Аналіз методів виявлення прихованих даних, що застосовуються у стегоаналізі

Analysis of Data Hiding Detection Methods Used in Steganalysis

Костянтин Семібаламут [A]
канд. техн. наук, доц., заступник начальника кафедри, e-mail: balamut-7@meta.ua, ORCID: 0000-0002-5962-8412

Володимир Молдован [A]
канд. техн. наук, доц., доцент кафедри, e-mail: vl.mold@ukr.net, ORCID: 0000-0001-9668-4117

Сергій Стефанцев [A]
Corresponding author: канд. техн. наук, старший викладач кафедри, e-mail: stefancevss@gmail.com, ORCID: 0000-0002-7629-7563

Kostiantyn Semibalamut [A]
Ph.D. (Tech.), Assoc. Prof., Deputy Head of the Department, e-mail: balamut-7@meta.ua, ORCID: 0000-0002-5962-8412

Volodymyr Moldovan [A]
Ph.D. (Tech.), Assoc. Prof., Associate Professor of the Department, e-mail: vl.mold@ukr.net, ORCID: 0000-0001-9668-4117

Serhii Stefantsev [A]
Corresponding author: Ph.D. (Tech.), Senior Lecturer of the Department, e-mail: stefancevss@gmail.com, ORCID: 0000-0002-7629-7563

[A] Воєнна академія імені Євгенія Березняка, м. Київ, Україна

[A] Yevgeny Bereznyak Military Academy, Kyiv, Ukraine

Received: June 19, 2025 | Revised: June 26, 2025 | Accepted: June 30, 2025

DOI: 10.33445/sds.2025.15.3.18

Мета роботи: проаналізувати методи виявлення прихованих даних, що застосовуються у стегоаналізі.

Метод дослідження: Аналітичний метод.

Результати дослідження: здійснено системний аналіз сучасних методів виявлення прихованої інформації у цифрових контейнерах, зокрема в зображеннях, аудіо- та відеофайлах. Встановлено, що стегоаналіз є критично важливою складовою інформаційної безпеки, особливо в умовах тотального цифрового моніторингу, кібершпигунства та поширення несанкціонованого обміну даними.

Теоретична цінність дослідження: полягає в систематизації та класифікації сучасних методів стегоаналізу, а також у виявленні їх сильних і слабких сторін. Розгляд класичних і сучасних підходів дозволяє сформувати цілісне уявлення про напрям розвитку стеганографії та засобів її виявлення. Дослідження розширює наукове розуміння взаємозв'язку між типами носіїв, характеристиками алгоритмів приховування та ефективністю методів аналізу.

Цінність дослідження: полягає в можливості адаптації результатів для підвищення рівня кіберзахисту в організаціях, які працюють з конфіденційною інформацією. Описані методи можуть бути використані як фахівцями з інформаційної безпеки, так і розробниками систем виявлення кіберзагроз. Застосування комбінованого підходу, який об'єднує статистичні, сигнатурні та машинні алгоритми дозволяє значно покращити точність виявлення прихованих даних у цифровому середовищі.

Майбутні дослідження: у ході подальших досліджень доцільно розробити спосіб зменшення демаскувальних ознак під час стеганографічного захисту повідомлення.

Тип статті: теоретичний.

Purpose: To analyze the methods of detecting hidden data used in steganalysis.

Method: Analytical method.

Findings: A systematic analysis of modern methods for detecting hidden information in digital containers, particularly in images, audio, and video files, has been conducted. It has been established that steganalysis is a critically important component of information security, especially in the context of pervasive digital monitoring, cyber espionage, and the spread of unauthorized data exchange.

Theoretical implications: It involves the systematization and classification of modern steganalysis methods, as well as the identification of their strengths and weaknesses. The review of classical and contemporary approaches enables the formation of a comprehensive understanding of the development direction of steganography and its detection tools. The study expands scientific knowledge of the relationship between carrier types, characteristics of hiding algorithms, and the effectiveness of analysis methods.

Value: It lies in the ability to adapt the results to enhance the level of cybersecurity in organizations that handle confidential information. The described methods can be utilized both by information security specialists and by developers of cyber threat detection systems. The application of a combined approach that integrates statistical, signature-based, and machine learning algorithms allows for a significant improvement in the accuracy of detecting hidden data in digital environments.

Future research: In the course of further research, it is advisable to develop a method to reduce revealing features during steganographic protection of the message.

Paper type: theoretical.

Ключові слова: інформаційна безпека, стеганографія, стегоаналіз, цифрові контейнери, LSB-метод, приховування інформації.

Key words: information security, steganography, steganalysis, digital containers, LSB-method, information hiding.

Вступ

У сучасну цифрову епоху, коли обсяг переданої та збереженої інформації постійно зростає, забезпечення інформаційної безпеки залишається актуальним питанням. Однією з технологій, яку використовують як для забезпечення конфіденційності інформації є стеганографія – це приховування інформації всередині інших даних [1]. У відповідь на зростання використання

стеганографії, з'явився напрямок досліджень під назвою стегоаналіз, головним завданням якого є виявлення факту приховування інформації.

Методи стегоаналізу відіграють критично важливу роль у виявленні та запобіганні несанкціонованій передачі прихованих даних, особливо в контексті кібербезпеки, криміналістики та цифрового моніторингу. Існує широкий спектр підходів до виявлення прихованої інформації – від статистичних методів до застосування сучасних технологій машинного навчання та глибинного аналізу даних [2].

Тому виникає нагальна потреба в аналізі сучасних методів виявлення прихованих даних, що застосовуються у стегоаналізі, а також оцінка їх ефективності, переваг і недоліків. У ході дослідження розглянуто як класичні підходи, так і новітні алгоритми, що демонструють високу точність виявлення стеганографічного впливу. Розробка таких підходів сприяє підвищенню точності, надійності та універсальності таких методів у різних типах цифрових носіїв.

Теоретичні основи дослідження

Питанню захисту інформації, а також її прихованій та безпечній передачі присвячено багато наукових праць. У свій період часу серед відомих вітчизняних і зарубіжних вчених найбільший внесок зробили: К. Шеннон (C. E. Shannon), Г. Сіммонс (G.J. Simmons), Дж. Фрідрік (J. Fridrich), Р. Андерсон (R. J. Anderson), В. Бендер (W. Bender), Н. Морімото (N. Morimoto), К. Качін (C. Cachin), І. Питас (I. Pitas), Р. Попа (R. Popa), Н. Джонсон (N. F. Johnson), С. Волошиновський (S. Voloshynovskiy), Б. Пфіцманн (B. Pfitzmann), Б. Шнайєр (B. Schneier), С. Крейвер (S. Craver), В. О. Хорошко, О. Д. Азаров, М. Шелест та інші [3].

Актуальними питаннями застосування стеганографічних методів для приховування інформації в аудіо сигналах сьогодні займаються Є. Світловський, К. Трапезон, І. Казміді та В. Зубок [4, 8]. Зокрема, авторами описано метод LSB (Least Significant Bit), що використовує найменш значущий біт, аналізується з точки зору досягнення оптимального рівня прихованості тексту в аудіофайлі. Автори досліджують спроби збільшення обсягу прихованої інформації, що може призвести до значних змін у контейнері та зменшити ефективність стеганографії [4]. Попри це, метод LSB залишається популярним [5] і викликає інтерес серед науковців, які досліджують методи стеганографії та стегоаналізу.

Таким чином, теоретичні основи дослідження ґрунтуються на застосуванні різних методів приховування інформації способом стеганографії.

Постановка проблеми

Зі стрімким розвитком цифрових технологій та зростанням обсягів обміну інформацією в мережі "Інтернет", питання захисту даних та безпеки комунікації залишається актуальним. Одним із сучасних засобів приховування інформації є стеганографія. Стеганографію інколи розглядають як наступний етап після криптографії – мистецтва, науки та технології забезпечення секретності інформації [6]. На відміну від криптографії, що вивчає способи та методи захисту інформації від змін і неавторизованого втручання при передаванні, обробленні та зберіганні інформації, стеганографія – це спосіб приховування інформації, при якому факт передачі повідомлення є непомітним для стороннього спостерігача. Однак розвиток стеганографічних методів породжує і зростаючу потребу в ефективних інструментах для їх виявлення – стегоаналізі. Незважаючи на значний прогрес у цій сфері, існує ряд проблем, що ускладнюють виявлення прихованих даних. Наведемо характерні з таких проблем.

По-перше, методи стеганографії стають дедалі складнішими та більш адаптивними, що знижує ефективність традиційних методів стегоаналізу.

По-друге, різноманітність форматів і типів носіїв інформації (зображення, аудіо, відео) вимагає розробки універсальних підходів для їх аналізу.

По-третє, баланс між високою чутливістю виявлення та мінімізацією помилкових спрацьовувань залишається актуальним викликом для дослідників.

Таким чином, проблемою сучасного дослідження є пошук та аналіз ефективних методів виявлення прихованих даних, що застосовуються у стегоаналізі, з метою підвищення точності, надійності та універсальності таких методів.

Результати

Переваги стеганографії та методи виявлення прихованих даних

На цей час обсяг переданої та збереженої інформації зростає експоненціально, що супроводжується підвищенням ризиків несанкціонованого доступу та втручання у конфіденційні дані. Традиційні методи захисту, наприклад криптографія, не приховують факт передачі секретної інформації, що може бути критично у певних ситуаціях. У цьому контексті стеганографія набуває особливої актуальності, адже вона дозволяє не тільки захистити зміст повідомлення, а й приховати сам факт його існування.

Стеганографічні технології використовуються для маскування секретної інформації всередині різноманітних цифрових носіїв – зображень, аудіо- та відеофайлів, текстових документів, що значно ускладнює її виявлення і перехоплення зловмисниками. Використання стеганографії в сучасних інформаційних системах має низку важливих переваг, які сприяють підвищенню безпеки, збереженню приватності та забезпечують додаткові рівні захисту.

У таблиці 1 наведено ключові переваги застосування стеганографії в умовах сучасного цифрового середовища, що демонструють її потенціал і важливість як інструмента інформаційної безпеки [2–4].

Виявлення прихованих даних є ключовим завданням стегоаналізу – напряму, що спрямований на ідентифікацію та аналіз інформації, захованої за допомогою стеганографічних методів. З огляду на різноманіття технік приховування та різні формати цифрових носіїв (зображення, аудіо, відео, текст), розробка ефективних методів виявлення стає все більш складною і вимогливою до інструментарію дослідників.

Різні підходи до стегоаналізу базуються на аналізі статистичних, структурних, амплітудних, фазових і частотних характеристик носіїв інформації, а також використовують сучасні методи машинного навчання для підвищення точності та швидкості виявлення. Зокрема, статистичні методи дозволяють виявляти аномалії, які виникають через втручання у бітові або частотні характеристики файлів, тоді як методи машинного навчання здатні автоматично розпізнавати складні патерни прихованої інформації навіть у великому обсязі даних.

Важливою складовою є також оцінка ефективності кожного методу з урахуванням типу носія, обсягу прихованої інформації, стійкості до атак та рівня помилкових спрацьовувань.

У таблиці 2 наведено основні методи та підходи, які застосовуються для виявлення прихованих даних у стегоаналізі, з коротким описом їх принципів дії, переваг та обмежень [2, 3, 7]. Цей огляд дозволяє систематизувати існуючі рішення та визначити напрямки для подальших досліджень.

Так, основою статистичного аналізу є аналіз статистичних характеристик аудіо контейнеру. У якості статистичних характеристик використовуються гістограми, кореляції, ентропія, інші статистичні параметри аудіо файлів. Статистичні методи стегоаналізу спрямовані на вирішення задачі виявлення прихованої інформації в контейнері на факті порушення статистичного зв’язку. Шляхом аналізу статистичних характеристик певної послідовності бітів, визначається, чи корелює вона з характеристиками порожніх стеганографічних контейнерів того ж типу.

Таблиця 1 – Переваги використання стеганографії в умовах сучасного цифрового середовища

№ з/п	Перевага	Практичне значення
1.	Приховання факту комунікації	На відміну від криптографії, яка перетворює повідомлення у шифрований формат, стеганографічні методи приховування дозволяють вбудовувати інформацію у вигляд, який не викликає підозр у сторонніх осіб. Такий підхід є ефективним в умовах жорсткої цензури, тотального мережевого моніторингу або репресивного контролю над інформаційними потоками. У подібних ситуаціях навіть зашифроване повідомлення може бути маркером для подальшої перевірки, тоді як прихована інформація залишається непоміченою.
2.	Комплексний підхід до захисту інформації (стеганографія та криптографія)	Поєднання стеганографічних і криптографічних методів створює багаторівневу модель захисту даних. У цій моделі інформація спочатку шифрується криптографічними засобами, після чого зашифроване повідомлення вбудовується у несекретний носій за допомогою стеганографічних алгоритмів. Це дозволяє забезпечити приховування повідомлення, його змістовий захист у випадку виявлення.
3.	Подолання мережевого контролю та фільтрації	У комп'ютерних мережах часто використовуються системи фільтрації та моніторингу, що базуються на виявленні певних сигнатур, ключових слів або нетипових структур у трафіку. Стеганографічні методи дозволяють приховати повідомлення в легітимних на вигляд файлах, (наприклад, зображення або аудіо файли), що ускладнює або унеможливлює їх виявлення стандартними інструментами безпеки.
4.	Захист авторських прав та цифрове маркування (цифрові водяні знаки)	Однією з практичних реалізацій стеганографії є цифрове водяне маркування – вбудовування непомітних ідентифікаційних даних у цифрові файли з метою підтвердження авторства, встановлення джерела витоку або боротьби з нелегальним копіюванням. Такі водяні знаки можуть містити унікальні коди, інформацію про власника авторських прав, дату створення інше.
5.	Застосування у розвідувальних органах	У діяльності розвідувальних органів існує актуальна потреба в конфіденційному обміні інформацією, особливо у випадках, коли звичні канали зв'язку можуть бути перехоплені або відстежені. Стеганографія забезпечує можливість прихованої передачі даних, що дозволяє зменшити ризик виявлення комунікації з боку третіх осіб або контррозвідувальних органів. З урахуванням зростання загроз у кіберпросторі, включаючи кібершпигунство та несанкціонований доступ до каналів зв'язку, використання стеганографічних методів залишається актуальним та важливим елементом систем кіберзахисту, зокрема у сфері оборони.

Джерело: <узагальнено авторами>

Тобто, для стегоаналізу і вирішення задачі визначення кореляції необхідно мати порожній та заповнений стеганографічний контейнер. До переваг цієї групи методів стегоаналізу можна віднести велику область застосування. Основним недоліком таких методів є те, що неявно або явно проявляється існування деякого простого контейнера. Метод показує результат, при якому LSB елементів контейнера записується послідовно, і не працює, коли молодші біти записуються псевдо випадково, а повідомлення розподіляється по всій довжині контейнера.

Наступним методом аналізу є візуальний аналіз, який полягає у дослідженні зображень на предмет видимих ознак стеганографії. Візуальний метод аналізу є одним з базових підходів виявлення прихованих даних, який базується на зоровому сприйнятті людини. Суть методу полягає в тому, що експерт візуально перевіряє цифрові контейнери на предмет наявності

підозрілих шумів, спотворень, дефектів, артефактів, які можуть вказувати на стеганографічне маскування. Наприклад, стиснення зображень з вбудованими даними може призводити до появи специфічних артефактів та втрати чіткості. Аудіосигнали з прихованою інформацією при перетворенні у спектрограми також можуть мати характерні спотворення, або шумове забарвлення.

Таблиця 2 – Методи виявлення прихованих даних у стегоаналізі

№ з/п	Метод	Опис метода
1.	Статистичний	Аналіз гістограм, аналіз пар пікселів/значень, аналіз коефіцієнтів перетворення. Методи на основі матриць спільної появи (Co-occurrence Matrix), RS-аналіз.
2.	Спеціально розроблений для конкретних алгоритмів стеганографії	Виявлення демаскуючих ознак, залишених конкретними інструментами стеганографії, такими як JPHide, Steghide.
3.	Машинного навчання	Наприклад, Support Vector Machines, Random Forests, Convolutional Neural Networks. Навчання моделі по набору даних, що містять як стегофайли, створені різними методами, так і чисті кавер-файли (файл з метаданими), визначення ймовірності наявності в них прихованої інформації на основі вивчених закономірностей та результатів навчання моделей.
4.	Візуальний	Виявлення ознак стеганографії візуально та аналіз окремих колірних, частотних, фазових, часових каналів, особливо при збільшеному масштабі перегляду. Цей метод є суб'єктивним та ефективний лише для певних типів стеганографії.
5.	Сигнатурний	Виявлення характерних "відбитків" або сигнатур у файлах, які залишаються при використанні певних програм стеганографії.
6.	На основі аналізу метаданих	Виявлення стеганографії, яка є результатом змін у метаданих файлу, наприклад, час створення, модифікації.
7.	Комбінований	Використовують кілька різних методів стегоаналізу для підвищення ймовірності виявлення прихованої інформації.

Джерело: <узагальнено авторами>

Таким чином, існує широкий спектр методів виявлення прихованих даних у стегоаналізі, кожен із яких має свої особливості, переваги та обмеження. Статистичні підходи забезпечують базовий рівень виявлення, ґрунтуючись на аномаліях у характеристиках файлів, тоді як спеціалізовані методи орієнтовані на розпізнавання слідів конкретних стеганографічних алгоритмів. Методи машинного навчання відкривають нові можливості завдяки автоматизації та здатності аналізувати великі обсяги даних, підвищуючи точність детекції. Візуальні і сигнатурні методи доповнюють аналітичний арсенал, але часто мають обмежену сферу застосування та залежать від досвіду аналітика. Аналіз метаданих дозволяє виявляти приховану інформацію через нетипові зміни в атрибутах файлів. Поєднання кількох методів у комбінований підхід дозволяє значно підвищити ефективність стегоаналізу, мінімізуючи ризики пропуску або помилкових спрацьовувань.

Отже, застосування комплексного підходу до виявлення прихованих даних є ключовим фактором для забезпечення високої надійності систем інформаційної безпеки в умовах постійного розвитку стеганографічних технологій.

Обговорення

У контексті розвитку інформаційних технологій та зростанням загроз у кібербезпеці, стеганографія та стегоаналіз займають особливе місце серед інструментів захисту конфіденційної інформації. Порівняно з традиційними методами криптографії, стеганографія дає можливість не тільки захистити зміст повідомлення, а й приховати сам факт його існування. Це особливо важливо в умовах тотального моніторингу, цензури або репресивного контролю над інформаційними потоками. Тому, стеганографія є надзвичайно важливим інструментом у різних сферах, від розвідки до захисту авторських прав.

Одним з основних аспектів, який варто підкреслити є складність і багатогранність методів стегоаналізу, які використовуються для виявлення прихованої інформації. Виявлення таких даних є критично важливим завданням для забезпечення надійності та безпеки інформаційних систем. Розглянуті в роботі методи, а саме: статистичний, візуальний, методи машинного навчання, а також комбіновані підходи – мають свої переваги та недоліки, що вимагає від фахівців з кібербезпеки постійної адаптації та використання новітніх технологій.

Наприклад, статистичні методи стегоаналізу добре працюють для виявлення прихованої інформації в файлах, де зміни в бітових або частотних характеристиках можуть бути очевидними, проте вони можуть бути неефективними у випадках, коли інформація прихована з використанням більш складних методів, таких як псевдовипадкові розподіли бітів. Це підкреслює важливість комбінованого підходу до виявлення стеганографії, який здатний забезпечити високий рівень детекції за допомогою різних методів і технологій.

Машинне навчання відкриває нові можливості для стегоаналізу, дозволяючи автоматизувати процеси виявлення прихованих даних і значно підвищити точність та швидкість розпізнавання складних патернів. Однак, на практиці, застосування цих методів часто вимагає великих обсягів даних для навчання моделей, а також високих обчислювальних потужностей. Це може бути певним обмеженням, особливо у реальних умовах, де швидкість аналізу є критичною.

Візуальний та сигнатурний аналіз також мають свої специфічні переваги, але вимагають великої кваліфікації та досвіду від аналітика з безпеки інформаційно-комунікаційних систем. Наприклад, візуальний аналіз може бути ефективним для виявлення очевидних артефактів у зображеннях чи аудіофайлах, однак цей метод може бути менш ефективним у випадках, коли зміни є надто малими або складними для сприйняття без допомоги спеціалізованих інструментів.

Не менш важливим є аспект оцінки ефективності стегоаналізу з урахуванням типу носія інформації та рівня ризику, що виникає через використання певних методів стеганографії. Наприклад, у разі використання стеганографії для захисту розвідувальних даних чи для обміну важливою інформацією, висока точність і швидкість виявлення є критичними, оскільки будь-яке проміжне спрацьовування або пропущена загроза можуть призвести до катастрофічних наслідків.

Цікавою є також роль стеганографії в контексті цифрових прав, зокрема в боротьбі з нелегальним копіюванням і піратством. Завдяки вбудованим водяним знакам можна ефективно контролювати обіг цифрових продуктів, що надає додаткові можливості для захисту авторських прав.

Важливим напрямком є розвиток стеганографічних технологій для забезпечення їх ефективного застосування в умовах розвитку нових форм атак, таких як кіберзлочинність, кібершпигунство та несанкціонований доступ до інформаційних систем. З огляду на це, стає очевидним, що лише постійний розвиток методів стегоаналізу та стеганографії дозволить адекватно реагувати на нові виклики та забезпечити надійний захист конфіденційної інформації в умовах сучасного цифрового середовища.

Отже, використання стеганографії разом із сучасними методами стегоаналізу забезпечує надійний захист інформації, але потребує постійного вдосконалення технологій і адаптації до змінюваних умов кіберзагроз. Висока ефективність виявлення прихованих даних залежить від поєднання різних методів, що дозволяє забезпечити комплексний підхід до захисту інформації в умовах сучасної цифрової ери.

Висновки

У результаті дослідження сучасних методів стеганографії та стегоаналізу можна зробити кілька важливих висновків.

1. Зростання обсягів переданої та збереженої інформації створює нові виклики для забезпечення її безпеки, адже традиційні методи захисту не завжди здатні приховати сам факт комунікації. В цьому контексті стеганографія виступає потужним інструментом для забезпечення конфіденційності не тільки змісту, а й існування повідомлення. Вона забезпечує високий рівень захисту інформації, роблячи її непомітною для сторонніх осіб, що важливо в умовах інтенсивного моніторингу та цензури.

2. Стеганографія дозволяє приховувати дані в різноманітних даних, таких як зображення, аудіо та відеофайли, що значно ускладнює їх виявлення. Завдяки поєднанню стеганографії з криптографічними методами, можна створити багаторівневу модель захисту, що забезпечує як приховання фактів комунікації, так і додаткову безпеку в разі виявлення прихованого повідомлення.

3. Технології стегоаналізу постійно розвиваються і використовують різноманітні методи, від статистичних і візуальних до застосування машинного навчання. Кожен метод має свої переваги та недоліки, тому комбінований підхід є найбільш ефективним для забезпечення надійного виявлення стеганографічних прихованих даних.

Таким чином, для підтримки високого рівня безпеки інформаційних систем у сучасному цифровому середовищі необхідно використовувати комплексні методи захисту та детекції, які враховують всі особливості стеганографічних технологій і здатні ефективно протистояти новим викликам у сфері інформаційної безпеки.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. ESET. (2025). *Стеганографія*. ESET Glossary. URL : https://help.eset.com/glossary/uk-UA/steganography.html.
2. Кузнецов, О. О., Євсеєв, С. П., & Король, О. Г. (2011). *Стеганографія: Навч посібник.* ХНЕУ.
3. Конахович, Г. Ф., & Пузиренко, А. Ю. (2006). *Комп'ютерна стеганографія: Теорія і практика*. МК-Прес.
4. Світловський, Є., & Трапезон, К. (2023). Стеганографічні підходи до оброблення аудіосигналів. *Вісник КрНУ імені Михайла Остроградського*, 3(140), 185–192. URL : https://visnikkrnu.kdu.edu.ua/statti/2023_3_2023_3_185.pdf.
5. Корольов, В. Ю., Поліновський, В. В., Герасименко, В. А., & Горінштейн, М. Л. (2011). Планування досліджень методів стеганографії та стегоаналізу. *Вісник Хмельницького національного університету*, 4, 187–196. URL : https://journals.khnu.km.ua/vestnik/pdf/tech/2011_4/53kor.pdf.

6. Енциклопедія сучасної України. (2014). *Криптографія*. https://esu.com.ua/article-1576.
7. Юдін, О. К., Зюбіна, Р. В., & Фролов, О. В. (2015). Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів. *Радіоелектроніка та інформатика*, 3, 13–21.
8. Казміді, І. Д., & Зубок, В. Ю. (2025). Сучасний стан стеганографії цифрових зображень. *У Theoretical and Applied Cybersecurity: Матеріали третьої всеукраїнської науково-практичної конференції (TACS-2025)*. Київ: КПІ ім. Ігоря Сікорського.

References

1. ESET. (2025). Steganography. ESET Glossary. Available from : https://help.eset.com/glossary/uk-UA/steganography.html.
2. Kuznetsov, O. O., Yevseiev, S. P., & Korol, O. H. (2011). Steganography: Textbook. KhNEU [Kharkiv National University of Economics].
3. Konakhovych, H. F., & Puzirenko, A. Yu. (2006). Computer steganography: Theory and practice. MK-Press.
4. Svitlovskyi, Ye., & Trapezon, K. (2023). Steganographic approaches to audio signal processing. *Visnyk KrNU imeni Mykhaila Ostrohradskoho*, *3*(140), 185–192. Available from : https://visnikkrnu.kdu.edu.ua/statti/2023_3_2023_3_185.pdf.
5. Koroliov, V. Yu., Polinovskyi, V. V., Herasymenko, V. A., & Gorinshtein, M. L. (2011). Planning research of steganography and steganalysis methods. *Visnyk Khmelnytskoho natsionalnoho universytetu*, *4*, 187–196. Available from : https://journals.khnu.km.ua/vestnik/pdf/tech/2011_4/53kor.pdf.
6. Encyclopedia of Modern Ukraine. (2014). Cryptography. Available from : https://esu.com.ua/article-1576.
7. Yudin, O. K., Ziubina, R. V., & Frolov, O. V. (2015). Analysis of steganographic methods for hiding information flows in containers of various formats. *Radioelektronika ta Informatyka*, *3*, 13–21.
8. Kazmidi, I. D., & Zubok, V. Yu. (2025). Current state of steganography of digital images. In *Theoretical and Applied Cybersecurity: Proceedings of the Third All-Ukrainian Scientific and Practical Conference (TACS-2025)*. Kyiv: KPI im. Ihoria Sikorskoho [Igor Sikorsky Kyiv Polytechnic Institute].