

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

СЕКЦІЯ 22. ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТРИМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ

<i>Логінова Наталія Іванівна</i> ПОРІВНЯННЯ БІБЛІОТЕК PUTHON ДЛЯ КЕРУВАННЯ БАЗАМИ ДАНИХ	486
<i>Гура Володимир Ігорович</i> КОМПЛЕКСНИЙ АНАЛІЗ КІБЕРЗАГРОЗ В ІНТЕЛЕКТУАЛЬНИХ ЕНЕРГОСИСТЕМАХ	489
<i>Задержко Олександр Владиславович</i> АНАЛІЗ ПРОБЛЕМАТИКИ ФОРМУВАННЯ РЕЛЕВАНТНОСТІ ПОШУКУ НАУКОВОЇ ІНФОРМАЦІЇ	493
<i>Куклінова Тетяна Вікторівна, Куклінова Софія Іванівна</i> ШТУЧНИЙ ІНТЕЛЕКТ І ЗЕЛЕНИЙ ВОДЕНЬ ДЛЯ СТАЛОГО РОЗВИТКУ	497
<i>Лобода Юлія Теннадіївна</i> ЕФЕКТИВНІ ІНСТРУМЕНТИ ТА ПІДХОДИ ВІЗУАЛІЗАЦІЇ ДАНИХ В АНАЛІТИЧНОМУ ПРОЦЕСІ	501
<i>Манаков Сергій Юрійович</i> ПАТЕРНИ БЕЗСЕРВЕРНОЇ АРХІТЕКТУРИ	504
<i>Трофименко Олена Григорівна</i> ВПЛИВ ШТУЧНОГО ІНТЕЛЕКТУ НА КОНКУРЕНТОСПРОМОЖНІСТЬ В ІТ	506
<i>Чанишев Рашид Ібрагімович</i> PROTESTU – НОВА ВНУТРІШНЯ СТРАТЕГІЯ БЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ	510
<i>Чикунів Павло Олександрович</i> ПРОЄКТУВАННЯ ВЕБОРІЄНТОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ УНІВЕРСАЛЬНОЇ ПЛАТФОРМИ WINDOWS	513
<i>Щербина Юрій Володимирович</i> АНАЛІЗ ЕФЕКТИВНОСТІ ПРОГРАМНИХ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ...	517
<i>Дика Анастасія Іванівна</i> ЗАСТОСУВАННЯ NLP-МЕТОДІВ ДЛЯ ВИЯВЛЕННЯ XSS-АТАК	520
<i>Грезіна Олена Миколаївна</i> ЗАСТОСУВАННЯ СИСТЕМНОГО АНАЛІЗУ ДЛЯ ІНТЕГРАЦІЇ РІЗНИХ БАЗ ДАНИХ В ВЕБЗАСТОСУНКАХ	523
<i>Соловійов Артем Сергійович</i> ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ЯК КЛЮЧОВИЙ ЕЛЕМЕНТ КІБЕРБЕЗПЕКИ ОСОБИ В ЦИФРОВУ ЕПОХУ	526
<i>Толокнов Анатолій Арнольдович</i> ПРОЦЕДУРНА ГЕНЕРАЦІЯ У ВІДЕОІГРАХ:ОГЛЯД МЕТОДІВ, ЗАСТОСУВАНЬ ТА ПЕРСПЕКТИВ	529

СЕКЦІЯ 23. КІБЕРБЕЗПЕКА ОСОБИ, СУСПІЛЬСТВА ТА ДЕРЖАВИ ЯК ФУНДАМЕНТАЛЬНИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ ОБОРОНОЗДАТНОСТІ УКРАЇНИ

<i>Горбаченко Станіслав Анатолійович</i> ЗАСТОСУВАННЯ МЕТОДОЛОГІЇ SCRUM У ВИРІШЕННІ ЗАДАЧ КІБЕРБЕЗПЕКИ	533
<i>Соколов Артем Вікторович, Радуш Володимир Вячеславович</i> МЕТОД НЕДВІЙКОВОГО АФІННОГО ПЕРЕТВОРЕННЯ ДЛЯ ПІДВИЩЕННЯ КРИПТОГРАФІЧНОЇ ЯКОСТІ S-БЛОКІВ	536
<i>Ахматетьєва Ганна Валеріївна, Овчинников Микола Юрійович</i> ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ШИРОКОСМУГОВОГО ТА ФАЗОВОГО КОДУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В АУДІОСИГНАЛІ	539
<i>Бойко Віктор Дмитрович</i> ПРОБЛЕМИ ШВИДКОГО РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ У ВЕБ-СЕРВЕРАХ СЕРЕДНЬОГО ТА НИЗЬКОГО РІВНЯ	543

Таблиця 1. Криптографічні характеристики запропонованого S-блока у порівнянні з іншими конструкціями

S-box	Нелінійність	SAC	BIC нелінійність	BIC SAC	LAP	DAP	$\max\{ r_{ij} \}$	SAC 4-функцій
S-блок [1]	80	0.5	83.4286	0.4967	0.5	1	0	0.5
Запропон. S-блок	96	0.5	77.7143	0.4799	0.5	1	0	0.5
S-блок [2]	111.75	0.5029	103.7143	0.5006	0.125	0.0391	0.1250	0.6094
S-блок [3]	107	0.5781	102.93	0.4991	0.1719	0.0469	0.1562	0.6406

Список використаних джерел:

1. Sokolov A. V., Radush V. V. The method for synthesis of high-quality S-boxes based on many-valued logic functions. *Informatics and mathematical methods in simulation*. 2022. Vol. 12. No. 3. P. 219-225.

2. Aydın Y., Özkaynak F. Automated Chaos-Driven S-Box Generation and Analysis Tool for Enhanced Cryptographic Resilience. *IEEE Access*. 2024. Vol. 12. P. 312-328.

3. Artuğer F., Özkaynak F. A new chaotic system and its practical applications in substitution box and random number generator. *Multimedia Tools and Applications*. 2024. 83(42). P. 90053-90067.

Ключові слова: криптографія, S-блок, афінне перетворення.
Keywords: cryptography, S-box, affine transformation.

Ахматетьєва Ганна Валеріївна
Національний університет «Одеська юридична академія»,
доцент кафедри кібербезпеки, кандидат технічних наук, доцент
Овчинников Микола Юрійович
Національний університет «Одеська юридична академія»,
асистент кафедри кібербезпеки

**ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ШИРОКОСМУГОВОГО
ТА ФАЗОВОГО КОДУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В
АУДІОСИГНАЛІ**

У сучасних умовах активного використання цифрових технологій та стрімкого розвитку штучного інтелекту зростає потреба у захисті авторських прав і цифрових даних. Одним із найефективніших інструментів у цьому контексті

є цифрові водяні знаки (ЦВЗ), що дозволяють вбудовувати в аудіосигнал приховану інформацію, не погіршуючи її сприйняття слухачем. Серед численних методів додавання ЦВЗ у цій роботі розглядаються широкосмугове та фазове кодування. Обидва підходи мають свої сильні та слабкі сторони щодо стійкості до атак, непомітності та збереження цілісності вбудованої інформації. Проведено порівняльний аналіз зазначених методів з огляду на актуальні дослідження останніх років.

Метод широкосмугового кодування передбачає додавання до сигналу модульованого шуму, амплітуда якого трохи перевищує поріг маскування слуху. Для витягування прихованого біта використовується кореляція між отриманими коефіцієнтами та початковою випадковою послідовністю. Метод широкосмугового кодування характеризується високою стійкістю до лінійних атак, зокрема до компресії та фільтрації, а також забезпечує сумісність з більшістю форматів аудіо. Водночас він є чутливим до атак, заснованих на використанні штучного інтелекту, які модифікують структуру сигналу, а також має знижену стійкість до десинхронізації, зміни швидкості відтворення та масштабування по часу.

У вдосконаленому алгоритмі фазового кодування, запропонованому в [1], були внесені кілька ключових змін, спрямованих на подолання недоліків традиційного методу. Зокрема, інформація рівномірно розподіляється по всьому аудіосигналу шляхом поділу його на сегменти та вбудовування бітів у середньочастотний діапазон фази, що дозволяє уникати значних спотворень у низько-частотній області, зберігаючи тим самим прихованість ЦВЗ [1]. Крім того, автори алгоритму відмовилися від поширення фазових зсувів між сегментами, що значно спростило обчислення й зменшило ризик накопичення фазових помилок. Такий підхід також підвищив цілісність вбудованої інформації, оскільки її складніше відновити після редагування чи обрізання аудіо. Удосконалений алгоритм забезпечує кращий баланс між стійкістю до стеганоаналізу та збереженням високої якості звучання.

Метод фазового кодування ґрунтується на властивості людського слуху сприймати не абсолютні значення фази, а лише їхню різницю. Для реалізації цього підходу аудіосигнал розбивається на сегменти: перший сегмент використовується для кодування повідомлення, а фази наступних коригуються таким чином, щоб зберегти відносну різницю фаз між ними. Серед переваг методу варто відзначити високу непомітність для слухача, а також стійкість до атак, що змінюють амплітуду сигналу, наприклад, нормалізацію гучності. Водночас, метод є вразливим до атак, які порушують синхронізацію, і характеризується складністю точного витягання інформації у випадку спотворень аудіосигналу.

На рисунку 1 зображено процес нанесення водяних знаків на аудіо. Спочатку генератор водяних знаків кодує надані користувачем біти (наприклад, «0101110») в аудіосигнал, формуючи аудіо з вбудованим водяним знаком. Далі детектор водяних знаків витягує та декодує ці біти з аудіосигналу, перевіряючи його автентичність.



Рис. 1. Сценарій додавання водяного знаку до аудіо

Хоча процес нанесення водяних знаків на аудіо виглядає перспективним, його стійкість у реальних умовах застосування залежить від здатності подолати основні проблеми. Стійкість водяного знака визначається його здатністю витримувати різноманітні модифікації, такі як стиснення, шум, перетворення формату та інші поширені маніпуляції, при цьому залишаючи можливість точного витягнення інформації навіть за таких умов. Якщо водяний знак легко видаляється або його якість погіршується, його ефективність як інструменту для захисту інтелектуальної власності та автентифікації значно знижується. Крім того, в роботах [2], [3] підкреслюється, що будь-яка система водяного маркування повинна забезпечувати також високу точність відтворення.

У дослідженні [4] наголошується, що більшість існуючих схем водяного маркування, зокрема й ширококугові методи, демонструють обмежену ефективність в умовах сучасних загроз. Зокрема, автори вказують, що ширококугові алгоритми погано протистоять атакам, які включають генерацію або обробку аудіосигналів за допомогою моделей штучного інтелекту, таких як текст-в-мову (Text-to-Speech) або аудіо-генератори на базі дифузійних мереж [4]. Такі методи часто спотворюють або повністю видаляють приховані дані, навіть якщо візуально чи на слух сигнал здається незмінним. Генеративні моделі, як показано в дослідженні, не зберігають ті низькорівневі особливості сигналу, в яких зазвичай кодуються ширококугові ЦВЗ. У результаті водяні знаки стають вразливими до так званих “нейромережевих” атак, навіть без цілеспрямованого наміру їх видалення. Це ставить під сумнів ефективність ширококугових підходів у сучасному контексті, де штучний інтелект відіграє все більшу роль у створенні та редагуванні мультимедійного контенту.

У роботі [5] автори запропонували техніку додавання ЦВЗ на основі фазової модуляції, де інформація вбудовується шляхом зміни фази вибраних частот у спектрі сигналу. Основний акцент зроблено на досягненні високої непомітності, зокрема для мовленнєвих сигналів. Метод демонструє хорошу сумісність з кодеками типу MP3, однак має обмежену стійкість до синхронізаційних атак (наприклад, зміна швидкості відтворення чи вирізання фрагментів) [5].

У дослідженні [6] запропоновано вбудовувати дані у випадкові частоти за допомогою фазової маніпуляції. Це дозволяє значно підвищити стійкість до спроб несанкціонованого виявлення або видалення водяного знака, оскільки частоти вибираються псевдовипадково. Проте така схема потребує точного збереження синхронізації й сильно залежить від незмінності фазових характеристик сигналу після обробки [6]. Порівняння різних методів наведено в таблиці 1.

Таблиця 1. Порівняння ефективності методів

Критерій	Широкосмугове кодування	Фазове кодування
Непомітність для слухача	Середня	Висока
Стійкість до стиснення	Висока	Середня
Захист від десинхронізації	Низький	Середній
Стійкість до атак ШІ	Низька	Середня
Складність реалізації	Середня	Висока

Розглянуті роботи підкреслюють ключову перевагу фазового кодування – його високу непомітність для слухача. Водночас, як показує аналіз, фазові методи загалом демонструють вразливість до змін у часовій структурі сигналу, таких як десинхронізація або повторне кодування з фазовими спотвореннями. Це свідчить про необхідність подальшого вдосконалення, зокрема щодо стабільності до редагування аудіо. Сучасні дослідження, як наприклад покращений алгоритм Yang G. [1], розв’язують деякі з цих проблем, наприклад шляхом рівномірного розподілу інформації по сигналу та спрощення фазових обчислень. У поєднанні з підходами з попередніх років це дозволяє розробляти більш надійні гібридні системи водяного маркування для реальних сценаріїв використання.

Список використаних джерел:

1. Yang G. An Improved Phase Coding Audio Steganography Algorithm //arXiv preprint arXiv:2408.13277. 2024.
2. Li Y., Wang H., Barni M. A survey of deep neural network watermarking techniques *Neurocomputing*. 2021. Vol. 461. С. 171-193.
3. Lukas N. et al. Sok: How robust is image classification deep neural network watermarking? *2022 IEEE Symposium on Security and Privacy (SP)*. URL: <https://arxiv.org/pdf/2108.04974>.
4. Wen Y. et al. SoK: How Robust is Audio Watermarking in Generative AI models? //arXiv preprint arXiv:2503.19176. 2025.
5. Arnold M., Baum P. G., Voeßing W. A phase modulation audio watermarking technique. *International Workshop on Information Hiding*. Berlin, Heidelberg : Springer Berlin Heidelberg, 2009. P. 102-116.
6. Liew P. Y., Armand M. A. Inaudible watermarking via phase manipulation of random frequencies. *Multimedia Tools and Applications*. 2007. Vol. 35. P. 357-377.

Ключові слова: широкосмугове кодування, фазове кодування, цифровий водяний знак, стійкість до атак, непомітність, збереження цілісності, стеганографія, захист інформації, аудіо-сигнали.

Keywords: wideband encoding, phase encoding, digital watermark, robustness to attacks, invisibility, data integrity, steganography, information protection, audio signals.