Whirlpool and Grostl. In Josef Pieprzyk, editor, CT-RSA, volume 5985 of LNCS, pages 350-365. Springer, 2010. 4. M. Schlaffer. Updated Differential Analysis of Grøstl. Grøstl website, January, 2011. 5. Kota Ideguchi, Elmar Tischhauser, and Bart Preneel. Improved collision attacks on the reduced-round Grostl hash function. In Information Security Conference, 2011. To appear. 6. Florian Mendel, Thomas Peyrin, Christian Rechberger, and Martin Schlaffer. Improved Cryptanalysis of the Reduced Grostl Compression Function, ECHO Permutation and AES Block Cipher. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, Selected Areas in Cryptography, volume 5867 of LNCS, pages 16-35. Springer, 2009. 7. Thomas Peyrin. Improved Differential Attacks for ECHO and Grostl. In Tal Rabin, editor, CRYPTO, volume 6223 of LNCS, pages 370-392. Springer, 2010. 8. Gilbert, H., Peyrin, T.: Super-Sbox cryptanalysis: Improved attacks for AES-like permutations. In Hong, S., Iwata, T., eds.: Preproceedings of FSE 2010. (2010) 368–387. 9. Yu Sasaki, Yang Li, Lei Wang, Kazuo Sakiyama, and Kazuo Ohta. Non-full-active Super-Sbox Analysis: Applications to ECHO and Grostl. In Masayuki Abe, editor, ASIACRYPT, volume 6477 of LNCS, pages 38–55. Springer, 2010. 10. Руженцев, В. И. Доказуемая стойкость Rijndael-подобных шифров к атаке усеченных дифференциалов. // Науково-технічний журнал: Радіоелектронні і комп'ютерні системи. – 2012. № 5. – С. 51–55. 11. L. R. Knudsen. Truncated and Higher Order Differentials. In B. Preneel, editor, Fast Software Encryption — Second International Workshop, Volume 1008 of Lecture Notes in Computer Science, pp. 196–211. Springer-Verlag, Berlin, Heidelberg, New York, 1995. 12. І. Д. Горбенко, В. І. Долгов, Р. В. Олійников, В. І. Руженцев та ін. Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікація // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – Харьков. – 2007 – Т. 6. – №2. – С. 195–208.

УДК 004.(056.53: 932)

С.М. Кущ, Д.О. Прогонов
Національний технічний університет України
"Київський політехнічний інститут"
Фізико-технічний інститут,
кафедра фізико-технічних засобів захисту інформації

АЛГОРИТМ ФОРМУВАННЯ СТЕГАНОГРАМ НА ОСНОВІ LSB-МЕТОДУ ТА ЙОГО ВИКОРИСТАННЯ ДЛЯ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ МЕТОДІВ АКТИВНОГО СТЕГОАНАЛІЗУ

Розроблено алгоритм формування стеганограм у цифрових зображеннях на основі LSB-методу. Алгоритм дає можливість у широких межах варіювати параметри методу приховання стегоданих. Розглянуто використання запропонованого алгоритму для розроблення нових методів активного стегоаналізу.

Ключові слова: стеганографія, LSB-метод, активний стегоаналіз.

The paper discusses the development of an algorithm for data embedding into digital images according to LSB method. The algorithm allows changing the parameters of the embedding method. Application of the proposed algorithm for creating new methods of active stegoanalysis is considered.

Key words: steganography, LSB method, active stegoanalysis.

Вступ

Забезпечення надійного захисту інформації з обмеженим доступом (ІзОД), зокрема конфіденційних даних організацій та підприємств від несанкціонованого доступу сьогодні є особливо актуаль-

ною задачею [1]. Постійне зростання обчислювальної потужності персональних комп'ютерів (ПК), а також поширення високошвидкісних телекомунікаційних мереж дає можливість стороні перехоплення використовувати комплексні методи як віддаленого впливу на ПК, так і створення прихованих каналів передавання ІзОД.

При формуванні прихованих каналів передавання конфіденційних даних з локальної обчислювальної мережі організації використовуються різноманітні методи цифрової стеганографії [2,3]. Вбудовуються дані найчастіше у різні види мультимедійних файлів (цифрові зображення (ЦЗ), аудіо- та відеодані) [4].

Стеганографічні програми, що знаходяться у вільному доступі (OutGuess, S-Tool, Steghide, OpenPuff, Masker тощо), як правило, мають закритий програмний код та не дозволяють змінювати параметри використовуваного методу приховання даних [4]: ступінь заповнення контейнеру, метод вибору пікселів для приховання даних, енергію окремого стегобіту тощо. Внаслідок цього зростає складність оцінювання ефективності застосовуваних методів пасивного та активного стегоаналізу, якщо a priori відсутня інформація щодо основних параметрів використовуваного алгоритму приховання даних. Тому перспективним стає розроблення програмних комплексів, що реалізують відомі стеганографічні методи вбудовування стегоданих у мультимедійні файли, з метою створення досконаліших методів стеганоаналізу, а також використання їх для підготовки фахівців з інформаційної безпеки.

Метою статті є розроблення та програмна реалізація алгоритму формування стеганограм у ЦЗ на основі методу Куттера–Джордана–Боссена (МКДБ), що належить до класу Least Significant Bits (LSB) методів. Алгоритм повинен надавати можливість:

1. Варіації ступеня заповнення контейнеру;
2. Зміни енергії окремого стегобіту при вбудовуванні його до контейнеру;
3. Зміни методу вибору пікселів ЦЗ для приховання окремих стегобітів.

Приховання інформації у цифрових зображеннях

Як контейнери для прихованого передавання інформації широко використовуються ЦЗ [3,5], що пояснюється такими причинами:

1. Значна надлишковість цифрового представлення зображень – відносно великий об'єм графічних файлів дає можливість або збільшувати розмір прихованого повідомлення, або підвищувати стійкість (робастність) сформованої стеганограми до відомих методів активного та пасивного стеганоаналізу;

2. Наявність текстурних областей з шумоподібною структурою – більшість реальних (не змодельованих з використанням ПК) ЦЗ внаслідок впливу шумів різної природи при формуванні зображення (шум матриці, шум квантування тощо) характеризуються наявністю областей з шумоподібною структурою. Використання таких областей дає змогу "замаскувати" наявність вбудованого повідомлення, що підвищує робастність стеганограм до можливих атак;

3. Особливості системи зору людини (СЗЛ) – людське око характеризується відносно низькою чутливістю до незначних змін кольорів, наявності шуму з невеликим значенням дисперсії, локальних змін яскравості та контрастності;

4. Значна кількість методів обробки зображень (фільтрація від шумів, стиснення тощо) – внаслідок цього можливо використовувати композицію декількох методів обробки ЦЗ з метою підвищення робастності стеганограми до можливих атак чи спотворень під час передавання їх каналами зв'язку із завадами.

Існуючі методи приховання інформації у ЦЗ можливо поділити на такі класи [2,3]:

1. Адитивні методи – ґрунтуються на додаванні стегоданих до контейнеру у просторовій або частотній областях. Ці методи є одними з найпоширеніших, зважаючи на відносно прості алгоритми приховання/екстракції повідомлень, а також можливість вбудовування даних у режимі реального часу;

2. Методи на основі квантування – під операцією квантування розуміється процес зіставлення великої множини можливих значень та деякої кінцевої множини чисел. Приховуються дані зміною

параметрів квантувателя (наприклад, кроку квантування, порядку розміщення кодових векторів тощо) або додаванням до сигналу (зображення) деякої константи d, яка віднімається після проведення квантування (дизеризовані квантувателі);

3. Статистичні (стохастичні) методи – повідомлення вбудовуються зміною статистичних параметрів контейнеру (наприклад, дисперсії значень яскравості окремого блоку пікселів) з подальшою перевіркою статистичних гіпотез та використанням тестових функцій для екстракції стегоданих;

4. Структурні методи – для приховання даних здійснюють послідовні афінні перетворення (поворот, зсув, масштабування) окремих блоків пікселів, вибраних за заданими критеріями (наприклад, ступінь кореляції з сусідніми блоками ЦЗ).

У статті розглядається МКДБ як один з найпоширеніших адитивних методів приховання даних у просторовій області ЦЗ. За цим методом вбудовуються стегодані у каналі синього кольору цифрового зображення [6], представленого у системі кольорів RGB. Використання каналу синього кольору обумовлено тим, що СЗЛ має відносно низьку чутливість до змін саме цієї компоненти кольору.

Вбудовування i-го біта повідомлення Q згідно із МКДБ проводиться зміною яскравості B_{xy} псевдовипадково обраного пікселя p_{xy} зображення C з розмірами $M \times N$ (пікселів) [6]:

$$\tilde{B}_{xy} = \begin{bmatrix} B_{xy} - u \cdot l_{xy}, q_i = 0 \\ B_{xy} + u \cdot l_{xy}, q_i = 1 \end{bmatrix} = B_{xy} + (2 \cdot q_i - 1) \cdot u \cdot l_{xy}, x \in [1; M], y \in [1, N], \quad (1)$$

$$l_{xy} = 0.2989 \cdot R_{xy} + 0.5866 \cdot G_{xy} + 0.1145 \cdot B_{xy}, x \in [1; M], y \in [1, N],$$

де R_{xy}, G_{xy} – значення яскравості обраного пікселя p_{xy} відповідно в каналах червоного та зеленого кольорів; $B_{xy}, \tilde{B}_{xy}$ – значення яскравості пікселя в каналі синього кольору, відповідно до та після проведення вбудовування; l_{xy} – загальна яскравість обраного пікселя p_{xy}; u – константа, що визначає енергію окремого стегобіту при прихованні повідомлення Q; q_i – i-й біт повідомлення Q.

Для забезпечення робастності прихованого повідомлення при проведенні можливих атак на стеганограму або передаванні її по каналу зв'язку із завадами необхідно збільшувати значення константи u. З іншого боку, занадто велике значення u може призвести до видимих (візуальних) спотворень контейнеру, що є демаскувальним фактором наявності вбудованого повідомлення.

Для підвищення ймовірності правильного розпізнавання окремого стегобіту на приймальній стороні кожний біт прихованого повідомлення Q повинен бути вбудованим у ЦЗ $t\,(t \geq 1)$ разів [3].

Екстракція прихованого повідомлення відбувається за відсутності вихідного "чистого" контейнера (випадок "сліпого" стеганодекодера). Для виявлення i-го біта прихованого повідомлення проводиться порівняння "прийнятого" (B^*_{xy}) та "очікуваного" ($\tilde{B}^*_{xy}$) значень яскравості пікселя p_{xy} в каналі синього кольору [6]:

$$\tilde{B}^*_{xy} = \frac{1}{4 \cdot s} \left[\sum_{i=(-s)}^{s} B^*_{x+i,y} + \sum_{j=(-s)}^{s} B^*_{x,y+j} - 2 \cdot B^*_{xy} \right], x \in [s+1; M-s], y \in [s+1; N-s], \quad (2)$$

$$d = \frac{1}{t} \sum_{i=1}^{t} \left[B^*_{xy,i} - \tilde{B}^*_{xy,i} \right] \Rightarrow \begin{bmatrix} q_i = 1, d > 0 \\ q_i = 0, d < 0 \end{bmatrix} \quad (3)$$

де s – кількість пікселів згори/знизу/справа/зліва відносно аналізованого пікселя; t – кількість "копій" i-го стегобіту.

Алгоритм формування стеганограм на основі методу Куттера–Джордана–Боссена

Враховуючи особливості МКДБ, запропоновано алгоритм формування стеганограм у ЦЗ (рис. 1):

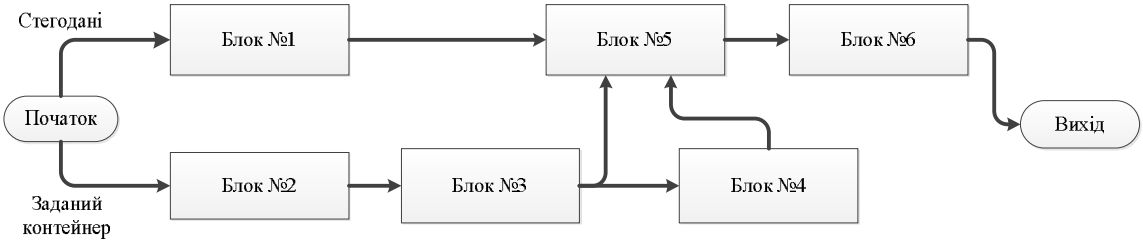


Рис. 1. Блок-схема алгоритму формування стеганограм за методом Куттер–Джордана–Боссена

На 1-му етапі роботи розробленого алгоритму відбуваються декомпресія та декомпозиція заданого ЦЗ. Декомпресія проводиться у блоці №2 для відновлення вихідного вигляду зображення у вигляді bmp-файла, а декомпозиція ЦЗ (блок №3) – з метою перетворення зображення на систему кольорів RGB та виділення каналу синього кольору. У блоці №1 інформаційне повідомлення перетворюється на бітовий потік. Пікселі для вбудовування окремих стегобітів за цим методом (послідовне, псевдовипадкове приховання) вибирають у блоці №4.

Формується стеганограма на 2-му етапі роботи алгоритму з використанням сформованого у блоці №1 бітового потоку, що відповідає стегоданим, каналу синього кольору заданого ЦЗ та масиву координат пікселів для приховання стегобітів.

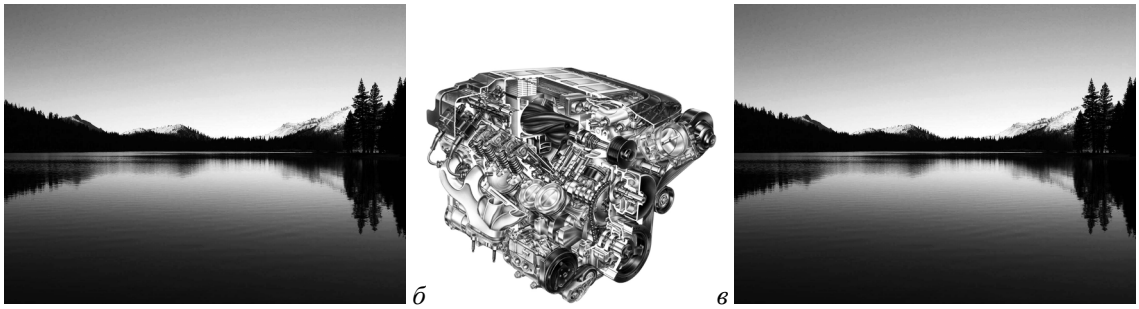
У блоці №6 проводиться компресія стеганограми шляхом об'єднання усіх каналів кольору зображення, а також відновлення вихідного графічного формату представлення ЦЗ.

Розроблений алгоритм було реалізовано програмно у вигляді m-файла програмного середовища MATLAB з графічним інтерфейсом користувача. Алгоритм дозволяє формувати стеганограми у ЦЗ, представлених у форматах bmp, jpeg, jp2, pcx, png, tiff.

На рис. 2 наведено приклад використання розробленого алгоритму для приховання графічних стегоданих. Як тестове зображення та стегодані (аксонометрія автомобільного двигуна) було використано повнокольорові ЦЗ (на рис. 2 подано у градаціях сірого кольору). Для цього випадку константи u, s та t у виразах (1–3) відповідно дорівнюють $u = 2$, $s = 3$, $t = 1$. Параметри тестового зображення та стегоданих наведено у таблиці:

Параметри тестового зображення та стегоданих

	Тестове зображення	Стегодані
Розмір (пікселів)	3264×2448	567×463
Глибина кольору $(бітів/(піксель \cdot канал))$	8	8
Роздільна здатність $(точок/дюйм)$	72	72
Формат представлення	JPEG True Color (v1.1)	BMP



а *б* *в*

Рис. 2. Приклад вбудовування даних з використанням розробленого алгоритму (15 % заповнення):

а – тестове зображення; б – стегодані; в – сформована стеганограма

Як видно із рис. 2, візуально розрізнити чистий (рис. 2, *а*) та заповнений контейнери (рис. 2, *в*) практично неможливо.

Активний стегоаналіз з використанням розробленого алгоритму формування стеганограм

Розроблений алгоритм дає можливість змінювати ступінь заповнення контейнера та параметри МКДБ на етапі приховання даних, тому перспективним є використання його для оцінювання ефективності різних методів активного стегоаналізу.

Враховуючи, що приховання даних у ЦЗ згідно із LSB-методами можливо трактувати як додавання до зображення деякого адитивного шуму, для деструкції прихованих повідомлень можна використовувати різні методи очищення цифрових зображень від шумів.

З метою придушення адитивних шумів у ЦЗ широко використовуються різні методи просторової фільтрації зображень [7], зокрема середньогеометричний (4) та середньогармонічний (5) фільтри:

$$\hat{f}(x,y)=\left[\prod_{(s,t)\in S_{xy}} f(s,t)\right]^{\frac{1}{m\cdot n}}; \tag{4}$$

$$\hat{f}(x,y)=\frac{m\cdot n}{\sum\limits_{(s,t)\in S_{xy}} \frac{1}{f(x,y)}}, \tag{5}$$

де $f(x,y), \hat{f}(x,y)$ – відповідно, значення яскравості пікселя p_{xy} до та після фільтрації ЦЗ; S_{xy} – окіл навколо "опорного" пікселя p_{xy}, в якому проводиться фільтрація; m,n – розміри околу S_{xy}.

Оцінювали ефективність середньогеометричного (СГмФ) та середньогармонічного (СГрФ) фільтрів за розробленим алгоритмом формування стеганограм на основі МКДБ для 100 тестових ЦЗ. На основі експертної оцінки тестові зображення було поділено на 2 групи по 50 ЦЗ – зображення з високим та низьким рівнем деталізації. Параметри тестових зображень та стегоданих наведено у таблиці. Дослідження проводили за таких рівнів заповнення контейнера – 5 %, 10 %, 15 %, 20 %, 25 %, 35 %, 45 %, 55 %, 65 %, 75 %, 85 %, 95 %. Розглядався випадок вбудовування стегобіту у псевдовипадково обрані пікселі контейнера.

Оскільки досліджувалося використання СГмФ та СГрФ з метою деструкції стеганограми як критерію ефективності наведених фільтрів було використано ступінь спотворення стегоданих – відсоток неінвертованих бітів прихованого повідомлення після обробки ЦЗ.

На рис. 3 наведено контурні графіки ступеня спотворення стегоданих з використанням СГмФ та СГрФ для груп зображень з високим та низьким ступенем деталізації.

Шкали відтінків контурних ліній (рис. 3) відповідають діапазону зміни відсотка неінвертованих стегобітів при фіксованих значеннях ступеня заповнення контейнера та розміру околу S_{xy}, в якому проводиться фільтрація з використанням СГмФ та СГрФ.

Необхідно зазначити, що для різних рівнів заповнення контейнера зі зростанням розміру околу S_{xy} ступінь спотворення стеганограми змінюється нерівномірно (рис. 3) – обидва фільтри характеризуються наявністю точки перегину на ізолініях наведених контурних графіків. Виявлену особливість можна пояснити так: оскільки близько розташовані пікселі ЦЗ характеризуються значною кореляцією значень яскравості, тому відгук як СГмФ, так і СГрФ у випадку відносно малого околу буде практично збігатися зі значенням яскравості "центрального" пікселя околу.

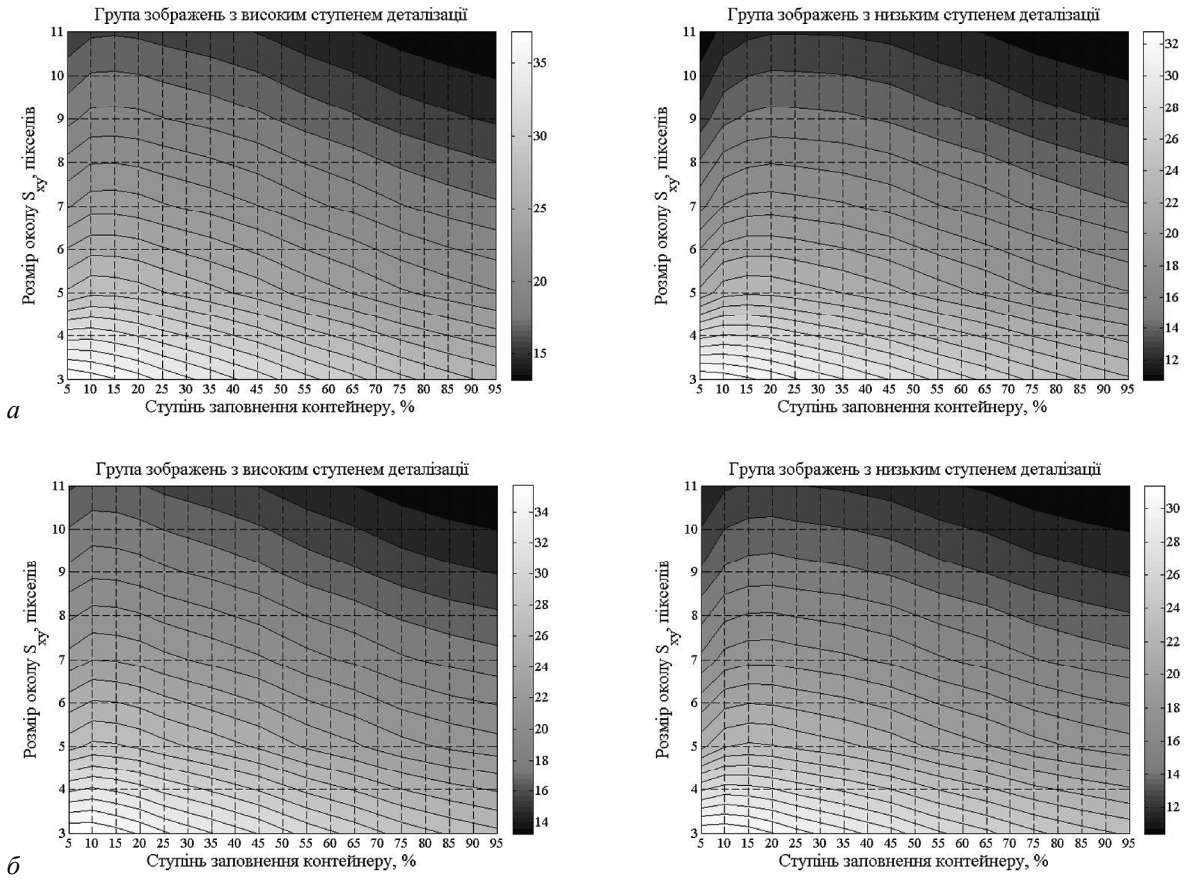


Рис. 3. Ступінь спотворення стеганограм при використанні:
а – середньогеометричного фільтра; б – середньогармонічного фільтра.

Приховання стегобітів у псевдовипадково обраних пікселях контейнера дає можливість зменшити "негативний" вплив вбудовування на ступінь кореляції значень яскравості близько розташованих пікселів ЦЗ. Тобто на наведених графіках (рис. 4) існує деяка точка перегину, для якої зменшення кореляційних зв'язків між сусідніми пікселями ще буде "компенсуватися" псевдовипадковим вибором пікселів для приховання стегобітів.

Висновки

Розроблений алгоритм формування стеганограм у цифрових зображеннях на основі методу Куттера–Джордана–Боссена дає змогу в широких межах варіювати параметри методу приховання даних. Алгоритм було застосовано для оцінювання ефективності різних методів як активного, так і пасивного стеганоаналізу [8,9]. За результатами проведених досліджень зроблено висновки щодо доцільності та високої ефективності використання алгоритму для створення досконаліших методів виявлення та деструкції прихованих даних у ЦЗ. Розроблений алгоритм також можна використати під час підготовки фахівців з інформаційної безпеки.

1. Домарев В.В. Безопасность информационных технологий. Системный подход [Монография]. – К.: ООО ТИД Диа Софт, 2004. – 992 с. 2. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография [Монография]. – М.: "Солон-Пресс", серия "Аспекты зашиты", 2002. – 272 с., ил. 3. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика [Монография]. – К.: "МК-Пресс", 2006. – 288 с., ил. 4. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стегоанализ [Монография]. – М.: Вузовская книга, 2009. – 220 с., ил. 5. Кущ С.М., Луценко В.М., Прогонов Д.О. Виявлення прихованих повідомлень як складова комплексної системи захисту інформації [Текст]. – Наук.-практ. журн. "Захист інформації", №3 (56). – К.: НАУ, 2012. – С. 65–71. 6. Kutter M., Jordan F.,

Bossen F. Digital signature of color images using amplitude modulation [Text]. – Proc. Of the SPIE Storage and Retrieval for image and video databases V, 1997. – Vol. 3022. – pp. 518-526. 7. Гонсалес Р., Вудс Р. Цифровая обработка изображений [Монография]. – Изд. 3-е, испр. и доп. – М.: Техносфера, 2013. – 1104 с., ил. 8. Прогонов Д. Выявление и деструкция информационных сообщений, встроенных в 2D-контейнеры на основе метода Куттера-Джордана-Боссена [Текст]. – Сборник тезисов участников XV Юбилейной Международной научно-практической конференции "Безопасность информации в информационно-телекоммуникационных системах". – К.: ООО "ИП Эдельвейс", 2012. – с. 34. 9. Прогонов Д., Кущ С. Оценка эффективности статистических методов стегоанализа 2D-контейнеров [Текст]. – Сборник тезисов участников XVI Международной научно-практической конференции "Безопасность информации в информационно-телекоммуникационных системах". – К.: ООО "ИП Эдельвейс", 2013. – с.52

УДК 004.950.430

А. А. Замула[1], В. И. Черныш[1], Ю. В. Землянко[2]
[1]Харьковский национальный университет радиоэлектроники,
[2]Харьковский государственный университет питания и торговли

КОНЦЕПТУАЛИЗАЦИЯ ИНФОРМАЦИОННЫХ ПРОЦЕССОВ И ТЕХНОЛОГИЙ В МЕТОДЕ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Запропоновано метод оцінювання ризиків інформаційної безпеки з використанням методу Байєса. Концептуалізуються параметри оцінювання системи організації повітряного руху.

Ключові слова: інформаційна безпека, ризик, обслуговування повітряного руху.

The paper discusses a method of information security risk assessment using Bayes' method. Assessment parameters for the air traffic management system are conceptualized.

Key words: information security, risk, air traffic management.

Введение и постановка задачи

За последнее время авиация достигла значительного развития. Этот прогресс был бы невозможен без достижений в области радиотехники, метеорологии, производства, информационных систем и технологий.

Управление различными технологическими процессами в авиации базируется на использовании информационных систем (ИС), к которым относятся источники информации, средства ее передачи, обработки, отображения, хранения, общесистемное и специальное программное обеспечение. Во всех информационных технологических процессах, а также процессах управления важную роль играет человеческий фактор [1].

Существование и функционирование воздушного транспорта связано с эффективностью использования аэронавигационной системы (АНС) и системы организации воздушного движения (ОрВД). Однако сегодня в литературе недостаточно четко определены положения, которые бы