

УДК 621.391

## МЕТОДИКА ОЦІНКИ СТЕГANOГРАФІЧНИХ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В ЗОБРАЖЕННЯХ

DOI 10.36994/2788-5518-2021-02-02-23

**Туровський О.Л.**, д.т.н., доц. Національний авіаційний університет, Київ, Україна. [s19641011@ukr.net](mailto:s19641011@ukr.net);

**Лазаренко С.В.**, д.т.н., доц. Національний авіаційний університет, Київ, Україна. [zzi.lazarenko@nau.edu.ua](mailto:zzi.lazarenko@nau.edu.ua);

**Щербак Т.Л.**, к.т.н., доц. Національний авіаційний університет, Київ, Україна. [tetiana.shcherbak@npp.nau.edu.ua](mailto:tetiana.shcherbak@npp.nau.edu.ua)

**Рябова Л.В.**, Національний авіаційний університет, Київ, Україна, [lubanau@ukr.net](mailto:lubanau@ukr.net)

**Мелешко Т.В.**, Національний авіаційний університет, Київ, Україна. [tetiana.meleshko@npp.nau.edu.ua](mailto:tetiana.meleshko@npp.nau.edu.ua)

**Анотація.** В роботі розглянуті питання оцінки стенографічних методів приховування інформації в зображеннях. А саме: систематизована система критеріїв оцінки стенографічних методів. В якості критеріїв запропоновано пропускну здатність, стійкість, невидимість, захищеність, складність вбудовування та вилучення інформації.

Подана узагальнена методика оцінки стенографічних методів. Яка включає часткову методику розрахунок вагових характеристик відносно обраних методів приховування інформації. На її основі побудовані матриці пріоритетів відповідно вимогам до методів приховування інформації. Узагальнена методика оцінки стеганографічних методів та проведена їх оцінка відносно двох критеріїв оцінки. Встановлено, що найбільш важливими характеристиками стеганографічних методів є захищеність, складність виявлення і стійкість.

**Ключові слова:** приховування інформації, стенографія, метод оцінки, пропускну здатність, стійкість, невидимість, захищеність, складність вбудовування та вилучення інформації

## METHOD OF EVALUATION OF STEGANOGRAPHIC METHODS OF HIDDEN INFORMATION IN IMAGES

**Olexander Turovsky**, Dr. habil., Ass. Prof. National Aviation University, Kyiv, Ukraine. [s19641011@ukr.net](mailto:s19641011@ukr.net)

**Sergey Lazarenko**, Dr. habil., Ass. Prof. National Aviation University, Kyiv, Ukraine. [zzi.lazarenko@nau.edu.ua](mailto:zzi.lazarenko@nau.edu.ua)

**Tatiana Shcherbak**, Ph.D., Ass. Prof. National Aviation University, Kyiv, Ukraine. [tetiana.shcherbak@npp.nau.edu.ua](mailto:tetiana.shcherbak@npp.nau.edu.ua)

**Liubov Ryabova**, National Aviation University, Kyiv, Ukraine. [lubanau@ukr.net](mailto:lubanau@ukr.net)

**Tatiana Meleshko**, National Aviation University, Kyiv, Ukraine.  
[tetiana.meleshko@npp.nau.edu.ua](mailto:tetiana.meleshko@npp.nau.edu.ua)

**Abstract.** *The advent and rapid development of computer technology, as well as the development of new ways of transmitting hidden information have given impetus to the development of technologies related to the hidden transmission of information through images - steganography. Which caused the rapid development of steganographic technologies and the emergence of low methods of hiding information and transmitting it through images.*

*The paper considers the evaluation of stenographic methods of hiding information in images.*

*The article presents a system of criteria for evaluating steganographic methods in accordance with the generalized areas and areas of their application; the most important criteria for evaluating steganographic methods are substantiated; a holistic method of evaluation of steganographic methods according to the most significant criteria of their evaluation has been developed; the approbation of the developed technique is carried out.*

*The criteria proposed are bandwidth, stability, invisibility, security, complexity of embedding and removing information.*

*It is determined that the most important criteria for evaluating steganographic methods are the security of the steganographic container, the difficulty of detecting hidden information in images and its stability.*

*The generalized technique of estimation of stenographic methods is given. Which includes a partial method of calculating the weight characteristics of the selected methods of concealing information. Based on it, matrices of priorities are built in accordance with the requirements for methods of hiding information. For the implementation of this technique used the method of expert evaluation, the essence of which is that the expert evaluation of steganographic methods involves an appropriate expert group, which includes independent experts*

*During the approbation of the proposed method, it was determined that the best results were shown by integrated methods based on discrete wavelet transform and discrete cosine transform.*

*The proposed system of criteria and developed evaluation methods can be used in the selection and evaluation of the effectiveness of steganographic methods in solving problems of covert transfer of information and protection of property rights to information presented in digital form*

**Keywords:** *information concealment, shorthand, estimation method, bandwidth, stability, invisibility, security, complexity of embedding and removing information*

## **Вступ**

Проблема прихованої та захищеної передачі даних була актуальна на протязі усього часу існування нашої цивілізації. З стародавніх часів різні епохи людство використовували тайнопис та моно алфавітні шифри для захисту своїх повідомлень. З тих часів до нас дійшли перші зразки та приклади оригінальних рішень в області приховування інформації в зображеннях - стеганографії[1,2].

Поява та швидкий розвиток комп'ютерної техніки дав поштовх таким взаємопов'язаним галузям як стеганографія та криптографія. З'явилися нові напрями стеганографії та методи вбудовування інформації. Поява мобільних терміналів (смартфонів, комунікаторів та згодом планшетів) надала нові можливості по застосуванню стеганографії. Розмаїття блоків розміщення прихованої інформації - контейнерів, шляхів їх передачі та популярність мобільної платформи передачі даних зумовлює актуальність розвитку стеганографічних методів як актуальної наукової проблеми.

Стеганографія – це процедури, технології способи та методи, які приховання конфіденційних даних в зображеннях. Її основною задачею є приховання саме факту існування таємних даних при передачі, зберіганні або обробці зображення.

Розвиток стеганографії відродився в останнє двадцятиріччя і був викликаний широким розповсюдженням технологій мультимедіа. Не менш важливим було виникнення нових типів каналів передачі інформації, що у сукупності із першим фактором дало новий імпульс розвитку і удосконаленню стеганографії, сприяло виникненню нових стеганографічних методів, в основу яких були покладені особливості представлення інформації у комп'ютерних файлах, обчислювальних мережах і т. і. Це, в свою чергу, дає можливість говорити про розвиток нового напрямку у сфері захисту інформації – комп'ютерної стеганографії [2,3].

Можна виділити три фактора популярності розвитку технологій у сфері стеганографії у даний час: актуальність розвитку нових каналів прихованої передачі інформації; обмеження на використання крипто засобів у низці країн світу і появу проблеми захисту прав власності на інформацію, представлену у цифровому вигляді. Перші два фактора спричинили велику кількість досліджень у дусі класичної стеганографії (тобто приховання факту передачі інформації), третій фактор – іще більш численні роботи у сфері так званих цифрових водяних знаків. (ЦВЗ) – спеціальної мітки, що непомітно впроваджується у зображення або інший сигнал з метою тим чи іншим чином контролювати його використання [3,4].

Найбільш поширені стеганографічні методи використовують просторову область зображення чи область перетворення зображення для приховування інформації [4,5].

В сучасних сферах прихованої передачі даних та розвитку мультимедійних технологій існує широке коло областей застосування стеганографічних методів [1,2]. Кожен з цих програмних додатків висуває різні вимоги до методу вбудовування даних. Одночасно необхідно прийняти до уваги, що окремі стеганографічні методи мають свої переваги та недоліки в реалізації та застосуванні для кожної сфери та області використання [5,6].

Врахування таких особливостей вимагає, в тому числі і оцінки безпосередньо кожного методу відповідно до прийнятої системи критеріїв відносно його оптимальності застосування для вирішення стеганографічної задачі в обраній області застосування.

Тобто, виникає проблема оцінки стеганографічних методів і пов'язана з цією проблемою наукове завдання щодо розробки системи критеріїв оцінки стеганографічних методів у в подальшому, з їх залученням, розробки цілісної методики оцінки стеганографічних методів [2,5].

Вищевказане наукове завдання найбільш оптимально вирішити по етапам та напрямкам:

- розробити систему критеріїв оцінки стеганографічних методів відповідно до узагальнених областей та сфер їх застосування;
- визначити найбільш важливі критерії оцінки стеганографічних методів;
- розробити цілісну методику оцінки стеганографічних методів відповідно найбільш значних критеріїв їх оцінки;
- провести апробацію розробленої методики.

Питанню розробки системи критеріїв стеганографічних методів та оцінки їх ефективності, присвячено ряд робіт.

Роботи [1,2,3] присвячені розгляду основ стеганографії. В них на достатньому рівні описані вимоги до стеганографічних методів та проведено огляд тих областей, де вказані методи найбільш доцільно застосовувати. Але вказані роботи не містять узагальненої системи вимог до стеганографічних методів та систематизованих методик оцінки поданих в них методів приховування інформації в зображеннях. Відповідно не можуть в повній мірі бути використаними для оцінки цих методів при застосуванні в тій чи іншій сфері приховування інформації.

Поданий в роботах [5,6] матеріал стосується, та в достатній мірі розкриває сутність одного з основних критеріїв оцінки, що можуть бути пред'явлені до стеганографічних методів. Але в них відсутня систематизація вимог до методів стеганографії та в явному вигляді не узагальнена цілісна методика оцінки стеганографічних методів..

В роботі [7] в загальному вигляді визначено систему критеріїв та вимог до певних стеганографічних методів. Але відсутня їх повна систематизація та не здійснена оцінка ефективності їх застосування для вирішення тих чи інших стеганографічних задач.

Роботи [8,9] присвячено розгляду окремих стеганографічних методів по критерію стійкості. Інші критерії оцінки стеганографічних методів в роботі не розглянута та цілісна методика їх оцінки в даній роботі відсутня.

Достатньо показовою є роботи [10,11,12], в яких якісно та повно викладено основи методики оцінки ефективності застосування стеганографічних методів. Але відсутня систематизація критеріїв оцінки та не в повній мірі подано результати оцінки тих чи інших методів приховування інформації.

Таким чином, систематизація критеріїв оцінки стеганографічних методів та узагальнення методики оцінки ефективності їх застосування є актуальною науковою задачею, вирішенню якої присвячена дана стаття.

Методи, що використовують просторову область зображення вбудовують приховувані дані в області первинного зображення. Їх перевага полягає в тому, що для вбудовування немає необхідності виконувати обчислювально складні

і тривалі перетворення зображень. Найбільш поширені з них, це метод заміни найменш значущого біта (НЗБ) та метод Куттера-Джордана-Боссена, як один з кращих в просторовій області.

Стійкішими до різних спотворень, у тому числі і компресії, є методи, що використовують для приховання даних не просторову область контейнера, а його частотну область [1,2,5].

### **Виконання досліджень**

Існує декілька способів представлення зображення в частотній області. При цьому використовується та або інша декомпозиція зображення, що використовується як контейнер. Наприклад, існують методи засновані на використанні дискретного косинусного перетворення (ДКП), дискретного перетворення Фур'є (ДПФ), вейвлет-перетворення, перетворення Карунена-Лоєва і деяких інших. Подібні перетворення можуть застосовуватися або до окремих частин зображення, або до зображення в цілому.

Основними методами, що застосовують область перетворення для приховування інформації є [4,5,6]:

- метод відносної заміни величин коефіцієнтів дискретно - косинусного перетворення (метод Коха і Жао);
- метод Бенгама – Мемона – Ео – Юнга;
- методи на основі дискретного Вейвлет-перетворення (ДВП);
- методи розширення спектру, які вбудовують водяний знак шляхом модуляції коефіцієнтів дискретно - косинусного перетворення (ДКП).

До найважливіших якісних характеристик стеганографічних систем, утворених на основі використання різних методів приховування інформації, відносяться [3,4,5]:

Пропускна здатність – кількість бітів прихованого повідомлення, що можуть бути передані за допомогою вказаного методу в зображенні фіксованого розміру.

Стійкість – здатність вилучити приховану інформацію після загальних операцій по обробці зображення.

Невидимість – характеристика, що забезпечує за неспроможності людського зору виявити стеганографічне повідомлення без використання спеціальних засобів.

Захищеність – вбудована корисна прихована інформація не може бути видалена з контейнера цілеспрямованими атаками, заснованими на відомому алгоритмі вбудовування та вилучення (окрім секретного ключа), і знанні принаймні одного носія з прихованим повідомленням.

Складність вбудовування і вилучення – кількість стандартних операцій, які будуть проведені для вбудовування і виявлення прихованого повідомлення.

Для визначення оптимального стеганографічного методу для прихованої передачі даних по мережах зв'язку представляється оптимальним використати результати досліджень, що базуються на застосуванні методу експертного оцінювання за обраними критеріями [10,11,12].

Сутність якого полягає в тому, що до експертного оцінювання стеганографічних методів залучається відповідна експертна група, до складу якої входять незалежні фахівці [10].

В ході експертного оцінювання обрані параметри підлягають оцінці з експертами з складу групи і в подальшому проводиться обробка отриманих даних з метою їх узагальнення та формування кінцевих результатів експертизи. Початковою інформацією для обробки є твердження та судження, що відображають переваги метода у числовій і лінгвістичній формі. Для цього застосовуються якісні та кількісні методи обробки результатів експертної оцінки. Кількісні методи є найбільш зручними з точки зору їх застосування під час такого оцінювання [9, 10].

Для узагальнення результатів експертизи виникає необхідність використання параметру, який би відображав оцінку експерта. Для цього запропоновано використати коефіцієнт важливості (KB), який широко застосовується при побудові рішення в багатокритеріальних задачах [9, 10, 13] та математичному програмуванні [10, 14].

У роботах [10,15] було подано результати детального дослідження та оцінені вимоги до характеристик окремо для кожної з розповсюджених стеганографічних сфер застосування за кольоровою шкалою (рис. 1).



Рис. 1. Области використання та їх вимоги до характеристик стеганографічних методів

Використовуючи набір вище запропонованих характеристик, Рис.1, пропонується провести попарне порівняння показників методом аналізу ієрархій для кожного з додатків.

Формою представлення попарних порівнянь [10,11,15] є зворотно-симетрична матриця (табл. 1), елементи якої  $W_{ij}$  є проявами інтенсивності

елементів ієрархії і відносно ієрархії  $j$ , що оцінюється за шкалою інтенсивності від 1 до 9, де оцінки мають наступні значення [10,15-18]:

- 1 – рівні значення;
- 3 – помірна перевага одного над іншим;
- 5 – істотна перевага одного над іншим;
- 7 – значна перевага одного над іншим;
- 9 – дуже сильна перевага одного над іншим;
- 2, 4, 6, 8 – відповідні проміжні значення.

Після цього були побудовані матриці пріоритетів (табл. 1, табл. 2, , що включають: пропускну здатність (a), стійкість (b), невидимість (c), захищеність (d), складність вбудовування (e) і складність вилучення (f).

Таблиця 1.  
Матриця пріоритетів (додаток - прихована передача інформації)

| $W$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |
|-----|-----|-----|-----|-----|-----|-----|
| $a$ |     | 7   | 1   | 1   | 6   | 6   |
| $b$ | 1/7 |     | 1/7 | 1/7 | 1/2 | 1/2 |
| $c$ | 1   | 7   |     | 1   | 6   | 6   |
| $d$ | 1   | 7   | 1   |     | 6   | 6   |
| $e$ | 1/6 | 2   | 1/6 | 1/6 |     | 1   |
| $f$ | 1/6 | 2   | 1/6 | 1/6 | 1   |     |

При заповненні матриць пріоритетів керуються правилом: якщо при порівнянні елемента  $i$  з елементом  $j$  отримано  $W_{ij} = b$ , тоді  $W_{ji} = 1/b$ .

Після побудови матриці пріоритетів, пріоритет кожного об'єкта в ієрархії визначається обчисленням відповідного елемента нормованого головного власного вектору матриці  $V$ .

Шляхом усереднення результатів для всіх додатків (рис. 1) отримуємо ваги (важливість) кожної з характеристик стеганографічних методів (табл. 3). [5,11,12,15-17].

Таблиця 2.  
Матриця пріоритетів (додаток - захист цілісності зображення)

| $W$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |
|-----|-----|-----|-----|-----|-----|-----|
| $a$ |     | 1/5 | 1/4 | 1/6 | 1/6 | 1   |
| $b$ | 5   |     | 2   | 1/2 | 1/2 | 5   |
| $c$ | 4   | 1/2 |     | 1/3 | 1/3 | 4   |
| $d$ | 6   | 2   | 3   |     | 1   | 6   |
| $e$ | 6   | 2   | 3   | 1   |     | 6   |
| $f$ | 1   | 1/5 | 1/4 | 1/6 | 1/6 |     |

Таким чином, результати оцінки показали, що найбільш важливими характеристиками стеганографічних методів є захищеність (вага  $R = 0,3$ ), складність виявлення (вага  $R = 0,22$ ) і стійкість (вага  $R = 0,2$ ) [5,10-12].

Таблиця 3.  
Загальні ваги характеристик

| Характеристика ( <i>i</i> ) | Вага ( <i>R</i> ) |
|-----------------------------|-------------------|
| Пропускна здатність         | 0,084             |
| Стійкість                   | 0,203             |
| Невидимість                 | 0,128             |
| Захищеність                 | 0,299             |
| Складність вбудовування     | 0,070             |
| Складність виявлення        | 0,218             |

Отримані оцінки використовуються для аналізу обраних стеганографічних методів вбудовування інформації та для багатокритеріального вибору найкращого методу. На основі інформації, представленої в [1,5,10,15-18], та використовуючи метод присвоєння коефіцієнтів факторам, була створена Табл. 4, де:

A1 – метод заміни найменш значущих біт (НЗБ);

A2 – метод Куттера-Джордана-Боссена;

A3 – метод Коха-Жао;

A4 – метод Бенгама-Мемона-Ео-Юнга;

A5 – метод із розширенням спектру;

A6 – метод, заснований на 3-рівневому ДВП.

Де: *a* – пропускна здатність; *b* – стійкість; *c* – невидимість; *d* – захищеність; *e* – складність вбудовування; *f* – складність виявлення.

У табл. 4 показник «8» є кращим значенням характеристики, «1» – найгіршим. Для розуміння значень, що описані в табл. 4, застосовувався розрахунок середніх значень коефіцієнтів для пропускної здатності [5,10-12].

Таблиця 4.  
Порівняльний аналіз методів вбудовування

|    | <i>a</i> | <i>b</i> | <i>c</i> | <i>d</i> | <i>e</i> | <i>f</i> |
|----|----------|----------|----------|----------|----------|----------|
| A1 | 8        | 1        | 7        | 1        | 8        | 8        |
| A2 | 6        | 4        | 7        | 4        | 7        | 7        |
| A3 | 2        | 7        | 5        | 7        | 5        | 5        |
| A4 | 1        | 6        | 6        | 7        | 4        | 4        |
| A5 | 4        | 7        | 8        | 6        | 3        | 3        |
| A6 | 3        | 8        | 8        | 8        | 1        | 1        |

Після розрахунку середніх значень були визначені коефіцієнти пропускної здатності (перша колонка в табл. 4) шляхом прямої розстановки методів.

Щодо інших характеристик, то стійкість була оцінена через кількість загальних операцій з обробки зображення, які можливо здійснити зі стеганографічною системою, утвореною певним методом, без втрати можливості детектувати вбудовану інформацію [10,11]. Невидимість оцінювалася кількісним показником якості зображення (IF). Захищеність оцінювалася на основі даних вказаних в публікаціях [1,2,10,11] і враховувала стійкість методів до атак.

Складність вбудовування і вилучення розраховувалася за кількістю стандартних операцій, які необхідно виконати для вбудовування і вилучення прихованого повідомлення. При цьому стеганографічний контейнер заповнювався лише на 10% від максимальної пропускної здатності.

Отже, на основі даних, наведених у табл. 4 можна провести комплексний порівняльний аналіз обраних методів A1 – A6. Для цього використовується методика попарних порівнянь.

Порівняльний аналіз методів, заснований на детальному аналізі кожної з характеристик, відображений у вигляді матриць в табл. 5, табл. 6 [10,15].

Таблиця 5.  
Матриця порівняння методів  
(за пропускною здатністю)

|    | A1  | A2  | A3  | A4 | A5  | A6  |
|----|-----|-----|-----|----|-----|-----|
| A1 |     | 3   | 7   | 8  | 5   | 6   |
| A2 | 1/3 |     | 5   | 6  | 3   | 4   |
| A3 | 1/7 | 1/5 |     | 2  | 1/3 | 1/2 |
| A4 | 1/8 | 1/6 | 1/2 |    | 1/4 | 1/3 |
| A5 | 1/5 | 1/3 | 3   | 4  |     | 2   |
| A6 | 1/6 | 1/4 | 2   | 3  | 1/2 |     |

Таблиця 6.  
Матриця порівняння методів  
(за захищеністю)

|    | A1 | A2  | A3  | A4  | A5  | A6  |
|----|----|-----|-----|-----|-----|-----|
| A1 |    | 1/4 | 1/7 | 1/7 | 1/6 | 1/8 |
| A2 | 4  |     | 1/4 | 1/4 | 1/3 | 1/5 |
| A3 | 7  | 4   |     | 1   | 2   | 1/2 |
| A4 | 7  | 4   | 1   |     | 2   | 1/2 |
| A5 | 6  | 3   | 1/2 | 1/2 |     | 1/3 |
| A6 | 8  | 5   | 2   | 2   | 3   |     |

Підсумувавши значення всіх параметрів таблиць 5, 6 та пронормувавши їх, отримуємо параметри зваженої оцінки якості методів, що наведені в табл. 7 [10-12,15].

*Таблиця 7.  
Порівняння методів, не враховуючи  
важливість (вагу) характеристик*

| Метод (a) | Значення (WW) |
|-----------|---------------|
| A1        | 0,266         |
| A2        | 0,181         |
| A3        | 0,126         |
| A4        | 0,097         |
| A5        | 0,137         |
| A6        | 0,193         |

Як видно з табл. 7, найвище значення продемонстрував метод НЗБ (A1, WW = 0,27). Але зважаючи на оцінку важливості характеристик табл. 7 може бути видозмінена до табл. 8, де значення параметрів були отримані з врахуванням їх важливості [10-12]:

Таким чином, при комплексному порівнянні методів вбудовування інформації для використання у стеганографічних додатках при передачі по мережах зв'язку, найкращий результат показали інтегровані методи, засновані на ДВП (A6, WW1 = 0,34) та дискретному косинусному перетворенні (ДКП) (A3, WW1 = 0,185) [10-12].

*Таблиця 8.  
Порівняння методів, враховуючи  
важливість (вагу) характеристик*

| Метод (a) | Значення (WW1) |
|-----------|----------------|
| A1        | 0,081          |
| A2        | 0,086          |
| A3        | 0,184          |
| A4        | 0,146          |
| A5        | 0,170          |
| A6        | 0,333          |

## Висновки

1. Проведено вибір та обґрунтування коефіцієнта важливості та критеріїв оцінки стеганографічних методів. В якості критеріїв запропоновано пропускну здатність, стійкість, невидимість, захищеність, складність вбудовування та вилучення інформації. Узагальнено вимоги до стеганографічних методів приховування інформації.

2. Проведено розрахунок вагових характеристик відносно обраних методів приховування інформації та побудовані матриці пріоритетів відповідно вимогам до методів приховування інформації.

3. Проведено оцінку ефективності застосування стеганографічних методів та встановлено, що найбільш важливими характеристиками стеганографічних методів є захищеність, складність виявлення і стійкість.

## Література

1. Конахович, Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. –Київ : МК-Пресс, 2006. – 288с.
2. Кузнецов, О. О. Стеганографія : навчальний посібник / О.О.Кузнецов, С. П. Євсеев; під загальною редакцією О. Г. Короля. –Х. : Вид. ХНЕУ, 2011. –232с.
3. Рябко, Б. Я., Фионов, А. Н. Основы современной криптографии и стеганографии. 2-е изд. / Б. Я. Рябко, А. Н. Фионов. –М. : Горячая линия - Телеком, 2013. –232 с.
4. Кінзерявий, О.М. Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень: дис. ... канд. техн.. наук. Спеціальність 05.13.21 – Системи захисту інформації. Київ , 2015, 324 с.
5. Вовк, О.О. Методи підвищення стійкості та пропускну здатності систем прихованої передачі інформації: дис. ... канд. техн.. наук. Спеціальність 05.12.02 – Телекомунікаційні системи та мережі. Харків, 2016, 177 с.
6. Грибунин, В. Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков; под общей редцией И.В. Туринцева. – М. : СОЛОН-Пресс, 2002. – 272 с.
7. Kutter, M. A fair benchmark for image watermarking systems / M. Kutter, F. Petitcolas // Proc. of SPIE: Security and Watermarking of Multimedia Contents. – San Jose, France, 1999. – vol. 3657 – P. 226 – 239.
8. Юдін, О.К., Захист інформації в мережах передачі даних : Підручник. / О.К. Юдін, Г.Ф. Конахович, О.Г.; під загальною редакцією Г.Ф. Корченко. –К. : ТОВ НВП «ІНТЕРСЕРВІС», 2009. –716 с.
9. Лагун, А.В. Використання вейвлет-перетворення для приховування інформації в нерухомих зображеннях / А.В. Лагун, І.А. Лагун // Захист інформації і безпека інформаційних систем. – Львів, 2013. – С. 98 – 99.
10. Вовк, О.О. Розроблення методики оцінювання важливості характеристик стеганографічних алгоритмів / О.О. Вовк, А.А. Астраханцев // Вісник національного університету «Львівська політехніка» «Інформаційні системи та мережі». – Львів, 2014. – № 805. – С. 52 – 60.
11. Вовк, О.О. Синтез стеганографічного методу передачі даних, ефективного за критеріями надійності та захищеності / О.О. Вовк, А.А. Астраханцев // Електронне наукове фахове видання ХНУРЕ «Проблеми телекомунікацій». – Харків, 2015. – № 1 (16). – С. 103 – 115.
12. Vovk, O. Synthesis of optimal steganographic method meeting given criteria / O. Vovk, A. Astrahantsev // Informatyka Automatyka Pomiaru w Gospodarce i Ochronie Środowiska (technical and scientific journal). – Lublin, Poland, 2015. – P. 27-34
13. Тоценко, В.Г. Методы и системы поддержки принятия решений. Алгоритмический аспект / В. Г. Тоценко. – Киев : Наук. думка, 2002. – 381 с.
14. Литвак, Б.Г. Экспертная информация. Методы получения и анализа / Б.Г. Литвак. – М.: Радио и связь, 1982. – 185 с.
15. Fridrich, J. Applications of Data Hiding in Digital Images / J. Fridrich // Tutorial for the ISPA S'98 Conferece. – Melbourne, Australia, 1999. – 33 p.
16. Середи, С.А. Сравнение методов стеганографии в изображениях / С.А. Сейеди, Р.Х. Садыхов // Информатика. – БГУИР. Белгород, 2013. – С. 66 – 75.
17. Горніцька, Д.А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, В.В. Волянська; під загальною редакцією Г.Ф. Корченко. // Захист інформації. –Київ, – 2012. – №1. – С. 108 – 121.

18. Ruanaidh, Ó. J. Rotation, scale and translation invariant digital image watermarking / J. Ó. Ruanaidh, T. Pun. // Proc. of the ICIP'97. – California, 1997. – vol. 1, P. 536–539.

## References

1. Konakhovich, G.F. Komp'yuterna steganohrafiya. Teoriya i praktyka / G.F. Konakhovich, A. Y. Puzirenko. - Kyiv: MK-Press, 2006. – 288 C.
2. Kuznetsov, O. O. Steganohrafiya [Tekst]: navchal'nyy posibnyk / O. O. Kuznetsov, S.P. Evseev; under the general editorship of O.G. Korolya. –X. : View. XHEU, 2011. –232 C.
3. Ryabko, B. Y. Osnovy sovremennoy kriptografii i steganografii. 2-ye izd / B. Y. Ryabko, A.N. Fionov. –M. : Hotline - Telecom, 2013. –232 C.
4. Kinzyayiy, O.M. Steganohrafichni metody prykhovuvannya danykh u vektorni zobrazhennya, stiyki do aktyvnykh atak na osnovi afinnykh peretvoren': dys. ... kand. tekhn.. nauk. Spetsial'nist' 05.13.21 – Systemy zakhystu informatsiyi. Kyiv, 2015, 324 C.
5. Wolf, O.O. Metody pidvyshchennya stiykosti ta propusknoyi zdatsnosti system prykhovanoi peredachi informatsiyi: dys. ... kand. tekhn.. nauk. Spetsial'nist' 05.12.02 – Telekomunikatsiyni systemy ta merezhi. Kharkiv, 2016, 177 C.
6. Gribunin, V.G. Tsfirovaya steganografiya / V.G. Gribunin, I.N. Shackles; under the general editorship of I.V. Turitseva. - M.: SOLON-Press, 2002. - 272 C.
7. Kutter, M. A. fair benchmark for image watermarking systems / M. Kutter, F. Petitcolas // Proc. of SPIE: Security and Watermarking of Multimedia Contents. - San Jose, France, 1999. - vol. 3657 - P. 226 - 239.
8. Yudin, O.K. Zakhyst informatsiyi v merezhakh peredachi danykh : Pidruchnyk. / O.K. Yudin, G.F. Konahovich; under the general editorship of G.F. Korchenko. –K. : "INTERSERVICE", 2009. – 716 C.
9. Lagoon, A. Vykorystannya veyvlet-peretvorenniya dlya prykhovuvannya informatsiyi v nerukhomykh zobrazhennyakh / A.V. Lagoon, I.A. Lagoon // Protection of information and security of information systems. - Lviv, 2013. - C. 98 - 99.
10. Vovk, O.V. Rozroblennya metodyky otsinyuvannya vazhlyvosti kharakterystyk steganohrafichnykh alhorytmiv / O.V. Vovk, O., A.A. Astrakhantsev // Bulletin of the National University "Lviv Polytechnic" "Information Systems and Networks". - Lviv, 2014. - № 805. - C. 52 - 60.
11. Vovk, O.V. Synthesis of steganographic data transmission method, effective in terms of reliability and security / O.V. Vovk, , A.A. Astrakhantsev // Electronic scientific professional publication of KNURE "Problems of telecommunications". - Kharkiv, 2015. - № 1 (16). - C. 103 - 115.
12. Vovk, O. Synthesis of optimal steganographic method meeting given criteria / O. Vovk, A. Astrakhantsev // Informatyka Automatyka Pomiar y Gospodarce i Ochronie Środowiska (technical and scientific journal). - Lublin, Poland, 2015. - C. 27-34
13. Totsenko, V.G. Metody i systemy podderzhki prinyatiya resheniy. Algoritmicheskyy aspekt / V.G. Totsenko. - Kiev: Science. opinion, 2002. - 381 C.
14. Litvak, B.G. Ekspertnaya informatsiya. Metody polucheniya i analiza / B.G Litvak. - M. : Radio and communication, 1982. - 185 C.
15. Fridrich, J. Applications of Data Hiding in Digital Images / J. Fridrich // Tutorial for the ISPAC S'98 Conferece. - Melbourne, Australia, 1999. - 33 C.
16. Seedy, S.A. Sravneniye metodov steganografii v izobrazheniyakh / S.A. Seyedi, R.H. Sadykhov // Informatics. - BGUIR. Belgorod, 2013. - P. 66 - 75.
17. Gornitska, D.A. Vyznachennya koefitsiyentiv vazhlyvosti dlya ekspertnoho otsinyuvannya u haluzi informatsiynoyi bezpeky / D.A. Gornitska, V.V. Volyanska; under the general editorship of G.F. Korchenko // Information protection. - Kyiv, - 2012. - №1. - P. 108 - 121.
18. Ruanaidh, Ó. J. Rotation, scale and translation invariant digital image watermarking / J. O. Ruanaidh, T. Pun // Proc. of the ICIP'97. - California, 1997. - vol. 1, pp. 536–539.