УДК: 623.618:004.056.2 DOI: **10.33099/2311-7249/2026-55-1-199-205**

МАКСИМОВ Іван Олексійович,
Національний університет оборони України, Київ, Україна
https://orcid.org/0000-0002-1285-2564

УДОСКОНАЛЕНИЙ МЕТОД ОЦІНЮВАННЯ ДОСТОВІРНОСТІ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Метою статті *є удосконалення методу оцінювання достовірності інформації у інформаційно-комунікаційних системах військового призначення завдяки використанню інтегрованого механізму стеганоаналізу, що враховує параметри непомітності та стійкості мультимедійних даних для виявлення прихованого втручання. Удосконалення зводиться до визначення інтегрального показника достовірності інформації з урахуванням доданого коефіцієнта надійності контейнера.*

Методи дослідження. *Для досягнення поставленої мети у роботі застосовано методи системного аналізу, положення теорії інформації та математичне моделювання процесів розбіжності у законах розподілу ймовірностей подій. Такий підхід дав змогу формалізувати процес визначення інтегрального показника достовірності інформації з урахуванням надійності медіаконтейнерів.*

Отримані результати дослідження. *Удосконалено математичний апарат, що ідентифікує деструктивні зміни в мультимедійних потоках, які свідчать про впровадження шкідливого програмного забезпечення. Обґрунтовано базові сценарії адаптивного розподілу вагових коефіцієнтів параметрів достовірності залежно від інтенсивності кібернетичного впливу та умов застосування засобів радіоелектронної боротьби. Аргументовано використання показників надійності контейнера як інструменту превентивного захисту серверного обладнання.*

Наукова новизна *отриманих результатів зводиться до удосконалення методу оцінювання достовірності, який вперше базується на виявленні фактів приховування додаткової інформації у легітимних потоках інформації.*

Теоретичне та практичне значення викладеного у статті. *Обґрунтовано використання показників надійності контейнера як інструменту превентивного захисту серверного обладнання. Запропонований підхід забезпечує ефективне відокремлення навмисного кібернетичного втручання від технічних помилок передавання даних.*

Ключові слова: *достовірність інформації, інформаційно-комунікаційні системи, стеганоаналіз, кібернетичний вплив, мультимедійні дані, шкідливе програмне забезпечення, підтримка прийняття рішень.*

Вступ

Постановка проблеми. Досвід війни за Незалежність України, свідчить про кардинальну зміну природи збройної боротьби: сучасний конфлікт став першим в історії повномасштабним протистоянням, де кібернетичні операції є невід'ємною частиною гібридної стратегії агресора. Інформаційно-комунікаційні системи (далі – ІКС) військового призначення опинилися під постійним тиском цілеспрямованого кібернетичного та інформаційного впливу, метою якого є викрадення даних, дезорганізація управління, виведення з ладу критичного обладнання та масове поширення дезінформації.

Особливу небезпеку становить використання противником технологій цифрової стеганографії для приховування шкідливого програмного забезпечення (далі – ПЗ) або вірусів усередині легітимних медіафайлів (зображень, аудіо- та відеопотоків). Реальні приклади кібератак 2022–2025 років свідчать про наступне [1]:

1. Аналіз кіберінцидентів за період 2022–2025 рр. свідчить про системне використання стеганографічних методів угрупованнями Armageddon та Worok для впровадження шкідливого коду, що дає змогу обходити стандартні засоби антивірусного захисту.

2. Приховані команди управління та віруси-шифрувальники, замасковані під метадані або пікселі зображень, використовуються для несанкціонованого доступу до серверного обладнання ІКС військового призначення, що веде до його блокування або повної втрати працездатності.

3. Противник може маніпулювати змістом повідомлень, впроваджуючи фальшиві дані, які сприймаються системою як достовірні через відсутність інструментів виявлення прихованої інформації.

Аналіз останніх досліджень і публікацій. Сьогодні основна увага дослідників зосереджена на алгоритмах вбудовування даних, тоді як питання оцінювання достовірності інформації за умов приховування додаткової інформації залишаються розробленими фрагментарно.

Фундаментальні підходи до верифікації цифрових об'єктів у технічних системах та методи контролю цілісності інформації розглядаються у [2]. Математичні моделі приховування інформації в

цифрових зображеннях на основі застосування ключів аутентифікації досліджено у [3]. Проблема ідентифікації прихованих аномалій у зображеннях за допомогою методів глибокого навчання піднімається у [4]. Питання загального огляду стеганоаналізу на основі глибокого навчання також детально висвітлено у [5]. Отже, у наведених роботах закладено теоретичні та методичні основи приховування додаткової інформації в цифрові медіаповідомлення та її виявлення. Однак, основна увага дослідників зосереджена на розробленні алгоритмів приховування та методів стеганоаналізу, тоді як питання оцінювання достовірності інформації з урахуванням можливого прихованого втручання залишаються недостатньо дослідженими.

У [6] вказано на різноманітність застосування методів стеганоаналізу згідно їх класифікації та використання медіафайлу, як контейнера з приховуваною додатковою інформацією. Математичний апарат для розв'язання задач стеганоаналізу на основі аналізу ознак низької складності запропоновано у [7]. Новітні виклики та можливості, що виникають при інтеграції штучного інтелекту в стеганографічні системи, розглянуті у [8]. Перспективи використання нового S-контейнеру адверсаріальної стеганографії як нового погляду на приховування інформації досліджено в [9]. Отже, результати цих досліджень спрямовані на вдосконалення математичного апарату стеганоаналізу та використання методів штучного інтелекту для виявлення прихованих змін у цифрових даних. Водночас зазначені підходи орієнтовані переважно на детекцію факту приховування інформації і не інтегруються безпосередньо в системи оцінювання достовірності інформації.

Високонадійні та непомітні схеми відеостеганографії на основі кодів Геммінга розглядаються у [10]. Важливий внесок у висвітлення прогалин в існуючих метриках якості та аналіз останніх досягнень у стеганографії зображень зробили [11]. Проведені дослідження сприяли розвитку ефективних методів відеостеганографії та удосконаленню метрик оцінювання якості прихованої інформації в медіаконтейнерах. Разом із тим, у зазначених роботах основний акцент зроблено на забезпеченні непомітності та стійкості прихованих даних, тоді як їхній вплив на достовірність інформації в ІКС військового призначення не розглядається.

Сучасні дослідження 2024–2025 років окреслюють нові виклики у сфері приховування інформації, пропонуючи актуальні методи захисту інформаційних потоків від новітніх загроз. Гібридні фреймворки для захищеного зв'язку військового призначення, що поєднують шифрування AES та адаптивну аудіостеганографію, запропоновано в [12]. Питання розвитку методів приховування даних у просторовій області та їхній вплив на майбутні системи безпеки аналізується в [13]. У виданні [14] акцентується увага на різноманітних моделях стеганоаналізу та необхідності їх використання для виявлення прихованого повідомлення в цифрових зображеннях. Наведені дослідження демонструють активний розвиток комбінованих підходів до захисту інформації, що поєднують криптографічні та стеганографічні методи. Проте навіть у новітніх роботах питання комплексного оцінювання достовірності інформації з урахуванням специфіки медіаконтейнерів та можливості прихованого впливу на інформаційні потоки залишаються відкритими.

Також огляд методів стеганографії, стеганоаналізу та їхньої наукової строгості у критичних інфраструктурах представлено в [15]. Нарешті, методи приховування великих обсягів даних за допомогою динамічних таблиць відображення, які майже не спотворюють візуальну структуру файлу, досліджено в [16]. Дослідження підтверджують зростання складності загроз, пов'язаних із приховуванням додаткової інформації та використанням штучного інтелекту у стеганографічних системах. Водночас у визначеній літературі відсутні універсальні методи, які давали б змогу поєднати процедури виявлення прихованих даних із оцінюванням достовірності інформації в ІКС військового призначення.

Незважаючи на значну кількість технічних рішень, у сучасних наукових джерелах відсутні методи оцінювання достовірності, які б враховували специфіку медіаконтейнерів передачі та обробки інформації в ІКС військового призначення. Існуючі методи та методики оцінювання достовірності інформації мають суттєвий методологічний недолік – вони фокусуються виключно на змістовних показниках, залишаючи поза увагою факт можливого приховування додаткової інформації. Це створює ситуацію, при якій, система може оцінити відеофайл із розвідувальними даними (зокрема, з БпЛА) як цілком достовірний, оскільки він вчасно отриманий та має високу якість зображення. Однак, якщо в цей потік ворогом вбудовано прихований код, що спотворює реальні координати цілі або впроваджує вірус на пункті управління, класичні підходи не здатні ідентифікувати загрозу.

Удосконалення науково-методичного апарату оцінювання достовірності інформації є важливим науковим завданням, що може бути виконане завдяки інтеграції механізму стеганоаналізу безпосередньо у процес оцінювання достовірності. Такий підхід дає змогу:

1. Ідентифікувати аномалії в структурі повідомлення, що свідчать про наявність стороннього контенту, ще до моменту його розгортання в системі.

2. Використовувати методи приховування для передачі критичної інформації (наприклад, точних координат з БпЛА) всередині відеопотоку. Навіть у разі перехоплення противник не зможе ідентифікувати та вилучити ці дані без знання алгоритму та ключів.

3. Відокремлювати навмисне втручання кіберпідрозділів противника від звичайних технічних помилок передавання даних.

Метою статті є удосконалення методу оцінювання достовірності інформації в інформаційно-комунікаційних системах військового призначення завдяки використанню інтегрованого механізму стеганоаналізу, що враховує параметри непомітності та стійкості мультимедійних даних для виявлення прихованого втручання. Удосконалення зводиться до визначення інтегрального показника достовірності інформації з урахуванням доданого коефіцієнта надійності контейнера.

Виклад основного матеріалу дослідження

Існуючі підходи стосовно оцінювання достовірності інформації в інформаційно-комунікаційній системі військового призначення фокусуються переважно на змісті повідомлень, що може створювати загрозу для такої системи, оскільки не враховується факт приховування додаткової інформації (шкідливе програмне забезпечення, віруси шифрувальники тощо). Система може оцінити файл-контейнер як достовірний, хоча прихована в ньому критично важлива інформація може бути пошкоджена внаслідок навмисного втручання (кібератаки, радіоелектронний вплив тощо). Тому під час оцінювання достовірності інформації в ІКС військового призначення доцільно ввести додатковий демонструє підпроцес оцінювання – аналіз надійності самого процесу доставки прихованої інформації та визначення стану такої інформації. Загальний вираз, що формалізує процес визначення інтегрального показника достовірності інформації в ІКС військового призначення D ґрунтується на зваженій сумі часткових коефіцієнтів:

$$D = \sum_{i=1}^{n} W_i K_i \ , \qquad (\sum W_i = 1) \tag{1}$$

де W_i – ваговий коефіцієнт i-го параметра достовірності ($i = 1, \ldots, N$);

K_i – кількісний коефіцієнт i-го часткового критерію достовірності.

Вираз, що визначає достовірність інформації ІКС військового призначення наведено в [17]:

$$D = W_1 K_{\text{точн}} + W_2 K_{\text{повн}} + W_3 K_{\text{акт}} + W_4 K_{\text{над дж}} + W_5 K_{\text{несуп}} + W_6 K_{\text{доступн}} \tag{2}$$

де $K_{\text{точн}}$ – коефіцієнт точності інформації, що характеризує ступінь відповідності отриманих даних реальному стану об'єктів і процесів;

$K_{\text{повн}}$ – коефіцієнт повноти, який відображає достатність обсягу інформації для прийняття обґрунтованого рішення;

$K_{\text{акт}}$ – коефіцієнт актуальності, що визначає своєчасність надходження даних;

$K_{\text{над дж}}$ – коефіцієнт надійності джерела, який характеризує рівень довіри до джерела інформації;

$K_{\text{несуп}}$ – коефіцієнт несуперечності, що відображає узгодженість інформації з різних каналів і відсутність взаємовиключних відомостей;

$K_{\text{доступн}}$ – коефіцієнт доступності, який визначає можливість своєчасного отримання інформаційного ресурсу в умовах завад і обмежень.

Аналіз виразу (2) свідчить, що він орієнтований виключно на зовнішні характеристики інформаційного повідомлення та його відповідність операційним вимогам. Однак у сучасних умовах мультимедійний файл може бути цілком актуальним і точним за змістом, але водночас виступати прихованим носієм деструктивного коду або каналом несанкціонованої передачі даних. Класичні метрики не враховують структурну цілісність медіаконтейнера на мікрорівні, що дає змогу стеганографічним методам залишатися непоміченими для стандартних засобів контролю.

Це створює критичну вразливість, при якій система оцінює дані як достовірні, ігноруючи факт стороннього втручання в саму структуру носія інформації. Для усунення цього недоліку доцільно удосконалити вираз (2) завдяки введенню коефіцієнта, який здатний кількісно оцінювати безпеку та надійність самого процесу приховування (або його відсутність) у використовуваному контейнері. Тому вираз (2) доцільно записати у такому вигляді:

$$D_{\text{удоскон}} = W_1 K_{\text{точн}} + W_2 K_{\text{повн}} + W_3 K_{\text{акт}} + W_4 K_{\text{над дж}} + W_5 K_{\text{несуп}} + W_6 K_{\text{доступн}} + W_7 K_{\text{над контейн}} \tag{3}$$

де $K_{\text{над контейн}}$ – додатковий коефіцієнт надійності контейнера, що враховує параметри непомітності та стійкості мультимедійних даних.

Важливим аспектом практичного застосування виразу (3) є коректне визначення вагових коефіцієнтів $W_1, \ldots, W_7$, що характеризують пріоритетність відповідного коефіцієнта K_i, зазначеного у виразі (1), залежно від специфіки бойового завдання та поточного стану інформаційного середовища ІКС військового призначення.

У традиційних системах оцінювання основна вага, зазвичай, розподіляється між показниками точності (W_1) та актуальності (W_3). Проте в умовах інтенсивного навмисного впливу та використання ворогом технологій цифрової стеганографії, пропонується перерозподіл вагових значень на користь додаткового коефіцієнта надійності контейнера (W_7).

Коефіцієнт надійності контейнера характеризує якість і надійність процесу передачі прихованої інформації всередині файлу-контейнера. Він визначається як зважена сума коефіцієнтів непомітності ($K_{\text{непом}}$) та стійкості ($K_{\text{стійк}}$):

$$K_{\text{над контейн}} = W_{\text{непом}} K_{\text{непом}} + W_{\text{стійк}} K_{\text{стійк}} \tag{4}$$

Для автоматизованих систем підтримки прийняття рішень пропонується використання таких базових сценаріїв розподілу ваг:

1. Висока інтенсивність кіберпротидії. Пропонується значення W_7 встановлювати на рівні 0,25–0,30. Це обумовлено потребою превентивного захисту серверного обладнання від прихованого шкідливого програмного забезпечення. У цьому випадку система ідентифікує навіть незначні аномалії у структурі мультимедійних даних як критичну загрозу;

2. Робота в умовах РЕБ. Пріоритет зміщується на коефіцієнт доступності (W_6) та надійності джерела (W_4). Вага W_7 має зберігатися на рівні 0,15 для диференціації навмисного втручання від звичайних помилок передавання.

3. Передача наказів командування (верифікація аудіо). У цьому випадку пріоритетна вага надається коефіцієнтам W_7 (через метрику перцептивного оцінювання якості мовлення, Perceptual evaluation of speech quality (далі – PESQ) – та W_5 (несуперечність).

Це дає змогу ефективно виявляти синтезовані за допомогою штучного інтелекту голоси.

Математичне обґрунтування вибору значень вагових коефіцієнтів W_i базується на методі експертного оцінювання або адаптивному алгоритмі, що враховує динаміку зміни оперативної обстановки. Такий підхід трансформує ІКС військового призначення в активний елемент системи кіберзахисту, що може забезпечити часову перевагу в циклі прийняття рішень.

Для *відеоконтейнерів* непомітність приховування додаткової інформації визначається на основі пікового співвідношення сигнал/шум (peak signal-to-noise ratio, PSNR), нормалізованого до діапазону [0; 1]:

$$K_{\text{непом}} = \frac{PSNR_{\text{поточне}} - PSNR_{min}}{PSNR_{max} - PS_{min}} \quad (5)$$

Коефіцієнт стійкості ґрунтується на бітових помилках BER (bit error rate):

$$K_{\text{стійк}} = 1 - BER = 1 - \frac{N}{N_{\text{загальне}}} \quad (6)$$

де N – кількість помилкових бітів зображення в контейнері;

$N_{\text{загальне}}$ – загальна кількість бітів в контейнері;

Для *аудіоконтейнерів* непомітність оцінюється через співвідношення сигнал/шум SNR (signal-to-noise ratio):

$$K_{\text{непом}} = \frac{SNR_{\text{поточне}} - SNR_{min}}{SNR_{max} - SNR_{min}} \quad (7)$$

Коефіцієнт стійкості визначається за метрикою перцептивного оцінювання якості мовлення PESQ (perceptual evaluation of speech quality):

$$K_{\text{стійк}} = \frac{PESQ_{score} - 1}{3{,}5} \quad (8)$$

Слід зазначити, що за ідеальної якості звука ($PESQ$ = 4,5) – $K_{\text{стійк}}$ = 1, при жахливій ($PESQ$ = 1) – $K_{\text{стійк}}$ = 0 [18].

Для забезпечення математичної однорідності моделі (3), усі вхідні параметри підлягають процедурі лінійної або нелінійної нормалізації. Це дає змогу порівнювати фізично різнорідні величини стосовно пікового співвідношення сигнал/шум PSNR та відсоткові частки для бітових помилок BER.

Показник пікового співвідношення сигналу до шуму (PSNR) є основним для оцінювання прозорості вбудовування прихованої інформації. Для ІКС військового призначення встановлюються такі граничні значення [8]:

1. $PSNR_{max} = 50$дБ (відсутність візуальних та статистичних викривлень);

2. $PSNR_{min} = 30$дБ (поріг, нижче якого контейнер вважається деградованим або скомпрометованим).

Визначення PSNR здійснюється за виразом (5), де поточне значення $PSNR_{\text{поточне}}$ інтерполюється між вказаними межами. Якщо $PSNR < 30$дБ, коефіцієнт $K_{\text{непом}}$ автоматично набуває значення 0, що сигналізує про високу ймовірність деструктивного втручання або використання низькоякісних алгоритмів стеганографії противником.

Метрика перцептивного оцінювання якості мовлення (PESQ) згідно з рекомендацією ITU-T P.863 варіюється від –0,5 до 4,5. Проте для оцінювання достовірності використовується стандартизований діапазон мовного сигналу: [18]

1. PESQ = 4,5 – ідеальна якість, автентичний сигнал ($K_{\text{стійк}}$ = 1);

2. PESQ ≤ 1,5 – критичні спотворення, характерні для агресивного синтезу мовлення або deepfake-технологій (технологія глибинної фальсифікації аудіо- або відеоматеріалів за допомогою алгоритмів глибинного навчання) ($K_{\text{стійк}}$ = 0).

Використання нормалізації за виразом (8) дає змогу системі підтримки прийняття рішень автоматично класифікувати аудіопотік як «критичний» ($D < 0{,}5$), у разі виявлення ознак цифрової ресинтезації голосу.

Коефіцієнт бітових помилок (BER) нормалізується інверсивно за виразом (6). У каналах зв'язку ІКС військового призначення за умов PLR = 1,0% (packet loss rate – втрата пакетів) випадкові втрати від цілеспрямованого спотворення структури повідомлення визначаються через аналіз динаміки зміни BER у часі.

Вибір показників PSNR та PESQ обумовлений їх широким застосуванням у задачах оцінювання якості мультимедійних сигналів та наявністю усталених порогових значень, що дає змогу виконувати нормалізацію результатів у діапазоні [0; 1]. Метрика PSNR є чутливою до мікроспотворень на рівні пікселів і широко використовується для виявлення змін структури відеоконтейнерів, зокрема, стеганографічного вбудовування, а PESQ, у свою чергу, забезпечує перцептивне оцінювання якості мовлення та дає змогу виявляти цифрові зміни структури сигналу, характерні для синтезованого або модифікованого аудіоповідомлення. Сукупне використання зазначених метрик забезпечує комплексне оцінювання непомітності та стійкості контейнера в умовах цілеспрямованого кібернетичного впливу.

Особливістю запропонованого методу є його спрямованість на виявлення специфічних аномалій, характерних для сучасних кіберзагроз. Зокрема, для відеопотоків, що циркулюють в ІКС військового призначення, використання інтегрального показника на основі пікового співвідношення сигналу до шуму дає змогу ідентифікувати мікро-спотворення на рівні окремих пікселів або метаданих контейнера. Такі аномалії часто є дескрипторами присутності вірусів-шифрувальників або модулів віддаленого доступу, що використовувалися кіберпідрозділами противника для впровадження шкідливого коду в графічні та відеофайли. Навіть за умови візуальної цілісності відео, відхилення $K_{\text{непом}}$ від еталонних значень сигналізує про деструктивне втручання ще до моменту виконання коду на серверному обладнанні.

У сегменті голосового радіообміну та передачі аудіоданих, застосування метрики перцептивного оцінювання якості мовлення виконує роль інструменту верифікації автентичності джерела. В умовах застосування противником технологій штучного інтелекту для створення синтезованих голосів, які імітують накази командування, класичні методи перевірки цілісності виявляються безсилими. Удосконалений метод дає змогу ідентифікувати цифрові складові синтезу мовлення, що характеризується зниженням коефіцієнта стійкості контейнера $K_{\text{стійк}}$. Це дає змогу технічній системі

класифікувати такий аудіопотік як «критичний» ($D < 0,5$) і блокувати дезінформацію в реальному часі.

Інтеграція стеганоаналізу в метод оцінювання достовірності трансформує ІКС в механізм адаптивного захисту інформаційного середовища. Запропонований математичний апарат забезпечує диференціацію між природними завадами в бойових умовах та цілеспрямованою маніпуляцією структурою даних, що є вирішальним для збереження стійкості управління в умовах високої інтенсивності бойових дій.

На відміну від традиційних методів, що обмежуються аналізом лише змістовних параметрів (точність, повнота тощо), удосконалений метод передбачає паралельне виконання процедури стеганоаналізу та містить такі етапи:

1. Ідентифікація типу медіаданих для вибору відповідних метрик аналізу.

2. Визначення показників непомітності (*PSNR/SNR*) та стійкості (*BER/PESQ*), що дає змогу виявити аномалії, характерні для впровадження шкідливого ПЗ.

3. Визначення остаточного значення рівня достовірності інформації на основі введеного коефіцієнта надійності контейнера.

4. Автоматичне внесення інформації до одного з чотирьох рівнів довіри, що дає змогу скоротити час у циклі прийняття рішення.

Для прийняття обґрунтованих управлінських рішень розраховане значення $D_{\text{удоскон}}$ (3) зіставляється зі шкалою якісних оцінок у (табл.1):

Таблиця 1

Рівні достовірності та рекомендації до дії

Рівень достовірності	Кількісний критерій	Рекомендації до дії
Високий (Confirmed)	$D > 0,9$	Інформація підтверджена, надійна. Рекомендовано до використання для прийняття критично важливих рішень без додаткових перевірок.
Достатній (Probable)	$D \in [0,7; 0,9]$	Інформація ймовірно достовірна. Може використовуватись, але варто враховувати ризики, пов'язані з компонентами, що мають низьку оцінку.
Задовільний (Possible)	$D \in [0,5; 0,7]$	Інформація сумнівна, потребує перевірки. Використовувати тільки за відсутності альтернатив та з обов'язковим підтвердженням.
Критичний (Unreliable)	$D < 0,5$	Інформація недостовірна. Використання заборонено, оскільки може призвести до тяжких наслідків.

Визначення коефіцієнта надійності контейнера $K_{\text{над контейн}}$ є важливою особливістю удосконаленого методу, що використовує інтегрований механізм стеганоаналізу. Такий підхід дає змогу:

1. Ідентифікувати аномалії в інформаційних структурах, що свідчать про наявність прихованого шкідливого програмного забезпечення або несанкціонованих каналів витоку даних.

2. Успішно аналізувати розбіжності у законах розподілу ймовірностей подій для чіткого відокремлення навмисного втручання ворога від звичайних технічних помилок передавання даних.

3. Реалізувати превентивний захист серверного обладнання ІКС від деструктивного впливу.

Впровадження удосконаленого методу дасть змогу інтегрувати механізми стеганоаналізу безпосередньо в процес оцінювання достовірності для ідентифікації аномалії в інформаційних структурах мультимедійних потоків, що може свідчити про використання ворогом шкідливого програмного забезпечення. Це забезпечить превентивний захист серверного обладнання ІКС та мінімізує ризики використання противником дезінформації для викривлення оперативної обстановки.

Висновки

У статті виконано поставлене наукове завдання щодо удосконалення методу оцінювання достовірності інформації в інформаційно-комунікаційних системах військового призначення та обґрунтовано використання показника, що враховує параметри непомітності та стійкості інформації для виявлення прихованого втручання, оскільки наявність такого втручання може свідчити про впровадження шкідливого програмного забезпечення або вірусів-шифрувальників у мультимедійних контейнерах.

Наукову новизну дослідження формалізовано через удосконалення математичного апарату (вирази 1–8), що дає змогу перейти від якісного до кількісного оцінювання рівня достовірності інформації. Математично обґрунтовано визначення показників надійності для відео- та аудіоконтейнерів, що забезпечують ідентифікацію прихованого деструктивного втручання на рівні структури даних. Результати розрахунків інтегрального показника узагальнено у формі чотирирівневої шкали (табл. 1), яка верифікує ступінь достовірності отриманих даних та надає автоматизовані рекомендації щодо подальшого прийняття критично важливих рішень.

Застосування обраних метрик сформувало превентивний механізм захисту серверного обладнання інформаційно-комунікаційних систем військового призначення шляхом виявлення стеганографічних аномалій у мультимедійних потоках.

Диференціація загроз може забезпечити автоматичну класифікацію інформаційних потоків за рівнем ризику в системах підтримки прийняття рішень. Ймовірність прийняття хибних рішень на основі скомпрометованих розвідувальних даних може бути мінімізована завдяки аналізу статистичних розбіжностей у медіаконтейнерах.

Перспективами подальших досліджень слід вважати розроблення методики (алгоритму)

динамічної адаптації вагових коефіцієнтів для автоматизованих систем підтримки прийняття рішень залежно від зміни інтенсивності радіоелектронної та кібернетичної протидії противника.

Конфлікт інтересів. Конфлікти інтересів, що впливають на результати дослідження відсутні.

Фінансування. Фінансування дослідження не здійснювалося.

Доступність даних. Дослідження виконано з використанням виключно відкритих даних, доступних у публічних джерелах.

Використання засобів штучного інтелекту (ШІ). У процесі підготовки статті автором було використано ШІ, як допоміжний засіб, з метою покращення лінгвістичної якості тексту, пошуку джерел за тематикою дослідження та лінгвістичної корекції англомовного резюме. Автор підтверджує повну перевірку інформації запропонованої ШІ, яка не вплинула на наукову новизну, достовірність та цілісність результатів дослідження.

Список бібліографічних посилань

1. Netlok. The rise of steganography bots and AI: strategic analysis for 2025. URL: https://netlok.com/the-rise-of-steganography-bots-and-ai-strategic-analysis-for-2025 (Accessed: 8 February 2026). **2. Хорошко В. О., Азаров О. С., Шєлєст М. Є., Яремчук Ю. Є.** Основи комп'ютерної стеганографії. Вінниця : Вид-во ВДТУ, 2003. 143 с. URL: http://ir.lib.vntu.edu.ua/handle/123456789/12616 (дата звернення: 20 січня 2026). **3. Zhyvylo Y., Kuchma Y.** Mathematical modeling of intellectual and cryptographic protection of authentication keys. *Information Technology and Security*. 2025. Vol. 13. № 2. P. 162–177. DOI: https://doi.org/10.20535/2411-1031.2025.13.2.344591. **4. Sam A. R., Selvaraj A., Ezhilarasan A., Wellington S. L. J.** Digital image steganalysis: a survey on paradigm shift from machine learning to deep learning based techniques. *IET Image Processing*. 2021. Vol. 15. № 2. P. 504–522. DOI: https://doi.org/10.1049/ipr2.12043. **5. Chen C., Zhang Y., Xiao B., Cheng M., Zhang J., Li H.** Deep learning-based image steganography for visual data cybersecurity in construction management. *Journal of Construction Engineering and Management*. 2024. Vol. 150. № 10. P. 118–132. DOI: https://doi.org/10.1061/JCEMD4.COENG-14718. **6. Nissar A., Mir A. H.** Classification of steganalysis techniques: a study. *Digital Signal Processing*. 2010. P. 1758–1770. DOI: https://doi.org/10.1016/j.dsp.2010.02.003. **7. Holub V., Fridrich J.** Low-complexity features for JPEG steganalysis using undecimated DCT. *IEEE Transactions on Information Forensics and Security*. 2015. Vol. 12. № 1. P. 135–146. DOI: https://doi.org/10.1109/TIFS.2014.2364918. **8. Kumar A., Kumar S., Kumar C., Solak S.** Exploring AI in steganography and steganalysis: trends, clusters, and sustainable development potential. *Cryptography and Security.* 2025. DOI: https://doi.org/10.48550/arXiv.2511.12052. **9. Li L., Liu J., Guo Y., Liu B.** A new S-box construction method meeting strict avalanche criterion. *Journal of Information Security and Applications*. 2022. Vol. 66. DOI: https://doi.org/10.1016/j.jisa.2022.103135. **10. Wang Zh., Wang Y., Tang M.** High-capacity adaptive steganography based on LSB and Hamming code. *Optik*. 2020. Vol. 213. № 1. DOI: https://doi.org/10.1016/j.ijleo.2020.164685. **11. Subramanian N., Elharrouss O., Bouridane A., Al-ma'adeed S.** Image steganography: a review of recent advances. *IEEE Access*. 2021. Vol. 9. P. 23409–23423. DOI: https://doi.org/10.1109/ACCESS.2021.3053998. **12. Musa A. I., Ngene C. U., Bali B.** Hybrid advanced encryption standard-counter mode and adaptive least significant bit audio steganography framework for secure military communication. *Journal of Scientific Development Research*. 2025. Vol. 10, № 9. DOI: https://doi.org/10.70382/hujsdr.v10i9.014. **13. Ye J.** Advancements in spatial domain image steganography: techniques, applications, and future outlook. *Applied and Computational Engineering.* 2024. Vol. 94. № 1. P. 6–29. DOI: https://doi.org/10.54254/2755-2721/94/2024MELB0058. **14. Fridrich J., Kodovsky J.** Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*. 2012. Vol. 7. № 3. P. 868–882. DOI: https://doi.org/10.1109/TIFS.2012.2190402. **15. Li Q., Luo W., Wei K., Ye M.** A comprehensive survey of digital image steganography and steganalysis. *APSIPA Transactions on Signal and Information Processing*. 2024. Vol. 13. № 1. P. 1-67. DOI: https://doi.org/10.1561/116.20240038. **16. Fatima K., Wu N., Chan C., Hwang M.** A high-payload data hiding method utilizing an optimized voting strategy and dynamic mapping table. *Electronics*. 2025. Vol. 14. № 17. DOI: https://doi.org/10.3390/electronics14173498. **17. Бржевська З. М., Киричок Р. В., Платоненко А. В., Гулак Г. М.** Оцінка передумов формування методики оцінки достовірності інформації. *Кібербезпека: освіта, наука, техніка.* 2022. Т. 3, № 15. С. 164–174. DOI: https://doi.org/10.28925/2663-4023.2022.15.164174. **18. ITU-T Recommendation P.863.** Perceptual objective listening quality prediction. International Telecommunication Union. 2018. URL: https://www.itu.int/rec/T-REC-P.863. (Accessed: 16 February 2026).

IMPROVED METHOD FOR ASSESSING INFORMATION RELIABILITY IN MILITARY INFORMATION AND COMMUNICATION SYSTEMS

MAKSYMOV Ivan, National Defence University of Ukraine, https://orcid.org/0000-0002-1285-2564

Formulation of the problem in general. *The experience of Ukraine's war for Independence demonstrates a shift in the nature of armed conflict, where cyber operations are an integral part of the aggressor's hybrid strategy. Military information and communication systems face constant pressure from targeted cyber-attacks aimed at data theft, command disruption, and the spread of disinformation. A particular threat is the use of digital steganography to hide malware or viruses within legitimate multimedia files (images, audio, and video streams).* ***Purpose of the article.*** *The objective is to improve the method for assessing information reliability in military information and communication systems by implementing an integrated steganalysis mechanism that utilises a container reliability coefficient.*

Research methods. *To achieve this goal, the study employs systems analysis, information theory, and mathematical modelling of discrepancies in the probability distributions of events.*

Literature review. *Existing research focuses on embedding algorithms or general steganalysis, but the impact of hidden interference on information reliability remains insufficiently explored. While scholars like Khoroshko and Azarov laid the foundations for digital verification, and Fridrich analysed the complexity of steganalysis, there is a lack of universal methods that combine hidden data detection with reliability assessment for military information and communication systems.*

Research results. *A mathematical apparatus has been developed to identify destructive changes in multimedia streams, thereby indicating the presence of malware. The reliability assessment model was improved by introducing an integral indicator that incorporates the container reliability coefficient based on peak signal-to-noise ratio, bit error rate, and perceptual evaluation of speech quality metrics. Furthermore, basic scenarios for adaptive weighting of reliability parameters were established, allowing for prioritised protection during intense cyber-attacks or electronic warfare. A four-level qualitative scale (Confirmed, Probable, Possible, Unreliable) was formulated to automate data classification in decision support systems.*

Research novelty. *The scientific novelty lies in improving the reliability assessment method, which, for the first time, is based on detecting hidden information within legitimate data streams rather than analysing content.*

The theoretical and practical significance. *The use of container reliability indicators as a tool for the preventive protection of server equipment has been theoretically substantiated. The proposed approach effectively separates intentional cyber interference from common technical data transmission errors. The practical application of the method reduces the time required to assess the operational situation, providing a temporal advantage in the decision-making cycle and minimising the risk of disinformation distorting the operational environment.*

Conclusions and future work. *The study provides a scientific and methodological framework for enhancing information reliability assessment through the integration of steganalysis. Future research will focus on developing algorithms for dynamically adapting weighting coefficients in response to changing intensities of electronic and cyber warfare.*

Keywords: *information reliability, information and communication systems, steganalysis, cybernetic influence, multimedia data, malicious software, decision support.*

References

1. Netlok, (2025). The rise of steganography bots and AI: strategic analysis for 2025. *Cyber Defence Insights*. Available at: https://netlok.com/the-rise-of-steganography-bots-and-ai-strategic-analysis-for-2025 [Accessed: 16 February 2026]. **2. Khoroshko, V. O., Azarov, O. S., Shelest, M. Ye., Yaremchuk, Yu. Ye.,** (2003). *Osnovy komp'iuternoi stehanohrafii*. Vinnytsia: VDTU. Available at: http://ir.lib.vntu.edu.ua/handle/123456789/12616 [Accessed: 20 January 2026]. **3. Zhyvylo, Y., Kuchma, Y.,** (2025). Mathematical modeling of intellectual and cryptographic protection of authentication keys. *Information Technology and Security*. 13(2), 162–177. DOI: https://doi.org/10.20535/2411-1031.2025.13.2.344591. **4. Sam, A. R., Selvaraj, A., Ezhilarasan, A., Wellington, S. L. J.,** (2021). Digital image steganalysis: a survey on paradigm shift from machine learning to deep learning based techniques. *IET Image Processing*. 15(2), 504–522. DOI: https://doi.org/10.1049/ipr2.12043. **5. Chen, C., Zhang, Y., Xiao, B., Cheng, M., Zhang, J., Li, H.,** (2024). Deep learning-based image steganography for visual data cybersecurity in construction management. *Journal of Construction Engineering and Management*. 150(10), 118–132. DOI: https://doi.org/10.1061/JCEMD4.COENG-14718. **6. Nissar, A., Mir, A. H.** (2010). Classification of steganalysis techniques: a study. *Digital Signal Processing*. 1758–1770. DOI: https://doi.org/10.1016/j.dsp.2010.02.003. **7. Holub, V., Fridrich, J.,** (2017). Low-complexity features for JPEG steganalysis using undecimated DCT. *IEEE Transactions on Information Forensics and Security*. 12(1), 135–146. DOI: https://doi.org/10.1109/TIFS.2014.2364918. **8. Kumar, A., Kumar, S., Kumar, C., Solak, S.,** (2025). Exploring AI in steganography and steganalysis: trends, clusters, and sustainable development potential. *Cryptography and Security*. DOI: https://doi.org/10.48550/arXiv.2511.12052. **9. Li, L., Liu, J., Guo, Y., Liu, B.,** (2022). A new S-box construction method meeting strict avalanche criterion. *Journal of Information Security and Applications*. 66(1). DOI: https://doi.org/10.1016/j.jisa.2022.103135. **10. Wang, Zh., Wang, Y., Tang, M.,** (2020). High-capacity adaptive steganography based on LSB and Hamming code. *Optik*. 213(1). DOI: https://doi.org/10.1016/j.ijleo.2020.164685. **11. Subramanian, N., Elharrouss, O., Bouridane, A., Al-ma'adeed, S.,** (2021). Image steganography: a review of recent advances. *IEEE Access*. 9, 23409–23423. DOI: https://doi.org/10.1109/ACCESS.2021.3053998. **12. Musa, A. I., Ngene, C. U., Bali, B.,** (2025). Hybrid advanced encryption standard-counter mode and adaptive least significant bit audio steganography framework for secure military communication. *Journal of Scientific Development Research*. 10(9). DOI: https://doi.org/10.70382/hujsdr.v10i9.014. **13. Ye, J.,** (2024). Advancements in spatial domain image steganography: techniques, applications, and future outlook. *Applied and Computational Engineering*. 94(1), 6–29. DOI: https://doi.org/10.54254/2755-2721/94/2024MELB0058. **14. Fridrich, J., Kodovsky, J.,** (2012). Rich models for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*. 7(3), 868–882. DOI: https://doi.org/10.1109/TIFS.2012.2190402. **15. Li, Q., Luo, W., Wei, K., Ye, M.,** (2024). A comprehensive survey of digital image steganography and steganalysis. *APSIPA Transactions on Signal and Information Processing*. 13(1), 1–67. DOI: https://doi.org/10.1561/116.20240038. **16. Fatima, K., Wu, N., Chan, C., Hwang, M.,** (2025). A high-payload data hiding method utilizing an optimized voting strategy and dynamic mapping table. *Electronics*. 14(17). DOI: https://doi.org/10.3390/electronics14173498. **17. Brzhevska, Z., Kyrychok, R., Platonenko, A., Hulak, H.** (2022). Assessment of the preconditions of formation of the methodology of assessment of information reliability. *Cybersecurity: education, science, technique.* 3(15), 164–174. DOI: https://doi.org/10.28925/2663-4023.2022.15.164174. **18. International Telecommunication Union (ITU).** (2018). *ITU-T Recommendation P.863: Perceptual objective listening quality prediction*. Available at: https://www.itu.int/rec/T-REC-P.863 [Accessed: 16 February 2026]

Рукопис надійшов до редакції *16.03.2026*
Рукопис прийнято до друку після рецензування *08.04.2026*
Дата публікації *30.04.2026*