УДК 621.39

DOI: 10.18372/2310-5461.38.12828

Бараннік В. В., д-р техн. наук, проф.
Харківський національний університет Повітряних Сил імені І. Кожедуба
orcid.org/0000-0002-2848-4524
vvbar.off@gmail.com

Шатун О. М.
Харківський національний університет Повітряних Сил імені І. Кожедуба
orcid.org/0000-0003-1337-2404
shatun_oleg@ukr.net

Бараннік Д. В.
Харківський національний університет радіоелектроніки
orcid.org/0000-0003-4235-300X
d.v.barannik@gmail.com

МЕТОД НЕПРЯМОГО СТЕГАНОГРАФІЧНОГО ВБУДОВУВАННЯ ДАНИХ В ЗОБРАЖЕННЯ-КОНТЕЙНЕР З УРАХУВАННЯМ ІНФОРМАЦІЇ КОНТУРУ

Вступ

У сучасному світі для забезпечення оперативності та якості інформації широко застосовують інформаційно-телекомунікаційні системи (ІТС) для передачі даних. Під час функціонування державних структур для підвищення економічного, оборонного та соціального впливу застосовують системи критичного призначення (СКП). Функціонування СКП характеризується наявністю зловмисника, який може провести активні впливи. Це може призвести до порушення конфіденційності, витоку важливої інформації та призвести до значних матеріальних та людських втрат. Тому захист інформації в системах передачі даних є однією з найважливіших проблем сучасної науки.

Криптографічний захист даних використовують для шифрування інформаційних ресурсів в СКП, що забезпечує надійний захист від несанкціонованого доступу. Оскільки криптографія лише шифрує, а не приховує дані, то противник може перехопити зашифроване повідомлення та спотворити його. Тому альтернативою для криптографії доцільно використання методів цифрової стеганографії .

Цифрова стеганографії (ЦС) — напрям стеганографії, що приховує дані в комп'ютерних файлах що мають аналогове походження. Найбільш опрацьованими та розповсюдженими методами ЦС є вбудовування даних в зображення-контейнер (ЗК). Це зумовлено такими причинами [1–4]:

− розповсюдження зображень в інформаційному просторі;

− наявністю в зображенні високої надмірності, яка потенційно може бути використана для вбудовування інформації;

− відносно великою пропускною спроможністю стеганографічного каналу з використанням ЗК;

− несприятливість людського зору до незначних спотворень у кольорі та яскравості.

Методи вбудовування даних в ЗК поділяють на безпосередні та непрямі. У разі приховування інформації в безпосередніх методах біти вбудовуються в зображення, що веде до спотворень та зниження стійкості контейнера до атак. У разі непрямого приховування даних інформація вбудовується шляхом створення залежностей між певними елементами зображення. Дані методи є складнішими за рахунок наявності математичних обчислень, але є більш стійкими до атак.

Аналіз останніх досліджень і публікацій

Аналіз останніх публікацій показав, що застосування непрямих методів приховування даних в зображення забезпечує надійність та достовірність прихованих даних. Концепція непрямого приховування даних заснована на створенні залежності елементів зображення.

Найчастіше це відбувається після проведення дискретно-косинусного перетворення (ДКП).

Використання ДКП при вбудовуванні інформації зумовлено тим, що існуючі зображення, У разі передачі обробляються технологією з втратами JPEG, частиною якої є ДКП.

Узагальнений аналіз і методів вбудовування даних в ЗК показав такі недоліки:

– існуючі методи не задовольняють вимоги до стеганографічної ємності контейнеру;

– використовувані методи є нестійкими до відомих атак на стеганографічну систему;

– низький рівень зображень до візуального аналізу;

– методи мають невисоку ймовірність правильного вилучення даних.

Перераховані вище недоліки ведуть до зниження стійкості стеганосистем та ймовірність утрати інформації під час передачі через канали.

Таким чином, необхідно використовувати такий спосіб приховування даних, який дозволить збільшити стійкість контейнера до атак та збільшити ймовірність правильного вилучення даних. В основу такого підходу пропонується застосовувати блоки, які будуть стійкими до атак і не спотворюватимуться під час передачі. Тому, ***метою статті*** є розробка методу приховування даних в стійкі блоки контуру зображення, а саме елементи, які містять інформацію про контур.

Механізм виявлення областей стійких до атакуючих впливів

Для цифрових зображень найбільш корисне семантичне навантаження мають контури об'єктів. Контури являють собою лінії, які проходять по границях однорідних областей. Елементи $\{z_{ij}\}$ просторово-часового подання зображення, значення яких не перевищують певного порогу, формують однорідні області. Це задається такою умовою:

$$\left|z_{\max} - z_{\min}\right| \le 1, \qquad (1)$$

де $z_{\max}$ — найбільший елемент області зображення; $z_{\min}$ — найменший елемент області зображення.

Існуючі алгоритми стиснення зображення скорочують надмірність, при цьому вносять найменші спотворення, тобто зберігають високу якість, що забезпечує несприятливість людського зору до спотворень. Отже, для виявлення областей стійких до компресійних впливів необхідно застосовувати методи виділення контурів зображення, для подальшого їх використання в стеганографічному вбудовуванні.

Контури зображень формуються на межах однорідних областей зображення.

Для того, щоб визначити належність елементів просторового представлення зображення до однорідної області одночасно з перевіркою наявності контуру необхідно виконання такої умови:

– належність елемента z_{ij} зображення до однорідної області задається умовою:

$$\left|z_{i,j} - z_{i\pm1,j\pm1}\right| \le 1, \qquad (2)$$

де $i = \overline{1,x}, j = \overline{1,y}.$

– належність елемента z_{ij} зображення до сусідньої однорідної області задається умовою:

$$\left|z_{i,j} - z_{i\pm1,j\pm1}\right| > 1, \qquad (3)$$

де $i = \overline{1,x}, j = \overline{1,y}.$

Найчастіше в практиці застосовують для виділення контурів зображення градієнтні методи.

Найбільш розповсюдженим способом пошуку контурів є обробка зображення Z ковзаючою маскою K. Маска K являє собою квадратну матрицю з коефіцієнтами {k}. Процес обробки зображення Z на основі матриці K називається *фільтрацією* або *маскуванням* і задається таким функціоналом $f(\bullet)$:

$$\mathrm{M} = f(\mathrm{Z}, \mathrm{K}), \qquad (4)$$

де M — зображення отримане в результаті обробки зображення Z на основі маски K.

Процес фільтрації заснований на поступовому просторовому переміщенню маски фільтра від елементу до елементу зображення. Значення елементу $m_{\mathrm{i,j}}$ (відгуку фільтрації) обчислюється з використанням значень попередніх і наступних елементів в двовимірному просторі.

У цьому випадку значення елементу $m_{\mathrm{i,j}}$ зображення M, отриманого в результаті маскування обраховують за формулою:

$$m_{i,j} = \sum_{\xi=i-1}^{i+1} \sum_{\tau=i-1}^{\tau+1} z_{\xi,\tau} k \qquad (5)$$

Як метод виділення контурів зображення пропонується застосовувати оператор Собеля. Даний оператор найчастіше застосовують на практиці і він має такий вигляд:

$$m_{i,j} = \sqrt{G_i^2 + G_j^2}\,; \qquad (6)$$

$$G_i = K_i m_{i,j} = \begin{bmatrix} -1 & 0 & +1 \\ -2 & 0 & +2 \\ -1 & 0 & +1 \end{bmatrix} m_{i,j}; \qquad (7)$$

$$G_j = K_j m_{i,j} = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ +1 & +2 & +1 \end{bmatrix} m_{i,j}. \qquad (8)$$

де K_i і K_j — оператори для визначення приросту значення елемента зображення по горизонталі та вертикалі відповідно; G_i і G_j — блоки зображен-

ня, кожний елемент якого містить наближені значення похідних по горизонталі і вертикалі відповідно.

Таким чином, застосування ковзаючої маски Собеля дозволяють виявити контури об'єктів на границях однорідних областей. Пропонується використовувати розглянуту технологію для виявлення областей, які будуть використовуватися при стеганографічному вбудовуванні.

Метод вбудовування даних в зображення з урахуванням інформації контуру

Сформулюємо вимоги до розроблюваного методу. Даний метод повинен забезпечувати надійність приховування інформації в зображеннях, вбудовування відносно великого обсягу інформації та стійкість до спотворень. Тому, пропонується здійснювати стеганографічне вбудовування, шляхом непрямої модифікації елементів блоків зображення, які містять інформацію контура [5–10].

Крок 1. Необхідно вибрати контури зображення для вбудовування даних. При виборі контурів було виявлено, що елементи розташовані на позиціях контурів, виявленні за допомогою маски зображення володіють такими властивостями:

1) обмеженою кількістю елементів, які містять інформацію про контур, тобто область значень для вбудовування інформації обмежена шириною контуру. У більшості випадків контур не широкий (рис. 1).

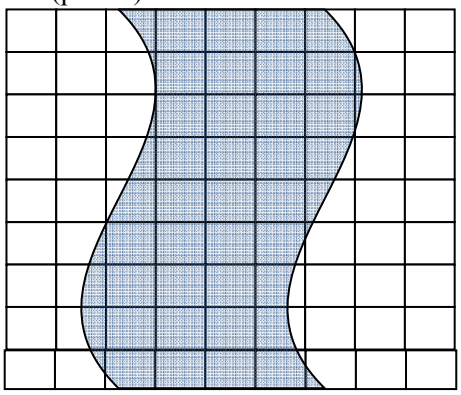
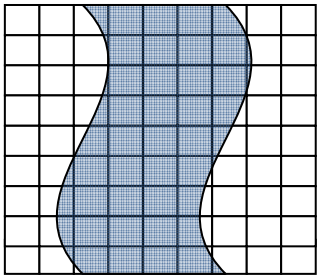
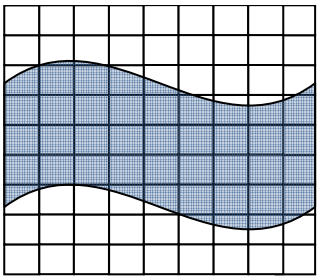


Рис. 1. Ширина контура зображення

2) через велику кількість контурів в зображенні, для успішного вбудовування даних при стеганографічних перетвореннях, необхідно враховувати різні напрями контуру зображення: вертикальний та горизонтальний (рис. 2).



а — вертикальна позиція

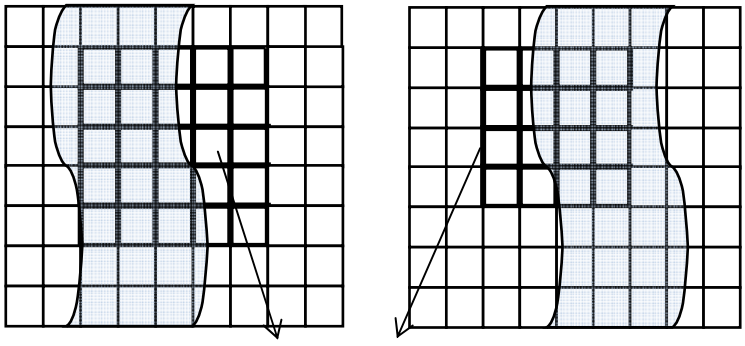


б — оризонтальна позиція

Рис. 2. Напрями контуру в зображені

Крок 2. Розглянемо можливі варіанти вибору матриці контуру елементів для вбудовування інформації, враховуючі ці особливості. Необхідно врахувати, що при виділенні широкого блоку для вбудовування в контурі зображення, в нього можуть попасти елементи, які не входять до елементів контуру.

У цьому разі при передачі повідомлення, дані що містяться в ЗК можуть бути пошкодженні. Тобто, при виборі блоку розмірністю 4×4 або 5×5 та вбудовуванні в нього інформації повідомлення буде виходити за межі контуру, що не задовольняє вимогам, висунутим до розроблюваного методу (рис. 3).



Елементи які не входять до контуру

Рис. 3. Приклад вибору блоків для вбудовування

Звідси випливає,що найбільш оптимальним розміром контуру для вбудовування є матриця розмірністю 3×3 елементи (рис. 4).

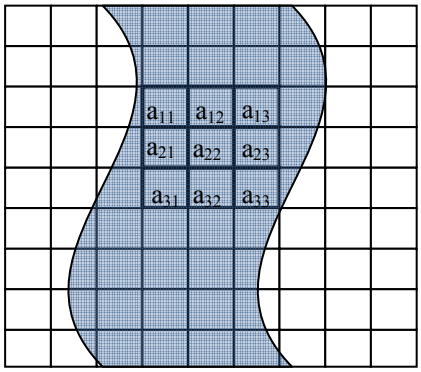


Рис. 4. Вибір блоку для вбудовування даних

Вибравши належний блок та виділивши в ньому матрицю А 3×3 необхідно для подальших розрахунків визначити такі елементи:

– не змінюванні в процесі вбудовування (еталонні елементи);

– елементи, які модифікуються в процесі вбудовування.

Для вибору елементів, які не будуть змінюватись у процесі вбудовування необхідно провести:

а) в матриці А потрібно визначити максимальний та мінімальний елементи. Ці елементи будуть залишатися незмінними для виділення інтервалу на якому вбудовано дані.

$$A = \begin{matrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{matrix} \quad (9)$$

Наприклад, $a_{12} = a_{\min}$, $a_{32} = a_{\max}$.

б) обчислити ширину інтервалу d. Це значення потрібне для обчислення границь інтервалів і характеризується динамічним діапазоном елементів у матриці блоків. Визначається за формулою:

$$d = \frac{a_{\max} - a_{\min}}{3}. \quad (10)$$

Крок 3. На даному етапі обчислюють границі інтервалів. Ці елементи використовують для порівняння. Ці елементи не модифікуються в процесі вбудовуванні даних — еталонні елементи, їх використовують у процесі створення залежності при непрямому вбудовуванні. Оскільки діапазон значень необхідно розбити на три інтервали, то необхідно визначити чотири еталонні елементи. Ці елементи обчислюють за формулою:

$$z_i = a_{\min} + d(i-1) \quad (11)$$

де z_i — i-й еталонний елемент для порівняння, $i = [1,4]$.

Крок 4. Необхідно елементи, вибраної для вбудовування матриці А, які будуть приймати участь при вбудовуванні поділити по інтервалах. Ці елементи дозволяють змінювати в процесі вбудовування даних — модифіковані елементи. Модифіковані елементи необхідно розмістити в порядку зростання та визначити їх належність до інтервалів між еталонними елементами $\{z_i\}$, $i = \overline{1,4}$,

Отже, $z_1 = a_{\min}$, $z_4 = a_{\max}$ та інші модифіковані елементи можуть потрапляти між еталонними елементами в різній кількості, це залежить від значень елементів блоку для вбудовування. Пронумеруємо елементи матриці А в порядку зростання, як це показано на рис. 4.

Крок 5. Необхідно обчислити середнє значення модифікованих елементів S_j, які потрапляють в інтервал між двома еталонними елементами $\{z_i\}$, $i = \overline{1,4}$, Дані значення будуть використовуватись для подальшого вбудовування даних за допомогою модифікованих елементів.

Обчислення, даного значення необхідне для створення залежності при вбудовуванні даних. Його обчислюють за формулою:

$$S_j = \frac{\sum_{m=1}^{n} a_m}{n}, \quad (12)$$

де j — номер інтервалу, $j = [1,3]$; a_m — модифікований елемент матриці, $m = [1,n]$; n — кількість елементів на інтервалі.

Крок 6. Для реалізації непрямого вбудовування інформації в контури зображення необхідно обчислити еталонний коефіцієнт порівняння k. Даний коефіцієнт є постійним, тобто не буде змінюватись від модифікації елементів блоку. Цей коефіцієнт обчислюється для кожного блоку вбудовування окремо, приймає значення $0 < k \le 1$ та обчислюється за формулою:

$$k = \frac{z_4}{z_2 + z_3}. \quad (13)$$

Вбудовування даних буде проводитися шляхом модифікації елементів блоку за правилом:

$$b = \begin{cases} 0, \text{ якщо } H > k; \\ 1, \text{ якщо } H \le k. \end{cases}, \quad (14)$$

де b — біт, який необхідно вбудувати в даний блок контуру; H — коефіцієнт порівняння, обчислюється за формулою:

$$H = \frac{S_3}{S_1 + S_2}. \quad (15)$$

Якщо умова виконується, то вбудовування даних завершено. Тобто, мається на увазі, що елементи мають такі значення, які задовольняють умові вбудовування.

Розглянемо випадки, коли умова вбудовування не виконується.

При невиконанні правила вбудовування М необхідно збільшувати або зменшувати для виконання умови вбудовування. Тоді правило вбудовування буде мати такий вигляд:

$$b = \begin{cases} 0, \text{якщо } H = \dfrac{S_3 + x}{(S_1 - x) + (S_2 - x)} > k; \\ 1, \text{якщо } H = \dfrac{S_3 - x}{(S_1 + x) + (S_2 + x)} \le k. \end{cases}, \quad (16)$$

де x — коефіцієнт модифікації, $x \in [-255;255]$.

Вбудовування буде відбуватися підбором значення H таким чином, щоб забезпечити виконання умови 16.

Значення модифікованих елементів a'_{ij} блоку містить інформацію про контур і обчислюється за такою формулою:

$$a_i' = a_i + x. \quad (17)$$

Значення x обчислюється за формулою:

$$x = \begin{cases} \dfrac{H(S_1 + S_2) - S_3}{1 + 2H}, \text{ для } b = 0; \\ \dfrac{S_3 - H(S_1 + S_2)}{1 + 2H}, \text{ для } b = 1. \end{cases} \quad (18)$$

Перепишемо формулу знаходження a_i' з урахуванням x:

$$a_i' = \begin{cases} a_i + \dfrac{H(S_1 + S_2) - S_3}{1 + 2H}, \text{для } b = 0; \\ a_i + \dfrac{S_3 - H(S_1 + S_2)}{1 + 2H}, \text{для } b = 1. \end{cases} \quad (19)$$

Після знаходження значень модифікованих елементів проводимо стеганографічне вбудовування даних в блоки за правилом 14.

Вилучення даних відбувається після отримання стеганографічного зображення шляхом аналізу зображення, та порівняння значень H і k в блоках.

Висновки

1. Розглянуто актуальні напрями захисту інформації, запропоновано застосовувати методи цифрової стеганографії для захисту даних для підвищення захисту та достовірності під час передачі інформації. Використання зображення-контейнера є найбільш перспективним для приховування даних.

2. Аналіз існуючих методів приховування даних в зображення-контейнер показав, що дані методи мають низьку ймовірність правильного вилучення даних, нестійкі до існуючих атак та мають невелику стеганографічну пропускну спроможність.

3. Розроблено метод виділення блоків контурів зображення на основі ковзаючої маски. Дані блоки є стійкими до компресійних атак та вносять незначні спотворення до зображення, що дозволяє використовувати маски зображення для стеганографічного приховування даних.

4. Розроблено метод непрямого стеганографічного приховування даних в контурах зображення. Даний метод дозволяє приховувати біти в блоки зображення високу ймовірність правильного вилучення вбудованих даних. Розроблений метод є стійким до відомих активних атак та стеганографічного аналізу з боку противника.

ЛІТЕРАТУРА

1 **Мельник А. С.** Інформаційні системи та мережі / А. С. Мельник, М. М. Голобородько // Вісник НУ «Львівська політехніка». — № 673.— Львів, 2010. — С. 365–374.

2 **Аграновський А. В.** Стеганографія, цифрові водяні знаки та стегоаналіз / А. В. Аграновський, А. В. Балакін, В. Г. Грибунин. — К. : Вузовская книга, 2015. — 220 с.

3 **Грибунін В. Г.** Цифрова стеганографія / В. Г. Грибунін . — К. : СОЛОН-Пресс, 2012. — 272 с.

4 **Конахович Г. Ф.** Компьютерна стеганографія. Теорія та практика / Г. Ф. Конахович, А. Ю. Пузиренко. — К. : К-Пресс, 2016. — 288 с.

5 **Yudin O., Boiko Y., Frolov O.** Organization of decision support systems for crisis management // Problems of Infocommunications Science and Technology (PIC S&T), 2015 Second International Scientific-Practical Conference. — IEEE, 2015. — P. 115–117. DOI: 10.1109/INFOCOMMST.2015.7357287.

6 **Баранник В. В.** Основы теории структурно-комбинаторного стеганографического кодирования: монография / В. В. Баранник, Д. В. Баранник, А. Э Бекиров. — Х. : Изд-во «Лидер», 2017. — 256 с.

7 **Barannik D., Bekirov A., Frolov O., Suprun O.** The new method of secure data transmission on the indirect steganography basis // East-West Design & Test Symposium (EWDTS). — IEEE, 2016. — P. 1–4. DOI: 10.1109/EWDTS.2016.7807754.

8 Barannik V., Ryabukha Yu., Tverdokhlib V., Dodukh A., Suprun O., Tarasenko D. Integration the non-equilibrium position encoding into the compression technology of the transformed images // East-West Design & Test Symposium (EWDTS). — IEEE, 2017. — P. 1-4. DOI: 10.1109/EWDTS.2017.8110030.

9 **Barannik V., Barannik D., Bekirov A., Lekakh A.** A steganographic method based on the modification of regions of the image with different saturation // Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), 14th International Conference, 2018. — P. 542–545. DOI: 10.1109/TCSET.2018.8336260.

10 **Barannik V., Alimpiev A., Bekirov A., Barannik D., Barannik N.** Detections of sustainable areas for steganographic embedding // East-West Design & Test Symposium (EWDTS). — IEEE, 2017. — P. 555-558. DOI: 10.1109/EWDTS.2017.8110028.

Бараннік В. В., Шатун О. М., Бараннік Д. В.

МЕТОД НЕПРЯМОГО СТЕГАНОГРАФІЧНОГО ВБУДОВУВАННЯ ДАНИХ В ЗОБРАЖЕННЯ-КОНТЕЙНЕР З УРАХУВАННЯМ ІНФОРМАЦІЇ КОНТУРУ

У статті розглядаються питання, пов'язані з використанням методів цифрової стеганографії для захисту інформації в системах критичного призначення. Обумовлена необхідність застосування приховування даних в зображення. Виділенні основні недоліки існуючих методів вбудовування в зображення-контейнер. Розглянуті проблемні питання стиснення зображення JPEG для цифрової стеганографії. Пропонується виділення стійких областей до атакуючих впливів на основі ковзаючої маски. Показаний математичний апарат для маскування зображень методом Собеля. Розробляється метод непрямого стеганографічного приховування даних в блоки елементів, які містять інформацію про контур.

Ключові слова: зображення-контейнер, контур зображення, дискретно косинусне перетворення, непрямий метод.

Barannik V. V., Shatun O. M., Barannik D. V.

THE INDIRECT METHOD OF STEGANOGRAPHIC EMBEDDING OF DATA IN AN IMAGE CONTAINER BASED ON THE INFORMATION OF THE CONTOUR

The article discusses issues related to the use of methods of digital steganography for information security in systems of critical appointment. Due to the necessity of concealing data in an image. The main disadvantages of the existing methods of embedding in the image container. The issues of JPEG image compression for digital steganography. Proposed allocation of sustainable regions in the attacking effects on the basis of the moving mask. Shown the mathematical apparatus for masking images by the method of Sobel. Developed an indirect method of steganography is hiding data in blocks which contain information about the circuit.

Keywords: image-container, the contour of the image, discrete cosine transformation, the indirect method.

Баранник В. В., Шатун О. Н., Баранник Д. В.

МЕТОД КОСВЕННОГО СТЕГАНОГРАФИЧЕСКОГО СОКРЫТИЯ ДАННЫХ В ИЗОБРАЖЕНИЕ-КОНТЕЙНЕР С УЧЕТОМ ИНФОРМАЦИИ КОНТУРА

В статье рассматриваются вопросы, связанные с использованием методом цифровой стеганографии для защиты информации в системах критического назначения. Обусловлена необходимость применения сокрытия данных в изображение. Выделены основные недостатки существующих методов встраивания в изображение-контейнер. Рассмотрены проблемные вопросы JPEG для цифровой стеганографии. Предлагается выделение стойких областей к атакующим воздействиям на основе скользящей маски. Показан математический аппарат для маскирования изображения методом Собеля. Разрабатывается метод косвенного стеганографического сокрытия данных в блоки элементов, которые содержат информацию о контуре

Ключевые слова: изображение-контейнер, контур изображения, дискретно косинусное превращение, косвенный метод.

Стаття надійшла до редакції 21.05.2018 р.
Прийнято до друку 04.06.2018 р.
Рецензент — д-р техн. наук, доц. Корнієнко Б. Я.