DOI: 10.58254/viti.9.2026.15.187

УДК 004.056.5:355.4

Носков О. О. ORCID: 0009-0002-8047-3029 (ВІТІ ім. Героїв Крут)

МОДЕЛЬ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМ ПЕРЕДАЧІ ДАНИХ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ З УРАХУВАННЯМ ВИМОГ КОНФІДЕНЦІЙНОСТІ, ЦІЛІСНОСТІ ТА ДОСТУПНОСТІ

У статті розглянуто особливості архітектури сучасних військових систем передачі даних, які класифіковано на три основні типи: тактичні мобільні мережі, стаціонарні вузли та хмарні платформи типу C4ISR. Показано, що кожен із зазначених типів має специфічні переваги та вразливості за умов дії радіоелектронних, кібернетичних та інфраструктурних загроз, а їх ефективне поєднання є критичним для забезпечення безперервного та захищеного управління військами. Теоретично обґрунтовано необхідність формалізації базових критеріїв інформаційної безпеки: конфіденційності, цілісності та доступності CIA у вигляді метричних функцій, на основі яких запропоновано інтегральний індекс ефективності безпеки SEI як зважену комбінацію складових CIA з урахуванням вагових коефіцієнтів, диференційованих за типами систем (тактичні, стаціонарні, хмарні). На основі розробленої моделі виконано порівняльний аналіз низки реальних систем (Delta, Kropyva, GIS Arta, BFT, JADC2), що дозволило кількісно оцінити рівень їхньої захищеності та виявити критичні зони ризику. Запропоновано матрицю інтерпретації значень SEI, яка забезпечує перехід від кількісних результатів багатокритеріальної оцінки до якісних висновків і рекомендацій щодо підвищення ефективності захисту. Наукова новизна роботи полягає у поєднанні архітектурного аналізу військових систем передачі даних із формалізованою моделлю SEI та інтерпретаційною матрицею, а практичне значення у можливості використання отриманих результатів для проєктування адаптивних, живучих і масштабованих систем зв'язку та підтримки прийняття рішень у сфері кіберзахисту. Додатково підкреслено, що запропонований підхід забезпечує інструментальну базу для системного порівняння різних архітектур за умов багатокомпонентних загроз. Отримані результати можуть бути використані під час планування модернізації існуючих військових платформ та створення нових рішень, орієнтованих на підвищення стійкості інформаційної інфраструктури. Застосування моделі SEI також відкриває можливості для подальшого розвитку методів ризик-орієнтованої оцінки та оптимізації заходів захисту в умовах мережоцентричних операцій.

Ключові слова: *військові системи передачі даних, архітектура C4ISR, інформаційна безпека, індекс SEI, критерії CIA, кіберзагрози, тактичні мережі, системи військового управління.*

O. Noskov. Development of a model for determining the efficiency of various types of data transmission systems taking into account the requirements for confidentiality, integrity and availability

The article examines the architectural features of modern military data transmission systems, which are classified into three main types: tactical mobile networks, fixed nodes and cloud platforms of the C4ISR type. It is shown that each of these types has specific advantages and vulnerabilities under the conditions of radio-electronic, cybernetic and infrastructure threats, and their effective combination is critical for ensuring continuous and secure command and control of troops. The need for formalization of the basic criteria of information security: confidentiality, integrity and availability CIA in the form of metric functions is theoretically substantiated, on the basis of which the integral index of security effectiveness SEI is proposed as a weighted combination of CIA components taking into account weighting factors differentiated by system types (tactical, stationary, cloud). Based on the developed model, a comparative analysis of a number of real systems (Delta, Kropyva, GIS Arta, BFT, JADC2) is performed, which allowed to quantitatively assess the level of their security and identify critical risk zones. A matrix for interpreting SEI values is proposed, which provides a transition from quantitative results of multi-criteria assessment to qualitative conclusions and recommendations for improving protection efficiency. The scientific novelty of the work lies in the combination of architectural analysis of military data transmission systems with a formalized SEI model and an interpretative matrix, and the practical significance lies in the possibility of using the obtained results for the design of adaptive, survivable and scalable communication and decision support systems in the field of cyber defense. It is additionally emphasized that the proposed approach provides an instrumental basis for the systematic comparison of different architectures under conditions of multi-component threats. The obtained results can be used when planning the modernization of existing military platforms and creating new solutions aimed at increasing the resilience of the information infrastructure. The application of the SEI model also opens up opportunities for further development of methods for risk-based assessment and optimization of protection measures in conditions of network-centric operations.

Keywords: *military data transmission systems, C4ISR architecture, information security, SEI index, CIA criteria, cyber threats, tactical networks, military control systems.*

Постановка завдання. Сучасні військові системи передачі даних за архітектурними ознаками можна розділити на три основні типи: тактичні мобільні мережі, стаціонарні вузли та хмарні платформи (cloud-based C4ISR). Кожен із цих типів має специфічну структуру й принцип дії, що визначають їх застосування та ефективність у різних умовах [1; 2]. Тактичні мобільні мережі – це польові мережі зв’язку тактичного рівня, призначені для забезпечення командування і взаємодії безпосередньо на полі бою. Вони об’єднують підрозділи, що діють у русі (піхотні підрозділи, бойові машини, мобільні командні пункти тощо), і надають їм можливість обмінюватися даними в реальному часі навіть за відсутності розвиненої інфраструктури. Такі мережі часто будуються за принципом ad hoc (тобто самоорганізованих мереж) і можуть функціонувати в умовах мінливої топології, коли вузли (радіостанції, термінали тощо) додаються або вибувають динамічно. Виходячи з цього, постає завдання дослідження – формалізувати підходи до оцінювання ефективності військових систем передачі даних з урахуванням архітектурних особливостей кожного типу та різної природи загроз, а також розробити універсальний інструмент для порівняльного аналізу їхнього рівня інформаційної безпеки. Для цього необхідно визначити релевантні критерії оцінювання, побудувати метричну модель їх вимірювання та забезпечити можливість інтерпретації отриманих результатів у контексті практичних потреб військового управління та кіберзахисту.

Аналіз літературних джерел. Проведений аналіз наукових і прикладних досліджень свідчить про зростаючу увагу до проблеми підвищення ефективності військових систем передачі даних та їхньої інформаційної безпеки. У роботі Андрушка М. В., Аркушенка П. Л., Кузнецова В. О. та Андрушка А. М. [1] обґрунтовано узагальнену модель функціонування перспективних інформаційно-вимірювальних систем, що є важливим підґрунтям для подальшого формування метричних підходів до оцінювання військових комунікаційних платформ. Дослідження Поморцевої О. Є. та Кобзана С. М. [2], присвячене геопросторовому моделюванню, демонструє значення просторово-аналітичних інструментів для підвищення точності та оперативності обробки даних у військових системах підтримки рішень. У матеріалі Brandi V. [3] підкреслюється роль штучного інтелекту в трансформації підходів НАТО до геопросторової розвідки, що актуалізує питання інтеграції AI-модулів у сучасні C4ISR-архітектури.

У роботі Купера Т. [6] акцентовано на високій вразливості засобів радіолокації до засобів ворожої радіотехнічної та сигнальної розвідки, що визначає необхідність підвищення стійкості каналів передачі даних у тактичних мережах. Публікації Коломійця В. [7], Данилова О. [8], Найєма М. [9] та Морфінова С. [10] висвітлюють еволюцію української системи ситуаційної обізнаності «Delta», її функціональні можливості, роль у мережоцентричних операціях та реакцію противника на її використання. Окреме місце займає стаття Кобзана С., Поморцевої О., Паньківа В. та Андронова В. [16], де наведено підходи до побудови геоінформаційної системи для потреб Збройних Сил України, що є релевантним у контексті формування архітектурних вимог до військових систем управління.

Додаткові матеріали щодо функціонування українських та міжнародних платформ – таких як Delta, GIS Arta, BFT, JADC2, Griselda та інших – узагальнено у відкритих оглядах і технічних описах, які демонструють різноманітність архітектур, рівнів автоматизації та ступеня інтеграції систем ситуаційної обізнаності в операційну діяльність військ. Сукупність проаналізованих джерел підтверджує необхідність формалізації підходів до оцінювання захищеності військових систем передачі даних та обґрунтовує актуальність розробки універсальних індексів і моделей для порівняльного аналізу.

Мета статті. Метою статті є теоретичне обґрунтування та розробка інтегральної моделі оцінки ефективності інформаційної безпеки військових систем передачі даних різних архітектурних типів (тактичних мобільних мереж, стаціонарних вузлів і хмарних платформ C4ISR) на основі формалізації критеріїв CIA (конфіденційність, цілісність, доступність) та індексу Security Effectiveness Index – (SEI), здійснення їх порівняльного аналізу за критеріями

гнучкості, живучості й масштабованості, а також побудова адаптивної архітектурної моделі взаємодії зазначених систем і матриці інтерпретації значень SEI для підтримки управлінських рішень у сфері кіберзахисту.

Виклад основного матеріалу. В Збройних силах України прикладом тактичної мережі нового покоління є система Кропива – бойова система управління тактичної ланки, що працює на планшетах і смартфонах. Функціонал включає електронні карти з GPS, обмін повідомленнями між підрозділами, розрахунок артилерійських даних, інтеграцію з безпілотниками та радарами. Аналогічного класу системи: GIS Arta – геоінформаційна система для артилерії, що забезпечує надшвидку передачу цілевказань на артпідрозділи (до 1 хвилини) і дозволяє використовувати звичайні смартфони як пристрої наведення. Також до цього класу можна віднести ситуаційно-інформаційну систему Delta, коли вона використовується безпосередньо тактичними ланками на полі бою на рівні окремих підрозділів, які отримують дані про противника через портативні термінали. (Варто зазначити, що Delta за своєю архітектурою ближча до хмарних платформ, але польові термінали, що працюють з Delta, фактично виступають елементами тактичної мережі.) Сучасні армії світу також мають подібні системи: наприклад, переносні комплекси Blue Force Tracker (BFT), що на рівні взвод – рота передають координати своїх сил через супутник для побудови цифрової картини поля бою. Усі ці системи створені для підвищення ситуаційної обізнаності і швидкості реагування на рівні тактичних підрозділів [7; 12].

Стаціонарні вузли – це фіксовані (стаціонарні) компоненти мереж зв’язку та управління, розгорнуті у постійних або довготривалих місцях дислокації. До них належать командні центри, штаби, стаціонарні вузли зв’язку, серверні центри і вузли обробки даних, які не переміщуються разом з військами. Такі системи зазвичай формують ядро військової інформаційної інфраструктури в тилу або на оперативному рівні. Вони характеризуються високою продуктивністю, більш надійними каналами зв’язку (порівняно з польовими) та централізованим управлінням ресурсами мережі [5].

Стаціонарні системи зв’язку хоча й працюють у більш комфортних умовах (ніж польові), але теж піддаються випробуванням:

Обмежений зв’язок: якщо військова інфраструктурна мережа зазнає пошкоджень – наприклад, фізичне переривання кабелю через диверсію чи обстріл, або вихід з ладу вузла, – то комунікація може частково втрачатися. На цей випадок передбачені резервні маршрути і канали.

Пікове навантаження: стаціонарна інфраструктура, як правило, має запас потужності, але надзвичайні ситуації (масований кібервплив, раптова необхідність обробити великий обсяг даних розвідки тощо) можуть викликати сплески трафіку. Система балансування навантаження перенаправляє запити на менш завантажені сервери, задіює резервні обчислювальні потужності. Наприклад, при піку запитів до баз даних система може тимчасово відмовитися від неважливих запитів або затримати непершочергові задачі, щоб не допустити краху сервера. На відміну від тактичних мереж, пікове навантаження тут більше стосується пропускної здатності центрів обробки та мережевого обладнання.

Кібератаки: стаціонарна мережа – привабливa ціль для кібернетичних атак, адже вона містить стратегічні дані і часто має вихід до глобальних мереж. DDoS-атаки (розподілені атаки на відмову в обслуговуванні) можуть здійснюватися на вузли, що мають підключення до Інтернету або суміжних мереж: масований трафік може перевантажити сервери чи канали. Для протидії використовуються міжмережеві екрани (фаєрволи), системи виявлення та запобігання вторгнень, а також хмарні служби очистки трафіку (якщо допустимо). Jamming (радіопридушення) безпосередньо менше стосується стаціонарних вузлів, бо їхні канали здебільшого дротові; однак, якщо є радіолінії чи супутникові сегменти, противник може спробувати їх глушити – тому критичні канали дублюються кабельними. Spoofing в стаціонарних системах може проявлятися як підробка даних або проникнення в мережу

шляхом видавання себе за довірений вузол. Високий рівень аутентифікації (сертифікати, апаратні маркери) покликаний цьому запобігти [6].

До цього типу можна віднести класичні автоматизовані системи управління військами, розгорнуті в стаціонарних пунктах. Історично в Україні існували проєкти на кшталт Єдиної автоматизованої системи управління ЗСУ, що мали на меті створити опорну стаціонарну мережу для обміну даними між штабами. У країнах НАТО прикладами можуть бути стаціонарні компоненти систем типу AFATDS (Advanced Field Artillery Tactical Data System) – американська система управління вогнем артилерії: вона встановлюється на командних пунктах і пов’язує між собою штаби артилерійських підрозділів через захищені мережі. AFATDS поєднує ознаки тактичної і стаціонарної системи: програмно вона децентралізована (кожна батарея чи взвод можуть діяти самостійно, обмінюючись повідомленнями), але розгортається на стаціонарних або напівмобільних командних пунктах, які з’єднані дротовими чи стабільними радіолініями.

Хмарні платформи типу Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) – це мережево-центричні системи управління та розвідки, що використовують технології хмарних обчислень для зберігання, обробки та поширення даних. Їхній архітектурний принцип полягає в централізованому (або розподілено-централізованому) агрегуванні великого обсягу інформації з різних джерел та наданні доступу до неї численним користувачам у реальному часі. Cloud-based C4ISR платформи, по суті, є розвитком стаціонарних систем, адаптованим до роботи у хмарному середовищі, що підвищує гнучкість, масштабованість і інтеграцію між видами збройних сил. Такі системи охоплюють всі рівні – від тактичного до стратегічного – і дозволяють об’єднати дані з наземних, повітряних, морських, космічних та кібернетичних доменів в єдину інформаційну мережу. Концепція Joint All-Domain Command and Control (JADC2), яку розвиває Міністерство оборони США, є прикладом саме такого підходу: поєднання сенсорів усіх родів військ у єдину мережу на базі штучного інтелекту для швидкого ухвалення рішень. Хмарна C4ISR система покликана забезпечувати управління навіть у найскладніших ситуаціях, але і вона має свої межі стійкості [3; 4]:

Обмежений зв’язок: якщо противнику вдається значно порушити комунікацію (наприклад, масштабним радіоелектронним придушенням супутникового зв’язку чи знищенням вузлів передачі), то окремі частини сил можуть опинитися без доступу до хмари. В такому разі система переходить до деградованого режиму: використання резервних каналів з меншою швидкістю, зниження якості переданих даних (напр., замість відео надсилати тільки координати цілей), збільшення інтервалів оновлення інформації. Ключове завдання – не втратити життєво важливі дані: хмара може вибірково передавати критичні повідомлення найстійкішими каналами (приміром, через короткі текстові пакети по УКХ-радіо, якщо інше недоступне). Якщо ж якесь угруповання повністю ізольоване, воно має діяти автономно, спираючись на заздалегідь отримані розвідувальні дані і локальні тактичні системи. Одночасно, хмарна система, як тільки з’явиться вікно зв’язку, затоплює ізольований сегмент усіма накопиченими даними (і приймає від нього дані) для якнайшвидшого синхронізування картини бою.

Пікове навантаження: хмарні платформи спроєктовані масштабованими, але раптовий пік (скажімо, початок масштабної операції з тисячами потоків даних від всіх сенсорів) випробовує їхню еластичність. Завдяки хмарним технологіям система може автоматично масштабуватися: додавати нові віртуальні сервери, перерозподіляти бази даних на більшу кількість вузлів, тимчасово використати комерційні хмарні потужності (як резерв) тощо. Відомо, що українська система Delta після розширення фронту російського вторгнення була перенесена на закордонні хмарні майданчики для захисту і масштабування.

Такі рішення дозволяють витримати різке збільшення навантаження. Також застосовуються механізми пріоритезації: на піку навантаження менш важливі задачі

(наприклад, аналітичні запити або резервне копіювання) відкладаються, щоб не заважати бойовим запитам в реальному часі. Завдяки розподіленості різні компоненти системи можуть масштабуватися незалежно: якщо, скажімо, відеостріми з дронів генерують основний трафік, то збільшується число серверів відеообробки, тоді як інші частини залишаються незмінними.

Кожен розглянутий архітектурний тип має свої переваги і недоліки, що виявляються при порівнянні за критеріями гнучкості, живучості та масштабованості. Результати порівняльного аналізу представлено в таблиці 1.

Таблиця 1

Порівняльний аналіз архітектурних типів мереж

Критерій	**Тактичні мобільні мережі (Kropyva)**	**Стаціонарні мережі (GIS Arta)**	**Хмарні платформи (Delta)**	**Коментар / приклад**
Гнучкість	Висока просторово: розгортання без інфраструктури; обмежена функціонально через ресурси	Низька просторово, висока функціонально; додавання серверів та сервісів	Найвища функціональна гнучкість; динамічне масштабування; залежність від каналів зв’язку	Kropyva – автономна; Delta потребує Starlink; GIS Arta – гнучка сервісно
Живучість	Децентралізована; вузли працюють незалежно; вразливість до масового радіопридушення	Чутливість до точкових атак на центри; резервування частково вирішує	Висока живучість у дата-центрах; критична залежність від комунікацій	Kropyva функціонує локально; Delta вразлива до втрати зв’язку
Живучість	Децентралізована; вузли працюють незалежно; вразливість до масового радіопридушення	Чутливість до точкових атак на центри; резервування частково вирішує	Висока живучість у дата-центрах; критична залежність від комунікацій	Kropyva функціонує локально; Delta – вразлива до втрати зв’язку
Масштабо-ваність	Обмежена: лише в межах роти/батальйону; потребує частотного планування	Може масштабуватись вертикально та горизонтально; обмеження в інфраструктурі	Найвища: автоматичне додавання ресурсів, охоплення нових зон	Delta – легко підключає нові підрозділи; GIS Arta потребує налаштувань

Джерело: розроблено автором на основі [7; 9; 12].

Отже, три основні архітектурні типи систем передачі даних доповнюють один одного, забезпечуючи зв’язок і управління на різних рівнях і в різних умовах. Тактичні мережі надають гнучкість і незалежність підрозділам на полі бою, дозволяючи їм обмінюватися інформацією безпосередньо і діяти автономно навіть при розривах зв’язку з вищими штабами. Стаціонарні системи забезпечують потужну основу – сполучну інфраструктуру й обчислювальні центри, що збирають і аналізують дані, підтримують безперервність управління та великий обсяг інформації. Хмарні платформи інтегрують всі рівні в єдине інформаційне середовище, даючи можливість максимально швидко використовувати дані з будь-яких джерел для ухвалення рішень у реальному часі. Кожен тип систем має свої переваги: тактичні переважають у польових умовах, стаціонарні характеризуються надійністю, хмарні мають переваги у масштабі та швидкості обробки даних. Але кожен має і вразливі місця, що проявляються за екстремальних ситуацій.

Таким чином, адаптивна модель побудови військової системи зв’язку і передачі даних повинна поєднувати ці класи та гнучко перемикатися між ними залежно від обстановки. Для тактичних мереж доцільно реалізувати адаптивні алгоритми маршрутизації та динамічне керування частотами, щоб протистояти перешкодам і мінімізувати затримки. Стаціонарні

вузли мають бути вбудовані в адаптивну інфраструктуру з автоматичним переключенням на резерви при збоях та можливістю масштабування під навантаження. Хмарні C4ISR-системи потребують адаптації до якості каналів, наприклад, зменшувати обсяг переданих даних або переходити в режим децентралізації (edge computing) при деградації зв’язку. Інтеграція трьох типів в єдину мережево-центричну екосистему з інтелектуальним керуванням дозволить використати сильні сторони кожного: забезпечити надійний зв’язок і управління військами навіть у умовах, коли один з елементів (мобільний, стаціонарний чи хмарний) тимчасово обмежений або зазнає атаки. Отже, адаптивна модель архітектури є найбільш доцільною для підвищення живучості, гнучкості та ефективності сучасних військових систем передачі даних, оскільки враховує особливості кожного класу і мінімізує їхні недоліки завдяки взаємному дублюванню та підтримці [4; 16].

У сучасних системах передавання даних інформаційна безпека ґрунтується на тріаді CIA: конфіденційності, цілісності та доступності. Кожен із цих критеріїв є необхідним для оцінки захищеності системи і служить окремим показником ефективності заходів безпеки. У цьому підпункті здійснено наукове обґрунтування кожного з критеріїв CIA в контексті систем передачі даних, надано їхні формальні визначення через відповідні математичні вирази, а також запропоновано інтегральний індекс ефективності безпеки, що поєднує три критерії з урахуванням вагових коефіцієнтів.

Конфіденційність визначає властивість системи забезпечувати доступ до інформації лише уповноваженим суб’єктам і запобігати розголошенню даних стороннім особам. З позиції інформаційної безпеки мережі передачі даних, конфіденційність означає, що передані повідомлення не можуть бути прочитані або перехоплені зловмисниками. На практиці досягнення конфіденційності забезпечується, зокрема, криптографічними методами (шифруванням трафіку) та керуванням доступом. Для кількісної оцінки цього критерію вводиться метрика, яка відображає частку передач, здійснених без порушення конфіденційності. Формально коефіцієнт конфіденційності можна визначити як відношення числа успішно захищених передач до загального числа передач. Зручним є доповнення цього відношення до 1, що дає міру втрати конфіденційності при наявності витоків. Таким чином, запропонована метрика конфіденційності може бути виміряна за формулою (1):

$$C = 1 - \frac{L}{N}, \tag{1}$$

де L – кількість зафіксованих витоків (несанкціонованих розголошень інформації);
N – загальна кількість передач даних у системі.

Значення $C = 1$ відповідає повному збереженню конфіденційності (відсутності витоків), тоді як значення, наприклад, $C = 0{,}9$ (або 90 %), означає, що 10 % передач призвели до компрометації даних. Чим ближче значення C до 1, тим вищий рівень конфіденційності забезпечує система передачі даних.

Цілісність – це властивість інформації залишатися повною, достовірною і незміненою при зберіганні та особливо при передачі. З точки зору захисту мережевих даних, цілісність означає, що пакетні дані доходять від відправника до отримувача без спотворень, модифікацій чи знищення неавторизованими діями. Порушення цілісності можуть відбутися через навмисну підміну або спотворення даних (атаки типу man-in-the-middle, внесення шкідливих змін), а також через випадкові помилки чи збої, що призводять до пошкодження пакетів. Для оцінки цього критерію вводять формальну метрику як частку даних, що зберегли цілісність під час передачі. Показник цілісності можна подати формулою (2):

$$I = 1 - \frac{D}{P}, \tag{2}$$

де P – загальна кількість переданих пакетів (або інших блоків даних) у мережі;

D – кількість деформованих (ушкоджених або невалідних) пакетів, виявлених на приймальній стороні.

За такого визначення $I = 1$ у випадку, коли всі пакети отримано без спотворень (жодного пошкодженого пакета), що відповідає ідеальній цілісності переданих даних. Зменшення значення показника I сигналізує про втрату або зміну частини інформації. Наприклад, $I = 0{,}98$ означає, що 2 % пакетів були втрачені чи змінені під час транспортування. Метрика цілісності дозволяє кількісно виміряти ефективність механізмів забезпечення цілісності (таких як контрольні суми, коди перевірки цілісності, протоколи виявлення збоїв) у системі передачі даних.

Доступність характеризує здатність системи забезпечувати своєчасний і безперервний доступ користувачів до інформації та сервісів. З погляду мережі передачі даних, доступність означає, що мережевий сервіс або канал зв'язку функціонує без тривалих простоїв, і авторизовані користувачі можуть отримати доступ до даних у потрібний момент. Порушення доступності найчастіше пов'язане з відмовами обладнання, збоями програмного забезпечення або зловмисними діями типу Denial of Service (DoS), що призводять до простою мережі. Для вимірювання цього критерію використовують метрику безперервності сервісу – відносний час, протягом якого система є працездатною. Коефіцієнт доступності обчислюється за формулою (3):

$$A = \frac{T_{up}}{T_{total}}, \tag{3}$$

де T_{up} – сумарний час безвідмовної роботи системи (uptime) за певний інтервал спостереження;

T_{total} – загальний час роботи системи (включно з плановим часом функціонування, часовими інтервалами простою тощо).

Значення $A = 1$ відповідає 100 % доступності, коли система не мала простоїв у заданому інтервалі часу. Якщо ж, наприклад, протягом доби мережа була недоступна сумарно 1 годину (тобто $T_{up} = 23$ год, $T_{total} = 24$ год), показник доступності становитиме $A \approx 0{,}9583$ (95,83 %). Високе значення метрики A свідчить про надійну, безперебійну роботу системи, тоді як низьке значення сигналізує про часті або тривалі простої, що можуть бути критичними для користувачів систем передачі даних.

Після визначення окремих базових показників C, I та A постає задача інтегральної оцінки сукупної ефективності захисту. Зважаючи на те, що конфіденційність, цілісність і доступність є різними за значенням для різних систем, доцільно об'єднати їх в один узагальнений показник із урахуванням пріоритетності кожного критерію. У межах цього дослідження пропонується індекс ефективності безпеки, що об'єднує критерії CIA шляхом зваженого підсумовування. Формально SEI визначається як лінійна комбінація метрик C, I, A з відповідними ваговими коефіцієнтами (4):

$$SEI = w_C C + w_I I + w_A A, \tag{4}$$

де w_C, w_I, w_A – вагові коефіцієнти, що відображають відносну важливість (пріоритетність) кожної складової безпеки для цієї системи, при цьому $w_C + w_I + w_A = 1$.

Коефіцієнти w_j (де $j \in \{C, I, A\}$) можуть приймати значення від 0 до 1 і призначаються експертним шляхом або на основі вимог до системи. Чим більше значення w_j, тим більшого значення надається відповідному критерію при оцінці загальної ефективності. Таким чином,

індекс SEI агрегує триєдиний показник безпеки: значення SEI, близьке до 1, вказує на високий рівень загальної захищеності (за прийнятої конфігурації ваг), тоді як менші значення сигналізують про наявність слабких місць у конфіденційності, цілісності або доступності (залежно від того, який компонент має недостатній рівень або малу вагу).

Вагові коефіцієнти в моделі SEI слід обирати з урахуванням специфіки та призначення конкретної системи, оскільки різні типи систем висувають різні пріоритети щодо CIA. Іншими словами, тип системи безпосередньо впливає на розподіл ваг w_C, w_I, w_A. Тактичні системи (наприклад, військові або екстрені системи зв’язку, що працюють в реальному часі) зазвичай найбільше залежать від безперервної роботи, тому критерій доступності для них є пріоритетним. Для таких систем навіть короткочасна відмова зв’язку може мати неприпустимі наслідки, тому ваговий коефіцієнт w_A обирається найбільшим. Конфіденційність і цілісність у тактичних мережах теж важливі, проте можуть мати дещо менші ваги, оскільки в критичних умовах безперервність сервісу (зв’язку) часто важливіша за повну таємницю передач. Хмарні системи (наприклад, сервіси хмарного зберігання або обробки даних) натомість приділяють першочергову увагу захисту даних від несанкціонованого доступу та помилок. У хмарних платформах витік конфіденційної інформації або порушення цілісності даних може призвести до значних збитків та підриву довіри користувачів, тоді як короткочасна недоступність сервісу (наприклад, для планового обслуговування) є відносно менш критичною. Відповідно, для хмарної системи вагові коефіцієнти w_C та w_I встановлюються вищими, ніж w_A [3; 11].

Наведемо приклади конфігурації ваг для зазначених типів систем. Для тактичної мережі зв’язку можна обрати такі вагові коефіцієнти: $w_C = 0{,}2,\ w_I = 0{,}3,\ w_A = 0{,}5$. У цьому випадку найбільша вага (50 %) надається доступності, що відображає критичну важливість безперервного зв’язку, тоді як конфіденційність отримує 20 %, а цілісність – 30 % від загального індексу. Для хмарного середовища доцільно збільшити внесок критеріїв конфіденційності та цілісності. Наприклад, для хмарного сховища даних можна задати $w_C = 0{,}4,\ w_I = 0{,}4,\ w_A = 0{,}2$, тобто 40 % ваги припадає на кожен із показників конфіденційності та цілісності, а доступність оцінюється у 20 %. Така конфігурація відображає пріоритетність запобігання витокам даних і гарантування коректності інформації для користувачів хмарного сервісу, при тому що показник доступності залишається важливим, але не домінуючим. Зрозуміло, що наведені ваги є умовними прикладами – у реальних проєктах їхні значення встановлюються на основі вимог замовника, нормативних рекомендацій та експертної оцінки ризиків. У цілому, тактичні (час-критичні) системи мають схильність до конфігурацій, де w_A максимальний, тоді як інформаційно-орієнтовані (центри обробки даних, хмарні сервіси) – до конфігурацій з вищими w_C та w_I.

Таким чином, формалізовано три базові критерії ефективності інформаційної безпеки – конфіденційність, цілісність і доступність – шляхом відповідних метричних виразів, а також побудовано інтегральний індекс SEI як зважену суму складових CIA. Запропонований підхід дозволяє кількісно оцінити загальний рівень захищеності системи передачі даних з урахуванням її особливостей та пріоритетів. Отримані формалізації закладають основу для подальшої побудови моделі SEI. У наступному підпункті буде детально розглянуто розробку самої SEI-моделі та практичне застосування індексу ефективності безпеки.

Доцільно провести математичну формалізацію базових критеріїв Confidentiality, Integrity, Availability (CIA), що використовуються в моделі оцінки ефективності систем передачі даних.

1. Формалізація CIA як критеріїв.

Визначено три функції для кожного з критеріїв системи передачі даних – (x):

$C(x)$ – рівень конфіденційності;

$I(x)$ – рівень цілісності;

$A(x)$ – рівень доступності.

Визначено метрики для обчислення кожного з показників:
$C = 1 - (N_{data\ leak} / N_{total\ tx})$;
$I = 1 - (N_{corrupted\ packets} / N_{total\ packets})$;
$A = T_{uptime} / T_{total}$.

Вагова модель оцінки ефективності за CIA. Інтегральний індекс ефективності безпеки SEI розраховується за формулою (5):

$$SEI = w_C\, C(x) + w_I\, I(x) + w_A\, A(x), \quad (5)$$

де $w_C + w_I + w_A = 1$, а ваги залежать від типу системи (тактична, хмарна, стаціонарна).

Приклад вагового розподілу від автора.

Для тактичних систем: $w_C = 0{,}25$, $w_I = 0{,}25$, $w_A = 0{,}50$.

Для хмарних систем: $w_C = 0{,}4$, $w_I = 0{,}4$, $w_A = 0{,}2$.

Для стаціонарних систем: $w_C = 0{,}3$, $w_I = 0{,}5$, $w_A = 0{,}2$.

Таким чином, формалізована модель SEI дозволяє враховувати особливості кожного типу системи через змінні ваги. Представимо модель у вигляді схеми (рис. 1).

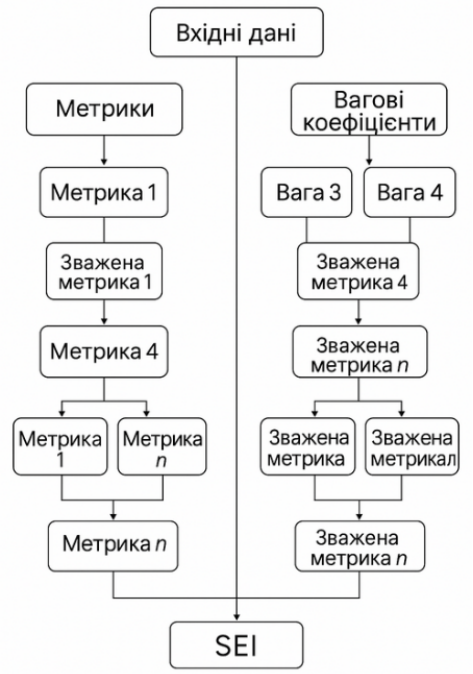

Рис. 1. Схематична візуалізація моделі SEI
(джерело: розроблено автором)

За допомогою запропонованих вище формул та послідовності проведення оцінки проведемо розрахунки індексу ефективності безпеки системи SEI. Вхідні дані для проведення розрахунків представлені наступним чином:

SEI = 0,25 × 0,85 + 0,30 × 0,92 + 0,20 × 0,88 + 0,15 × 0,75 + 0,10 × 0,70;
SEI = 0,2125 + 0,276 + 0,176 + 0,1125 + 0,070 = 0,847;
SEI = 0,847 (або 84,7 %).

У таблиці 2 подано інформацію з вихідними значеннями технічних метрик, результатами нормалізації, а також проміжними формулами та ваговими коефіцієнтами, що

використовуються для розрахунку індексу SEI для 5 об'єктів: Delta, Kropyva, GIS Arta, BFT, JADC2.

Таблиця 2

Розрахунок індексу SEI для 5 об'єктів: Delta, Kropyva, GIS Arta, BFT, JADC2*

Нормалізоване виявлення Norm. Detection	Затримка (мс) Latency (мс)	Нормалізована затримка Norm Latency	Доступність (хв) Availability (хв)	Нормалізована доступність Norm Avail	Втрата пакетів (%) Packet Loss (%)	Нормалізована цілісність Norm. Integrity	Витоки даних / Кількість переданих повідомлень Data Leaks / Tx	Нормалізована конфіденційність Norm. Confid	Час виявлення (хв) Detection Time (хв)
Delta	110	0,500	1 390	0,727	2,5	0,565	3 / 15 000	0,533	2,5
Kropyva	130	0,000	1 350	0,000	3,8	0,000	4 / 12 000	0,081	3,2
GIS Arta	90	1,000	1 405	1,000	1,9	0,826	2 / 18 000	0,835	2,1
BFT	125	0,125	1 365	0,273	2,0	0,783	5 / 14 000	0,000	4,0
JADC2	100	0,750	1 380	0,545	1,5	1,000	1 / 16 000	1,000	1,7

Джерело: розраховано автором на основі [8; 11].

Значення нормалізовані за принципом benefit/cost-критеріїв:

Для latency, packet loss, data leak rate та detection time застосовано інверсну нормалізацію (менше – краще).

Для availability – звичайна нормалізація (більше – краще).

Джерело: розраховано автором.

Матриця нижче (табл. 3) є шаблоном для якісного тлумачення кількісного інтегрального індексу ефективності безпеки SEI, отриманого в результаті багатокритеріального аналізу.

Таблиця 3

Матриця інтерпретації кількісного інтегрального індексу ефективності безпеки SEI, отриманого в результаті багатокритеріального аналізу

Діапазон значення SEI	**Рівень ефективності безпеки**	**Інтерпретація**	**Рекомендації**
0,90–1,00	Високий (Оптимальний)	Система демонструє високі значення всіх ключових метрик. Захист є збалансованим і стійким.	Підтримувати чинні політики. Можливе впровадження інновацій (AI-based monitoring, adaptive controls)
0,75–0,89	Добрий (Контрольований)	Система працює стабільно, проте є локальні вразливості. Основні критерії задовільні	Поглиблений аудит окремих показників. Рекомендовані точкові покращення
0,60–0,74	Середній (Помірний ризик)	Частина ключових показників у межах допустимого, але спостерігається деградація окремих метрик	Необхідно підсилити конкретні зони безпеки. Розробити план покращення та контроль динаміки
0,40–0,59	Низький (Небезпечний)	Система має критичні недоліки. Конфіденційність або доступність перебувають на межі прийнятного	Негайний аналіз архітектури. Провести оновлення засобів захисту. Вжити організаційні заходи
< 0,40	Критичний (Неприйнятний)	Інформаційна система практично не захищена. Є суттєві порушення цілісності, відмови зв'язку тощо	Ризик неприйнятний. Необхідне повне переосмислення архітектури системи та стратегії захисту

Джерело: розроблено автором.

З метою забезпечення об’єктивного аналізу отриманих результатів комплексної оцінки ефективності систем передачі даних, побудованої на основі інтегрального індексу SEI, доцільним є використання формалізованого інструменту – матриці інтерпретації значень SEI. Така матриця виконує роль методологічного містка між кількісною метрикою та її якісним тлумаченням, трансформуючи обчислені значення SEI у контекстні висновки щодо рівня інформаційної безпеки об’єкта дослідження [16].

Відповідно до засад метрологічного підходу в інформаційній безпеці, кожне значення інтегрального показника має бути приведене до інтервальної шкали, на якій встановлюється порогова градація – від критичного до оптимального рівня. Запропонована інтерпретаційна матриця базується на п’яти рівнях ефективності: критичний (< 0,40), низький (0,40–0,59), середній (0,60–0,74), добрий (0,75–0,89), високий (0,90–1,00). Таке розбиття є не лише формально обґрунтованим з позицій імовірнісного аналізу ризиків, а й адаптивним до сучасних міжнародних практик (наприклад, NIST SP 800-53, ISO/IEC 27004), де рекомендовано класифікувати результати оцінки інформаційної безпеки за багаторівневими критеріями.

Кожному інтервалу відповідає якісна характеристика поточного стану системи, яка враховує не лише значення SEI, а й контекст системної архітектури, функціонального навантаження та вразливості до зовнішніх впливів. Таким чином, матриця поєднує кількісну об’єктивність і аналітичну змістовність, що є критично важливим для формування подальших управлінських рішень, таких як розробка політик безпеки, розподіл ресурсів, оновлення архітектурних компонентів тощо.

Крім того, матриця містить рекомендаційний блок, який слугує аналітичним орієнтиром для формування рішень щодо усунення виявлених проблем. Наприклад, для систем із рівнем $SEI < 0,40$ рекомендовано проведення повного аудиту архітектури та перегляд політик захисту, тоді як системи з $SEI > 0,90$ можуть перейти до адаптивного моделювання та впровадження інноваційних технологій на кшталт автоматизованих платформ реагування на інциденти (SOAR), поведінкового аналізу загроз (UEBA) або засобів на базі штучного інтелекту [14; 15].

Висновки. Таким чином, матриця інтерпретації значень SEI виступає не лише інструментом аналітичного контролю, але й елементом концептуальної моделі оцінки стану інформаційної безпеки, забезпечуючи відтворюваність, інтерсуб’єктивність та орієнтованість на практичне впровадження.

Отже, запропонована в межах дослідження матриця інтерпретації значень SEI виступає методологічним інструментом, що забезпечує семантичне осмислення результатів багатокритеріальної оцінки ефективності захисту систем передачі даних. Її розробка дозволяє поєднати кількісно формалізовані значення інтегрального показника безпеки з якісними характеристиками стану інформаційної системи, що забезпечує прозорість і відтворюваність прийняття управлінських рішень у сфері кіберзахисту.

Матриця побудована з урахуванням принципів шкалювання критеріальних оцінок, методів ризик-орієнтованого менеджменту та практик стандартизованого моніторингу ефективності (зокрема NIST, ISO/IEC 27004). Такий підхід дозволяє не лише здійснювати класифікацію поточного рівня захисту, а й формувати рекомендації адаптаційного характеру залежно від контексту архітектури, типу загроз і пріоритетів застосування системи.

Інтерпретаційна матриця SEI є ключовим елементом валідації результатів розробленої моделі та її подальшого практичного впровадження у процедурах аудиту, управління ризиками та розробки архітектур захищених систем зв’язку. Її впровадження забезпечує базис для автоматизованого аналізу, побудови інформаційних дашбордів та динамічного моніторингу живучості системи в умовах змінного кіберсередовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Андрушко М. В., Аркушенко П. Л., Кузнецов В. О., Андрушко А. М. Обґрунтування узагальненої моделі функціонування перспективної інформаційно-вимірювальної системи збору та обробки інформації // Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки. 2023. Вип. 3 (17). С. 7–14. DOI: https://doi.org/10.37701/dndivsovt.17.2023.01.

2. Pomortseva O. E., Kobzan S. M. Geospatial modeling of the location of bomb shelters in residential areas of the city. IOP Conference Series: Earth and Environmental Science. 2023. Т. 1254. №. 1. URL: DOI: 10.1088/1755-1315/1254/1/012136

3. Brandi V. AI will “revolutionize” the way NATO looks at geospatial intelligence. 2024. URL: https://defensescoop.com/2024/05/07/nato-geoai-revolutionize-geoint-scott-bray/.

4. Navigating the Future: Key Findings from Allied Command Transformation’s 2023 Strategic Foresight Analysis, 2024. URL: www.act.nato.int.

5. Автоматизована система управління військами – зброя перемоги // Військовий кур’єр. URL: https://mil.co.ua/avtomatyzovana-systema-upravlinnya-vijskamy-zbroya-peremogy/?utm_source=chatgpt.com.

6. Купер Т. Будь-який радар, який вмикається нині на території України, стає видимим для цілої системи ворожих засобів радіотехнічної та сигнальної розвідки. URL: https://tyzhden.ua/tom-kuper-bud-iakyj-radar-iakyj-vmykaietsia-nyni-na-terytorii-ukrainy-staie-vydymym-dlia-tsiloi-systemy-vorozhykh-zasobiv-radiotekhnichnoi-ta-syhnalnoi-rozvidky/.

7. Коломієць В. Українську систему ситуаційної обізнаності презентували на щорічному заході НАТО. Про що йдеться? 2022.URL: https://hromadske.ua/posts/ukrayinsku-sistemu-situacijnoyi-obiznanosti-prezentuvali-na-shorichnomu-zahodi-nato-pro-sho-jdetsya (дата звернення: 01.06.2024).

8. Данилов О. Унікальну українську систему ситуаційної обізнаності Delta презентували на щорічному заході НАТО. 2022. URL: https://mezha.media/2022/10/28/delta-for-nato/ (дата звернення: 01.06.2024).

9. Найєм М. Істерика російських пропагандистів, або Чому орки бояться Дельти. 2022. URL: https://www.pravda.com.ua/columns/2022/11/2/7374610/.

10. Морфінов С. Delta для ЗСУ: Що відомо про новітню систему управління української армії. 2023. URL: https://www.bbc.com/ukrainian/features-64585182.

11. Аеророзвідка. Система ситуаційної обізнаності «Дельта». URL: https://dou.ua/lenta/projects/ukrainian-miltech-guide/.

12. Асоціація виробників озброєння та військової техніки України. ГІС “Арта”, 2018. URL: https://audm.org.ua/pidpriyemstva/gis-arta/.

13. ГІС Арта. Автоматизована система управління військами. URL: https://dou.ua/lenta/projects/ukrainian-miltech-guide/.

14. Griselda. Програмний ШІ-комплекс. URL: https://dou.ua/lenta/projects/ukrainian-miltech-guide/.

15. Mantis Analytics. Платформа моніторингу інформації на основі ШІ. URL: https://dou.ua/lenta/projects/ukrainian- miltech-guide/.

16. Кобзан С., Поморцева О., Паньків В., Андронов В. Погляди щодо побудови геоінформаційної системи для використання у Збройних Силах України // Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2024. Том 2. № 3 (83). С. 40–46. DOI: https://doi.org/10.33099/2304-2745/2024-3-83/40-46.

Надійшла до редколегії 21.04.2026.
Схвалена до друку 22.05.2026.
Дата публікації 29.05.2026.