&0\\0&1&1&0&0&0&0\\0&0&0&0&4&0&0\\0&0&0&0&0&1&0\\0&1&0&0&0&0&0\\0&0&0&1&0&0&0\\0&0&0&1&0&0&0\\0&0&0&0&0&0&1\\0&0&0&0&0&0&1\\0&0&0&0&0&0&1\\0&0&0&0&0&0&1\end{vmatrix};\quad \Phi(t,p)=\begin{vmatrix}0&0&0&0&0&0&0&0&0&0&0\\0&1&0&0&0&1&1&0&0&0&0\\1&0&0&0&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0&0&0&0\\0&1&0&0&0&0&1&1&2&3&0\\0&0&1&0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&0&0&0&0\end{vmatrix}.$$

© О.В. Барабаш, Н.В. Лукова-Чуйко, А.П. Мусієнко, А.О. Смірнов, 2017

На рис. 5 зображений граф мережі Петрі в початковій розмітці, виконання якого характеризує функціонування стеганографічної системи при отриманні стегоконтейнерів і витяганні символів повідомлення. Безліч досяжних розміток цього графа відповідає підмоделі обслуговування TCP-з'єднань при отриманні стегоконтейнерів і витяганні символів повідомлення.

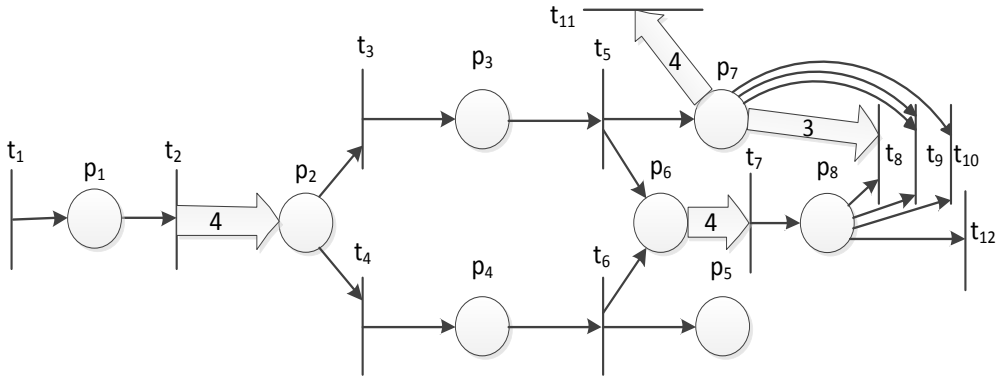

Рис. 5. Граф мережі Петрі в початковій розмітці $M_0 = \{0,0,0,0,0,0,0,0\}$.
СГС готова до прийому СГК і витяганню символів повідомлення

Висновки

Таким чином, відомості, отримані в результаті аналізу моделі обслуговування TCP-з'єднань для прихованої передачі даних в інформаційній системі, дозволяють врахувати усі тонкощі, необхідні при розробці програмної реалізації методу прихованої передачі даних в інформаційній системі.

Основні результати, отримані в цій статті відображені в наступних пунктах.

1. Розроблений метод прихованої передачі даних в інформаційній системі на основі генерації початкових номерів послідовності протоколу TCP.

2. Виконаний детальний аналіз процесу прихованої передачі даних в інформаційній системі по розробленому методу на основі дослідження властивостей вдосконаленої моделі обслуговування TCP- з'єднань.

3. Описана можливість функціональної декомпозиції повного циклу передачі одного повідомлення на три етапи: формування стегоконтейнерів і відправки повідомлення, передача стегоконтейнерів в загальнодоступній глобальній мережі, прийом стегоконтейнерів і відновлення повідомлення. Наявність такої можливості дозволяє зробити висновок про те, що для стороннього спостерігача функціонування стеганографічної системи, що розробляється, не внесе тимчасових затримок у функціонування протоколу TCP, як сигнатури для ухвалення рішення про наявність потайного каналу передачі даних в межах аналізованого віртуального з'єднання.

Список використаної літератури

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

2. Рубан И.В. Анализ возможностей утечки информации в ИТКС при использовании протоколов транспортного уровня модели OSI в качестве стегоконтейнера / И.В. Рубан, А.О. Смирнов // Системи обробки інформації. – 2015. – Вип. 7(132). – С. 132-135.

3. "Internet protocol – DARPA Internet Program Protocol Specification" RFC-793 USC / Transmission control protocol, September 1981 [Electr. resource]. – Accessed to: https://tools.ietf.org/html/rfc793.

4. Питерсон Дж. Теория сетей Петри и моделирование систем: Перевод с английского. – М.: Мир, 1984. – 264 с.

5. Котов В.Е. Сети Петри. – М.: Наука. Главная редакция физико-математической литературы, 1984. – 160 с.

Надійшла: 22.10.2017 Рецензент: д.т.н., проф. Вишнівський В.В.

© О.В. Барабаш, Н.В. Лукова-Чуйко, А.П. Мусієнко, А.О. Смірнов, 2017