

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

Матеріали Міжнародної науково-практичної конференції

2



ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ: НОВІ ВИМІРИ У ВОЄННИЙ ЧАС

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Одеса, 16 травня 2025 року

Том 2

Одеса
2025

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)
Є 24

*Рекомендовано до друку вченою радою
Національного університету «Одеська юридична академія»
(протокол № 8 від 16.05.2025 р.)*

За загальною редакцією **С. В. Ківалова**

Є 24 **Європейські орієнтири розвитку України: нові виміри у воєнний час** : у 2 т. : матеріали Міжнар.наук.-практ. конф. (Одеса, 16 травня 2025 р.) / за заг. ред. С. В. Ківалова. – Одеса : Фенікс, 2025. – Т. 2. – 716 с.
ISBN 978-617-8430-61-0

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири України: нові виміри у воєнний час» містять результати наукових досліджень і практичних напрацювань вчених, фахівців і військовослужбовців, здійснені в умовах повномасштабної війни. У збірнику представлено як теоретичні, так і емпіричні дослідження у галузях філософії, загальної теорії держави і права, історії права, сучасних соціально-політичних процесів, соціології та психології.

Особливу увагу приділено аналізу загроз національній безпеці в конституційному, міжнародному та європейському правовому контекстах, а також питанням трудового, соціального, земельного, аграрного та екологічного права. Окремі розділи присвячено функціонуванню економіки та підприємництва в умовах євроінтеграції.

У збірнику також розглянуто проблематику цифрової трансформації, захисту інформації та кібербезпеки в умовах воєнного часу, методику викладання іноземних мов, перекладознавство, лінгвістику і журналістику. Висвітлено наукові здобутки в адміністративному, фінансовому, морському та митному праві, реформуванні судової системи, діяльності прокуратури, правоохоронних органів та адвокатури. Окремо проаналізовано питання кримінального права, кримінального процесу, кримінології, криміналістики, судової експертизи, медико-психологічного забезпечення правосуддя, а також аспекти цивільного, сімейного, господарського права, інтелектуальної власності та патентного судочинства. Розглянуто також актуальні питання діяльності бібліотек у закладах вищої освіти та фізичної підготовки здобувачів вищої освіти.

Збірник адресовано науковцям, викладачам, здобувачам вищої освіти, а також практикам у галузях права, економіки, соціології, політології, психології, філології, журналістики та кібербезпеки.

УДК 005.332.2(4):316.42(477)“364”“20”(062.552)

Відповідальний за випуск **М. Р. Аракелян**

ISBN 978-617-8430-61-0

© НУ «Одеська юридична академія, 2025
© Автори статей, 2025

<i>Кухаренко Сергій Вікторович</i> СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ У СФЕРІ МЕДІА В УКРАЇНІ	546
<i>Чепурна Олена Євгенівна</i> АНАЛІЗ ТЕОРЕТИКО-ІГРОВИХ МЕТОДІВ СУЧАСНОЇ КІБЕРБЕЗПЕКИ	548
<i>Соколов Артем Вікторович, Баландіна Наталія Миколаївна, Зігінова Юлія Костянтинівна</i> КОНЦЕПТУАЛЬНА ІДЕЯ ЗБІЛЬШЕННЯ БЛОКУ ДЛЯ МЕТОДУ З КОДОВИМ УПРАВЛІННЯМ ТА СЛІПИМ ДЕКОДУВАННЯМ	551
<i>Черевко Євген Володимирович</i> ЧИСЕЛЬНЕ РОЗВ'ЯЗУВАННЯ РІВНЯННЯ СТРУНИ ЗАСОБАМИ БІБЛІОТЕК PYTHON	555
<i>Овчинников Микола Юрійович</i> КОМПАРАТИВНИЙ АНАЛІЗ МЕТОДІВ ВПРОВАДЖЕННЯ ЦВЗ В АУДІОФАЙЛИ	558
<i>Слатвінська Валерія Миколаївна</i> ІНТЕГРАЦІЯ УМОВНОГО ГЕНЕРАТИВНО-ЗМАГАЛЬНОГО ПІДХОДУ ТА LSTM-МЕРЕЖ ДЛЯ ІНТЕЛЕКТУАЛЬНОЇ ДІАГНОСТИКИ АНОМАЛІЙ У КІБЕРБЕЗПЕЦІ МЕРЕЖЕВОГО ОБЛАДНАННЯ	563
<i>Скідан Владислав Сергійович</i> ПИТАННЯ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ВИКОРИСТАННІ ГЕЙМІФІКАЦІЇ НАВЧАЛЬНОГО ПРОЦЕСУ	565
<i>Поворознюк Олексій Олегович</i> МЕТОДИ ЗАХИСТУ МУЛЬТИМЕДІЙНИХ ДАНИХ ПІД ЧАС ВІЙНИ	568

СЕКЦІЯ 24. КОГНІТИВНО-ПРАГМАТИЧНІ ДОСЛІДЖЕННЯ ДИСКУРСУ, ТЕОРІЯ ТА ПРАКТИКА ПЕРЕКЛАДУ В АСПЕКТІ ВИКЛАДАННЯ ІНОЗЕМНИХ МОВ

<i>Томчаковська Юлія Олегівна</i> ТИПОЛОГІЯ АНГЛОМОВНИХ МЕДІАТЕКСТІВ	571
<i>Строченко Леся Василівна</i> ДОСЛІДНИЦЬКІ ПРИНЦИПИ ПАРАДИГМАЛЬНОГО ПРОСТОРУ СУЧАСНОЇ ЛІНГВІСТИКИ	573
<i>Varieshkina Natalia</i> COMMUNICATIVE PRINCIPLE IN READING SKILLS FORMATION	575
<i>Дихта Наталія Миколаївна</i> ОСОБЛИВОСТІ ПСИХОЛОГІЧНОЇ ТЕРМІНОЛОГІЇ ТА АКТУАЛЬНІСТЬ ЇЇ ВЖИВАННЯ	578
<i>Єрьоменко Світлана Василівна</i> ОСОБЛИВОСТІ АНГЛОМОВНОГО ВІЙСЬКОВО-МОРСЬКОГО ДИСКУРСУ	580
<i>Іванова Наталія Георгіївна</i> ЦИФРОВІ СТРАТЕГІЇ ВИВЧЕННЯ ІСПАНСЬКОЇ МОВИ ЯК ТРЕТЬОЇ ІНОЗЕМНОЇ: РЕАЛІЗАЦІЯ ДЕСКРИПТОРІВ INTERACCIÓN EN LÍNEA НА ПОЧАТКОВОМУ РІВНІ В УМОВАХ ВИЩОЇ ФІЛОЛОГІЧНОЇ ОСВІТИ	583
<i>Козак Тетяна Борисівна</i> БІНАРНІСТЬ ПОНЯТТЯ 'ЧОРНИЙ'/'БІЛИЙ' У МОВАХ ПЕРВІСНОЇ ФОРМАЦІЇ	586
<i>Марчук Ірина Петрівна</i> DEVELOPING INDIVIDUAL PROFESSIONAL PROGRAMS OF A TUTOR	589
<i>Пеліван Оксана Костянтинівна</i> ВВІЧЛИВІСТЬ В ІСТОРИЧНОМУ АСПЕКТІ	592
<i>Потенко Людмила Олександрівна</i> ЕФЕКТИВНІСТЬ РЕАЛІЗАЦІЇ ІНКЛЮЗИВНОГО НАВЧАННЯ У ВИЩІЙ ШКОЛІ В УМОВАХ ВІЙНИ	595
<i>Телецька Тетяна Володимирівна</i> ПРОФЕСІЙНО-ОРІЄНТОВАНЕ НАВЧАННЯ ІНОЗЕМНОЇ МОВИ У ПІДГОТОВЦІ ФАХІВЦІВ ПРАВНИЧОЇ ГАЛУЗІ: КОМПЕТЕНТНІСНИЙ ПІДХІД	598

умовах гібридних загроз і кіберконфліктів. Вони дозволяють не лише прогнозувати можливі сценарії атак, але й оптимізувати стратегії реагування на них, що є особливо важливим для України на етапі європейської інтеграції. Адаптація цих методів до національної системи кібербезпеки допоможе не лише ефективно протистояти поточним загрозам, але й забезпечити стійкість до майбутніх кібератак, сприяючи зміцненню національної безпеки в цілому.

Список використаних джерел:

1. Patterson W., Winston-Proctor C. E. Game Theory. Behavioral Cybersecurity. First edition. Boca Raton : CRC Press, 2021., 2020. P. 69–79. URL: <https://doi.org/10.1201/9781003052029-9>
2. CERT-UA минулого року опрацювала 4315 кіберінцидентів. *Державна служба спеціального зв'язку та захисту інформації України*. URL: <https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv>
3. Кучма О., Котух Є. Критична інфраструктура та кіберзагрози: досягнення стратегічних цілей державного аудиту щодо кіберзахисту критичної інфраструктури. *Наукові перспективи (Naukovi perspektivi)*. 2023. № 10(40). URL: [https://doi.org/10.52058/2708-7530-2023-10\(40\)-161-](https://doi.org/10.52058/2708-7530-2023-10(40)-161-)
4. Metcalf L., Casey W. Game theory. *Cybersecurity and Applied Mathematics*. 2016. P. 95–112. URL: <https://doi.org/10.1016/b978-0-12-804452-0.00006-3>

Ключові слова: кібербезпека, теорія ігор, оптимізація стратегій захисту кіберпростору.

Keywords: cybersecurity, game theory, optimization of cyberspace protection strategies.

Соколов Артем Вікторович

*Національний університет «Одеська юридична академія»,
професор кафедри кібербезпеки, доктор технічних наук, професор*

Баландіна Наталія Миколаївна

*Національний університет «Одеська юридична академія»,
старший викладач кафедри кібербезпеки*

Зігінова Юлія Костянтинівна

*Національний університет «Одеська політехніка»,
студентка магістратури*

КОНЦЕПТУАЛЬНА ІДЕЯ ЗБІЛЬШЕННЯ БЛОКУ ДЛЯ МЕТОДУ З КОДОВИМ УПРАВЛІННЯМ ТА СЛІПИМ ДЕКОДУВАННЯМ

Наразі серед стеганографічних методів захисту інформації особливо актуальними є методи, що володіють високою обчислювальною ефективністю при збереженні таких характеристик, як стійкість до атак проти вбудованого пові-

домлення, забезпечення надійності сприйняття, висока пропускна спроможність.

До таких сучасних методів відносять стеганографічний метод з кодовим управлінням, який був запропонований в роботі [1], та модифікований в роботі [2], що дозволило забезпечити вилучення додаткової інформації, що вбудована за допомогою зазначеного методу без наявності оригінального контейнера, тобто сліпе декодування для розміру блоків 8×8 . Натомість, ряд практичних завдань, наприклад, передавання захищеної інформації у каналах з можливістю значних збурень, або робота з цифровим відео, можуть потребувати більшого рівня захищеності, що можливо із застосуванням кодових слів більшого порядку, наприклад, T_{16} .

Проведені дослідження дозволяють зробити висновок, що просте збільшення порядку кодового слова не дає бажаного підвищення стійкості стеганографічного методу з кодовим управлінням та сліпим декодуванням, тому важливим є розробка ефективного методу збільшення порядку кодових слів для стеганографічного методу з кодовим управлінням та сліпим декодуванням.

Дослідження присвячено підвищенню стійкості стеганографічного методу з кодовим управлінням та сліпим декодуванням шляхом збільшення порядку застосовуваних у ньому кодових слів.

У роботі запропоновано модифікацію алгоритму з кодовим управлінням вбудовуванням додаткової інформації із збільшеним розміром кодового слова.

Алгоритм вбудовування.

Вбудовування додаткової інформації d_j відбувається у адитивний спосіб, тоді як блок стеганоповідомлення визначатиметься як

$$M = C + (-1)^{d_j} L_{16}, \quad (1)$$

де L_{16} – кодове слово розміру 16×16 , яке формується наступним чином

$$L_{16} = \begin{bmatrix} T_8 & T_8 \\ T_8 & T_8 \end{bmatrix}, \quad (2)$$

тоді як кодове слово T_8 формується за допомогою наступної конструкції

$$T_8 = \left[\begin{array}{c|c} t_1 & t_1 \\ \hline -t_1 & -t_1 \end{array} \right] + \left[\begin{array}{c|c} t_2 & t_2 \\ \hline -t_2 & -t_2 \end{array} \right], \quad (3)$$

де t_1, t_2 – кодові слова розміру 4×4 , що мають елементарну структуру [3] перетворення Уолша-Адамара $\{(\mu/2)^2(1), 0((\mu/2)^2 - 1)\}$, тобто кожне з кодових слів $\left[\begin{array}{c|c} t_1 & t_1 \\ \hline -t_1 & -t_1 \end{array} \right]$ і $\left[\begin{array}{c|c} t_2 & t_2 \\ \hline -t_2 & -t_2 \end{array} \right]$ при адитивному вбудовуванні (1) здатне забезпечити вибіркового впливу на задану трансформанту перетворення Уолша-Адамара підблоків.

Алгоритм вилучення.

Крок 1. Оригінальне зображення розбивається на блоки розміру 16×16 стандартним способом. Для кожного блоку визначаємо матрицю $P = \begin{bmatrix} p_1 & p_2 \\ p_3 & p_4 \end{bmatrix}$.

Крок 2. Для кожного блоку Y_j виконати його розбиття стандартним чином на чотири блоки $X_i, i = 1, 2, \dots, 4$ розміру 8×8 .

Крок 3. Для чергового блоку X_i розміру 8×8 виконати його розбиття ще на 4 блоки розміру 4×4 відповідно до наступної конструкції $X_i = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}$.

Крок 4. Для кожного блоку X_i розрахувати матриці

$$u_{i,1} = \frac{\begin{bmatrix} \sum_{a=1}^4 \sum_{b=1}^4 x_1(a,b)t_1(a,b) & \sum_{a=1}^4 \sum_{b=1}^4 x_2(a,b)t_1(a,b) \\ \sum_{a=1}^4 \sum_{b=1}^4 x_3(a,b)t_1(a,b) & \sum_{a=1}^4 \sum_{b=1}^4 x_4(a,b)t_1(a,b) \end{bmatrix}}{\begin{bmatrix} \sum_{a=1}^4 \sum_{b=1}^4 x_1(a,b)t_2(a,b) & \sum_{a=1}^4 \sum_{b=1}^4 x_2(a,b)t_2(a,b) \\ \sum_{a=1}^4 \sum_{b=1}^4 x_3(a,b)t_2(a,b) & \sum_{a=1}^4 \sum_{b=1}^4 x_4(a,b)t_2(a,b) \end{bmatrix}}, \quad (4)$$

$$u_{i,2} = \frac{\begin{bmatrix} \sum_{a=1}^4 \sum_{b=1}^4 x_1(a,b)t_2(a,b) & \sum_{a=1}^4 \sum_{b=1}^4 x_2(a,b)t_2(a,b) \\ \sum_{a=1}^4 \sum_{b=1}^4 x_3(a,b)t_2(a,b) & \sum_{a=1}^4 \sum_{b=1}^4 x_4(a,b)t_2(a,b) \end{bmatrix}}{\begin{bmatrix} \sum_{a=1}^4 \sum_{b=1}^4 x_1(a,b)t_1(a,b) & \sum_{a=1}^4 \sum_{b=1}^4 x_2(a,b)t_1(a,b) \\ \sum_{a=1}^4 \sum_{b=1}^4 x_3(a,b)t_1(a,b) & \sum_{a=1}^4 \sum_{b=1}^4 x_4(a,b)t_1(a,b) \end{bmatrix}},$$

де запис $x(a,b)$ означає елемент матриці x з індексом (a,b) .

Крок 5. Знайти середні значення

$$\overline{u_{i,1}} = \sum_{l=1}^2 \sum_{m=1}^2 u_{i,1}(l,m); \quad \overline{u_{i,2}} = \sum_{l=1}^2 \sum_{m=1}^2 u_{i,2}(l,m).$$

Крок 6. Знайти значення $p_i, i = 1, 2, \dots, 4$ для даного блоку Y_j як

$$p_i = \text{sign} \left(\sum_{l=1}^2 \left((u_{i,l}(1,1) - \overline{u_{i,l}}) + (u_{i,l}(1,2) - \overline{u_{i,l}}) - (u_{i,l}(2,1) - \overline{u_{i,l}}) - (u_{i,l}(2,2) - \overline{u_{i,l}}) \right) \right). \quad (5)$$

Крок 7. Обчислити біт додаткової інформації у блоці Y_j як $d_j = \text{sign} \left(\sum_{l=1}^4 p_l \right)$.

Експерименти із запропонованою модифікацією методу проводилися на вибірці з 100 зображень у які відбувалося вбудовування додаткової інформації із подальшим їх збереженням у форматі із втратами JPEG з заданим коефіцієнтом якості QF. Далі відбувалося вилучення вбудованої інформації із розрахунком кількості помилок, що відбулися.

В якості кодових слів t_1 та t_2 застосовувалися кодові слова $\xi_4 = \begin{bmatrix} 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$,

$$\xi_7 = \begin{bmatrix} 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \end{bmatrix} \text{ та } \xi_{11} = \begin{bmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{bmatrix}. \text{ Результати щодо стійкості запропо-}$$

нованої модифікації стеганографічного методу з кодовим управлінням у порівнянні з методом [2] показані на рис. 1.

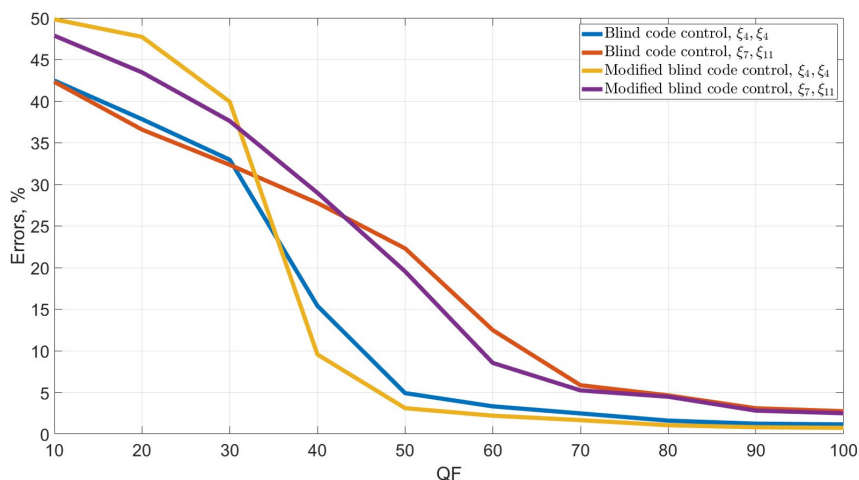


Рисунок 1. Графік залежності значення відсотку помилок від QF для наборів кодових слів $\xi_4 - \xi_4, \xi_7 - \xi_{11}$

Як видно з графіку, який зображено на рис. 1 збільшення розміру кодового слова з 8×8 до 16×16 дозволило отримати підвищення стійкості стеганографічного методу з кодовим управлінням та сліпим декодуванням до атаки стисненням при практично застосовуваних значеннях коефіцієнта QF . Так, наприклад, для набору застосованих кодових слів $\xi_4 - \xi_4$ та значенні $QF = 40$ кількість помилок при вилученні додаткової інформації зменшилася на 5.8%, що є досить значним результатом.

Список використаних джерел:

1. Kobozeva A. A., Sokolov A. V. Robust Steganographic Method with CodeControlled Information Embedding. *Problemele Energeticii Regionale*. 2021. Vol. 4. No. 52. P. 115-130.
2. Sokolov A. V., Ihnatenko O. O., Balandina N. M. Increasing the Efficiency of Blind Decoding of the Steganographic Method with Code Control of Additional Information Embedding. *Problemele Energeticii Regionale*. 2024. Vol. 2. No. 62. P. 121-137.
3. Sokolov A. V., Barabanov N. A. Algorithm for removing the spectral equivalence of component Boolean functions of Nyberg-design S-boxes. *Radioelectronics and Communications Systems*. 2015. Vol. 58. No. 5. P. 220-227.

Ключові слова: стеганографія, кодове управління, перетворення Уолша-Адамара.

Keywords: steganography, code control, Walsh-Hadamard transform.