https://doi.org/10.31891/2219-9365-2022-70-2-8
УДК 004.056:621.397.3:004.942

Володимир ДЖУЛІЙ
Хмельницький національний університет
http://orcid.org/0000-0003-1878-4301
e-mail: dzhuliivm@khmnu.edu.ua
Марія КАПУСТЯН
Хмельницький національний університет
https://orcid.org/0000-0001-9200-1622
e-mail: kapustian.mariia@gmail.com
Юрій КЛЬОЦ
Хмельницький національний університет
https://orcid.org/0000-0002-3914-0989
e-mail: klots@khmnu.edu.ua
Вікторія ОРЛЕНКО
Хмельницький національний університет
https://orcid.org/0000-0001-9601-1916
e-mail: orlenkovs@khmnu.edu.ua
Віктор ЧЕШУН
Хмельницький національний університет
https://orcid.org/0000-0002-3935-2068
e-mail: cheshunvn@khmnu.edu.ua

МОДЕЛЬ СТЕГАНОСИСТЕМИ НА ОСНОВІ ПРОСТОРОВИХ ТА ФОРМАТНИХ ПРИНЦИПІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ

Розглянуто актуальне завдання вибору математичної моделі стеганографічної системи для приховування інформації в рамках інфраструктури мережевого спілкування інтернет-учасників в медіа-просторі. Запропонована модель орієнтована на розробку і оцінку ефективності стеганоалгоритмів для приховування інформації великого об'єму в цифрових зображеннях та реалізації функції роботи з форматами JPEG і BMP. Передбачено, що робочі алгоритми стеганографічної системи аналізують і змінюють структуру сегментів файлів.

Ключові слова: стеганографія, математична модель, растрове зображення, прихований канал зв'язку, стеганографічна система.

Volodymyr DZHULIY, Mariia KAPUSTIAN,
Yurii KLOTS, Viktoriia ORLENKO, Viktor CHESHUN
Khmelnytskyi National University

MODEL OF STEGANOGRAPHIC SYSTEM BASED ON SPATIAL AND FORMAT PRINCIPLES OF INFORMATION HIDING

The actual task of choosing a mathematical model of the steganographic system for hiding information within the network communication infrastructure of Internet participants in the media space is considered. The proposed model is focused on the development and evaluation of the effectiveness of steganographic algorithms for hiding large amounts of information in digital images and the implementation of the function of working with JPEG and BMP formats. It is assumed that the working algorithms of the steganographic system analyze and change the structure of file segments.

In today's world, there are several practical reasons for the practical interest in computer and, above all, digital steganography. In our opinion, this is the presence of such practical problems as: restrictions on the use of cryptographic protection of information in some countries and new technological opportunities for the activities of special services in modern conditions; management of computer incidents and computer forensics, due to the wide technological possibilities for violation of supervision over the actions of users and processes of information and telecommunication systems, which can lead to threats of leakage, imposition, destruction and blocking of information; protection of property rights to information presented in digital form, and development of technologies to protect information from forgery and unauthorized duplication.

Studies have shown that the conversion area is not well suited for the introduction of large amounts of data, but is well suited for the introduction of digital watermarks, which are a limited sequence of bytes. The principal requirement is also the many restrictions imposed on the container. Carrying out of research of features of formats of JPEG-files and BMP-files allowing to make secret introduction of the information of large volume. In addition, the requirement not to degrade the quality of digital photos is required. The BMP format, compared to the JPEG format, has a large spatial area of the image. JPEG format contains a fairly large set of file structure segments. Some segments are skipped by JPEG file reader software. Writing information in the LSB area of a BMP file makes it possible to implement a large number of bytes of information. Disadvantage - such an implementation is quite easy to detect.

Keywords: steganography, mathematical model, raster image, hidden communication channel, steganographic system.

Постановка проблеми у загальному вигляді
та її зв'язок із важливими науковими чи практичними завданнями

Під час ведення військових дій інформаційне суспільство потребує активізації наукових досліджень і розробок в області приховування інформації, що пов'язане, зокрема, з багаточисельним використанням цифрових форматів мультимедіа, але при цьому виникають проблеми управління ресурсами і дотримання авторських прав на цифрові файли. Звідси постає актуальне завдання приховання інформації в рамках інфраструктури мережевого спілкування інтернет-учасників в медіа-просторі.

Сучасна стеганографія та її методи активно розвиваються, використовуючи новітні можливості сучасних інформаційних технологій для реалізації, за суттю, класичних підходів [1,2,3] до приховування інформації з використанням:

апаратних функцій управління накопичувачами електронної інформації;

файлової структури операційних систем; форматів представлення даних (файлів);

протоколів інформаційного обміну (включно із тими, що використовуються в методах криптографічного і технічного захисту інформації).

У сучасному світі можна виокремити кілька практичних причин, що зумовлюють практичний інтерес до комп'ютерної і, насамперед, цифрової стеганографії [1]. На наш погляд, це наявність ряду практичних проблем:

обмеження на використання засобів криптографічного захисту інформації в деяких країнах світу та новими технологічними можливостями для діяльності спеціальних служб в сучасних умовах;

управління комп'ютерними інцидентами та комп'ютерною криміналістикою внаслідок широких технологічних можливостей для порушення нагляду за діями користувачів і процесів інформаційно-телекомунікаційних систем, що може призвести до реалізації загроз витоку, нав'язування, знищення та блокування інформації;

захист прав власності на інформацію, представлену в цифровому вигляді, та розвиток технологій захисту інформації від підробки та несанкціонованого тиражування.

Постановка задачі

Сьогодні методи комп'ютерної (цифрової) стеганографії все активніше находять поширення в завданнях кібербезпеки, що пов'язане з їх використанням в задачах автоматизації пошуку по електронних файлах, маркування файлів необхідними допоміжними атрибутами, захисту авторських прав на об'єкти інтелектуальної власності і забезпечення таємниці листування за рахунок прихованої передачі інформації. Принциповою проблемою стає велика кількість вимог-обмежень, що пред'являються до контейнера, тому виникає потреба узгодження контейнера приховування даних і типу приховуваних даних. Проведені дослідження вказують, що область перетворення погано підходить для впровадження великих об'ємів даних, проте добре підходить для впровадження цифрових водяних знаків, що представляють собою обмежену послідовність байтів.

Дослідження доступних стеганосистем впровадження цифрових водяних знаків в цифрові фотографії показали, що існуючі відкриті технологічні рішення не можна широко використовувати в Internet унаслідок наявності досить простих засобів для знищення цифрових водяних знаків.

Для розробки стеганографічних методів і алгоритмів роботи стеганосистеми, що вбудовують і приховують великі об'єми інформації в графічні зображення з подальшою передачею цієї інформації, а також для подальшого обґрунтування ефективності роботи алгоритмів і системи в цілому першочергово необхідно вирішити завдання вибору адекватної і достовірної математичної моделі стеганосистеми.

Основна частина

В математичній моделі стеганосистеми генерацію цифрового водяного знаку можна формально записати у вигляді операцій над елементами трьох множин:

$Y_{ЦВЗ}$ - множина цифрових водяних знаків;

$X_{КЛЮЧ}$ - множина ключів;

$X_{КОНТЕЙНЕР}$ - множина контейнерів;

$X_{ПОВІДОМЛЕННЯ}$ - множина приховуваних повідомлень.

На основі запропонованих елементів моделі, формально, генерація цифрового водяного знаку може бути представлена у вигляді:

$$F : X_{КОНТЕЙНЕР} \times X_{КЛЮЧ} \times X_{ПОВІДОМЛЕННЯ} \to Y_{ЦВЗ}, \quad (1)$$

$$y_{ЦВЗ} = F\left(x_{КОНТЕЙНЕР}, x_{КЛЮЧ}, x_{ПОВІДОМЛЕННЯ}\right), \quad (2)$$

де $y_{ЦВЗ} \in Y_{ЦВЗ}$, $x_{КОНТЕЙНЕР} \in$, $x_{КЛЮЧ} \in X_{КЛЮЧ}$, $x_{ПОВІДОМЛЕННЯ} \in X_{ПОВІДОМЛЕННЯ}$.

ISSN 2219-9365

Функція F (відображення) може бути довільна, але для практичного використання додають умови робастності цифрового водяного знаку, наприклад:

$$y_{ЦВЗ} = F\left(x_{КОНТЕЙНЕР}, x_{КЛЮЧ}, x_{ПОВІДОМЛЕННЯ}\right) \approx F\left(x_{КОНТЕЙНЕР} + \varepsilon, x_{КЛЮЧ}, x_{ПОВІДОМЛЕННЯ}\right). \quad (3)$$

Тобто, згідно (3) модифікований стеганоконтейнер не приводить до руйнування цифрового водяного знаку.

Крім того, функція F часто є складеною:

$$F = T \circ G, \quad (4)$$

де:

$$G : X_{КЛЮЧ} \times X_{ПОВІДОМЛЕННЯ} \to X_{КОД}, \quad (5)$$

$$T : X_{КОНТЕЙНЕР} \times X_{КОД} \to Y_{ЦВЗ}. \quad (6)$$

Реалізація G здійснюється із застосуванням генератора псевдовипадкових послідовностей. За початкове значення береться $x_{КЛЮЧ} \in X_{КЛЮЧ}$.

Відліки цифрового водяного знаку належать множині {-1,1}. Для відображення {0,1}→{-1,1} зазвичай застосовується двійкова відносна фазова модуляція (BPSK). Оператор T перетворить множину кодових слів $X_{КОД}$ в множину цифрових водяних знаків - $Y_{ЦВЗ}$. На даний оператор не накладають умову існування у нього зворотного перетворення, з огляду на те, що вибір G не гарантує зворотнє перетворення F. Оператор T будується так, щоб незаповнений контейнер $X_{КОНТЕЙНЕР_0}$, заповнений контейнер $X_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}}$ і заповнений контейнер з невеликими змінами $X'_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}}$ породжували б одні і ті ж цифрові водяні знаки:

$$T\left(X_{КОНТЕЙНЕР_0}, x_{КОД}\right) = T\left(X_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}}, x_{КОД}\right) = T\left(X'_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}}, x_{КОД}\right). \quad (7)$$

Тобто, оператор T має бути стійким до невеликої модифікації стеганоконтейнера.

Процес впровадження цифрового водяного знаку $y_{ЦВЗ}(i,j)$ в оригінальне зображення $X_{КОНТЕЙНЕР_0}(i,j)$ описується суперпозицією сигналів:

$$\psi : X_{КОНТЕЙНЕР} \times Y_{ЦВЗ} \times X_{МАСКА} \to X_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}}, \quad (8)$$

$$x_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}}(i,j) = x_{КОНТЕЙНЕР_0}(i,j) \oplus x_{МАСКА} \cdot y_{ЦВЗ}(i,j) \cdot p(i,j), \quad (9)$$

де $x_{МАСКА}$ - маска вбудовування цифрового водяного знаку, яка враховує особливості людської зорової системи, і призначена для зменшення помітності цифрового водяного знаку; p(i,j) - залежна від ключа проєктуюча функція; через символ $\oplus$ позначається оператор суперпозиції, що складається з операцій додавання, усікання і квантування.

Функція p(i,j) проводить «розподіл» цифрового водяного знаку за всім зображенням. Її використання аналогічне до функції розподілу даних паралельними каналами. Додатково p(i,j) володіє заданою просторовою структурою з кореляційними властивостями, що використовується для протидії геометричним атакам.

Одним з найважливіших пристроїв системи є стеганодетектор. Залежно від завдання, він видає двійкові або M-кратні рішення про присутність/відсутність цифрового водяного знаку (стеганодетектор з м'якими рішеннями).

Спочатку досліджено ситуацію «жорсткого» стеганодетектора, який є простішим. Формально оператор детектування D описується виразом:

$$D : X_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}} \times Y_{ЦВЗ} \to \{0,1\}, \quad (10)$$

$$D\left(x_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}} \times y_{ЦВЗ}\right) =$$
$$= D\left(x_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}}, F\left(x_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}}, x_{КЛЮЧ}, x_{ПОВІДОМЛЕНЬ}\right)\right) = \begin{cases} 1, \text{якщо } y_{ЦВЗ} \text{ присутній} \\ 0, \text{якщо } y_{ЦВЗ} \text{ відсутній} \end{cases} \quad (11)$$

В якості детектора цифрового водяного знаку часто застосовують кореляційний приймач [1].

Без втрати наочності передбачимо, що в певної частини пікселів фотографії величина інтенсивності збільшилася на 1, а в частини, що залишилася, не змінилася, або зменшилася на 1. Тоді

$$x_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}} = x_{КОНТЕЙНЕР_0} + y_{ЦВЗ} \quad (12)$$

Таким чином, кореляційний приймач отримує наступне значення:

$$x_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}} \cdot y_{ЦВЗ} = \left(x_{КОНТЕЙНЕР_0} + y_{ЦВЗ}\right) \cdot y_{ЦВЗ} = x_{КОНТЕЙНЕР_0} \cdot y_{ЦВЗ} + y_{ЦВЗ} \cdot y_{ЦВЗ} \quad (13)$$

Оскільки $y_{ЦВЗ}$ належить множині {-1,1}, то $x_{КОНТЕЙНЕР_0} \cdot y_{ЦВЗ}$ є невеликою величиною, а $y_{ЦВЗ} \cdot y_{ЦВЗ}$ більше нуля. Таким чином, $x_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}} \cdot y_{ЦВЗ}$ наближається до $y_{ЦВЗ} \cdot y_{ЦВЗ}$. Тому вірогідність неправильного детектування стеганодетектором записується як додаткова (комплементарна) функція помилок з квадратного кореня відношення $y_{ЦВЗ} \cdot y_{ЦВЗ}$ («енергії сигналу») до дисперсії величин пікселів яскравості («енергія шуму»).

В разі м'якого детектора є дві основні міри схожості:

нормований коефіцієнт взаємної кореляції 1

$$\delta = \frac{x_{КОНТЕЙНЕР_0} \cdot x_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}}}{\left\| x_{КОНТЕЙНЕР_0} \right\| \left\| x_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}} \right\|}; \quad (14)$$

відстань Хеммінга

$$\delta = N - \sum_{i}^{N} x_{КОНТЕЙНЕР_0}(i) \cdot x_{КОНТЕЙНЕР_{ЗАПОВНЕНИЙ}}(i). \quad (15)$$

У стеганографії найбільш популярні два перетворення [5,7]: дискретне вейвлет-перетворення (ДВП) і дискретне косинусне перетворення (ДКП).

ДКП застосовується під час стиснення JPEG-зображень. Даний факт пояснює велику популярність застосування ДКП у стеганографії JPEG. А ось ДВП є базою для стиснення в алгоритмі JPEG 2000.

ДКП застосовують як до всього зображення, так і до окремих блоків точок зображення. Зазвичай контейнер розбивають на блоки розміром 8×8 пікселів, а потім до кожного блоку застосовують ДКП. Отримані матриці коефіцієнтів ДКП мають розмір 8×8 [5]. Позначимо елементи цих матриць як $c_b(j,k)$, де b - номер блоку, (j,k) - місце коефіцієнта усередині блоку. Якщо блок сканується в зигзагоподібному порядку (як, наприклад, у JPEG), то позначення буде $c_{b,j}$. Елемент у лівому верхньому куті $c_b(0,0)$ (0,0), прийнято називати DC коефіцієнтом. Він говорить про яскравість всього блоку. Усі інші елементи називають AC-коефіцієнтами. У деяких випадках виконують ДКП не окремих блоків, а всього зображення.

На прикладі алгоритму Koch [6,8], розглянемо впровадження/вилучення інформації з допомогою ДКП. У даному стеганоалгоритмі здійснюється впровадження одного біта цифрового водяного знаку в блок 8x8. Існують дві реалізації алгоритму, за якими випадково вибираються 2 або 3 коефіцієнти ДКП. Впровадження інформації відбувається наступним чином: для вставки біта 0 роблять абсолютну величину різниці значень коефіцієнтів більше заданого додатнього значення ε. При передачі одного біта цю різницю роблять менше $-\varepsilon$:

$$\begin{aligned} \left|c_b\left(j_{i,j}, k_{i,1}\right)\right| - \left|c_b\left(j_{i,2}, k_{i,2}\right)\right| > \varepsilon, \text{ якщо } s_i = 0, \\ \left|c_b\left(j_{i,j}, k_{i,1}\right)\right| - \left|c_b\left(j_{i,2}, k_{i,2}\right)\right| < \varepsilon, \text{ якщо } s_i = 1. \end{aligned} \quad (16)$$

Це означає, що вхідна фотографія спотворюється за рахунок модифікацій коефіцієнтів ДКП. При читанні цифрового водяного знаку декодер робить ту саму процедуру вибору коефіцієнтів. Правило вибору рішення:

$$\begin{aligned} s_i &= 0, \text{ якщо} \left|c_b\left(j_{i,j},k_{i,1}\right)\right| > \left|c_b\left(j_{i,2},k_{i,2}\right)\right|, \\ s_i &= 1, \text{ якщо } \left|c_b\left(j_{i,j},k_{i,1}\right)\right| < \left|c_b\left(j_{i,2},k_{i,2}\right)\right|. \end{aligned} \tag{17}$$

У стеганодетекторі системи існує вірогідність появи помилок двох видів: помилкове визначення цифрового водяного знаку в порожньому стеганоконтейнері (помилка першого роду) та невиявлення впровадженого цифрового водяного знаку (помилка другого роду). Зменшення помилки першого викликає збільшення помилки другого роду. Прийнято оцінювати якість стеганодетектора величиною помилки першого роду [6].

Стеганосистема цифрового водяного знаку повинна будуватись так, щоб мінімізувати вірогідність виникнення помилок першого і другого роду, зважаючи на те, що будь-яка з них може привести до неправильної роботи стеганодетектора системи. Для оцінки стійкості водяного знаку використовується коефіцієнт помилкових бітів (Bit Error Rate), який застосовується при оцінці модифікацій бітової послідовності цифрового водяного знаку[3]:

$$BER\left(S,S^{''}\right)=\frac{\sum p_i}{N}, \tag{18}$$

де N – загальна кількість біт, p_i= 1, якщо $s_i \neq s_i^{''}$ і p_i= 0, якщо $s_i = s_i^{''}$, де s_i - і-й біт в рядку початкового зображення, $s_i^{''}$ - і-й біт в рядку вихідного зображення.

У протилежність зовнішнім атакам, властивості яких можна відтворити для будь-яких стеганоконтейнерів цифрових водяних знаків, вбудованих різними стеганографічними алгоритмами, параметри Р і метод впровадження є унікальними для будь-якого стеганографічного алгоритму [8]. Створюючи єдині початкові умови, які використовуються при порівняльному аналізі стійкості цифрового водяного знаку, зазвичай стежать за таким параметром як рівень модифікацій, які з'являються при вбудовуванні цифрового водяного знаку.

Однією з найуживаніших метрик обчислення рівня модифікацій, які упроваджуються в стеганографічний контейнер з цифровим водяним знаком є максимум співвідношення «сигнал/шум» (PSNR - Peak Signal Noise Range)[9]:

$$PSNR=\frac{XY\cdot\max\limits_{x,y}\left(C_{x,y}\right)^2}{\sum\limits_{x,y}\left(C_{x,y}-S_{x,y}\right)^2}, \tag{19}$$

де X,Y - габарити зображення; $C_{x,y}$ - розмір пікселя вхідного зображення; $S_{x,y}$ - розмір пікселя після зашумлення.

В ролі сигналу приймається початкова фотографія, а за шум - зміни, що з'являються при впровадженні цифрового водяного знаку. У наступній широко вживаній метриці використовується кореляція між початковим і зміненими сигналами (кореляційні показники викривлення). Нормовану взаємну кореляцію (Normalized-cross-Correlation) розраховують за формулою [4]:

$$NC=\frac{\sum\limits_{x,y}C_{x,y}S_{x,y}}{\sum\limits_{x,y}\left(C_{x,y}\right)^2} \tag{20}$$

Величину PSNR (NC), що задається, можна досягти, змінюючи параметр Р або об'єм упровадженої інформації М. Для якісного виконання оцінки стійкості, розмір цифрового водяного знаку вибирають незмінним і однаковим. Тому рішення даної задачі можливе лише зміною коефіцієнта Р.

BMP-формат дозволяє представляти колір пікселя 1,2 і 3 байтами. Звідси витікає, що зміни колірної складової залежить від представлення однієї точки. Тому, виходячи з вищесказаного, залежність потенційного розміру впроваджуваної інформації можна визначити за формулою:

$$V = f(x,i) = \frac{x \overset{jpeg \to bmptrans}{\to} x_{bmp} - H_{bmp}}{D_{bmp}} \times i \,, \tag{21}$$

де x - об'єм JPEG-файлу, $i \in \{1,2,3,4\}$ - число використовуваних молодших розрядів, $H_{bmp} = 54$ - розмір BMP- файлу, байт, $D_{bmp} \in \{1,2,3,4\}$ [1;4] - кількість бітів на 1 піксель BMP-зображення.

Оскільки найбільший об'єм виходить перетворенням в 24-бітове BMP-зображення, то розроблена модель стеганосистеми базується на ньому. Формат JPEG є форматом стискування з втратами, то обов'язково треба враховувати цю обставину при витяганні впровадженої інформації.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Розглянуто актуальне завдання вибору математичної моделі стеганографічної системи для приховування інформації в рамках інфраструктури мережевого спілкування інтернет-учасників в медіа-просторі. Запропонована модель орієнтована на розробку і оцінку ефективності стеганоалгоритмів для приховування інформації великого об'єму в цифрових зображеннях та реалізації функції роботи з форматами JPEG і BMP. Передбачено, що робочі алгоритми стеганографічної системи аналізують і змінюють структуру сегментів файлів.

Проведенні дослідження особливостей форматів JPEG- файлів і BMP-файлів, що дозволяють зробити таємне впровадження інформації великого об'єму. Крім того, потрібне дотримання вимоги про не погіршення якості цифрових фотографій. BMP-формат, в порівнянні з JPEG- форматом, має велику просторову область зображення. JPEG-формат містить досить великий набір сегментів файлової структури. Деякі сегменти пропускаються програмним забезпеченням читання JPEG-файлів. Запис інформації в області LSB BMP-файлу робить можливим впровадження великого числа байтів інформації. Недолік - таке впровадження досить легко детектується.

Література

1. Конахович, Г. Ф. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних / Г.Ф. Конахович, Д.О.Прогонов, О.Ю. Пузиренко // Підручник. – К. : «Центр навчальної літератури», 2018. – 558 с.

2. Хорошко, В.О. Комп'ютерна стеганографія / В.О. Хорошко, Ю.Є. Яремчук, В.В. Карпінець – Вінниця: ВНТУ, 2014. – 155 с.

3. Дурняк, Б. В. Стеганографічні методи захисту документів / Б. В. Дурняк, Д. В. Музика, В. І. Сабат. – Львів : Укр. акад. друкарства, 2014. – 159 с. : іл.

4. Ленков, С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, В.М. Джулій, В.С. Орленко, О.В. Сєлюков, А.В. Атаманюк // Збірник наукових праць ВІКНУ ім. Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.

5. Ленков, С.В. Методы и средства защиты информации. В 2-х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко – К: Арий, 2008. – 464с.

6. Кузнецов, О.О. Стеганографія : навчальний посібник / О.О.Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232с.

7. Хорошко, В.О. Основи комп'ютерної стеганографії / В.О. Хорошко, О. Д. Азаров, М. Є. Шелест, Ю. Є. Яремчук // Вінниця: ВДТУ, 2003. – 143 с.

8. Юдін, О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович // Підручник – К. : Вид-во DIRECTLINE, 2019. – 714 с.

9. Семкин, С. Н. Основи інформаційної безпеки об'єктів обробки інформації / С. Н.Семкин, А. Н. Семкин // Науч.-практ. посібник. Орел: 2018г. – 300 с.

10. Лавров, Є. А. Математичні методи дослідження операцій : підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик – Суми : Сумський державний університет, 2017. – 212 с.

11. Конахович, Г. Ф. Комп'ютерна стеганографія. Теорія і практика. / Г.Ф. Конахович, О.Ю.Пузиренко – К.: «МК-Пресс», 2006. – 288 с.

12. Бабенко, В.Г. Метод вбудовування стегоповідомлення на основі ключового елемента / В.Г. Бабенко, В.М. Зажома, О.Б. Нестеренко. // Захист інформації. 2014. – С. 53-58.

References

1. Konakhovych, H.F. (2018), Kompiuterna stehanohrafichna obrobka y analiz multymediinykh danykh / H.F. Konakhovych, D.O.Prohonov, O.Iu. Puzyrenko // Pidruchnyk. - K. : «Tsentr navchalnoi literatury» - 558 s.

2. Khoroshko, V.O. (2014), Kompiuterna stehanohrafiia / V.O. Khoroshko, Yu.Ie. Yaremchuk, V.V. Karpinets - Vinnytsia: VNTU – 155 s.

3. Durniak, B.V. (2014), Stehanohrafichni metody zakhystu dokumentiv / B. V. Durniak, D. V. Muzyka, V. I. Sabat. – Lviv : Ukr. akad. Drukarstva – 159 s. : il.

4. Lenkov, S.V. (2020), Model bezpeky poshyrennia zaboronenoi informatsii v informatsiino-telekomunikatsiinykh merezhakh / S.V. Lenkov, V.M. Dzhulii, V.S. ORLENKO, O.V. Sieliukov, A.V. Atamaniuk // Zbirnyk naukovykh prats VIKNU im. Tarasa Shevchenka. – K.: VIKNU. – №68. – ss. 53-64.

5. Lenkov, S.V. (2008), Metody y sredstva zashchyty ynformatsyy. V 2-kh tomakh / S.V. Lenkov, D.A. Perehudov, V.A. Khoroshko – K: Aryi – 464s.

6. Kuznetsov, O. O. (2011), Stehanohrafiia : navchalnyi posibnyk / O.O.Kuznetsov, S. P. Yevseiev, O. H. Korol. – Kh. : Vyd. KhNEU – 232s.

7. Khoroshko, V.O.(2003), Osnovy kompiuternoi stehanohrafii / V.O. Khoroshko, O. D. Azarov, M. Ye. Shelest, Yu. Ye. Yaremchuk // Vinnytsia: VDTU – 143 s.

8. Yudin, O.K. (2019), Zakhyst informatsii v merezhakh peredachi danykh / O.K. Yudin, O.H. Korchenko, H.F. Konakhovych // Pidruchnyk – K. : Vyd-vo DIRECTLINE - 714 s.

9. Semkyn, S. N. (2018), Osnovy informatsiinoi bezpeky obiektiv obrobky informatsii / S. N.Semkyn, A. N. Semkyn// Nauch.-prakt. posibnyk. Orel –300 s.

10. Lavrov, Ye. A. (2017), Matematychni metody doslidzhennia operatsii : pidruchnyk / Ye. A. Lavrov, L. P. Perkhun, V. V. Shendryk – Sumy : Sumskyi derzhavnyi universytet – 212 s.

11. Konakhovych, H. F. (2006), Kompiuterna stehanohrafiia. Teoriia i praktyka. / H.F. Konakhovych, O.Iu.Puzyrenko – K.: «MK-Press» – 288 s.

12. Babenko, V.H.(2014), Metod vbudovuvannia stehopovidomlennia na osnovi kliuchovoho elementa / V.H. Babenko, V.M. Zazhoma, O.B. Nesterenko. // Zakhyst informatsii – ss. 53-58.