Вісті Академії Інженерних Наук України • №2 (39)

УДК 004.056

Стеганографічна Персоналізація інформації на базі ПК

Корольов В.Ю., Поліновський В.В., Герасименко В.А.

Анотація. *Запропоновано інноваційний метод комп'ютерної стеганографії, що дозволяє збільшити об'єм прихованих даних та використати апаратно-програмні ресурси персоналізованих флеш-накопичувачів для підвищення ступеня захисту конфіденційної інформації.*

Аннотация. *Предложен инновационный метод компьютерной стеганографии, позволяющий увеличить объем скрытых данных, а также использовать аппаратно-программные ресурсы персонализированных флеш-накопителей для повышения степени защищенности конфиденциальной информации.*

Summary. *The new computer steganography method is presented. Based on hardware and software resources of personalized flash-drive this method increases the security of confidential information.*

Сучасна комп'ютерна стеганографія широко використовується для захисту інформації від несанкціонованого доступу та охорони авторських прав на інтелектуальну власність. Принципи стеганографічного приховування інформації у поєднанні з методами криптографії є базою для створення сучасних технологій комп'ютерної безпеки і пристроїв персоналізації як для корпоративного застосування, так і для особистого використання. Тому розробка нових стегано-криптографічних методів захисту і персоналізації інформації є актуальною науково-практичною задачею.

Введемо терміни, що необхідні для подальшого викладу.

Персоналізація інформації — це комплекс заходів по запобіганню несанкціонованого доступу до секретних даних, що ґрунтується на аутентифікації користувача технічних пристроїв, де зберігається таємна інформація, а також програм і протоколів для криптографічного і стеганографічного захисту файлів.

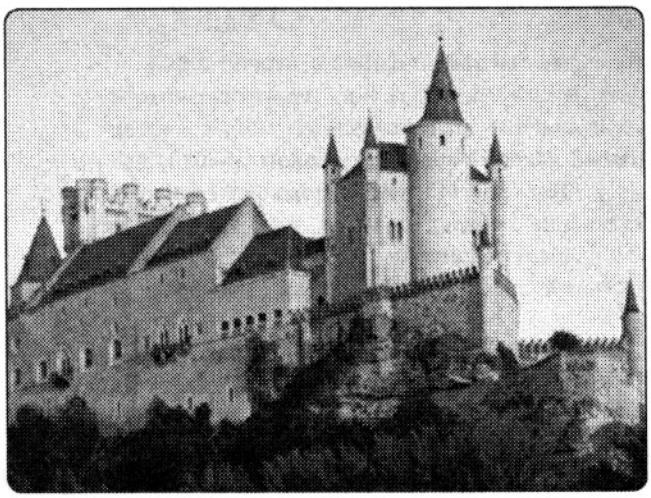
Стеганографія — це область захисту інформації, предметом якої є засоби та методи, що застосовуються для формування прихованого каналу передачі інформації.

Контейнер — будь-яка форма представлення даних, призначена для приховування таємних повідомлень.

Вбудоване повідомлення — це повідомлення, яке приховане у контейнері.

Стеганобіти — це біти даних повідомлення, що підлягають приховуванню стеганографічними методами у контейнері.

Рис. 1. Контейнер (тестове зображення) «замок у Іспанії»



Принципи стеганографічного приховування інформації

Принципи побудови систем передачі висококонфіденційних повідомлень і зберігання секретних даних в останні 3–5 років зазнали суттєвих змін, що обумовлено активним розвитком стеганографічних методів захисту інформації у комерційних системах. Концептуально стеганографічні системи відрізняються від криптографічних тим, що в них намагаються приховати сам факт передачі секретних даних. Більшість методів комп'ютерної стеганографії базується на **двох принципах** [3–5].

Перший принцип полягає в тому, що використовуються файли, які не вимагають абсолютної точності (наприклад, файли із зоб-

раженням, звуковою інформацією та ін.), і можуть бути до певного ступеня перетворені без втрати функціональності.

Другий принцип ґрунтується на нездатності органів чуттів людини без спеціального інструментарію надійно розрізняти незначні зміни в таких файлах.

Розглянемо стеганографічне приховування даних у зображеннях за методом заміни найменш значимого біта на прикладі чорно-білої фотографії (рис. 1). Сучасні комп'ютерні зображення являють собою масиви натуральних чисел (рис. 2), елементами яких є впорядковані 24-х бітні структури для кольорових зображень або 8-бітні додатні числа для монохромних зображень (рис. 3), що відповідають пікселям зображення.

На рис. 4 наведено бітове представлення фрагменту рядка зображення і схему стеганографічного приховування інформації за методом заміни найменш значимих бітів образу бітами текстового рядка. Для цього літери повідомлення замінюють числами відповідної кодової таблиці (наприклад, використовують код ASCII — American Standard Code for Information Interchange), а потім його перетворюють у бітову послідовність. Після

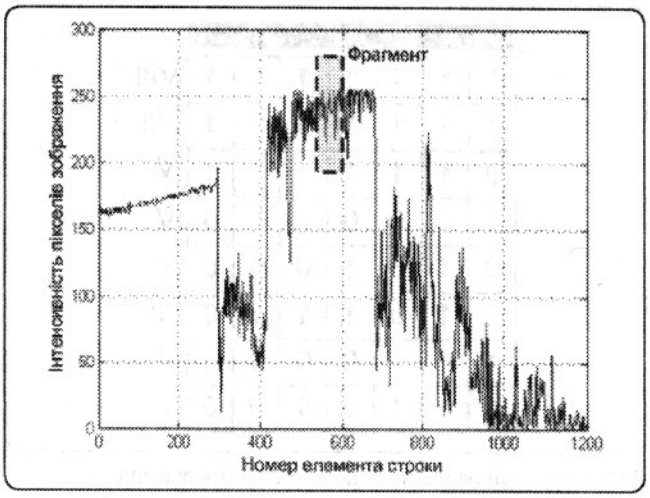


Рис. 2. Рядок контейнера (тестового зображення)

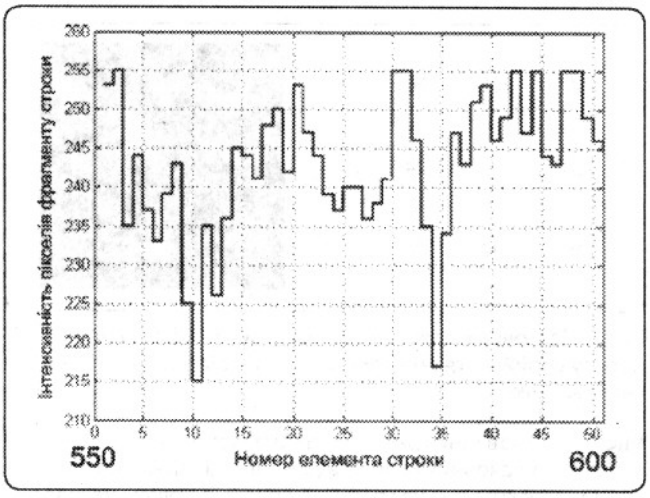
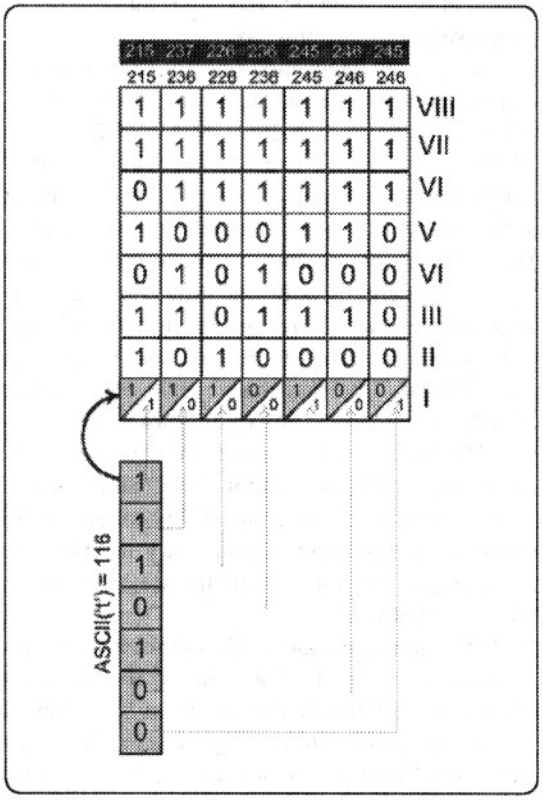


Рис. 3. Рядок контейнера (тестового зображення)

Рис. 4. Схема роботи алгоритму стеганографічного приховування інформації



цього найменш значимі (молодші) біти пікселів монохромного зображення (чисел, що відповідають яскравості) замінюють бітами прихованого тексту (рис. 4). В результаті, у зображення вбудовується текст без помітної зміни у якості фотографії (рис. 11а).

На рис. 4 схематично показано алгоритм вбудовування бітової послідовності літери «t» у пікселі зображення за методом заміни найменш значимого біта образу.

Числа у верхній частині схеми (рис. 4) відображають початкове значення елементів строки зображення, а білі цифри на чорному фоні представляють значення елементів рядка після вбудовування повідомлення у зображення. Видно, що зміни значень пікселів зображення елементів строки мінімальні, причому у половини випадків значення байтів пікселів після вбудовування не змінились.

Таким чином, після вбудовування прихованої інформації послідовність байтів пікселів зображення буде мати наступний вигляд (рис. 5).

Слід зазначити також, що стеганографічними методами захисту інформації користуються-

215	237	230	230	245	246	245	
1	1	1	1	1	1	1	VIII
1	1	1	1	1	1	1	VII
0	1	1	1	1	1	1	VI
1	0	0	0	1	1	0	V
0	1	0	1	0	0	0	VI
1	1	0	1	1	1	0	III
1	0	1	0	0	0	0	II
1	1	1	0	1	0	0	I

Рис. 5. Впорядкована послідовність байтів пікселів контейнера після внесення стеганографічних даних у зображення

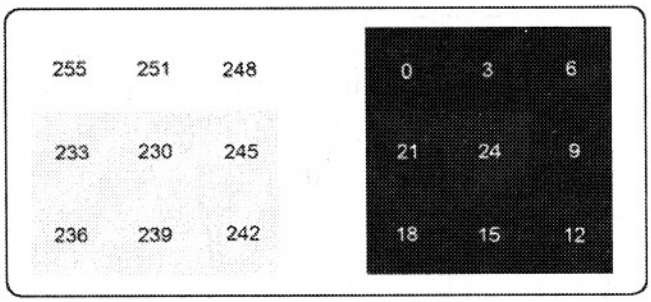
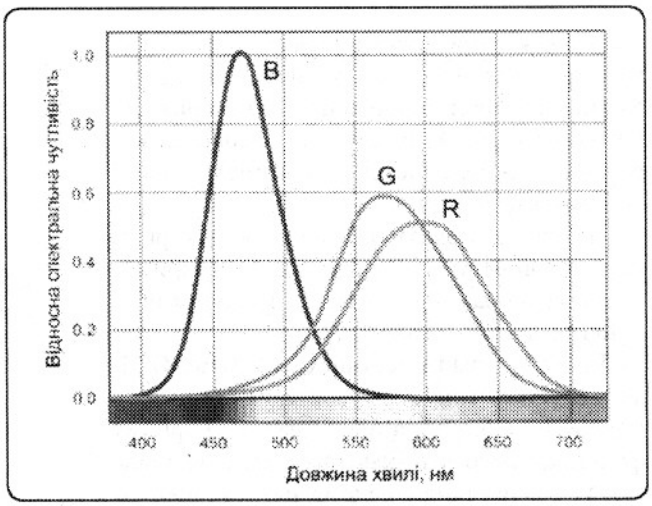


Рис. 6. Тестові зображення, які ілюструють обмеження порогу сприйняття інтенсивності кольорів зоровою системою людини

Рис. 7. Нормований графік чутливості зорової системи людини до основних кольорів (більше значення порогу сприйняття кольору на графіку відповідає гіршій чутливості до відповідного кольору)



ся як законослухняні громадяни, так і терористи, і злочинці. Тому державні спецслужби постійно шукають способи зламу або компрометації нових стеганографічних систем захисту інформації.

Головною задачею при зламі стеганографічних повідомлень є виявлення у носії прихованих даних, ідентифікація алгоритму їх внесення, а визначення кількості бітів у ключі захисту стає значимим лише після виконання двох попередніх етапів, що є нетривіальною задачею.

Так, за повідомленням у новинах psisorg.com в Інституті Іова, штат Огайо, США при фінансовій підтримці Військово-морських сил було розроблено систему виявлення стеганографічних даних у зображеннях з понад 90% ймовірністю. В основу цієї системи, як було повідомлено, покладено методи аналізу випадкових полів з використанням нейромереж. Аналіз публікацій по стеганографічному аналізу (стегоаналізу), доступних в мережі Інтернет, доводить, що прості методи приховування інформації досить легко виявляються на основі аналізу гістограм розподілу яскравості, типових значень розмірів файлів для зображень після їх перетворень. Отже, актуальною задачею є розробка нових методів і систем стеганографічного захисту інформації, що не дозволяють виявити факт приховування даних за допомогою очевидних засобів аналізу.

Спосіб варіативного заповнення кольорових каналів зображення стеганобітами

Розглянемо деякі характеристики зорової системи людини, які можна використати для збільшення обсягу прихованої інформації у зображеннях-контейнерах.

На рис. 6 наведено два зображення, які складається з дев'яти квадратів, в кожному з яких цифрами 255,251,248,245,242,239,236,233,230 та 0,3,6,9,12,15,18,21,24 показано значення відтінків сірого кольору, що відповідають змінам 4-5 молодших бітів зображення. Представлений рисунок переконливо ілюструє обмеженість зору людини у розрізненні малих варіацій інтенсивності кольорів, яка використовується у запропонованому методі комп'ютерної стеганографії для збільшення обсягу прихованих даних у зображенні.

На рис. 7 наведено графіки нормованого порогу чутливості зорової системи людини до блакитного (B), зеленого (G) і червоного (R) кольорів, що використовуються у телебаченні для обґрунтування зменшення смуги пропускання сигналу [6].

Оскільки переважна більшість зображень сьогодні кольорова, то можна використати неоднакову чутливість зору людини до кольорів для збільшення ємності контейнеру. Експериментально було встановлено, що без помітної

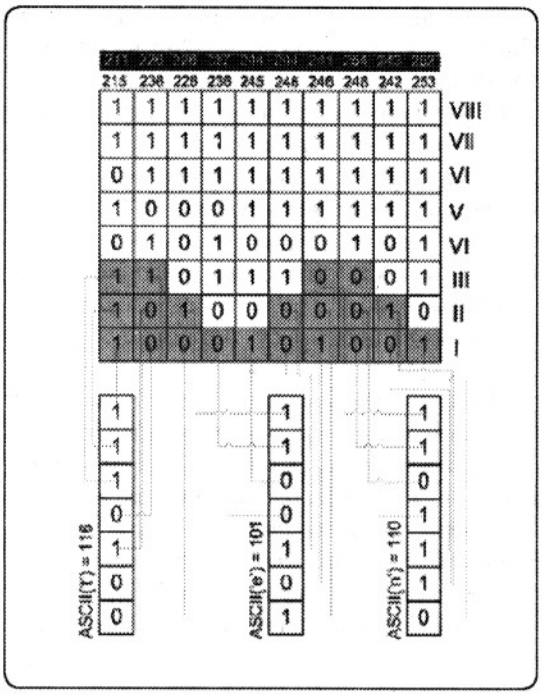


Рис. 8. Схема варіативного заповнення контейнера

втрати якості для більшості типових кольорових фотографій у блакитний канал можна вбудовувати до чотирьох біт повідомлення, у зелений і червоний до двох біт, при варіації рівнів (фігур) заповнення (рис. 9). Також можна запропонувати заповнення контейнера фігурами з випадковою формою, обмеженими тільки за висотою до чотирьох біт.

Алгоритм стеганографічного приховування інформації на базі варіації фігур заміни бітів контейнера

Крім кольорової психовізуальної надлишковості можна використати особливості сприйняття людиною сцени зображення. Амплітуди позицій стеганобітів пропонується зменшувати від периферії до центру для зниження візуальної здатності розпізнавання скритої інформації у зображеннях. При цьому найбільш природною закономірністю зменшення амплітуд концентричних областей образу є експоненційна. Таке психовізуальне ранжування амплітуд траєкторії для розстановки прихованих бітів у контейнері було використано для вдосконалення запропонованого стеганографічного алгоритму.

На рис. 8 наведено схему варіативного заповнення контейнеру. У пікселі зображення вбудовується англійське слово «ten». Видно, що навіть без використання технологій стискання даних ємність контейнера збільшується у 2 рази.

Типові приклади фігур заповнення бітів повідомлення показані на рис. 9.

Як було зазначено вище, виявити факт

довідка про автора

КОРОЛЬОВ
Вячеслав Юрійович

Закінчив НТУУ «КПІ» у 1999 р. за спеціальністю Радіотехніка. У 2004 р. отримав науковий ступінь кандидата технічних наук, у 2008 р. — атестат старшого наукового співробітника. З 2006 р. працює завідуючим відділом проблем моделювання таймерної обчислювальної техніки ЦТОС ІК. Область наукових інтересів: захист інформації, криптографія, цифрова обробка сигналів. Має близько 30 наукових публікацій.

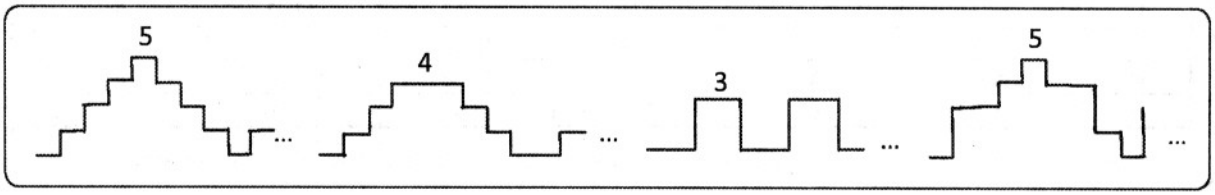
ПОЛІНОВСЬКИЙ
Вячеслав Васильович

У 2001 р. закінчив НТУУ «КПІ», у тому ж році почав працювати молодшим науковим співробітником та вступив до аспірантури, в Інститут кібернетики ім. В.М. Глушкова НАН України. З 2005 року переведений до Центру таймерних обчислювальних систем ІК на посаду старшого наукового співробітника і виконує обов'язки вченого секретаря. Автор понад 30 наукових праць. Область наукових інтересів: інформаційні технології, комп'ютерна телефонія, безпека ІТ-технологій.

ГЕРАСИМЕНКО
Вячеслав Анатолійович

У 2006 р. закінчив НТУУ «КПІ» за спеціальністю Комп'ютерні системи та мережі, після чого почав працювати молодшим науковим співробітником ЦТОС ІК НАНУ. Автор близь 10 наукових праць. Область наукових інтересів: інформаційні технології, безпека телекомунікаційних технологій.

Рис. 9. Приклади варіації фігур вбудовування бітів у рядки зображення-контейнера



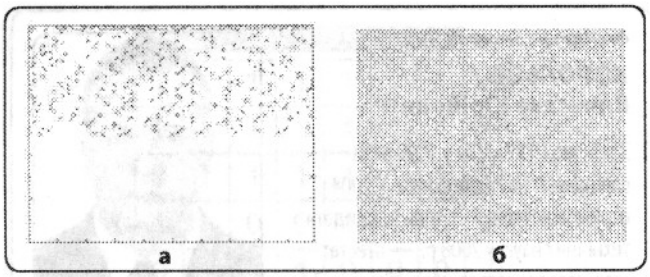


Рис. 10. Порівняння шаблонів маскування повідомлення для програм Steganos Privacy Suite 2008 (а) і ВІК-ВАК Стеганос (б)

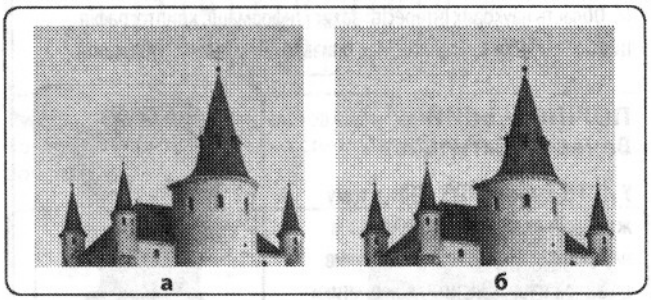


Рис. 11. Порівняння Steganos Privacy Suite 2008 (а) і ВІК-ВАК Стеганос (б)

внесення даних у молодші біти зображення, особливо коли текстом заповнено не все поле, іноді можна навіть на око. Тому для зменшення впливу цих факторів було запропоновано використовувати різні траєкторії заповнення контейнера [5].

У горизонтальній площині контейнера стеганобіти прихованого повідомлення можна розміщувати як по детермінованим траєкторіям, так і використовувати псевдовипадкові маскувальні шаблони [3-5].

Розглянемо шаблони приховування інформації програмами Steganos Privacy Suite 2008 і ВІК-ВАК Стеганос.

Видно, що алгоритм розміщення прихованих бітів програми ВІК-ВАК Стеганос забезпечує кращу імітацію природних шумів і тому менше спотворює зображення-контейнер при більшій ємності прихованого повідомлення у порівнянні з методом заміни найменш значимих бітів.

Узагальнений алгоритм роботи програми ВІК-ВАК Стеганос можна подати у вигляді наступних етапів.

1. Визначення даних, що підлягають захисту стеганографічними методами.
2. Вибір зображення-контейнера.
3. Введення секретного ключа.
4. Пакування файлів.
5. Шифрування упакованих даних методами криптографії.
6. Вбудовування даних у контейнер.

Наведемо результати вбудовування повідомлень у контейнер (рис. 1) найбільш відомою програмою Steganos 2008 та розробленим алгоритмом для збільшених фрагментів.

Наведемо числові показники ступеня спотворень байтів зображення після внесення у них стегобітів для оцінки розробленого методу комп'ютерної стеганографії (табл. 1). В результаті заміни молодших біт контейнера стегобітами прихованої інформації змінюються значення байтів початкового зображення, що належать множині маскувального шаблона (рис.10), створеного стеганографічним алгоритмом. Величину відхилення байтів від початкового значення задає висота фігур стегобіт. Наприклад, для фігури висотою у два біти значення відхилення буде від 0 до 3, у три біти — від 0 до 7, відповідно для фігури висотою у чотири біти буде від 0 до 15. Тобто максимальне і мінімальне значення відхилення байтів від початкового значення задається кількістю двійкових розрядів висоти стегобітної фігури. У таблиці 1 представлено середні дані чисельних експериментів, що дозволяють оцінити ступінь спотворення зображення після внесення у нього прихованої інформації.

У зображення (рис.1) було вбудовано приховані дані з такими параметрами: два молодші біти червоного каналу, три молодші біти

Таблиця 1. Кількість відхилень значень байтів пікселів після внесення стегобітів у зображення-контейнер на рис. 1

V,%	Кольорові складові пікселя (RGB-байти)					
	Байт червоного		Байт блакитного		Байт зеленого	
	0..1	4..7	0..3	4..7	0..1	4..7
10	192737	0	126343	67452	193113	0
30	580490	0	311791	203919	580458	0
60	1169924	0	760933	409713	1170504	0
90	1743776	0	1133229	610580	1743951	0

V — об'єм заповнення стеганографічного контейнера стегобітами прихованої інформації.

блакитного каналу і два молодші біти зеленого каналу було замінено стегобітами. Кількість байтів з вбудованими стегобітами, відхилення числових значень яких становлять від 0 до 7 (висота фігури складає три стегобіти) зведено у таблицю 1.

З табл. 1 видно, що найбільша кількість відхилень значень байтів для всіх кольорів припадає на малі величини (0..3), що пояснює відсутність візуально помітних спотворень на рис. 11б.

Обсяг інформації прихованої у тестовому зображенні (рис. 1) для програми Steganos 2008 склав 700 КВ, а для програми ВІК-ВАК Стеганос — 1600 КВ. Отже, алгоритм, на якому базується программа ВІК-ВАК Стеганос, дозволяє забезпечити більший обсяг прихованої інформації у 2,34 рази без помітної втрати візуальної якості зображення-контейнера у порівнянні з алгоритмом, де використовується один наймолодший біт.

Інтеграція засобів персоналізації пристроїв зберігання даних з стеганографічним алгоритмом

Більшість користувачів використовують прості паролі для доступу до інформаційних ресурсів. Так, за даними досліджень, найпоширенішим у зловмисників логіном виявився root, що використовується в 12 разів частіше, ніж другий по популярності — admin. У числі інших популярних логінів опинилися test, guest, info, adm, mysql, user, administrator і oracle. Дослідники також з'ясували, що найпоширенішим методом генерації пароля є копіювання логіна. В 43% випадків логін був одночасно і паролем. Вельми популярним паролем виявився набір цифр 123. В числі інших, що користуються успіхом — 123456, password, 1234, 12345, passwd, test і 1. Таким чином, посилення парольного захисту є дуже актуальною тематикою розробок.

Саме тому, важливою науково-практичною задачею є інтеграція апаратно-програмного комплексу персоналізації інформаційних ресурсів з високорівневими сервісними програмами, що забезпечують захист конфіденційних даних, який ґрунтується на введенні секретних паролів. Аутентифікацію користувача буде виконувати персоналізований рідер, вбудований у флеш-накопичувач, мікроконтролер якого також буде генерувати криптостійкі кодові комбінації для програм захисту інформації (в тому числі для стеганографічних додатків) на основі як стохастичних, так і псевдовипадкових послідовностей.

У порівнянні із сучасними системами персоналізації інформаційних ресурсів, захисту інформації та ідентифікації/аутентифікації користувачів, розробка, що пропонується, а саме персоналізований флеш-накопичувач з ріде-

Таблиця 2. Модель подій і умов стеганографічного захисту інформації на базі персоналізованого флеш-накопичувача для графа мереж Петрі

№	Передумови	Події	Наслідки
1	Встановлено захищене з'єднання між флеш-накопичувачем і ПК (p0)	Запуск програми стеганос (t0)	Програму стеганос відкрито (p1)
2	p1	Вибір контейнера (t1)	Початок роботи з новим контейнером (p2)
3	p2	Регулювання заповнення контейнера [додавання і видалення файлів] та редагування змісту файлів контейнера [виклики програм обробки файлів] (t2)	Контейнер заповнено [файли архівовані] (p3)
4	p3	Введення паролю і ключа для нового контейнера (t3)	Пароль і ключ введено (p4)
5	p4	Зашифрування файлів і встроювання їх у контейнер; видача запиту на збереження контейнера у захищеній області пам'яті пристрою зберігання (t4)	Контейнер збережено у постійній пам'яті пристрою (p5)
6	p5	Вихід з програми. Перехід у режим очікування (t5)	p0
7	Запуск процедури авторизації редагування існуючого контейнера (p2')	Ввод пароля і ключа (t6) [для авторизації доступу до змісту існуючого контейнера]	Доступ до змісту контейнера неавторизованно [невірний пароль або ключ; спроби вичерпано] (p6')
8	p6'	Вихід з програми (t7)	Немає
9	Доступ до змісту контейнера авторизовано (p6)	Перегляд змісту контейнера користувачем (t8)	Внести зміни у склад або зміст файлів контейнера (p7)
10	p7	Зняти заборону на зміну [модифікацію] змісту і складу файлів контейнера (t10)	p2
11	Не вносити зміни у склад і зміст файлів контейнера (p7')	Вихід з редагування. Перехід у режим очікування (t9)	Немає

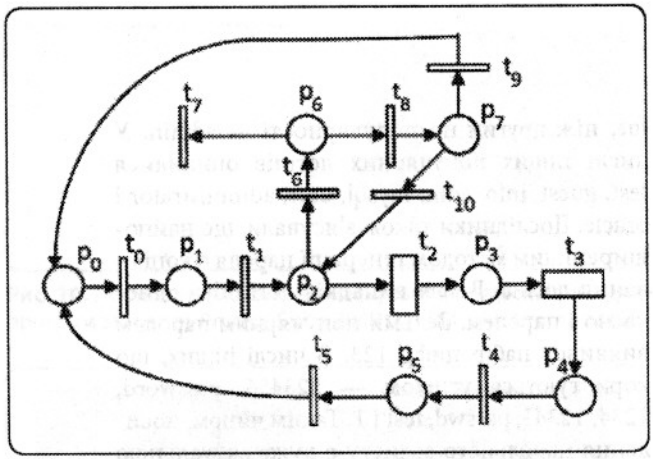


Рис. 12. Граф мережі Петрі для стеганографічного приховування інформації на базі флеш-накопичувачів

ром, що реалізує багатофакторну аутентифікацію, є значно дешевшою й головне більш надійною.

Щоб поєднати переваги стеганографічного приховування інформації з можливостями персоналізації інформації на базі пристроїв зберігання конфіденційної інформації, побудуємо модель «умови-події» і подамо результат у вигляді таблиці і графа мереж Петрі.

На основі моделі, опис якої наведено у табл. 2, побудуємо граф мережі Петрі для стеганографічного захисту інформації на базі персоналізованого флеш-накопичувача.

Таким чином, використання програм стеганографічного захисту інформації разом з персоналізованим пристроєм зберігання дозволяють підвищити рівень захисту конфіденційної інформації як для корпоративного, так і для особистого призначення.

Висновки

1. Створено інноваційний метод стеганографічної персоналізації інформації для ПК, що ґрунтується на обмеженнях кольорової чутливості зору людини і шумоподібному маскуванні даних.
2. Показано, що новий метод дозволяє суттєво збільшити обсяг прихованої інформації без помітних втрат у якості фотографічного зображення.
3. Запропоновано модель персоналізації інформаційних джерел, що базується на використанні апаратно-програмних ресурсів флеш-накопичувача для побудови системи безпечної передачі кодованої інформації у комп'ютерних системах і стегано-криптографічних методах захисту інформації.

Література

1. Корольов В.Ю., Поліновський В.В., Малікова О.В. Побудова системи захисту інформації на базі персоналізованого USB-флеш з використанням ключа-ідентифікатора // Вісник Хмельницького національного університету. — № 3. — 2008. — С. 175 — 181.
2. Корольов В.Ю. Персоналізація віртуальних обчислювальних ресурсів і інформаційних джерел в сервісно-орієнтованих архітектурах // Вісті академії інженерних наук України. — № 4 (34). — 2007. — С. 13 — 20.
3. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев — М.: СОЛОН-Пресс, 2002. — 272 с. (Серия «Аспекты защиты»)
4. В.О. Хорошко, Л.Д. Азаров, М.Є. Шелест, Ю.Є. Яремчук. Основи комп'ютерної стеганографії. Навчальний посібник. — Вінниця: ВДТУ, 2003. — 143 с.
5. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К.: «МК-Пресс», 2006.— 288 с., ил.
6. Радіотехніка: Енциклопедичний навчальний довідник: Навч. Посібник /за ред. Ю.Л. Мазора, Є.А. Мачуського, В.І. Правди. — К.: Вища шк., 1999. — 838 с.: іл.
7. Корольов В.Ю., Поліновський В.В. Система ВІК-персоналізації інформації для корпорацій // Захист інформації: збірник наукових праць НАУ. — Київ: НАУ. — 2007. — С. 145 — 148.

ВІСТІ АКАДЕМІЇ ІНЖЕНЕРНИХ НАУК УКРАЇНИ

Науково-технічний та громадський часопис Президії АІН України

Заснований:
в 1993 році

Періодичність:
щоквартально

Свідоцтво про реєстрацію:
Серія КВ №454 від 3.03.1994 р.

Засновник:
Академія інженерних наук України

Видавці:
Академія інженерних наук України, Національний технічний університет України «Київський політехнічний інститут»

У відповідності з постановою Президії ВАК України №2-05/6 від 12.06.2002 р. «Про відновлення статусу фахового журналу «Вісті Академії інженерних наук України» журнал є фаховим з інженерних наук (за погодженням з експертними радам).

Дизайн та верстка:
Гонжа Є.Ю. — www.gonzha.com

Матеріали номера рекомендовані до публікації Вченою радою Національного технічного університету України «Київський політехнічний інститут» Протокол №11 від 30.11.2009 р.

Адреса секретаріату АІН України:
03056, Київ, проспект Перемоги, 37
НТУУ «КПІ», корпус 2, к. 412
тел./факс +380 (44) 236-1052

Віддруковано:
У видавничо-друкарському комплексі Відкритого міжнародного університету розвитку людини «Україна»

ВІСТІ АКАДЕМІЇ ІНЖЕНЕРНИХ НАУК УКРАЇНИ

№2 (39) 2009

ЗМІСТ / СОДЕРЖАНИЕ / CONTENT