МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

БЕКІРОВ АЛІ ЕНВЕРОВИЧ

УДК 621.391.2: 004.056

МЕТОД ПІДВИЩЕННЯ БЕЗПЕКИ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ В КРИТИЧНИХ СИСТЕМАХ НА ОСНОВІ СТРУКТУРНОГО СТЕГАНОГРАФІЧНОГО КОДУВАННЯ

21.05.01 – інформаційна безпека держави

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2015

Дисертацією є рукопис.
Робота виконана в Харківському національному університеті радіоелектроніки, м. Харків.

Науковий керівник: доктор технічних наук, професор
Бараннік Володимир Вікторович,
Харківський університет Повітряних Сил імені Івана Кожедуба, Міністерство оборони України, начальник кафедри «Бойового застосування та експлуатації АСУ».

Офіційні опоненти: доктор технічних наук, професор
Конахович Георгій Филимонович
Національний авіаційний університет «НАУ», завідувач кафедри телекомунікаційних систем;

кандидат технічних наук, доцент
Бабенко Віра Григорівна,
Черкаський державний технологічний університет, доцент кафедри інформаційної безпеки та комп'ютерної інженерії.

Захист відбудеться « 04 » червня 2015 р. о 14 годині на засіданні спеціалізованої вченої ради Д 26.062.17 у Національному авіаційному університеті за адресою: 03680, м. Київ, просп. Космонавта Комарова, 1, ауд. 11-111.

З дисертацією можна ознайомитись у бібліотеці Національного авіаційного університету за адресою: 03680, м. Київ, просп. Космонавта Комарова, 1.

Автореферат розісланий «29» квітня 2015 р.

Учений секретар спеціалізова
вченої ради Д 26.062.17
к.т.н., доцент С.О. Гнатюк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Досвід функціонування критичних систем в умовах активної протидії противника виявив гостру необхідність забезпечення потрібного рівня безпеки спеціальних інформаційних ресурсів (СІР), які є складовою частиною державної інформації. Така необхідність з одного боку диктується підвищеною значимістю СІР для інформаційної підтримки функціонування систем критичного призначення у тому числі в умовах рішення конфліктних ситуацій. С іншого боку підвищуються загрози порушення конфіденційності та цілісності СІР, що обумовлено оперативно-програмними та інформаційно-технологічними можливостями противника. Тому підвищення безпеки спеціальних інформаційних ресурсів в інфокомунікаційних системах є актуальною ***науково-прикладною*** задачею.

Для рішення сформульованої задачі необхідно розробити нові шляхи забезпечення безпеки державної інформації. Одним з напрямків являється використання стеганографічних методів. Базою для реалізації такого підходу являються системи відеоконференційного зв'язку, широке використання мультимедійних засобів, наявність широкого відеоінформаційного поля, наявність прив'язки службової інформації до конкретного відеоматеріалу.

Вагомий внесок у розвиток теоретичних основ та технологій стеганографічних перетворень здійснили такі вчені, як Задирака В.К., Кобозєва А.А., Конахович Г.Ф, Корченко О.Г., Шелест М.Є., Юдін О.К. Щодо зарубіжних дослідників, то важливими є здобутки Грибуніна В.Г, Дармсдеттера В., Фридрих Ю.

Однак проведений аналіз існуючих методів стеганографічних перетворень виявив наступні проблемні недоліки: недостатнє значення відносної стеганографічної ємності; не припустиме значення стійкості вбудованих даних до атак противника; значні візуальні спотворення стеганограми. Такі недоліки обумовлені тим, що в процесі стеганографічних перетворень в основному враховуються психовізуальні закономірності. Вилучення вбудованої інформації здійснюється з використанням кореляційних залежностей, які порушуються внаслідок нелінійної обробки стеганограмм. Тому необхідно використовувати для побудови стеганографічних систем механізми виявлення структурних закономірностей. Таким чином тема науково-прикладних досліджень, яка пов'язана з розробкою методу підвищення безпеки спеціальних інформаційних ресурсів в системах критичного призначення на основі структурного стеганографічного кодування є *актуальною*.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційні дослідження проводились у відповідності з програмами та нормативними документами: Законів України «Про Концепцію Національної програми інформатизації» від 04.02.1998 № 75/98-ВР, «Про інформацію» від 02.10.1992 № 2657-XII, «Про державну таємницю» від 21.01.1994 №3855-XII,

«Про науково-технічну інформацію» від 25.06.1993 №3322-XII, Концепції технічного захисту інформації в Україні від 08.10.1997.№1126, Концепції (основи державної політики) національної безпеки України від 16.01.1997 №3/97-ВР, Концепції Національної безпеки України, Концепції розвитку зв'язку України, Комплексної програми розвитку і реформування Збройних Сил України на період до 2017 року, Національних космічних програм України від 30.09.2008 N 608-VI. Основні результати дисертаційної роботи відображені у звіті за НДР «Технології створення інтегрованих інформаційних систем на основі мереж цифрового мобільного зв'язку» (№ 0113U000360), у якій автор дисертації був виконавцем.

Мета і задачі дослідження. Мета дисертаційної роботи полягає у розробці методу підвищення безпеки спеціальної інформації для інфокомунікаційних систем критичного призначення на основі стеганографічних перетворень.

Для досягнення сформульованої мети необхідно вирішити такі завдання:

1. Обґрунтувати підхід для вдосконалення методів безпосереднього вбудовування інформації в цифрове зображення-контейнер.
2. Розробити метод структурного стеганографічного кодування для підвищення безпеки спеціальної інформації.
3. Створити метод для локалізації структурної стеганографічної надлишковості для підвищення стійкості щодо атак на виявлення факту вбудованої інформації.
4. Побудувати структурну стеганографічної систему з маскуванням стеганографічної надмірності.
5. Розробити програмну реалізацію і провести оцінку ефективності розробленої стеганографічної системи.

Об'єкт дослідження. Процеси підвищення безпеки спеціальних інформаційних ресурсів в інфокомунікаційних системах.

Предмет дослідження. Методи підвищення безпеки спеціальної інформації на основі технології стеганографічного вбудовування в зображення-контейнер.

Методи дослідження. Проведенні дослідження базуються на методах теорії функціонування складних систем, положеннях теорії цифрової обробки сигналів, методах захисту інформації, положеннях теорії стеганорафічних перетворень та теорії інформації.

Наукова новизна отриманих результатів дослідження полягає у тому, що: 1. Вперше розроблена стеганографічна система на основі безпосереднього вбудовування приховуваної інформації в відеопослідовність. На відміну від інших стеганосистем забезпечується одночасне вбудовування та вилучення прихованої інформації відповідно в процесі формування та реконструкції коду-контейнера в базисі основ нерівновагового позиційного числа. Це забезпечує вбудовування прихованої

інформації на основі обліку кількості структурної надлишковості фрагментів відеозображень.

2. Вперше розроблено метод структурного стеганографічного кодування з маскуванням. На відміну від інших методів забезпечується вбудовування приховуваної інформації в процесі нерівновагового позиційного кодування з подальшою локалізацією стеганографічної надмірності. Це дозволяє знизити можливість виявлення зловмисником факту наявності вбудованої інформації.

3. Вперше розроблено метод демаскуючого стеганографічного декодування. На відміну від існуючих методів вилучення прихованої інформації і відновлення нерівновагового позиційного числа проводиться на основі реконструкції стеганокода за біполярним принципом з демаскуванням стеганографічної надмірності. Це дозволяє підвищити ефективність вилучення прихованої інформації і локалізувати атаки зловмисника щодо виявлення факту наявності прихованої інформації.

4. Отримали подальше вдосконалення методи підвищення безпеки державної інформації на основі застосування стеганографічних систем. На відміну від інших систем застосовується структурне стеганографічне маскуюче та демаскуюче перетворення. Це дозволяє підвищити скритність і цілісність вибудуваної інформації.

Новизна отриманих результатів підтверджується відсутністю розроблених методів у існуючих стандартах цифрової обробки зображень та стеганографічного кодування.

Практичне значення одержаних результатів досліджень полягає у тому, що:

1. При однакових значеннях стеганографічної ємності виграш для розробленого методу щодо методу найменш значимого біту за величиною пікового відношення сигнал-шум складає в середньому від 8 до 32 дБ.

2. Для розробленого методу виграш у значенні стеганографічної ємності щодо методу на основі розширення спектру становить від 1,22 до 5,47%.

3. Для розробленого методу виграш у значенні ймовірності безпомилкового вилучення щодо методу найменш значимого біту і методу на основі розширення спектру становить: для методу найменш значимого біту 40%; для методу на основі розширення спектру 50%.

4. Для різних значень коефіцієнта квантування найбільшою стійкістю володіють дані, стеганографічно вбудовані в нерівновагове позиційне число довжиною шість елементів. Навпаки найменшою стійкістю володіють дані стеганографічно вбудовані в нерівновагове позиційне число довжиною, яка дорівнює двом елементам. Кількість безпомилково вилучених біт в умовах застосування противником атак для розробленого методу в середньому приймає значення 90%.

5. Виграш для розробленого методу щодо методу на основі розширення спектру і методу найменш значимого біту за кількістю безпомилково

вилучених даних в умовах застосування противником активних атак становить: щодо методу найменш значимого біту - 40%, щодо методу на основі розширення спектру - 40%.

Практична значущість отриманих результатів дисертації підтверджується їх застосуванням при виконанні дослідно-конструкторських робіт у Науково-технічному спеціальному конструкторському бюро «ПОЛІСВІТ» (акт реалізації від 23.03.2014) та у ДНДІ МВС України (акт реалізації від 23.01.2015).

Особистий внесок здобувача дисертаційної роботи в публікаціях, які виконано в співавторстві, полягає у тому, що: у статті [1] – розроблено стеганографічну систему на основі формування коду-контейнеру в нерівноваговому позиційному базисі; у статті [2; 4] – розроблено підхід для покращення характеристик безпосереднього стеганографічного вбудовування інформації в зображення-контейнер; у статті [3] – визначено кількість біт, які витрачені на представлення одного блоку і макроблоку для всіх складових кольорової моделі при кодуванні; у статті [5] – обґрунтовано необхідність підвищення безпеки інформаційних ресурсів в системах спеціального призначення; у статті [6] – визначено залежність сумарної кількості операцій від кількості типових операцій обробки зображень з виявлення значимих компонент трансформант; у статті [7] – проаналізовано можливості зловмисника щодо атак на відеоінформаційний ресурс в інформаційно-телекомунікаційних мережах; у статті [8] – сформульована концепція структурного стеганографічного кодування на базі нерівноваговго кодування; у статті [9] – обґрунтована можливість використання нерівноваговго кодування в якості функціонального перетворення для стеганографічного вбудовування; у статті [10] – розроблено стеганографічну систему з маскуванням стеганографічної надлишковості.

Апробація результатів дисертації. Основні результати дисертації доповідалися і були схвалені на XII міжнародній конференції «TCSET'2014», Львів-Славське, 25 лютого – 1 березня; на Шостій Міжнародній науково-практичній конференції ″Проблеми і перспективи розвитку IT-індустрії″, Харків, 17 - 18 квітня 2014 р.; на Четвертій міжнародній науково-практичній конференції «ITSEC», Київ, 20 - 23 травня 2014 р.; на Четвертій міжнародній науково-практичній конференції «Інформаційні технології та комп'ютерна інженерія», Вінниця, 28 - 30 травня 2014 р.; International Symposium «IEEE East-West Design & Test», Kiev, Ukraine, 26–29 September 2014; на Науково-методичній конференції "Сучасні проблеми телекомунікації і підготовка фахівців в галузі телекомунікацій - 2014″, Львів, 1-4 листопада 2014р; на Третій міжнародній науково-технічній конференції ″Проблеми інформатизації″, Київ, 11 - 13 грудня 2014 г.; на XIII міжнародній конференції CADSM'2015, Polyana-Svalyava (Zakarpattya), 24-27 February

2015; на науково-технічній конференції "Інформаційна безпека України", Київ, 12-13 березня 2015 р.

Публікації. Основні положення і результати дисертаційної роботи опубліковані у 20 наукових працях, серед яких 11 статей, дві з яких входять до міжнародних науково-метричних баз та одна одноосібна стаття. Апробація результатів дисертації відображена у 9 тезах доповідей на міжнародних науково-технічних та науково-практичних конференціях. Зокрема три апробації на конференціях, які входять до складу міжнародної організації IEEE.

Структура і обсяг дисертації. Дисертація складається із вступу, чотирьох розділів, списку використаної літератури та трьох додатків. Загальний обсяг дисертації становить 178 сторінок, з них: 49 ілюстрацій на 17 сторінках, 7 таблиць на 3 сторінках, список використаної літератури зі 120 джерел на 12 сторінках та трьох додатків на 13 сторінках. Дисертація написана російською мовою.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність тематики наукового дослідження, сформульовано науково-прикладну задачу та доведено її важливість, сформульовано мету і завдання дисертації, представлено наукову новизну та практичне значення отриманих наукових результатів.

У першому розділі обґрунтовується необхідність підвищення безпеки спеціальних інформаційних ресурсів в системах критичного призначення. Обґрунтовується необхідність застосування стеганографічних методів на основі безпосереднього вбудовування приховуваного повідомлення. Виявляються проблемні недоліки існуючих стеганогрфічних перетворень.

Підвищення безпеки СІР полягає в:

1) зменшенні імовірності $P_{від}$ правильного відновлення спеціальної інформації, що задається виразом $P_{від} \rightarrow 0$;

2) збільшенні часу $T_{пр}$, необхідного противнику для виявлення та правильної реконструкції інформації, що задається наступним чином $T_{пр} \rightarrow \max$.

У зв'язку з чим на ряду з методами криптографії необхідно використовувати стеганографічні методи.

Найважливішими показниками ефективності методів стеганографічного перетворення є:

1. Відносна стеганографічна ємність $w_{від}$ стеганографічної системи. У загальному випадку стеганографічна ємність $w_{від}$ залежить від об'єму $w_{вбуд}$ вбудованих даних та об'єму $W_{вих}$ зображення-контейнера:

$$w_{від} = w_{вбуд} / W_{вих}.$$

2. Імовірність $P_{вил}$ безпомилкового вилучення вбудованих даних авторизованим користувачем:

$$P_{вил} = w_{вил} / w_{вбуд},$$

де $w_{вил}$ - об'єм безпомилково вилучених даних.

3. Пікове відношення сигнал-шум h зображення з вбудованими даними.

Основними недоліками існуючих стеганографічних систем являються: низька стійкість вбудованих даних до атак противника, де втрачається до 50 % вбудованої інформації; недостатнє значення відносної стеганографічної ємності, не перевищує 7 %; значна кількість внесених спотворень в зображення-контейнер. Вони обумовлені використанням психовізуальних закономірностей зображень для прихованого вбудовування інформації.

Отже існуючі технології стеганографічних перетворень не забезпечують в повній мірі системних вимог в критичних умовах з активною протидією противника.

Звідси необхідно розробити метод підвищення безпеки спеціальної інформації для інфокомунікаційних систем на основі стеганографічного перетворення, яке задається функціоналом $F\{P_{вил}, w_{від}, h\}$ в умовах виконання наступних вимог:

$$P_{вил} \geq P_{вил}^{(нб)}; \; w_{від} \geq w_{від}^{(нб)}; \; h \geq h^{(нб)}.$$

Тут $F\{P_{из}, w_{отн}, h\}$ - функціонал, який реалізує стеганографічний метод вбудовування спеціальної інформації; $P_{вил}^{(нб)}$ - необхідне значення імовірності безпомилкового вилучення вбудованих даних авторизованим користувачем; $w_{від}^{(нб)}$ - необхідне значення відносної стеганографічної ємності системи; $h^{(нб)}$ - необхідне значення пікового відношення сигнал-шум.

У **другому розділі** розглядається клас методів безпосереднього вбудовування приховуваного повідомлення. Для усунення виявлених недоліків запропоновано синтезувати функціональне перетворення для числа з вбудованою інформацією. В цьому випадку під числом розуміється послідовність елементів зображення-контейнера.

Існуючі методи безпосереднього вбудовування інформації мають наступні недоліки.

У разі вбудовування в молодший біт, що задається виразом $a'_n = b_\xi$, $A'_2 = \{a_1, a_2, ..., a_{n-1}, a'_n\}$, забезпечується найменша візуальна помітність, що описується виразом $\varepsilon(A; A') \to 0$. Тут $\varepsilon(A; A')$ - кількісна метрика, яка вказує

на ступінь відмінності між значенням числа A до вбудовування інформації та A' з вбудованою інформацією. A'_2 - число, що містить вбудований біт; b_ξ - ξ-й елемент, вбудованої двійкової послідовності, $a'_i \in [0;1]$, $b_\xi \in [0;1]$. Але в цьому випадку досягається найменша стійкість до атак противника та описується виразом $P_{вил}(b'_\xi = b_\xi) \to 0$, де $P_{вил}$ - імовірність безпомилкового вилучення вбудованої інформації; b'_ξ - значення ξ-го елемента приховуваного повідомлення, який вилучається при наявності трансформуючого або атакуючого впливу.

Навпаки, вбудовування в старший біт, яке описується формулою $A'_2 = \{a'_1, a_2, a_n\}$, $a'_1 := b_\xi$, забезпечується стійкість до атак. Але в цьому випадку відбувається найбільша візуальна помітність, $\varepsilon(A; A') \to \max$.

Для усунення виявлених недоліків пропонується синтезувати функціонал $f(A')$ від числа з вбудованою інформацією A' в умовах забезпечення наступних вимог:

1) взаємнооднозначність прямого $f(A')$ і зворотнього $f^{(-1)}(C)$ функціональних перетворень $f(A') = f^{(-1)}(C)$;

2) можливість здійснювати зворотнє перетворення за біполярним принципом на основі наступних виразів: $A(\gamma)'' = f^{(-1)}(C; \Psi^{(\gamma)})$,

$$\delta(B'; B) \to \begin{cases} \max, \to \gamma = 1 \ \& \ \Psi = \Psi^{(1)}; \\ 0, \quad \to \gamma = 2 \ \& \ \Psi = \Psi^{(2)}, \end{cases}$$

де $A(\gamma)''$ - відновлене значення числа A; $\delta(B'; B)$ - кількісна метрика, яка вказує на ступінь відмінності між вихідним повідомленням B_2 і вилученим повідомленням B'_2; $\Psi^{(1)}$ - стандартні умови зворотнього перетворення; $\Psi^{(2)}$ - ключова інформація.

3) функціональне перетворення повинно бути інваріантним до атак.

В якості такого функціоналу пропонується використовувати кодообразуючу функцію для нерівновагового числа. В цьому випадку вихідний елемент зображення розглядається як нерівновагове позиційне число A, яке складається з m елементів, а саме $A = \{a_1; ...; a_{i,j}; ...; a_{m,j}\}$.

Імплантація біта b_ξ приховуваного повідомлення проводиться в нерівновагове число A, що задається наступною формулою: $A' = \varphi'(A; b_\xi)$

Другий етап включає формування значення стеганокода з урахуванням ключової інформації на основі виразу $N' = f'(A')$. На третьому етапі

будується результуюче кодове подання для числа з імплантованим бітом $C'_2 = \varphi_c(N'; \Psi^{(1)})$. Зворотне стеганографічне перетворення виконується за біполярним принципом. В цьому випадку для авторизованого користувача використовується наступна система формул:

$$\varphi'^{(-1)}(A''(2)) = \begin{cases} b'_\xi, & \to b'_\xi = b_\xi, \\ A''', & \to A''' = A, \end{cases}$$

де $\varphi'^{(-1)}$ - оператор вилучення при авторизованому доступі; A''' - відновлене значення вихідного нерівновагового числа.

Зворотне стеганографічне перетворення для неавторизованого користувача при стандартних умовах виконується на основі виразу $A(1)'' = f'^{(-1)}(C_2; \Psi^{(1)})$.

Тут $A(1)''$ - відновлене значення нерівновагового позиційного числа при неавторизованому доступі.

Таким чином синтезовано функціональне перетворення для числа із вбудованою інформацією, яке відповідає вимогам щодо візуальної скритності та стійкості до атак.

У третьому розділі будується стеганографічна система для вбудовування приховуваного повідомлення в процесі нерівновагового кодування з локалізацією структурної стеганографічної надлишковості.

Схема стеганографічної системи з маскуванням структурної стеганографічної надлишковості представлена на рис 1.

Процес стеганографічного кодування, який представляє собою формування стеганокоду на основі кодування нерівновагове число (НЧ) з імплантованим елементом прихованого повідомлення, включає наступні дії:

1. Імплантація елемента $a'_{\gamma,j}$ приховуваного повідомлення в НЧ $A(j)' = A(j) \bigcup b_\xi$, $b_\xi = a'_{\gamma,j}$, де $A(j)'$ - НЧ з елементом $a'_{\gamma,j}$, імплантованим на γ -ю позицію.

Однак для такого підходу існує стеганографічна надмірність $R(j)_{стег}$:

$$R(j)_{стег} = q(j)' - q(j) \geq 0,$$

де $q(j)$ - кількість біт для представлення кодограми НЧ; $q(j)'$ - кількість біт для представлення кодограми НЧ з імплантованим елементом.

Тоді для забезпечення мінімального значення стеганографічної надмірності повинна виконуватися наступна умова: $(\log_2 \psi'_{\gamma,j}) \to \min$.

Для цього пропонується в НЧ вбудовувати один біт інформації. У цьому випадку основа $\psi'_{\gamma,j}$ вбудованого елемента буде дорівнювати двом, а довжина кодограми буде визначатися за формулою:

$$q(j)' = [\log_2 \psi'_{\gamma,j} + \sum_{i=1}^{m} \ell og_2 \psi_{i,j}] + 1 = [\sum_{i=1}^{m} \ell og_2 \psi_{i,j}] + 2.$$

де $\psi_{i,j}$ основа елемента $a_{i,j}$ НЧ.

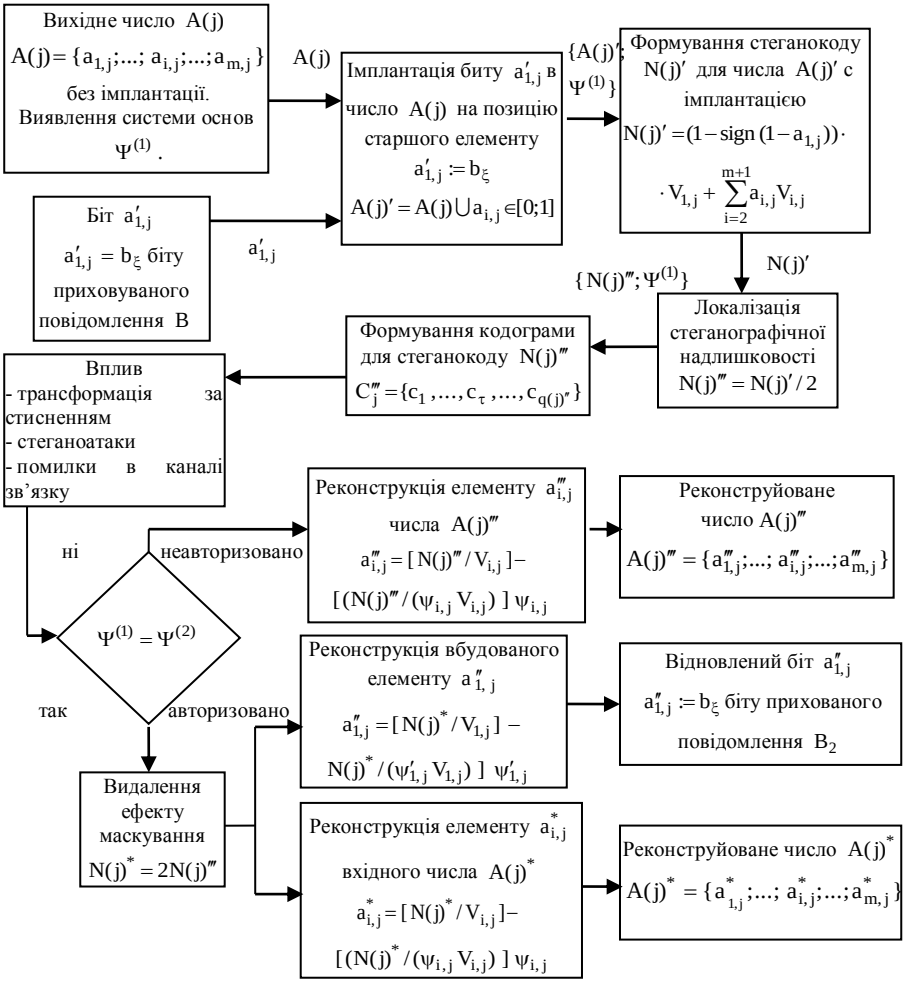

Рис. 1. Структурна схема стеганографічної системи на основі імплантації приховуваного двійкового елемента на старшу позицію НЧ з подальшим кодуванням і маскуванням

Враховуючи спотворення, які вносяться в результаті маскування, для стійкості вбудованих даних імплантацію біта приховуваного повідомлення пропонується проводити на позицію старшого елемента НЧ. У цьому випадку вага вбудованого елемента $V'_{1,j}$ в НЧ буде найбільшою і описуватиметься наступним виразом: $V'_{\gamma,j} = V'_{1,j} = \max\limits_{1\le i\le m+1} \{V'_{i,j}\}$.

Тоді імплантація біта b_ξ на позицію старшого елемента НЧ $A(j)$ буде здійснюватись за наступною формулою:

$$A(j)' = A(j) \cup b_\xi, \quad b_\xi = a'_{1,j} \in [0,\ 1].$$

2. Формування стеганокода $N(j)'$ для числа з імплантованим елементом. Для цього використовується наступна формула:

$$N(j)' = \begin{cases} \sum\limits_{i=2}^{m+1} a_{i,j} V'_{i,j} = N(j), & \to a'_{1,j} = 0; \\ V'_{1,j} + \sum\limits_{i=2}^{m+1} a_{i,j} V'_{i,j} = V'_{1,j} + N(j), & \to a'_{1,j} = 1; \end{cases}$$

де $V'_{i,j}$ - ваговий коефіцієнт елемента $a_{i,j}$: $V'_{i,j} = \prod\limits_{\xi=i+1}^{m+1} \psi_{\xi,j}$;

$V'_{1,j}$ - ваговий коефіцієнт елемента $a'_{1,j}$: $V'_{1,j} = \prod\limits_{i=2}^{m+1} \psi_{i,j}$.

3. Маскування структурної стеганографічної надлишковості.

Для локалізації стеганографічної надлишковості *пропонується* проводити маскування шляхом корекції кодограми стеганокоду як показано на рис. 2.

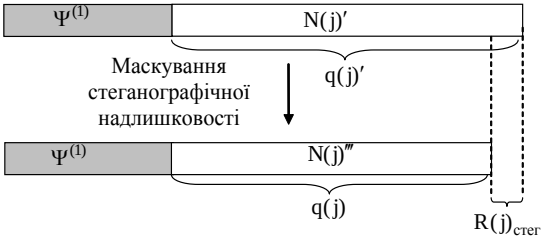

Рис. 2. Схема локалізації стеганографічної надмірності $R(j)_{стег}$

Процес маскування передбачає приведення довжини $q(j)'$ кодограми стеганокоду до довжини $q(j)$ коду-контейнеру шляхом відкидання молодшого біту на основі наступного виразу:

$$N(j)''' = N(j)'/2.$$

4. Формування кодограми C'''_j для кодового представлення скорегованого стеганокоду $N(j)'''$ на основі наступної формули: $C'''_j = \{c_1, ..., c_\tau, ..., c_{q(j)''}\}$.

Тут $q(j)''$ - довжина кодограми C'''_j, яка дорівнює $q(j)'' = [(\sum_{i=1}^{m+1} \ell og_2 \psi_{i,j})/2] + 1$.

На основі викладеного сформулюємо наступне визначення:

Формування стеганокоду на основі кодування нерівновагового числа з імплантованим елементом прихованого повідомлення називається *структурним стеганографічним кодуванням в нерівноваговому базисі.*

Метод стеганографічного декодування здійснюється за біполярним принципом для авторизованого та неавторизованого користувача.

У випадку неавторизованого доступу зловмисник не має інформації щодо наявності вбудованої інформації та позиції імплантованого елементу. Тоді декодування буде включати наступні дії:

1. Витяг з кодограми скорегованого стеганокода за допомогою системи основ нерівновагового позиційного числа.

2. Відновлення елементів $a'''_{i,j}$ вихідної відеопослідовності на основі наступного виразу: $a'''_{i,j} = [N(j)''' / V_{i,j}] - [N(j)''' / (\psi_{i,j} V_{i,j})] \psi_{i,j}$.

3. Оцінка якості візуального сприйняття реконструйованого зображення, тобто проведення атаки щодо факту наявності вбудованої інформації.

Навпаки, у разі авторизованого доступу користувачеві доступна наступна інформація: позиція стеганокоду в стисненому уявлені зображення; основа імплантованого біту $a'_{1,j}$; позиція імплантованого біту $a'_{1,j}$.

У цьому випадку стеганографічне декодування буде містити наступні етапи:

1. Витяг з кодограми скорегованого стеганокоду на основі системи основ нерівновагового позиційного числа.

2. Усунення ефекту маскування. Проведення демаскування стеганокоду виконується на основі наступного правила: $N(j)^* = N(j)''' \cdot 2$.

3. Відновлення вбудованого елемента $a''_{1,j}$. Даний етап реалізується на основі виразу: $a''_{1,j} = [N(j)^* / V'_{1,j}] - [N(j)^* / (\psi'_{1j} V'_{1,j})] \psi'_{1,j}$.

4. Відновлення решти елементів $a^{*}_{i,j}$ вихідної відеопослідовності здійснюється за формулою: $a^{*}_{i,j} = [\,N(j)^{*} / V'_{i,j}\,] - [\,N(j)^{*} / (\psi_{i,j}\, V'_{i,j})\,]\,\psi_{i,j}$.

Таким чином розроблена стеганографічна система для вбудовування прихованого повідомлення в нерівноваговому числі з маскуванням структурної стеганографічної надлишковості.

У четвертому розділі проводиться порівняльна оцінка розробленого стеганографічного методу та існуючих методів щодо ефективності використання для прихованої передачі спеціальної інформації.

Порівняльна оцінка величини відносної стеганографічної ємності і пікового відношення сигнал-шум різних класів зображень (рис. 3 і 4), декодованих при неавторизованому доступі, для розробленого методу (РМ) та методів найменш значущого біту спектральних коефіцієнтів зображення (НЗБ в режимі 2) і методу на основі розширення спектру (РС) приведені в табл. 1.

Рис. 3. Зображення «Знімок аеропорту» декодоване неавторизованим користувачем

Рис. 4. Зображення «Літак на фоні неба» декодоване неавторизованим користувачем

Дослідження табл. 1 дозволяє визначити що при однакових значеннях відносної стеганографічної ємності виграш для розробленого методу щодо існуючих за величиною пікового відношення сигнал-шум для різних класів зображень складає від 5 до 80%.

Порівняльна оцінка значень імовірності безпомилкового вилучення вбудованих даних при авторизованому доступі для методів НЗБ в режимі 2, РС і розробленого методу в умовах відсутності атак на вбудоване повідомлення розглядається на рис. 5.

Таблиця 1

Залежність значення $w_{отн}$ від ПВСШ для різних класів зображень

Відносна ємність, %	Метод стеганографічного вбудовування		Значення ПВСШ, дБ		
			«Знімок аеропорту»	«Фотознімок»	«Літак на фоні неба»
6,25	НЗБ режим 2	q = 1	14,67	14,12	14,62
		q = 2	11,17	12,03	11,13
		q = 4	8,69	9,11	8,79
	РМ	m = 2	41,799	37,768	42,911
4,1	РМ	m = 3	39,074	35,058	40,052
3,1	НЗБ режим 2	q = 1	32,12	33,42	31,43
		q = 2	26,43	22,15	20,45
		q = 4	18,54	18,27	18,03
	РМ	m = 4	37,94	33,978	38,973
2	РМ	m = 6	36,931	33,019	38,121
0,78	РС	ω = 16	16,93	13,019	18,121

Дослідження результатів на рис. 5 дозволяє зробити висновок, що виграш для розробленого методу щодо методів НЗБ в режимі 2 і РС за значенням імовірності безпомилкового вилучення в умовах відсутності атак на вбудоване повідомлення становить від 40% до 50%.

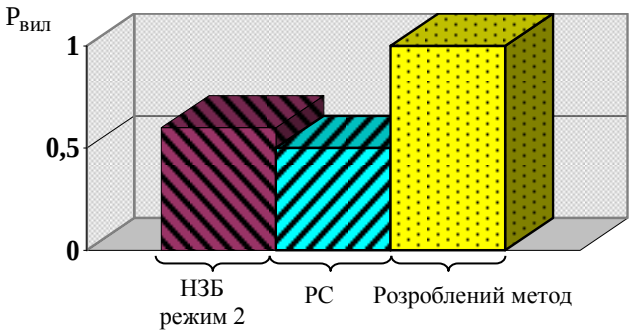

Рис. 5. Діаграма значень імовірності для методів НЗБ в режимі 2, РС і розробленого методу в умовах відсутності атак на вбудоване повідомлення

Порівняльна оцінка стійкості вбудованих даних для методів НЗБ в режимі 2, РС і розробленого методу в умовах застосування противником атаки ДКП з квантуванням проводиться за значенням імовірності безпомилкового вилучення і розглядається на рис. 6.

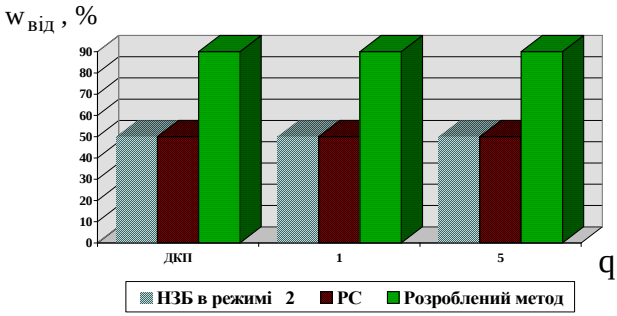

Рис. 6. Порівняльна діаграма значень кількості біт безпомилково вилучених даних для методу НЗБ в режимі 2, РС і розробленого методу в умовах атак

Дослідження результатів на рис. 6 дозволяє зробити висновок, що виграш для розробленого методу щодо методів НЗБ в режимі 2 і РС за значенням імовірності безпомилкового вилучення в умовах застосування противником атак на вбудоване повідомлення становить у середньому 40 %.

ВИСНОВКИ

У дисертаційній роботі вирішено науково-прикладну задачу, яка полягає у підвищенні безпеки спеціальних інформаційних ресурсів в системах критичного призначення. Необхідний рівень безпеки забезпечується за рахунок використання розробленого методу структурного стеганографічного кодування з локалізацією стеганографічної надлишковості.

У процесі здійснення досліджень було досягнуто таких ***наукових результатів:***

1. Правило вбудовування інформації для структурного стеганографічного кодування яке полягає в тому що, біт приховуваного повідомлення імплантується на позицію старшого елементу нерівновагового числа.

2. Метод структурного стеганографічного кодування, який дозволяє вбудовувати елемент приховуваного повідомлення використовуючи при цьому структурну надлишковість. Це дозволяє підвищити стеганографічну ємність відносно методу на основі розширення спектру на 1,22-5,47%.

3. Метод маскування структурної стеганографічної надлишковості на основі корекції кодограми стеганокоду для усунення потенційної можливості виявлення факту наявності вбудованої інформації. Це забезпечує збільшення рівня пікового відношення сигнал-шум у разі неавторизованого доступу на 8-32 дБ.

4. Метод демаскуючого стеганографічного декодування з усуненням ефекту маскування стеганографічної надлишковості, при якому відновлення

нерівновагового числа проводиться на основі реконструкції стеганокоду за біполярним принципом з демаскуванням стеганографічної надмірності. Це дозволяє підвищити ефективність вилучення прихованої інформації і локалізувати атаки зловмисника щодо виявлення факту наявності прихованої інформації. У такому випадку імовірність правильного вилучення вбудованої інформації для розробленого методу відносно методу найменш значущого біту та методу на основі розширення спектру збільшується на 0,4-0,5.

5. Стеганографічна система на основі імплантації прихованого двійкового елементу на старшу позицію нерівновагового числа з подальшим кодуванням та маскуванням, яка будується на прямому та зворотньому структурних стеганографічних перетвореннях з маскуванням структурної стеганографічної надлишковості.

Основні практичні результати. Побудовано систему стеганографічного кодування з маскуванням стеганографічної надлишковості, доведену до програмно-апаратних реалізацій. Відповідно, отримані такі результати:

1. Оцінка значення відносної стеганографічної ємності дозволила виявити наступне: виграш у значенні стеганографічної ємності для РМ щодо методу РС становить від 1,22 до 5,47%.

2. Порівняльний аналіз РМ та методу НЗБ в режимі 2 по кількості спотворень які вносяться в зображення показав, що при однакових значеннях об'єму вбудованих даних виграш для розробленого методу щодо методу НЗБ за величиною пікового відношення сигнал-шум складає в середньому від 8 до 32 дБ

3. Оцінка імовірності безпомилкового вилучення вбудованих даних дозволяє зробити висновок, що для РМ виграш у значенні імовірності безпомилкового вилучення становить: відносно методу НЗБ в режимі 2 - 40%, відносно методу РС – 50%.

4. Оцінка стійкості вбудованих даних в умовах застосування противником атаки ДКП з квантуванням показує, що кількість безпомилково вилучених біт в умовах застосування зловмисником атак для розробленого методу в середньому приймає значення 90%.

5. Порівняльний аналіз РМ і методів НЗБ в режимі 2 і РС по стійкості вбудованих даних в умовах атаки ДКП з квантуванням дозволив виявити наступне, що для РМ забезпечується виграш у значенні кількості безпомилково вилучених біт відносно методів НЗБ в режимі 2 і РС на рівні 40%.

Достовірність результатів дисертаційних досліджень підтверджується: адекватністю результатів експериментальних і теоретичних досліджень щодо відносної стеганографічної ємності та пікового відношення сигнал-шум зображення з прихованими даними, отриманих на основі програмної

реалізації та математичної моделі; не суперечливістю отриманих результатів існуючим положенням теорії стеганографічного кодування.

СПИСОК ОСНОВНИХ ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Barannik V.V. Design of steganographic system on the basis of a code container in nonequilibrium positional base / V.V. Barannik, A.E. Bekirov, A.V. Hahanova // Radioelectronics & informatics. – 2013. - №1. - С. 49 – 53.
2. Баранник В.В. Метод формування функціонала стеганографічного кодування стійкого до стегано-атак / В.В. Бараннік, А.Е. Бекіров // АСУ та прилади автоматики. - 2013. - Вип.165. - С. 34 – 43.
3. Баранник В.В. Методологическая база управления битовой скоростью при формировании предсказанных кадров / В.В. Баранник, Н.А. Харченко, А.Э. Бекиров // Радіоелектроніка та інформатика. - 2013. - №3. - С. 12 – 17.
4. Баранник В.В. Метод функционального преобразования чисел со встроенной информацией для стеганосистем / В.В. Баранник, А.Э. Бекиров, А.В. Хаханова // Радіоелектроніка та інформатика. - 2013. - №4. С.15 – 22.
5. Бекиров А.Э. Пути повышения безопасности информационных ресурсов в системах специального назначения / А.Э. Бекиров, К.Ю. Трифоненко // Наука і техніка Повітряних Сил України. - 2014. - №2(15). – С. 139-143.
6. Бекиров А.Э. Метод оценки вычислительной сложности обработки изображений с выявлением значимых компонент трансформант / В.Н. Кривонос, А.Э. Бекиров // Сучасна спеціальна техніка. – 2013. - №3. – С. 41 – 44.
7. Баранник В.В. Обоснование значимых угроз безопасности видеоинформационного ресурса систем видеоконференцсвязи профильных систем управления / В.В. Баранник, А.В. Власов, С.А. Сидченко, А.Э. Бекиров // Информационно-управляющие системы на ЖД транспорте. – 2014. - №3. - С. 24 – 31.
8. Баранник Д.В. Концепция структурного стеганографического кодирования с маскированием / Д.В. Баранник, А.Э. Бекиров // АСУ та прилади автоматики. - 2014. - Вип.168. - С. 4 - 11.
9. Баранник В.В. Технология неравновесного позиционного кодирования для функционального преобразования чисел со встроенной информаций / В.В. Баранник, Ю.Н. Рябуха, А.Э. Бекиров // Радиоэлектронные и компьютерные системы. – 2014. - №4. - С. 32 - 39.
10. Баранник В.В. Стеганографическая система на основе неравновесного позиционного кодирования / В.В. Баранник, А.Э. Бекиров, Д.В. Баранник // Радіоелектроніка та інформатика. - 2014. - №4. - С. 37 – 46.

11. Бекіров А.Е. Метод захисту інформації на основі стеганографічних систем // Озброєння та військова техніка. – 2015. - №1 - С. 29 – 36.

12. Vladimir Barannik. Quality indicators for steganographic transformations of images / Vladimir Barannik, Ali Bekirov, Konstantin Tryfonenko // XIIth International Conference ["Modern Problems of Radio Engineering, Telecommunications and Computer Science, TCSET'2014"], (Lviv-Slavske, Ukraine, February 25 – March 1, 2014) / Lviv-Slavske: 2014. – P. 533.

13. Бекіров А.Е. Спосіб компресії зображень в інфокомунікаціях на основі кодування кортежів / А.Е. Бекіров, В.В. Бараннік, С.В. Туренко, Д.І. Комолов // VI Международной научно-практической конференции [″Проблеми і перспективи розвитку ІТ-індустрії ″], (Харків, 17 - 18 квітня 2014 р.) / Харьковский национальный экономический университет, Харьков, 2014. – С. 233.

14. Бараннік В.В. Технологія кодування кортежів трансформованих зображень в інфокомунікаційних системах / В.В. Бараннік, С.В. Туренко, В.В. Твердохлеб, А.Е. Бекіров // IV Міжнародна науково-практична конференція [″International Scientific Conference, «ITSEC»″], (Київ, 20 - 23 травня 2014 р.) / Національний авіаційний університет, Київ, 2014. – С. 59.

15. Бекиров А.Э. Пути повышения информационной безопасности ресурсов в системах специального назначения / В.В. Баранник, Ю.Н. Рябуха, А.Е. Бекиров, Д.И. Комолов // Четверта міжнародна науково-практична конференція [«Інформаційні технології та комп'ютерна інженерія»], (Вінниця, 28 - 30 травня 2014 р.) / Вінницький національний технічний університет, Вінниця, 2014. – С. 151.

16. Barannik V. Functional transformation for direct embedding steganographic methods / Bladimir Barannik, Ali Bekirov, Roman Tarnopolov // International Symposium «IEEE East-West Design & Test», (Kiev, Ukraine, September 26–29, 2014).

17. Бекиров А.Э. Способ обработки потока кадров с предсказанием для систем телекоммуникаций / А.Э. Бекиров, Н.А. Харченко, Д.И. Комолов // Науково-методична конференція ["Сучасні проблеми телекомунікації і підготовка фахівців в галузі телекомунікацій - 2014″] / Національний університет "Львівська політехніка", - 1-4 листопада 2014р. - С. - 117-118.

18. Баранник В.В. Метод повышения безопасности видеоинформационного ресурса / В.В. Баранник, Ю.Н. Рябуха, А.Э. Бекиров // Третя міжнародна науково-технічна конференція ″Проблеми інформатизації″, (Київ, 11 - 13 грудня 2014 г.) / Державний університет телекомунікацій, Київ, 2014. – С. 9.

19. Barannik V. Design of steganographic system on the basis of a code container in nonequilibrium positional base / V. Barannik, A. Bekirov, S. Sidchenko, V. Larin // The XIIIth International Conference The Experience of

Designing and Application of CAD Systems in Microelectronics CADSM’2015 (24-27 February 2015 Polyana-Svalyava (Zakarpattya), Ukraine).

20. Баранник В.В. Анализ действий кибератак на видеоинформационный ресурс в информационно-телекоммуникационных сетях / В.В. Баранник, Ю.Н. Рябуха, С.А. Подлесный, А.Э. Бекиров // Науково-технічна конференція ["Інформаційна безпека України″] / Київський національний університет імені Тараса Шевченка, 12-13 березня 2015 р. - С. 34.

АНОТАЦІЯ

Бекіров А.Е. Метод підвищення безпеки спеціальних інформаційних ресурсів в системах критичного призначення на основі структурного стеганографічного кодування. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави. – Національний авіаційній університет «НАУ». Київ – 2015.

У дисертаційній роботі наведено рішення науково-прикладної задачі, яка полягає у підвищенні безпеки спеціальних інформаційних ресурсів в інфокомунікаційних системах. У зв'язку з чим, варіантом забезпечення даного аспекту інформаційної безпеки є напрям, заснований на використанні технологій стеганографічного вбудовування інформації в зображення-контейнер. У процесі проведення наукових досліджень були отримані такі основні науково-прикладні результати: обґрунтовано підхід для вдосконалення методів безпосереднього вбудовування, розроблено метод структурного стеганографічного кодування з локалізацією структурної стеганографічної надлишковості, побудовано структурну стеганографічну систему з маскуванням стеганографічної надлишковості, розроблено програмну реалізацію для оцінки ефективності розробленої стеганографічної системи.

Реалізація стеганографічного вбудовування спеціальної інформації на основі розробленого методу дозволяє підвищити безпеку спеціальних інформаційних ресурсів в відкритих інфокомунікаційних системах.

Ключові слова: структурне стеганографічне кодування, маскування стеганографічної надлишковості, нерівновагове позиційне кодування, підвищення безпеки інформаційних ресурсів.

АННОТАЦИЯ

Бекиров А.Э. Метод повышения безопасности специальных информационных ресурсов в системах критического назначения на основе структурного стеганографического кодирования. - Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 21.05.01 - информационная безопасность государства. - Национальный авиационный университет «НАУ». Киев - 2015.

В диссертационной работе приведены решения научно-прикладной задачи, которая заключается в повышении безопасности специальных информационных ресурсов в инфокоммуникационных системах. В связи с чем, вариантом обеспечения данного аспекта информационной безопасности является направление, основанное на использовании технологий стеганографического встраивания информации в изображение-контейнер. Обеспечение необходимого уровня безопасности достигается за счет использования разработанного метода стеганографического кодирования с маскированием структурной стеганографической избыточности. В процессе проведения научных исследований были получены следующие основные научно-прикладные результаты:

1. Разработана стеганографическая система на основе прямого и обратного функционального преобразования для неравновесного позиционного числа с имплантированным элементом, обеспечивающая встраивание и изъятие скрываемой информации на основе соответственно структурного стеганографического кодирования и декодирования.

2. Обосновано наличие структурной стеганографической избыточности в кодовом представлении стеганокода. Такая избыточность образуется в процессе стеганографического кодирования неравновесного позиционного числа с имплантированным на старшую позицию элементом. В случае неавторизированного доступа это явление создает дополнительную возможность для злоумышленника относительно установления факта наличия встроенной информации.

3. Создано правило встраивания информации для структурного стеганографического кодирования, заключающееся в том, что один бит скрываемого сообщения встраивается на старшую позицию неравновесного позиционного числа. В этом случае вес встроенного элемента в неравновесном позиционном числе будет наибольшим. Это обеспечивает встраивание скрываемой информации в условиях повышения устойчивости встроенных данных; восстановление элементов исходной видеопоследовательности независимо от наличия встроенной информации; снижение количества структурной стеганографической избыточности.

4. Разработано структурное стеганографическое кодирование с маскированием. В отличие от других методов обеспечивается встраивание скрываемой информации в процессе неравновесного позиционного кодирования с последующей локализацией стеганографической избыточности. Это позволяет снизить возможность выявления злоумышленником факта наличия встроенной информации.

5. Разработано демаскирующее стеганографическое декодирование. В отличие от существующих методов изъятие скрываемой информации и восстановление неравновесного позиционного числа проводится на основе реконструкции стеганокода по биполярному принципу с демаскированием стеганографической избыточности. Это позволяет повысить эффективность изъятия скрываемой информации и локализовать атаки злоумышленника относительно выявления факта наличия скрываемой информации.

Созданный метод повышения безопасности специальной информации в критических системах на основе структурного стеганографического кодирования доведен до программно-аппаратных реализаций.

Реализация стеганографического встраивания специальной информации на основе разработанного метода позволяет повысить безопасность специальных информационных ресурсов в инфокоммуникационных системах критического назначения.

Ключевые слова: структурное стеганографическое кодирование, маскирование стеганографической избыточности, неравновесное кодирование, повышение безопасности информационных ресурсов.

ANNOTATION

Bekirov A.E. Method of special information security increasing in critical systems based on structural steganographic coding. - Manuscript.

Thesis for the candidate degree in technical science in specialty 21.05.01 - information security of the state. - National Aviation University "NAU". Kiev - 2015.

The thesis shows the solution of scientific and applied tasks, which includes improvement of special information resources security in infocommunication systems. In this connection, the option for this aspect of information security is a direction based on the using technology of steganographic embedding information into an image-container. In the process of research the following basic scientific and applied results were received: based approaches for improving the methods of direct embedding, developed a method of steganographic structural encoding with localization of structural steganographic redundancy, built structural steganographic system with steganographic masking redundancy, designed software implementation to assess the efficiency of the developed steganographic system.

Implementation of steganographic embedding of specific information on the basis of this method can improve the security of special information resources in open infocommunication systems.

Keywords: structural steganographic encoding, steganographic redundancy masking, nonequilibrium coding, increasing of security of information resources.