DOI: 10.58254/viti.8.2025.10.124

УДК 621.39(06):004.056.55:623(06)

Максимов І. О. ORCID: 0000-0002-1285-2564 (НУОУ)
Загоровець О. В ORCID: 0009-0008-2566-9217 (ВІТІ ім. Героїв Крут)

АНАЛІЗ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ

Інформаційно-комунікаційні системи військового призначення відіграють ключову роль у забезпеченні планування, координації та оперативного управління підрозділами Збройних Сил України в умовах ведення бойових дій. Одним з найважливіших завдань у таких системах є забезпечення достовірності та стійкості до перехоплення критично важливої інформації. Це зумовлює актуальність дослідження приховування інформації, зокрема стеганографічних, криптографічних та комбінованих методів забезпечення достовірності інформації.

У контексті зростаючих загроз, з боку засобів радіоелектронної боротьби та кібератак противника, виникає необхідність оцінки ефективності та практичного застосування кожного з методів. Проблематика дослідження полягає в тому, що окреме використання стеганографічного або криптографічного методів має низку обмежень, які можуть бути подолані шляхом їх інтеграції у вигляді комбінування.

Метою статті є систематизація та порівняльний аналіз сучасних методів приховування інформації в інформаційно-комунікаційних системах військового призначення, а також обґрунтування доцільності застосування комбінованого методу як найбільш ефективного для захисту обміну та змісту інформаційних повідомлень в умовах сучасного інформаційного протиборства.

У ході дослідження застосовано методи порівняльного аналізу, критичного огляду літературних джерел та системного узагальнення. У статті проаналізовано основні види стеганографічних і криптографічних методів, охарактеризовано їхні ключові переваги та недоліки, представлено структурну схему комбінованого методу та проведено оцінку ефективності за основними критеріями: стійкість до виявлення, ресурсоємність, швидкість передачі, можливість застосування в бойових умовах.

Результати дослідження свідчать про те, що комбіновані методи забезпечують багаторівневий захист даних, що суттєво ускладнює перехоплення, аналіз або модифікацію інформаційного потоку. Вони дозволяють знизити ризики виявлення самої передачі повідомлення та забезпечити захист його змісту навіть у разі компрометації каналу зв'язку. Обґрунтовано доцільність широкого впровадження комбінованих методів приховування інформації в інформаційно-комунікаційні системи військового призначення з урахуванням рівня управління, умов бойової обстановки та потенційних загроз.

Перспективним напрямом подальших досліджень є розроблення методики оцінювання достовірності інформації в ІКС ВП на основі визначення показників із врахуванням сучасних методів приховування інформації в інформаційно-комунікаційних системах військового призначення

Ключові слова: *інформаційно-комунікаційна система, приховування інформації, стеганографія, криптографія, комбіновані методи, конфіденційність, достовірність.*

I. Maksymov, O. Zahorovets. Methods of information hiding in military communication and information systems: analysis and prospects

Military information and communication systems play a key role in ensuring the planning, coordination, and operational command of the Armed Forces of Ukraine units in combat conditions. One of the most critical tasks in such systems is to ensure the authenticity and resistance to interception of mission-critical information. This underscores the relevance of researching information hiding, particularly steganographic, cryptographic, and combined methods for ensuring information integrity.

In the context of growing threats from enemy electronic warfare and cyberattacks, the need arises to evaluate the effectiveness and practical application of each method. The research problem lies in the fact that the separate use of steganographic or cryptographic methods has a number of limitations that can be overcome through their integration in a combined approach.

The purpose of the article is to systematize and comparatively analyze modern methods of information hiding in military information and communication systems, as well as to substantiate the expediency of using a combined method as the most effective for protecting the exchange and content of information messages in the conditions of modern information warfare.

The study employed methods of comparative analysis, critical literature review, and systemic generalization. The article analyzes the main types of steganographic and cryptographic methods, characterizes their key advantages and disadvantages, presents a block diagram of the combined method, and evaluates its effectiveness based on key criteria: resistance to detection, resource intensity, transmission speed, and applicability in combat conditions.

The research results indicate that combined methods provide multi-layered data protection, which significantly complicates the interception, analysis, or modification of the information flow. They allow for reducing the risks of detecting the message transmission itself and ensure the protection of its content even if the communication channel is compromised. The feasibility of widespread implementation of combined information hiding methods in military information and communication systems is substantiated, taking into account the command level, combat environment conditions, and potential threats.

A promising area for further research is the development of a methodology for assessing information integrity in military information and communication systems, based on defining indicators that consider modern methods of information hiding.

Keywords: *information and communication system, information hiding, steganography, cryptography, combined methods, confidentiality, authenticity.*

Постановка проблеми. Аналіз досвіду застосування інформаційно-комунікаційних систем військового призначення (ІКС ВП) в умовах бойових дій на території України свідчить про критичне значення захищеного обміну інформацією для успішного виконання бойових завдань. Особливої актуальності набуває використання комплексних методів приховування інформації, що включають як криптографічне шифрування даних, так і стеганографічне приховування самого факту передачі повідомлень.

Широкомасштабне вторгнення продемонструвало системне застосування противником комплексних методів радіоелектронної боротьби, кібератак та засобів радіоелектронної розвідки, що призводить до дезорганізації системи управління військами та порушення ієрархічної структури проходження критично важливої інформації. Встановлено, що російські підрозділи радіоелектронної боротьби (РЕБ) цілеспрямовано блокують канали обміну даними між штабами та підрозділами, створюють завади для супутникової навігації, а також здійснюють масоване придушення радіозв’язку на тактичному та оперативному рівнях. Одночасно з цим зафіксовано численні випадки використання російськими кіберпідрозділами стеганографічних методів для прихованої передачі шкідливого коду та команд управління зловмисним програмним забезпеченням (ПЗ) [1].

Варто зазначити, що російська федерація активно застосовувала методи захисту та приховування інформації ще до початку широкомасштабного вторгнення. Яскравим прикладом стала кібератака "NotPetya" у 2017 році, коли технології стеганографії використовувались для інтеграції шкідливого коду в оновлення бухгалтерського програмного забезпечення, а криптографічні механізми забезпечували захист каналів управління шкідливим ПЗ. Після повномасштабного вторгнення було зафіксовано нові випадки застосування комплексних підходів приховування інформації, зокрема: впровадження шкідливого програмного забезпечення "Armageddon" через вбудований у зображення код, який активувався при перегляді контенту на інформаційних ресурсах; використання стеганографії в поєднанні з асиметричним шифруванням у модифікованих документах MS Office, які розповсюджувалися через фішингові атаки на урядові установи; приховування шифрованих команд управління для ботнет-мереж у метаданих зображень, розміщених на публічних ресурсах, що дозволяло обходити системи виявлення мережевої активності.

У 2022 році було задокументовано діяльність хакерської групи Worok, яка використовувала стеганографію для приховування шкідливого коду в графічних файлах формату PNG. Такий код активувався після обробки зображення зараженою системою та дозволяв отримувати контроль над пристроєм жертви без виявлення з боку традиційних засобів кіберзахисту [2].

Підрозділи Збройних Сил України активно впроваджують багаторівневі методи захисту та приховування інформації для підвищення безпеки власних комунікацій. Практичне застосування включає інтеграцію шифрованих повідомлень у голосові пакети протоколів реального часу (Real-time Transport Protocol, RTP), використання цифрових водяних знаків у медіафайлах із додатковим криптографічним захистом та спеціалізовані застосунки для прихованої передачі координат, інформації розвідки та оперативних даних. Комплексні

програмні рішення на основі OpenStego, DeepSound та rSteg у поєднанні з сучасними криптографічними протоколами стали важливими інструментами у забезпеченні достовірності та цілісності військових комунікацій.

Противник активно використовує технології Deep Packet Inspection (DPI) для виявлення фактів прихованої передачі даних навіть у зашифрованому трафіку, а також засоби криптоаналізу для спроб дешифрування перехоплених повідомлень. Сучасні методи стегоаналізу дозволяють виявляти статистичні аномалії, що виникають при вбудовуванні додаткової інформації в цифрові контейнери. Зафіксовано випадки цілеспрямованого глушіння каналів зв’язку та модифікації інформаційних потоків з метою пошкодження прихованих повідомлень і криптографічних ключів.

Аналіз останніх досліджень і публікацій. Аналіз наукових праць у сфері захисту інформації свідчить, що значна увага дослідників приділяється фундаментальному вивченню окремих методів приховування. Зокрема, праці українських вчених [3–5] містять ґрунтовний розгляд теоретичних і практичних основ стеганографії. Водночас криптографічні підходи, їхні математичні принципи та застосування детально висвітлено у роботі [6]. Ці публікації створюють міцний теоретичний базис, проте розглядають криптографію та стеганографію переважно як самостійні дисципліни.

Світова наукова спільнота активно розвиває інноваційні та вузькоспеціалізовані рішення спрямовані на створення доказово безпечних алгоритмів [7], підвищення пропускної спроможності каналів прихованої передачі [8] та розробку нових підходів безконтейнерної стеганографії [9]. Попри високу наукову цінність, ці роботи є розрізненими і не пропонують комплексного аналізу, який би дозволив адаптувати та систематизувати сучасні досягнення для потреб військових систем зв’язку.

У роботах [10] та [11] розглядаються комбіновані крипто-стеганографічні підходи, проте проведений аналіз має переважно фрагментарний характер та обмежується прикладами застосування без розробки системної методології для порівняльної оцінки їх ефективності. Питання комплексного застосування цих методів, особливо в контексті специфічних вимог до ІКС ВП, висвітлено недостатньо, що унеможливлює обґрунтований вибір оптимального методу для конкретних бойових завдань та умов функціонування.

Таким чином, існує потреба у проведенні системного аналізу методів приховування інформації, який би враховував їхні переваги й недоліки саме в контексті військового застосування.

Метою роботи є проведення порівняльного аналізу методів приховування інформації в інформаційно-комунікаційних системах військового призначення, визначення їх основних переваг та недоліків для удосконалення захисту військових комунікацій в умовах інформаційного протиборства.

Виклад основного матеріалу дослідження. Одним із найбільш поширених і перспективних методів до приховування інформації є стеганографія. Він базується на прихованні повідомлень у цифрових носіях, таких як зображення, аудіо- чи відеофайли, наявність котрих залишається непомітною для сторонніх осіб.

Актуальність використання стеганографічних методів значно зросла у зв’язку із збільшенням загроз в умовах сучасної інформаційної боротьби під час планування та виконання завдань підрозділами Збройних Сил України. Основні принципи цих методів охоплюють комплексний підхід для впровадження, збереження та захисту прихованих даних, забезпечуючи прозорість та безпеку обміну інформацією.

В основі стеганографії лежить принцип приховування самого факту існування таємного повідомлення шляхом його інтеграції у звичайні, на перший погляд, файли. Такі файли-носії називаються контейнерами, якими можуть виступати цифрові зображення, аудіо- та відеозаписи або навіть текстові документи.

Ключовою вимогою, що визначає ефективність будь-якого стеганографічного методу, є непомітність (прозорість) втручання. Для досягнення непомітності використовують надлишковість даних у цифрових контейнерах. При цьому внесені зміни не повинні візуально погіршувати якість зображення, спотворювати звучання аудіофайлу чи бути помітними для читача тексту (контейнер має залишатися функціонально та візуально ідентичним до оригіналу) [5].

Вибір конкретного методу приховування залежить від балансу між обсягом даних, необхідним рівнем стійкості до виявлення та типом контейнера. Залежно від способу роботи з контейнером, методи поділяють на просторові, частотні та адаптивні.

Розглянемо основні типи стеганографічних методів, які використовуються для приховування інформації.

1. Стеганографія у зображеннях:

1) метод Least Significant Bit (LSB) – здійснює заміну найменш значущих біт у зображенні на біти прихованої інформації [9] згідно з виразом (1):

$$C` = (C \wedge \neg 1) \vee m, \tag{1}$$

де C – вихідне значення байта контейнера;

$C`$ – нове значення байта контейнера після вбудовування;

m – один біт секретного повідомлення;

$\wedge$ – побітова операція ‘‘І’’;

$\vee$ – побітова операція ‘‘АБО’’;

$\neg$ – побітова операція ‘‘НЕ’’;

2) метод Spread Spectrum (SS) – приховує дані шляхом розподілу їх серед великої кількості пікселів за випадковим алгоритмом [9], створюючи результуючий сигнал $T(t)$, що передається в канал зв’язку та наведено у виразі (2):

$$T(t) = S(t) \cdot C(t), \tag{2}$$

де $S(t)$ – вихідний інформаційний сигнал;

$C(t)$ – псевдовипадкова кодова послідовність, швидкість значно вища за швидкість S(t);

3) метод Discrete Cosine Transform (DCT) – вбудовує приховані дані у частотні компоненти зображення (зокрема у JPEG-файлах), змінюючи амплітуду низькочастотних коефіцієнтів для стійкості до стиснення [12] згідно з формулою (3):

$$X[k] = \alpha(k) \sum_{n=0}^{N-1} x[n] \cos\left(\frac{\pi(2n+1)k}{2N}\right), \tag{3}$$

де $x[n]$ – вхідна послідовність даних, де n ==0, 1, …, $N-1$;

N – кількість елементів у послідовності;

$\alpha(k)$ – коефіцієнт нормалізації представлений виразом (4):

$$\alpha(k) = \begin{cases} \sqrt{\frac{1}{N}} & \text{якщо } k = 0 \\ \sqrt{\frac{2}{N}} & \text{якщо } k > 0 \end{cases}. \tag{4}$$

2. Стеганографія в аудіо:

1) метод ехо-модуляції (ЕМ) – приховує дані шляхом додавання слабкого відлуння до аудіосигналу, змінюючи затримку та амплітуду для мінімального впливу на сприйняття звуку [13]. Модифікований сигнал (із вбудованим ехом) у момент часу t представлено у виразі (5):

$$s'(t) = s(t) + \alpha \cdot s(t - d), \tag{5}$$

де $s(t) -$ вихідний аудіосигнал у момент часу t;

$\alpha -$ амплітуда еха, де $0 < \alpha < 1$. Вона має бути нижчою за поріг сприйняття слухача;

$d -$ затримка еха в часі;

2) метод Phase Coding (PhC) – вбудовує інформацію шляхом модифікації початкової фази аудіосигналу, що робить зміни практично непомітними для людського вуха [14] відповідно до виразу (6):

$$\phi_i^{`}(f) = \begin{cases} \phi_{i-1}(f) + \frac{\pi}{2}, & \text{якщо } m = 1 \\ \phi_{i-1}(f) - \frac{\pi}{2}, & \text{якщо } m = 0 \end{cases}; \tag{6}$$

3) метод Spread Spectrum Audio Steganography (SSAS) – розподіляє приховані дані по всьому частотному спектру аудіофайлу, що забезпечує високу стійкість до спотворень та атак [15] згідно з виразом (7):

$$S(t) = A(t) + \alpha \cdot \big(M(t) \cdot C(t)\big), \tag{7}$$

де $A(t) -$ вихідний аудіосигнал;

$M(t) -$ сигнал секретного повідомлення;

$C(t) -$ псевдовипадкова послідовність, швидкість набагато вища за швидкість $M(t)$;

α – коефіцієнт амплітуди (регулює гучність прихованого сигналу).

3. Стеганографія в тексті:

1) метод синонімічної стеганографії – приховує інформацію шляхом заміни слів у тексті на їхні синоніми, зберігаючи зміст, але модифікуючи структуру повідомлення;

2) метод Whitespace Steganography (WS) – використовує непомітні для читача пробіли, табуляції та переноси рядків для кодування прихованих даних у текстовому файлі;

3) метод зміни порядку слів – модифікує текст, переставляючи слова або фрази так, щоб це не змінювало сенс, але дозволяло передавати додаткову інформацію [16].

У таблиці 1 наведено найбільш поширені методи стеганографії, що застосовуються для приховання інформації в цифрових зображеннях, аудіофайлах і текстових документах.

Таблиця 1

Методи стеганографії в зображенні, аудіо та тексті

Тип носія	Методи стеганографії	Переваги	Недоліки
Зображення	LSB	Мінімальна зміна зображення	Легко виявляється статистичним аналізом
	SS	Висока стійкість до атак	Висока складність реалізації
	DCT	Найменш помітний для аналізу	Потребує обчислювальних ресурсів
Аудіо	ЕМ	Висока стійкість до виявлення	Потребує точного налаштування параметрів

Тип носія	Методи стеганографії	Переваги	Недоліки
	PhC	Важко виявити зміни	Висока складність реалізації
	SSAS	Захист від шумів та спотворень	Потребує великого обсягу даних
Текст	Синонімічна стеганографія	Використовує заміну слів на синоніми	Обмежена кількість інформації для приховування
	WS	Легке впровадження, малопомітність	Легко виявляється при аналізі форматування
	Зміна порядку слів	Висока стійкість до виявлення	Може викликати зміни в змісті

Стеганографічні методи приховування інформації мають як переваги, так і недоліки, що визначають їх ефективність у різних умовах. До основних переваг можна віднести непомітність передачі даних, оскільки прихована інформація інтегрується у цифрові контейнери так, що її існування важко виявити навіть за умов активного моніторингу. Також ці методи відзначаються гнучкістю у застосуванні, оскільки можуть використовувати різні типи контейнерів. Важливою перевагою є можливість їх поєднання з криптографічними технологіями, що дозволяє забезпечити як захист змісту повідомлення, так і приховування самого факту передачі даних. За умов правильного вибору алгоритму та контейнера, такі методи є досить стійкими до пасивних атак.

Одним із ключових недоліків є її висока чутливість до активних атак. При модифікації контейнера, шляхом стиснення або змін параметрів інформаційного повідомлення, може відбутись втрата прихованих даних, оскільки обсяг прихованої інформації залежить від розміру та типу обраного контейнера. Ефективність методу значною мірою залежить від відповідності контейнера умовам використання, що ускладнює його універсальність.

Існує базова схема процесу використання стеганографічних методів для приховування додаткової інформації, яка включає етапи вбудовування інформації у носій, передачу через стегоканал та подальше вилучення прихованого повідомлення на приймальному боці. Процес є двостороннім та потребує використання ключа як на етапі вбудовування, так і при вилученні інформації, що підвищує рівень захищеності передачі.

Стеганографічні методи мають значний потенціал для забезпечення конфіденційності в інформаційно-комунікаційних системах військового призначення. Їх практичне застосування потребує ретельного аналізу можливих загроз, обмежень та правильного вибору контейнера й алгоритму для досягнення максимальної ефективності.

Криптографічні методи є фундаментальним інструментом забезпечення конфіденційності та цілісності даних в ІКС ВП, головним завданням яких є перетворення інформації в шифротекст, що гарантує захист змісту повідомлення навіть у разі його перехоплення.

У сучасних системах застосовують симетричні та асиметричні методи криптографічних перетворень.

Симетричні криптографічні методи базуються на використанні одного й того ж секретного ключа як для шифрування, так і для дешифрування даних. Головною особливістю цих методів з сучасним стандартом симетричного шифрування є алгоритм Advanced Encryption Standard (AES), який широко використовується для захисту великих обсягів даних.

До основних переваг симетричних методів відносять високу швидкість роботи та відносно низькі вимоги до обчислювальних ресурсів, що дозволяє їх використовувати для шифрування файлів, баз даних та потокового трафіку, тощо. Основним недоліком є забезпечення безпечної передачі (розподіл) ключів, які мають бути відомі лише відправнику і отримувачу та збереження їх в таємниці від зловмисника [4].

Асиметричні криптографічні методи вирішують проблему розподілу ключів, використовуючи відкритий та закритий ключі, які математично пов’язані між собою.

Відкритий ключ вільно поширюється і використовується для шифрування даних, а закритий ключ зберігається в таємниці його власником і є єдиним засобом для дешифрування інформації, яка була зашифрована відповідним відкритим ключем. До асиметричних методів належать алгоритми Rivest–Shamir–Adleman (RSA) та Elliptic Curve Cryptography (ECC), які є основою для технологій цифрового підпису [6].

Основним недоліком асиметричних алгоритмів є висока обчислювальна складність та низька швидкість обробки великих обсягів даних.

У сучасних ІКС ВП, як правило, використовується гібридний підхід, що поєднує переваги обох методів. Асиметрична криптографія застосовується на початковому етапі для безпечної передачі симетричного ключа, після чого весь подальший обмін великими обсягами даних шифрується за допомогою швидкого симетричного алгоритму. Таке поєднання дозволяє ефективно протидіяти широкому спектру атак, але, попри високу надійність, супроводжується ризиком компрометації ключів, залежністю від продуктивності системи та потребою у своєчасному оновленні криптографічних протоколів.

Комбіновані методи приховування інформації поєднують криптографічні та стеганографічні підходи для підвищення рівня безпеки передачі інформаційних повідомлень. Сучасні методи комбінування можуть включати: шифрування перед стеганографією, подвійне приховування або розподіл секрету, що дозволяє досягти вищої безпеки та надійності передачі інформаційних повідомлень.

Основними характеристиками комбінованих методів є:

1. Ступінь прихованості (високий рівень прихованості забезпечується використанням ефективних алгоритмів стеганографії, які мінімізують помітність змін у цифровому контейнері);
2. Криптостійкість (залежить від складності використаного алгоритму шифрування);
3. Ресурсомісткість (застосування комбінованих технологій може збільшувати вимоги до обчислювальних ресурсів та впливати на швидкість обробки даних);
4. Стійкість до атак (визначає здатність методу протистояти розкриттю та спробам виявлення прихованої інформації).

На рисунку 1 подано структурну схему процесу комбінованого методу приховування інформації, який поєднує стеганографічні та криптографічні підходи.

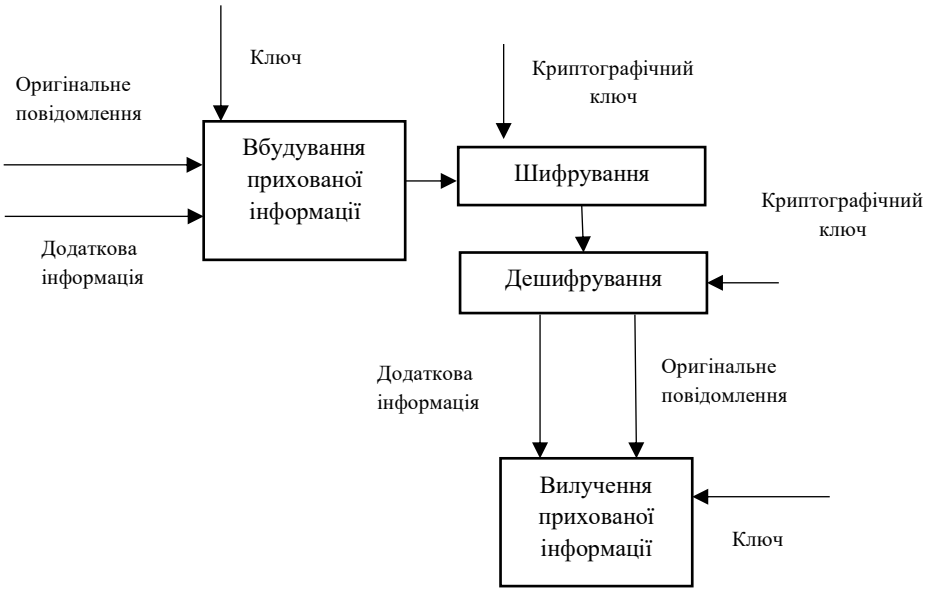

Рис. 1. Структурна схему процесу комбінованого методу приховування інформації

Перевагою комбінованих методів є подвійний рівень безпеки, оскільки інформація не лише шифрується, а й приховується, що ускладнює її перехоплення та аналіз. Такі методи забезпечують захист від аналізу трафіку, оскільки приховують сам факт передавання конфіденційних інформаційних повідомлень. Однак їх застосування може бути обмежене високими вимогами до продуктивності та складністю реалізації, особливо в системах з обмеженими ресурсами.

В таблиці 2 наведено порівняння методів приховування інформації їх переваги та недоліки

Таблиця 2

Порівняння методів приховування інформації

Метод	Переваги	Недоліки	Ключові характеристики
Стеганографія	Прихованість каналу передачі; Стійкість до виявлення засобами розвідки	Низька пропускна спроможність; Чутливість до зміни контейнера; Вразливість до стегоаналізу	Використовує для приховування зображення, аудіо, текст тощо
Криптографія	Надійний захист змісту; Гарантія цілісності даних; Автентифікація відправника	Складність правильної реалізації та масштабованість; Складність управління ключами; Високі обчислювальні витрати	Шифрування інформації, яка передається через відкриті канали зв’язку
Комбінований метод	Багаторівневий захист; Конфіденційність при виявленні; Максимальна стійкість	Складність реалізації; Високі вимоги до ресурсоємності; Успадкування вразливостей	Включає одночасно приховування та шифрування даних

Доцільність використання комбінованих методів приховування інформації обумовлена потребою в підвищеному рівні безпеки даних у ІКС ВП та кібербезпеці. У військових системах вони застосовуються для захисту стратегічно важливих інформаційних повідомлень, а в корпоративних мережах – для запобігання витоку критично важливої інформації. Таким чином, комбіновані методи є перспективним напрямом у сфері інформаційної безпеки, що поєднує переваги криптографії та стеганографії, проте вимагає ретельного підходу до вибору алгоритмів та їхньої реалізації.

Теоретичною основою для наведених оцінок слугували наукові праці, що аналізують як окремі підходи – стеганографію [3, 5] та криптографію [2, 4], – так і ефективність їх поєднання у комбінованих методах [12, 13]. З урахуванням цих факторів, таблиця 3 допоможе оцінити ефективність різних підходів за основними критеріями, де 1 – погано, 5 – дуже добре.

Таблиця 3

Оцінка ефективності методів з приховування інформації

Умова	Стеганографія	Криптографія	Комбінований метод
Висока швидкість передавання	4	3	4
Стійкість до виявлення	5	4	5
Ресурсоємність	3	4	4

Результати порівняльного аналізу окремих та комбінованих підходів приховування інформації дозволяють сформулювати ключові висновки щодо їх ефективності у ІКС військового призначення.

Висновки. У статті проведено порівняльний аналіз сучасних методів приховування інформації в інформаційно-комунікаційних системах військового призначення. Комбіновані методи, які поєднують криптографічні та стеганографічні підходи приховування інформації, дозволяють створити багаторівневий захист, який суттєво ускладнює виявлення та

розшифрування критично важливої інформації. Така інтеграція забезпечує не лише конфіденційність та цілісність даних, але й прихованість самого факту обміну інформацією. Проведена оцінка ефективності підтвердила їхню доцільність для використання в умовах сучасного інформаційного протиборства. Однак, впровадження таких методів супроводжується певними обмеженнями, зокрема збільшенням обчислювального навантаження, затримками передачі даних та необхідністю балансувати між рівнем захисту та ефективністю системи.

Перспективним напрямом подальших досліджень є розроблення методики оцінювання достовірності інформації в ІКС ВП на основі визначення показників із врахуванням сучасних методів приховування інформації в інформаційно-комунікаційних системах військового призначення, що дозволить забезпечити більш комплексну оцінку ефективності захисних механізмів та підвищити стійкість комунікацій у бойових умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Maurer T., Janz J. Cyber and Information Warfare in the Ukrainian Conflict / T. Maurer, J. Janz. Zurich: Center for Security Studies, ETH Zurich, 2018. 36 p. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf (дата звернення: 23.09.2025).

2. Яковенко С. В. Криптографія та стеганографія в інформаційних системах. Л.: Сполом, 2021. 315 с.

3. Жежнич П. Я. Методи та засоби стеганографії: основи теорії та практики. Л.: Вид-во ЛНУ, 2015. 312 с.

4. Романчук О. П. Захист інформації: криптографічні та стеганографічні методи. К.: Наукова думка, 2018. 284 с.

5. Кривошей Д. В. Технології приховування інформації: сучасний стан та перспективи. К.: Політехніка, 2019. 298 с.

6. Дудник В. С. Математичні основи захисту інформації. К.: КНУ ім. Т. Шевченка, 2019. 280 с.

7. Wang B., Zhang M., Liu F., Niu X. SparSamp: efficient provably secure steganography based on sparse sampling / B. Wang, M. Zhang, F. Liu, X. Niu // arXiv.org: e-Print archive. 2024. URL: https://arxiv.org/abs/2401.03669 (дата звернення: 23.09.2025).

8. Kumar S., Kumar R., Singh A. K. A novel reversible data hiding scheme with high payload based on pixel value ordering and prediction error expansion / S. Kumar, R. Kumar, A. K. Singh // Multimedia Tools and Applications. 2023. Т. 82. С. 2825–2849.

9. Al-Juaid A. A., Gutub A. A. A novel generative mathematical model for container-less steganographic system based on image generation / A. A. Al-Juaid, A. A. Gutub // IEEE Access. 2023. Т. 11. С. 83615–83630.

10. Бєляєв А. В. Захист інформації: комбіновані методи криптографії та стеганографії. Х.: Фоліо, 2021. 290 с.

11. Петренко О. В. Технології безпеки інформації у військових системах зв’язку. К.: МО України, 2016. 250 с.

12. Mohammed S. H., Othman W. M. Solvability and nilpotency of Lie algebras in cryptography and steganography / S. H. Mohammed, W. M. Othman // Journal of Computer Science and Technology Studies. 2024. Т. 6, № 1. С. 44–53.

13. Hasan Z. A., Jassim W. K. Steganographic cryptosystem based on the use of chaos theory and cellular automata / Z. A. Hasan, W. K. Jassim // Engineering and Technology Journal. 2024. Т. 42, № 3. С. 382–392.

14. Kumar S., Kumar R., Singh A. K. A novel reversible data hiding scheme with high payload based on pixel value ordering and prediction error expansion / S. Kumar, R. Kumar, A. K. Singh // Multimedia Tools and Applications. 2023. Т. 82. С. 2825–2849.

15. Гончарук В. І. Основи кіберзахисту інформаційних систем. О.: ОНПУ, 2017. 270 с.

16. Барановський О. М. Інформаційна безпека та захист інформації: теорія і практика. Х.: ХНУРЕ, 2020. 356 с.