© Martyniuk H, Martyniuk I., Protsenko B. Analysis of modern methods of audio signal stegoanalysis // Ukrainian Scientific Journal of Information Security, 2024, vol. 30, issue 3, pp. 393-398. ©

DOI: 10.18372/2225-5036.30.20360

АНАЛІЗ СУЧАСНИХ МЕТОДІВ СТЕГОАНАЛІЗУ АУДІОСИГНАЛІВ

Ганна Мартинюк [1, 2], Ігор Мартинюк [2], Богдан Проценко[3]

[1] *Маріупольський державний університет*
[2] *ДержНДІ технологій кібербезпеки*
[3] *Київський національний економічний університет імені Вадима Гетьмана*

МАРТИНЮК Ганна Вадимівна, к.т.н., доцент
Рік та місце народження: 1989 рік, м. Херсон, Україна.
Освіта: Національний авіаційний університет, 20011 рік.
Посада: доцент кафедри системного аналізу та інформаційних технологій Маріупольського державного університету з 2022 року.
Наукові інтереси: статистичні моделі інформаційних сигналів; методи математичного та комп'ютерного моделювання сигналів і даних вимірювань.
Публікації: більше 60 наукових публікацій, серед яких монографії, наукові статті, матеріали та тези доповідей на конференціях та патенти.
E-mail: ganna.martyniuk@gmail.com
ORCID: 0000-0003-4234-025X

МАРТИНЮК Ігор Вадимович
Рік та місце народження: 1988 рік, с. Верхнєдніпровський, Росія
Освіта: Національний авіаційний університет, 20011 рік.; аспірант, Державний університет «Київський авіаційний інститут» з 2024 року
Посада: інженер ДержНДІ технологій кібербезпеки
Наукові інтереси: методи моніторингу та безпека мереж
Публікації: 4, серед яких статті, матеріали та тези доповідей на конференціях.
ORCID: 0009-0003-5565-0828
E-mail: imartyniukiv@gmail.com

ПРОЦЕНКО Богдан Петрович
Рік та місце народження: 2002 рік, м. Київ, Україна
Освіта: Київський національний економічний університет імені Вадима Гетьмана 2025
Посада: Фахівець 1 категорії навчальної лабораторії інформаційного забезпечення освітнього процесу з 2025 року.
Наукові інтереси: комп'ютерні науки, системи штучного інтелекту
Публікації: 3 публікації (тези до наукових конференцій)
E-mail: bohdan.protsen@gmail.com

Анотація. *У статті наведено інформацію щодо сучасного стану проблеми стегоаналізу аудіосигналів. Інтерес до цієї тематики виникає через постійне зростання цифрового контенту та цифрової трансформації зокрема. Треба відмітити, що більшість літератури, пов'язаною зі стегоаналізом, зокрема в Україні, стосується аналізу виключно зображень. Інформації про використання аудіосигналу в якості контейнеру в українських публікаціях вкрай мало. Авторами проведено аналіз сучасної зарубіжної літератури у сфері виявлення прихованої інформації в аудіофайлах. Розглянуто класифікацію методів стегоаналізу, зокрема сигнатурних, статистичних та на основі глибокого навчання, а також їх переваги і недоліки.*

Ключові слова: *аудіосигнал, стегоаналіз, стеганографія, приховане повідомлення, контейнер.*

Вступ. У сучасних умовах цифрової трансформації проблема приховування інформації в мультимедійних даних, зокрема в аудіосигналах, набуває все більшої актуальності. Аудіостеганографія використовується як для законних цілей, таких як цифрові водяні знаки та захист авторських прав, так і для прихованого передавання інформації, що може бути потенційною загрозою для інформаційної безпеки. У зв'язку з цим стегоаналіз аудіосигналів стає важливим інструментом для виявлення прихованих даних, що має велике значення для сфери кібербезпеки.

Зарубіжні дослідження у сфері стегоаналізу аудіосигналів активно розвиваються, особливо в країнах Європи, США та Китаї. Вчені використовують методи статистичного аналізу, спектрального аналізу, машинного навчання та глибоких нейронних мереж для виявлення ознак стеганографічних змін в аудіофайлах. У спеціалізованих наукових журналах та міжнародних конференціях регулярно публікуються нові підходи та алгоритми для детектування прихованої інформації в аудіофайлах.

Водночас в Україні дослідження у сфері стегоаналізу аудіосигналів перебувають на початковому етапі розвитку. Незважаючи на загальний інтерес до проблеми інформаційної безпеки, кількість публікацій та наукових досліджень у цій галузі є значно меншою, ніж у провідних країнах світу. Це зумовлює необхідність подальших досліджень у цій сфері та впровадження сучасних методів аналізу аудіостеганографічних загроз.

Автори статті поставили перед собою задачу систематизувати відомі методи, навести їх переваги та недоліки для різних типів аудіосигналів. Дана стаття носить оглядовий характер і спрямована на глибокий огляд останніх досягнень у галузі стеганоаналізу і проведення всебічного огляду для нових зацікавлених дослідників з питань стеганоаналізу для аудіосигналів.

Постановка проблеми. Проаналізувати сучасні публікації у сфері стегоаналізу, виділити питання використання аудіосигналу в якості контейнера для прихованого повідомлення. Структурувати методи стегоаналізу аудіосигналу та можливості їх застосування на сьогодні в Україні.

Аналіз останніх досліджень і публікацій. Стеганографія полягає в тому, що до звичайного повідомлення додається додаткова інформація, так зване «конфіденційне повідомлення». Перевагою стеганографічних методів є те, що тільки цільові одержувачі стегоконтейнера можуть отримати приховане повідомлення. Третя сторона не буде знати про наявність прихованих даних у повідомленні. Проте варто відмітити – стеганографічні методи на сьогодні можуть бути використані також для різного роду атак або збору несанкціонованої інформації. .За останні десятиліття було декілька випадків використання стеганографії для шпіонажу чи кіберзлочинності, які є опублікованими в засобах масової інформації:

1. У 2019 році компанія Symantec заявила [1], що вони виявили російську кібершпигунську групу Waterbug (Turla), яка використовує WAV-файли для приховування та передачі шкідливого коду зі свого сервера до вже інфікованих жертв.

2. У 2020 році компанія Sansec виявила [2], що кіберзлочинні групи використовували стеганографію для крадіжки платіжної інформації з онлайн-магазинів. Вони приховували шкідливий код у зображеннях соціальних іконок, таких як логотипи Twitter або Reddit, що дозволяло їм непомітно збирати дані кредитних карток покупців.

3. У 2022 році було виявлено [3], що група Witchetty APT використовувала стеганографію для приховування шкідливого коду в зображеннях. Вони завантажували зображення з GitHub, які на перший погляд виглядали як звичайні логотипи Windows, але містили прихований шкідливий код, що ускладнювало виявлення та аналіз.

Варто відмітити, що використання аудіофайлів в якості контейнера для передачі повідомлень не є таким популярним, як використання зображень, і на сьогодні відомі тільки декілька таких випадків. Хоча конкретні публічні випадки використання стеганографії в аудіофайлах є рідкісними, існують дослідження та розробки, спрямовані на виявлення та запобігання таким методам приховування інформації.

У [4-5] наведено інформацію про методи стегоаналізу аудіосигналів, які були розбиті на 2 категорії: цільові та універсальні. По кожному з методів був зроблений теоретичний аналіз їх використання. У [6-7] наводять пояснення основних елементів стегоаналізу, які можна застосовувати до відео- та аудіосигналів.

Інші роботи вже включають виключно пояснення певних методів окремо з теоретичної та практичної сторін. Так, у [8-9] наведені метод цільового стегоаналізу для виявлення стеганографії для MP3-сигналів. А у роботах [10-14] наведено інформацію щодо специфічних універсальних методів стегоаналізу.

Аналіз відомих методів стегоаналізу. На сьогодні відома ціла низка різних стеганографічних методів для приховування контейнерів у медіа файлах. Для виявлення факту наявності прихованого повідомлення користуються методами стегоаналізу. Отже, для проведення стегоаналізу необхідно вибрати і виділити деякі ознаки повідомлення, а потім проаналізувати їх для виявлення будь-яких змін.

Загалом, існує ряд методів стегоаналізу, які на сьогодні використовуються на практиці (рис. 1).

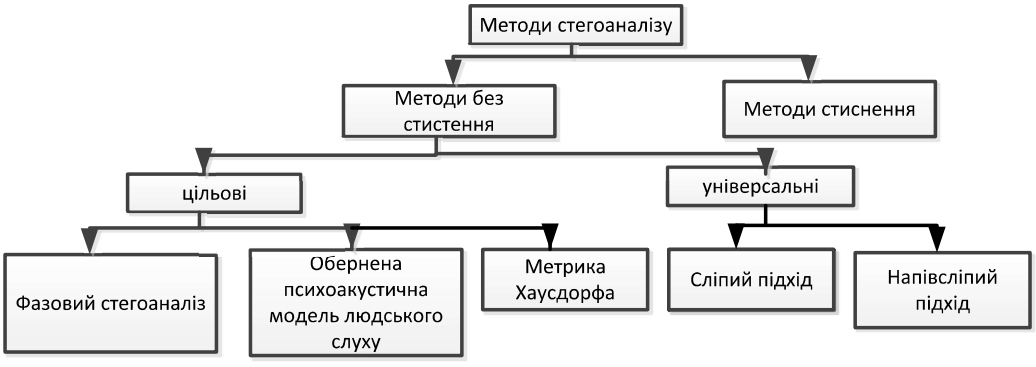

Рис. 1 Загальна класифікація методів стегоаналізу аудіосигналів

Методи стиснення полягають у тому, що вихідне звичайне повідомлення (порожній контейнер) стискається краще, ніж заповнений контейнер. Такі методи полягають в порівнянні коефіцієнтів стиснення вихідного контейнера і його повністю заповненої копії. До обох файлів застосовується метод стиснення даних, і аналізуються їх коефіцієнти стиснення. Якщо ці коефіцієнти близькі за значеннями, то з великою ймовірністю можна стверджувати, що вихідний файл містив приховане повідомлення, інакше йдеться про відсутність секретної інформації в об'єкті. З урахуванням цього твердження обирається деяке порогове значення щодо ступеня стиснення. Якщо ступінь стиснення більше даного порогового значення, то кажуть про ймовірність прихованого повідомлення в контейнері.

Методи без стиснення можна умовно розділити на два методи: цільовий та універсальний. Цільовий метод залежить від стеганографічного алгоритму: основним правилом цього методу є аналіз статистичних характеристик або «особливостей» контейнера до і після вбудовування прихованого повідомлення. Хоча цей метод здебільшого призводить до точних результатів, він дуже обмежений конкретними алгоритмами вбудовування і конкретним форматом контейнера. У протилежність цільовим методам існують універсальні. Методи цього типу розробляються незалежно від стеганографічного алгоритму, який був використаний для приховування повідомлення. Така універсальність робить методи більш практичними. Завдяки цьому цей тип дуже широко використовується, хоча він менш ефективний, ніж цільовий метод. Універсальний метод також поділяється на два підходи - сліпий і напівсліпий. Напівсліпий підхід можна також назвати частково універсальним, адже при використанні такого підходу частіше за все присутня інформація про метод стеганографії або сигнал (можливо навіть інформацію про оригінальний сигнал). Сліпий підхід не має жодної інформації про тип або метод стеганографії та не має доступу до оригінального сигналу.

З огляду на велику кількість методів доцільно зупинитися більше детально на алгоритмі стегоаналізу в загальному вигляді (рис. 2).

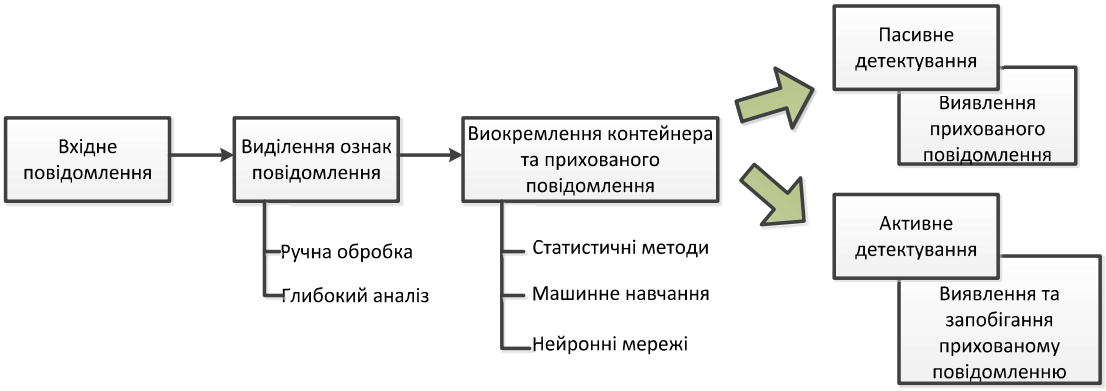

Рис. 2 Загальний алгоритм процесу стегоаналізу повідомлення

Як видно з рис. 2, стеганоаналіз починається з вилучення деяких ознак вхідного повідомлення, після чого відбувається аналіз та виокремлення прихованого повідомлення від контейнера. Існує два способи виділення ознак повідомлення: ручна обробка та глибокий аналіз. У першому випадку відомі ознаки знаходяться вручну, наприклад, за допомогою методів статистичної обробки знаходять статистичні ознаки прихованого повідомлення. Глибокий аналіз відбувається за допомогою нейронних мереж [4].

Після виділення ознак прихованого повідомлення відбувається виокремлення контейнера та самого прихованого повідомлення. Таке виокремлення може відбуватися декількома способами:

- використанням статистичних методів: приховане повідомлення виявляють за допомогою емпіричного порогу;
- методом машинного навчання для тренування і вивчення моделі контейнера: такий метод дозволить розрізнити приховане повідомлення та контейнер під час тестування;
- нейронними мережами: даний метод можна використовувати не тільки для виокремлення ознак повідомлень, а й для виокремлення самого прихованого повідомлення.

Процес виявлення повідомлення також можна поділити на два основних методи [4, 15]: пасивне детектування, сутність якого полягає виключно у виявленні прихованого повідомлення; активне детектування, коли повідомлення не тільки виявляється, але й надається більше інформації про приховане повідомлення.

У даній статті основна увага буде приділена виключно факту знаходження прихованого повідомлення в аудіосигналі. На основі цього далі увага буде приділена різним методам виділення ознак повідомлення.

Виділення ознак прихованого повідомлення. Виділення ознак повідомлення є одним з ключових етапів стегоаналізу. Як показано на рис. 2, методи виявлення можна розділити на так звані методи ручної обробки, та проведення глибокого аналізу сигналів. До методів ручної обробки можна віднести два методи – сигнатурний та статистичний. Інколи ці методи використовуються окремо, а інколи в поєднанні [16]. Варто також відмітити, що частково сигнатурні методи, як і методи стегоаналізу, використовують для аналізу сигналів нейронні мережі, тому варто відмітити, що класифікація на ручні методи та методи глибокого аналізу даних на сьогодні не є чіткою. Для кращого знаходження прихованих повідомлень варто використовувати поєднання всіх зазначених методів.

Сигнатурний метод - це метод виявлення прихованої інформації в аудіофайлах шляхом пошуку унікальних сигнатур, які залишають конкретні стеганографічні інструменти або алгоритми. Ці сигнатури можуть бути у вигляді специфічних байтових шаблонів, метаданих, змін у структурі файлу або інших артефактів, що виникають під час вбудовування прихованих повідомлень.

Сутність сигнатурного методу полягає у виявленні конкретних стеганографічних інструментів або технік. Таким чином проводиться виявлення та аналіз артефактів, коефіцієнтів MDCT тощо. В якості найпростіших сигнатурних методів стегоаналізу слід виділити StegAlyzerSS [17], MP3Stego Signature Detector [18]. Їх класифікація наведена в табл. 1.

Таблиця 1

Класифікація простих методів сигнатурного стегоаналізу

Назва методу	*Короткий опис*	*Підтримувані аудіоформати*
StegAlyzerSS	Інструмент для виявлення стеганографії в аудіофайлах шляхом пошуку відомих сигнатур, залишених стеганографічними програмами, з використанням бази даних SAFDB.	WAV
MP3Stego Signature Detector	Цей метод аналізує зміни у коефіцієнтах QMDCT (Modified Discrete Cosine Transform), які виникають внаслідок використання стеганографічного інструменту MP3Stego	MP3

Ці методи ефективні для виявлення стеганографії, коли відомі специфічні ознаки або сигнатури, залишені стеганографічними інструментами. Однак їх ефективність може знижуватися при використанні нових або модифікованих стеганографічних методів, які не залишають відомих сигнатур.

Статистичні методи стегоаналізу засновані на тому, що процес стеганографічного перетворення аудіосигналу вносить певні спотворення в статистичні характеристики сигналу-контейнера. Це дає змогу виявити факт приховування інформації [14].

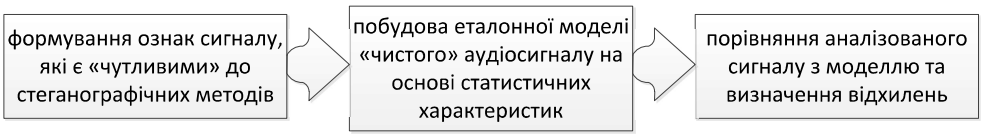

Рис. 3 Етапи використання статистичних методів стегоаналізу

В загальному вигляді аналізуються такі статистичні характеристики: гістограми амплітудних значень, коефіцієнти кореляції між сусідніми семплами, енергетичні спектри та їх ентропія, залишкові сигнали після фільтрації, а також особливості сигналу у частотній або вейвлет-області. Алгоритм використання статистичних методів представлений на рис. 3.

На відміну від простих сигнатурних методів, статистичні методи є більш універсальними, але вони потребують складної обробки сигналів та навчання моделей для подальшого їх використання. Проте у випадках відомих методів стеганографії, доцільніше використовувати сигнатурні методи, які дозволять заздалегідь підготувати базу даних сигнатур для пошуку.

Використання методів глибокого аналізу засновані в основному на використанні нейронних мереж. У загальному вигляді не можна виокремити такі методи в окрему категорію. Адже по своїй суті і сигнатурні методи, і статистичні методи на сьогодні в більшості випадків використовують нейронні мережі для навчання та обробки сигналів. Але варто відмітити, що поєднання сигнатурного та статистичного методів з глибоким аналізом дає змогу знаходити приховані сигнали незалежно від того, який метод стеганографії використовувався. Так, наприклад, метод Spec-ResNet [16] використовує сигнатурні особливості спектрограм та статистичні ознаки, об'єднуючи їх у глибинній мережі. Популярними на сьогодні також є методи LARXNet [19] та F3SNet [20]. Аналіз цих методів наведено у табл. 2.

Ці сучасні методи сигнатурного стегоаналізу демонструють значний прогрес у виявленні прихованої інформації, особливо завдяки

використанню глибоких нейронних мереж та вдосконалених стратегій аналізу. Крім того варто відмітити, що запропоновані у табл. 2 методи на сьогодні характеризуються високою точністю знаходження прихованого повідомлення, проте мають доволі складну реалізацію та обчислювальну складність.

Таблиця 2

Класифікація методів сигнатурного стегоаналізу з використанням нейронних мереж

№	*Назва методу*	*Короткий опис*	*Формати аудіо*
1	Spec-ResNet	Глибока залишкова мережа для спектрограм аудіо. В якості вхідних даних використовує спектрограми сигналів	AAC, MP3
2	ResNeXt	Зазвичай працює на спектограмах аудіосигналів. Проте також може бути використаний для статистичних ознак, таких як середнє, дисперсія чи автокореляційна функція	Загальні аудіоформати
3	LARXNet	Базується на алгоритмі ResNeXt для AAC-аудіо. Для зменшення кількості оцінюваних параметрів працює на основі групових згорток	AAC

Підсумовуючи наведений матеріал можна дійти висновку, що у випадку, коли відомі певні специфічні ознаки або сигнатури, які залишають певні стеганографічні інструменти, доцільніше використовувати звичайні сигнатурні методи. Проте у випадку, коли сигнатурні методи не дають результату, доцільніше використовувати статистичні методи. Такі методи є більш універсальними та дозволяють математично виміряти відхилення аудіосигналів, у які було приховано повідомлення. Варто відмітити, що на сьогодні більшої популярності набирають методи глибинного навчання, які дозволяють поєднувати сигнатурні особливості та статистичні характеристики у певну глибинну мережу і проводити досконаліший аналіз аудіосигналів.

Висновки. Проаналізовано дослідження у сфері виявлення прихованої інформації в аудіосигналах. Виконано систематизацію основних методів стегоаналізу аудіосигналів, зокрема сигнатурних, статистичних та методів із застосуванням глибокого навчання. Обґрунтовано переваги й недоліки кожного підходу, визначено їх практичну застосовність для різних форматів сигналів. Особлива увага приділена алгоритмічній структурі процесу виявлення прихованих повідомлень та методам виділення ознак, що є ключовим етапом стегоаналізу.

Література

[1] Catalin Cimpanu. WAV audio files are now being used to hide malicious code [Електронний ресурс]. 2019. Режим доступу: https://www.zdnet.com/article/wav-audio-files-are-now-being-used-to-hide-malicious-code/

[2] Tatum Hunter. Steganography: The Undetectable Cybersecurity Threat [Електронний ресурс]. 2022. Builtin. Режим доступу: https://builtin.com/articles/steganography.

[3] Using Steganography to Hide Malware – Witchetty APT Case Study [Електронний ресурс]. 2022. Hawkeye. Hunting Cyber Adversaries. Режим доступу: https://hawk-eye.io/2022/12/using-steganography-to-hide-malware-witchetty-apt-case-study.

[4] Ghasemzadeh H., Kayvanrad M. H. Comprehensive review of audio steganalysis methods. IET Signal Processing. 2018. Vol. 12, No. 6. P. 673–687.

[5] Мартинюк Г. В., Козловський В. В., Нестеренко К. С., Мелешко Т. В., Яковів І. І. Систематизація методів стегоаналізу для аудіосигналів. Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS' 2021). 2021. С. 23–25.

[6] Tabares-Soto R. та ін. Digital media steganalysis. In: Digital Media Steganography. Academic Press, 2020. P. 259–293.

[7] Shehab D. A., Alhaddad M. J. Comprehensive survey of multimedia steganalysis: Techniques, evaluations, and trends in future research. Symmetry. 2022. Vol. 14, No. 1. P. 117.

[8] Jin C., Wang R., Yan D. Steganalysis of MP3Stego with low embedding-rate using Markov feature. Multimedia Tools and Applications. 2017. Vol. 76. P. 6143–6158.

[9] Wang Y., Yi X., Zhao X. MP3 steganalysis based on joint point-wise and block-wise correlations. Information Sciences. 2020. Vol. 512. P. 1118–1133.

[10] Ghasemzadeh H., Khalil Arjmandi M. Universal audio steganalysis based on calibration and reversed frequency resolution of human auditory system. IET Signal Processing. 2017. Vol. 11, No. 8. P. 916–922.

[11] Han C., Xue R., Zhang R., Wang X. A new audio steganalysis method based on linear prediction. Multimedia Tools and Applications. 2018. Vol. 77. P. 15431–15455.

[12] Lin Y., Wang R., Yan D., Dong L., Zhang X. Audio steganalysis with improved convolutional neural network. Proceedings of the ACM Workshop on Information Hiding and Multimedia Security. 2019. P. 210–215.

[13] Ren Y., Liu D., Xiong Q., Fu J., Wang L. Spec-resnet: a general audio steganalysis scheme based on deep residual network of spectrogram. arXiv preprint arXiv:1901.06838. 2019.

[14] Martyniuk H., Kozlovskiy V., Meleshko T., Sorokun A. Method of Finding Cover Signal for Audio Steganalysis Calibrated Methods. 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). 2021. Vol. 2. P. 1095–1100. IEEE.

[15] Karampidis K., Kavallieratou E., Papadourakis G. A review of image steganalysis techniques for digital forensics. Journal of Information Security and Applications. 2018. Vol. 40. P. 217–235.

[16] Ren, Y., et al. (2019). "Spec-ResNet: A General Audio Steganalysis Scheme Based on Deep Residual Network of Spectrogram." *arXiv preprint arXiv:1901.06838*.

[17] Green, Jordan, et al. "Steganography analysis: Efficacy and response-time of current steganalysis software." *Journal of Computer Science* 9 (2015): 236-44.

[18] Ren, Yanzhen, et al. "Spec-resnet: a general audio steganalysis scheme based on deep residual network of spectrogram." *arXiv preprint arXiv:1901.06838* (2019).

[19] Shehab DA, Alhaddad MJ. Comprehensive Survey of Multimedia Steganalysis: Techniques, Evaluations, and Trends in Future Research. *Symmetry*. 2022; 14(1):117. https://doi.org/10.3390/sym14010117.

[20] Guo, Chuanpeng, et al. "F3SNet: A Four-Step Strategy for QIM Steganalysis of Compressed Speech Based on Hierarchical Attention Network." *Security and Communication Networks* 2021.1 (2021): 1627486.

УДК 004.056.55: 519.876.5 (045)

Martyniuk H, Martyniuk I., Protsenko B. Analysis of modern methods of audio signal stegoanalysis

Abstract. *The paper provides information on the current state of the problem of stegoanalysis of audio signals. Interest in this subject arises due to the constant growth of digital content and digital transformation in particular. It should be noted that most of the literature related to stegoanalysis, in particular in Ukraine, deals with the analysis of images only. There is very little information about the use of audio as a container in Ukrainian publications. The authors have analysed modern foreign literature in the field of detecting hidden information in audio files. The classification of stegoanalysis methods, in particular signature, statistical and deep learning based methods, as well as their advantages and disadvantages are considered*

Keywords: *audio signal, stegoanalysis, steganography, hidden message, container.*

Мартинюк Ганна Вадимівна, к.т.н., доцент, доцент кафедри системного аналізу та інформаційних технологій Маріупольського державного університету.
Martyniuk Hanna, Ph.D., Associate Professor, Associate Professor of the Department of System Analysis and Information Technologies, Mariupol State University

Мартинюк Ігор Вадимович, інженер ДержНДІ технологій кібербезпеки
Martyniuk Igor, engineer at the State Research Institute of Cybersecurity Technologies

Проценко Богдан Петрович, Фахівець 1 категорії навчальної лабораторії інформаційного забезпечення освітнього процесу.
Protsenko Bohdan, Specialist 1st category of the educational laboratory for information support of the educational process.