The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Received: *September 14, 2025* | **Revisions Requested: -** | **Revision Received:** -
Accepted: *December 1, 2025* | **Published Online:** *April 10, 2026*

Licensed (C) by Creative Commons Attribution International License 4.0 (CC BY-NC-SA)

DOI: 10.62524/msj.2026.4.1.17

Рекомендації щодо забезпечення інтероперабельності ситуаційних центрів України

Олексій Соломицький
доктор військових наук, професор
начальник відділу – заступник начальника управління
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: solosa1@gmail.com
ORCID: 0000-0001-8061-8895

Андрій Ігнатьєв
кандидат наук з державного управління
докторант
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: ertya1978@gmail.com
ORCID: 0000-0002-0482-6024

Максим Кудрицький
доктор військових наук
начальник відділу – заступник начальника управління
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: kma_13@ukr.net
ORCID: 0000-0003-1554-4732

Володимир Коваль
кандидат військових наук, старший науковий співробітник
e-mail: vladimerkoval69@gmail.com
ORCID: 0000-0002-6209-6779

Денис Молчанов
науковий співробітник науково-дослідної лабораторії
кафедри військової підготовки
Державний університет “Київський авіаційний інститут”
03048, вулиця Медова, 1, Київ, Україна
e-mail: mdbua2@gmail.com
ORCID: 0009-0007-9268-2764

Анотація. Актуальність дослідження зумовлена зростанням ролі ситуаційних центрів у системі забезпечення національної та воєнної безпеки України, а також необхідністю їх

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

ефективної взаємодії в умовах цифровізації управління та інтеграції до європейського й євроатлантичного безпекового простору. Розгалужена мережа ситуаційних центрів різних органів державної влади та сектору безпеки і оборони потребує узгоджених технологічних, організаційних та правових рішень, які забезпечують можливість обміну інформацією, спільного використання сервісів та однакового розуміння даних. Через наявність значної гетерогенності технічних засобів, програмного забезпечення та інформаційних ресурсів, а також відсутність уніфікованих підходів до оцінювання рівня взаємосумісності таких систем є потреба в розробленні науково обґрунтованих методичних рекомендацій щодо забезпечення інтероперабельності ситуаційних центрів України на національному та міжнародному рівнях. У дослідженні використано комплекс загальнонаукових та спеціальних методів, зокрема системний аналіз, структурно-функціональний підхід, методи наукової абстракції та узагальнення, аналіз нормативно-правових актів і міжнародного досвіду функціонування інформаційно-аналітичних систем моніторингу безпеки, а також експертні методи оцінювання. Методологічною основою дослідження є концепція інтероперабельності інформаційних систем, що передбачає узгодження правового, організаційного, семантичного та технічного рівнів взаємодії між системами моніторингу та ситуаційними центрами. У результаті дослідження обґрунтовано підхід до формування моделі верифікації інтероперабельності ситуаційних центрів України, який передбачає систематизацію вимог щодо взаємосумісності на різних рівнях, експертне оцінювання відповідності ситуаційних центрів цим вимогам та визначення інтегральних показників інтероперабельної придатності і релевантності. Запропоновано послідовність етапів методики оцінювання рівня інтероперабельності, що дозволяє кількісно та якісно визначати ступінь взаємодії ситуаційних центрів між собою, з Головним ситуаційним центром України та з інформаційно-аналітичними системами міжнародних партнерів. Отримані результати створюють передумови для підвищення ефективності функціонування системи моніторингу воєнної безпеки, удосконалення інформаційного забезпечення управлінських рішень та формування єдиного інформаційного простору у сфері безпеки і оборони. Результати дослідження можуть бути корисними для органів державної влади, суб’єктів сектору безпеки і оборони, наукових установ та аналітичних центрів, що займаються питаннями розвитку ситуаційних центрів, цифрової трансформації системи управління безпекою, створення інформаційно-аналітичних систем моніторингу та забезпечення сумісності інформаційних систем у контексті інтеграції України до безпекових структур ЄС і НАТО.

Ключові слова: воєнна безпека, ситуаційні центри, інтероперабельність, інформаційні системи, моніторинг воєнної безпеки, цифрове врядування, інформаційна взаємосумісність, сектор безпеки і оборони, інформаційно-аналітичні системи.

Вступ (Introduction)

У сучасних умовах трансформації безпекового середовища та зростання ролі інформаційно-аналітичних систем у процесах державного управління особливе значення має розвиток ситуаційних центрів як ключових елементів системи моніторингу та реагування на загрози національній безпеці. Ситуаційні центри забезпечують збирання, оброблення, аналізування і поширення інформації щодо стану безпекового середовища, що створює підґрунтя для підготовки та прийняття управлінських рішень на стратегічному, оперативному та тактичному рівнях. У контексті інтеграції України до європейського та євроатлантичного безпекового простору актуальним є питання забезпечення ефективної взаємодії між ситуаційними центрами різних органів державної влади, а також їх сумісності з аналогічними системами міжнародних партнерів.

Водночас функціонування мережі ситуаційних центрів України характеризується

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

значною різнорідністю технічних засобів, програмного забезпечення, інформаційних ресурсів і процедур оброблення даних. Така гетерогенність ускладнює обмін інформацією між системами, знижує ефективність їхньої взаємодії та створює бар'єри для формування єдиного інформаційного простору у сфері безпеки і оборони. У зв'язку із цим особливої ваги набуває проблема забезпечення інтероперабельності ситуаційних центрів, що передбачає досягнення їхньої взаємосумісності на правовому, організаційному, семантичному та технічному рівнях.

Огляд літератури (Literature review)

Проблематика інтероперабельності інформаційних систем, зокрема систем ситуаційних центрів та систем моніторингу безпеки, активно досліджується у наукових працях, присвячених цифровому врядуванню, інформаційним технологіям та управлінню у сфері безпеки. Значна частина досліджень зосереджена на формуванні концептуальних підходів до побудови взаємосумісних інформаційних систем та механізмів їх інтеграції у складні розподілені інформаційно-аналітичні середовища.

Питання інтероперабельності інформаційних систем державного управління та цифрового врядування ґрунтовно розглянуто у працях міжнародних дослідників і міжнародних організацій. Зокрема, у межах Європейської інтероперабельної рамки визначено основні рівні забезпечення взаємосумісності – правовий, організаційний, семантичний і технічний, що створюють основу для інтеграції державних інформаційних систем різних країн та організацій [1]. Подібні підходи застосовуються також у дослідженнях, присвячених архітектурам цифрового врядування та розвитку платформ державного управління, у яких підкреслюється важливість інтеграції інформаційних ресурсів та узгодженості інформаційних процесів між різними органами влади [2].

У наукових працях, присвячених інформаційним системам безпеки, значна увага приділяється ролі інформаційно-аналітичних та ситуаційних центрів у процесах моніторингу, аналізу та підтримки прийняття управлінських рішень. Дослідники зазначають, що ситуаційні центри є інтеграційними елементами систем управління безпекою, оскільки забезпечують об'єднання різнорідних джерел інформації, аналітичних інструментів та механізмів реагування на кризові ситуації [3]. У роботах з проблематики управління надзвичайними ситуаціями також підкреслюється значення інформаційних систем підтримки прийняття рішень, які дозволяють оперативно аналізувати великі обсяги даних та формувати узгоджені управлінські рішення [4].

Окремий напрям досліджень пов'язаний із застосуванням стандартів відкритих систем і архітектурних підходів до забезпечення взаємосумісності інформаційних систем. У працях дослідників розглядаються питання використання сервісно-орієнтованих архітектур, стандартів обміну даними та моделей інтеграції інформаційних ресурсів для створення взаємодіючих інформаційних середовищ [5]. Водночас наголошується, що забезпечення інтероперабельності складних організаційно-технічних систем потребує використання комплексних моделей інтеграції підприємств та інформаційних систем [6]. Подібні підходи застосовуються і в межах спеціалізованих моделей взаємосумісності інформаційних систем, які передбачають багаторівневу структуру взаємодії між системами [7].

У працях українських дослідників увага приділяється питанням стратегічного управління у сфері національної безпеки та розвитку інформаційно-аналітичних систем державного управління. Зокрема, дослідження підкреслюють важливість створення інтегрованих систем моніторингу безпеки та розвитку аналітичних інструментів підтримки прийняття управлінських рішень [8]. Також у наукових роботах розглядаються проблеми забезпечення інформаційної безпеки держави та розвитку інформаційної інфраструктури сектору безпеки і оборони [9].

Таким чином, аналіз наукових джерел свідчить про те, що проблема інтероперабельності

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

інформаційних систем є важливою складовою розвитку сучасних систем управління безпекою та цифрового врядування. Разом із тим питання кількісного та якісного оцінювання рівня інтероперабельності ситуаційних центрів, а також розроблення методичних підходів до її верифікації в умовах функціонування системи моніторингу воєнної безпеки України залишаються недостатньо дослідженими, що зумовлює необхідність подальших наукових досліджень у цьому напрямі.

Методологічна основа (Methodological Framework)

Базовим у дослідженні є системний підхід, який дозволив розглядати ситуаційні центри як складні організаційно-технічні системи, що функціонують у межах єдиної системи забезпечення національної та воєнної безпеки. Застосування цього підходу дало можливість визначити місце ситуаційних центрів у структурі інформаційно-аналітичного забезпечення управління безпекою, встановити взаємозв'язки між їхніми елементами та окреслити основні рівні забезпечення інтероперабельності (правовий, організаційний, семантичний і технічний).

Для аналізу структури та функціонування ситуаційних центрів використано структурно-функціональний метод, що дав змогу дослідити їхні складові елементи, функції та інформаційні зв'язки, а також визначити основні вимоги до взаємосумісності інформаційних систем, які забезпечують моніторинг і оцінювання стану безпекового середовища.

У процесі дослідження також застосовано методи аналізу та синтезу, що дозволили узагальнити наукові підходи до забезпечення інтероперабельності інформаційних систем, проаналізувати міжнародний досвід розвитку систем ситуаційної обізнаності та інтегрованих інформаційно-аналітичних систем, а також сформувати цілісне уявлення про напрями розвитку мережі ситуаційних центрів України.

Крім того, у дослідженні застосовано методи наукової абстракції та узагальнення, що дали змогу сформулювати методичні положення щодо верифікації інтероперабельності ситуаційних центрів, визначити послідовність етапів оцінювання її рівня та сформувати інтегральні показники інтероперабельної придатності й релевантності.

Застосування зазначених методів у сукупності забезпечило наукове обґрунтування запропонованого підходу до оцінювання інтероперабельності ситуаційних центрів України та створило методичну основу для подальшого удосконалення системи інформаційно-аналітичного забезпечення моніторингу воєнної безпеки.

Результати (Results)

Загальна структура системи ситуаційних центрів передбачає, що для оцінювання стану воєнної безпеки та аналізу результатів реалізації національних інтересів службовцями апарату РНБО України інформація має надходити від ситуаційних центрів нижнього рівня, а також аналогічних центрів наших міжнародних партнерів (ЄС/НАТО), з якими функціонують канали зворотного інформаційного зв'язку та постачання. Прикладом аналогічної системи ЄС є система НАТО – CITCEN, EUROSUR (Агентства Європейської прикордонної і берегової охорони (Frontex)), FIEP (Міжнародна асоціація жандармерії та поліції зі статусом військового формування) тощо [10]. Для отримання такої інформації необхідна технічна та операційна сумісність, здатність різних комп'ютерних систем, пристроїв або програм взаємодіяти та обмінюватися даними між собою, використовуючи уніфіковані інтерфейси або протоколи. Ця здатність дозволяє створювати складні системи з неоднорідних, розподілених компонентів, забезпечуючи їхню спільну роботу – інтероперабельність.

Під *інтероперабельністю ситуаційного центру* розуміємо властивість, що характеризує його експлуатаційну сумісність з іншими ситуаційними центрами та надсистемами: Головним ситуаційним центром України та ситуаційними центрами ЄС/НАТО. Під *верифікацією інтероперабельності ситуаційного центру* розуміємо визначення ступеня його відповідності

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

(тобто релевантність) вимогам, що висуваються до інтероперабельності [11]. Забезпечення інтероперабельності здійснюється в інтересах виявлення та усунення бар'єрів взаємосумісності, тобто перешкод щодо обміну інформацією з іншими суб'єктами, спільного використання сервісів або однакового розуміння обмінних інформаційних елементів.

Забезпеченню інтероперабельності систем різного призначення присвячено невелику кількість наукових та навчально-методичних праць, що зумовлює потребу у більш глибокому дослідженні цього аспекту та у формулюванні відповідних методичних рекомендацій для суб'єктів забезпечення воєнної безпеки, на яких покладається функція моніторингу та оцінювання стану воєнної безпеки.

У [12] зроблено висновок про те, що системи цифрового врядування мають бути інтероперабельними, будуватися на основі стандартів обов'язкового використання, які забезпечують суттєве зменшення витрат під час розроблення нових цифрових управлінських стратегій та систем.

Таким чином, для забезпечення інтероперабельності необхідно на абстрактному рівні використати розроблений науково-методичний інструментарій для діагностування її поточного стану, визначення потенціалу розвитку та вимірювання управлінських впливів. Як такий інструментарій запропоновано використовувати модель верифікації інтероперабельності.

Загалом інтероперабельність обладнання, мереж, програмних засобів, інформації та режимів роботи є необхідною умовою нормального функціонування ситуаційних центрів України, адже отримання первинної інформації про стан безпекового середовища (обстановку), своєчасне її постачання до розгалуженої мережі споживачів (до суб'єктів забезпечення безпеки на місцевому, національному, міждержавному та міжнародному рівнях) і подальше її використання для ефективного реагування на загрози (ситуації), а також обмін іншою актуальною інформацією є сутністю призначення самої системи моніторингу і невід'ємним принципом функціонування механізмів забезпечення воєнної та міжнародної безпеки.

Тобто справедливо констатувати, що забезпечення інтероперабельності є однією з головних засад формування, розвитку та інтеграції ситуаційних центрів України (особливо в частині автоматизації та інформатизації моніторингових досліджень).

Високий рівень інтероперабельності може досягатися за рахунок низького рівня гетерогенності систем. Однак за результатами проведеного авторами [11–12] аналізу стану існуючої технічної та технологічної складової моніторингу й оцінювання стану воєнної безпеки України виявлено, що ситуаційні центри характеризуються високим рівнем внутрішньої гетерогенності, яку, зокрема, зумовлено такими чинниками: необхідність забезпечення воєнної безпеки у різних її визначальних сферах, умовах безпекового середовища та порівняно широкого спектру різнорідних загроз; наявність великої кількості як сучасних, так і морально й фізично застарілих вітчизняних та закордонних моніторингових технологій на об'єктах відповідальності; "хронічне" недофінансування затверджених урядом програм та планів щодо створення моніторингової інфраструктури, недостатнє ресурсне забезпечення; спроби побудови локальних моніторингових систем на окремих об'єктах відповідальності суб'єктів забезпечення національної та, зокрема, воєнної безпеки, здебільшого, не досягли очікуваного результату з різних причин (несумісність програмно-апаратних засобів тощо); відсутність загальної концепції (концептуального проєкту) та систематизованих технологічних рішень щодо побудови єдиної централізованої інформаційно-телекомунікаційної системи моніторингу стану воєнної безпеки України; брак досліджень щодо побудови єдиної моніторингової системи.

Закономірно, що такий стан внутрішньої гетерогенності у діяльності ситуаційних центрів України не сприяє належному рівню їхньої взаємодії як між собою, так і з Головним

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

ситуаційним центром України, а також із системами моніторингу регіональної безпеки ЄС/НАТО.

Отже, на початковому етапі побудови моделі верифікації інтероперабельності ситуаційних центрів України адаптуємо до умов їх дослідження базову модель інтероперабельності [1] (рис. 1), а також врахуємо відомий та апробований спосіб послідовного використання принципів відкритих систем і методології функціональної стандартизації, який має широке застосування як для систем промислової автоматизації, так і для створення взаємосумісних систем широкого класу за масштабами та сферами застосування.

Правовий (юридичний) рівень. Кожна державна адміністрація під час реалізації функцій державного управління працює у власній національній правовій системі. Аналогічно, діяльність окремих суб'єктів забезпечення воєнної безпеки регламентується як загальним, так і спеціальним законодавством. Правова взаємосумісність полягає у тому, щоб забезпечити можливість суб'єктів, що працюють у різних правових рамках, політиках та стратегіях, виконувати завдання спільно. Своєю чергою, це зумовлює потребу у чіткому визначенні положень щодо шляхів подолання відмінностей у законодавстві та правових рамках, включаючи можливість ухвалення нових законів та інших нормативно-правових актів.

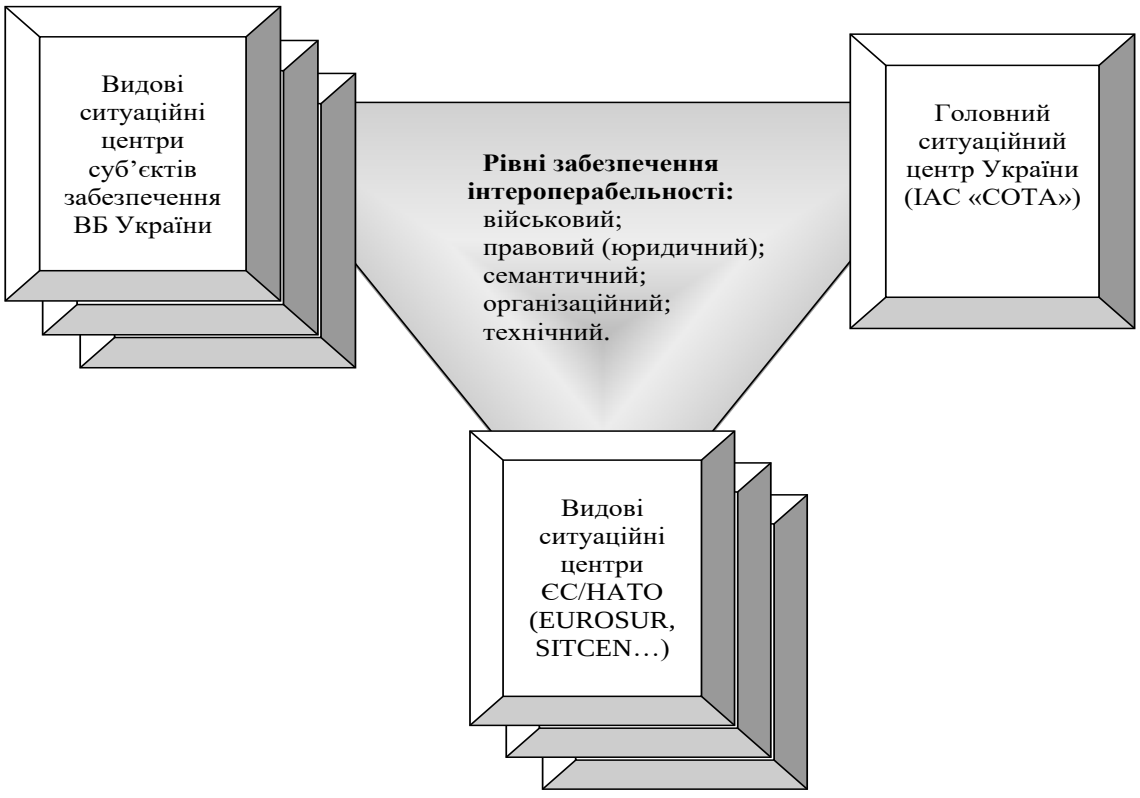


Рисунок 1. Базова модель інтероперабельності ситуаційних центрів України в контексті її європейської та євроатлантичної інтеграції

Першим кроком на шляху до вирішення проблеми правової взаємосумісності є проведення "аудиту сумісності" шляхом аналізу чинного законодавства для виявлення бар'єрів взаємосумісності, таких як галузеві або географічні обмеження у використанні та зберіганні даних, різні та "розмиті" ліцензійні відомості, надмірні обмеження щодо використання конкретних цифрових технологій чи режими їх постачання, суперечливі вимоги

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

до однакових чи подібних процесів (процедур), застарілі вимоги до рівня безпеки та захисту даних тощо.

Тому правову узгодженість в інтересах забезпечення сумісності слід аналізувати перед ухваленням концептуальних (стратегічних) рішень, а також регулярно оцінювати ефективність заходів щодо подальшого наближення стандартів після введення рішень у дію.

Зважаючи на те, що взаємодія державних інформаційних систем, зокрема, забезпечується цифровими каналами та інформаційно-комунікаційними технологіями, питання взаємосумісності на рівні законів та інших нормативно-правових актів слід розглядати якомога раніше, а відповідні документи мають пройти "цифрову перевірку". Зокрема, необхідно: переконатися, що документ відповідає вимогам не лише фізичного, а й цифрового середовища (наприклад, Інтернет); виявити будь-які перешкоди для цифрового обміну; визначити та оцінити вплив документа на інформаційно-комунікаційні технології стейкголдерів.

Це сприятиме взаємодії між державними службами на нижчих рівнях (семантичному, технічному, організаційному), а також збільшить потенціал для повторного використання існуючих рішень в галузі інформаційно-комунікаційних технологій, скоротивши ресурсні витрати та час на впровадження.

У разі зовнішньої взаємодії (з іноземними державами або міжнародними організаціями) юридична цінність будь-якої інформації, якою обмінюються, має зберігатися, має дотримуватися законодавство про захист даних як у державах походження інформації, так і її прийняття. Це може зумовити потребу в укладанні додаткових угод для подолання потенційних розбіжностей у застосуванні чинного законодавства.

Семантичний рівень. Цей рівень описує семантичні аспекти взаємодії, тобто змістовну сторону інформації, якою обмінюються системи. Семантична взаємосумісність – це здатність будь-яких взаємодіючих у процесі комунікації інформаційних систем однаковим чином розуміти сенс інформації, якою вони обмінюються. Тобто семантична взаємосумісність дозволяє системам комбінувати отриману інформацію з іншими інформаційними ресурсами і обробляти її смисловий зміст. Семантичної взаємосумісності може бути досягнуто, якщо застосувати стандарти розширюваної мови розмітки типу XML (зокрема XSLT, XAML, XUL, RSS, MathML, GraphML, XHTML, SVG, XML Schema).

Організаційний рівень фокусує увагу на прагматичних аспектах горизонтальної та вертикальної взаємодії ситуаційних центрів. На цьому рівні узгоджуються стратегічні цілі і досягаються угоди (меморандуми) про співпрацю між адміністративними органами, які мусять (або мають намір) обмінюватися інформацією, хоча мають різні внутрішню структуру і процеси. Організаційна взаємосумісність має на меті задовольнити вимоги спільноти користувачів: служби мають бути доступними, легко ідентифікуватися і бути орієнтованими на користувача. Організаційна взаємосумісність досягається шляхом застосування нормативно-правових документів (угод, конвенцій, договорів (меморандумів, протоколів) про співпрацю, стратегій тощо). Тобто організаційна взаємосумісність – це здатність брати участь у досягненні спільних цілей на рівні процесів (процедур).

Технічний рівень. Технічна взаємосумісність – здатність до обміну даними між системами, що беруть участь в обміні. Технічний рівень описує синтаксис або формати переданої інформації, фокусуючи увагу на тому, яким чином представлено інформацію в комунікаційному середовищі. Технічний рівень включає *такі ключові аспекти*, як відкриті інтерфейси, служби зв'язку, інтеграція даних і проміжний шар програмного забезпечення (Middleware), уявлення та обмін даними, служби доступу та захисту інформації. Технічна взаємосумісність досягається, головним чином, завдяки використанню стандартних протоколів зв'язку типу TCP/IP.

Основні етапи удосконаленого підходу забезпечення взаємосумісності відображено на

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

рис. 2. Сутність удосконалення існуючого підходу, задекларованого у документі ЄС [1], полягає у включенні після кожного етапу забезпечення взаємосумісності обов'язкових опитувань ключових стейкголдерів (замовників, постачальників, розробників, споживачів, персоналу, що супроводжує інформаційні системи і використовує програмне забезпечення та відповідні послуги), з метою виявлення та усунення проблемних питань, а також уможливлення впливу на результати попередніх етапів для їх покращення.

Послідовна реалізація етапів має привести до створення інтероперабельної мережі ситуаційних центрів.

Проте означений підхід не дозволяє кількісно оцінити стан інтероперабельності. Розуміння рівня інтероперабельності не відображається бінарними варіантами на зразок "так" або "ні" через багатоаспектність цього явища. Оскільки інтероперабельність не є фізичною величиною, її критерії (показники) мають визначатися на основі експертного оцінювання. Водночас найбільш дієвими виявляються шкали порядку або інтервалів, а також нечіткі шкали. Для зручності оцінювання рівня інтероперабельності прийнято п'ять рівнів оцінювання, які наведено в табл. 1 [1].

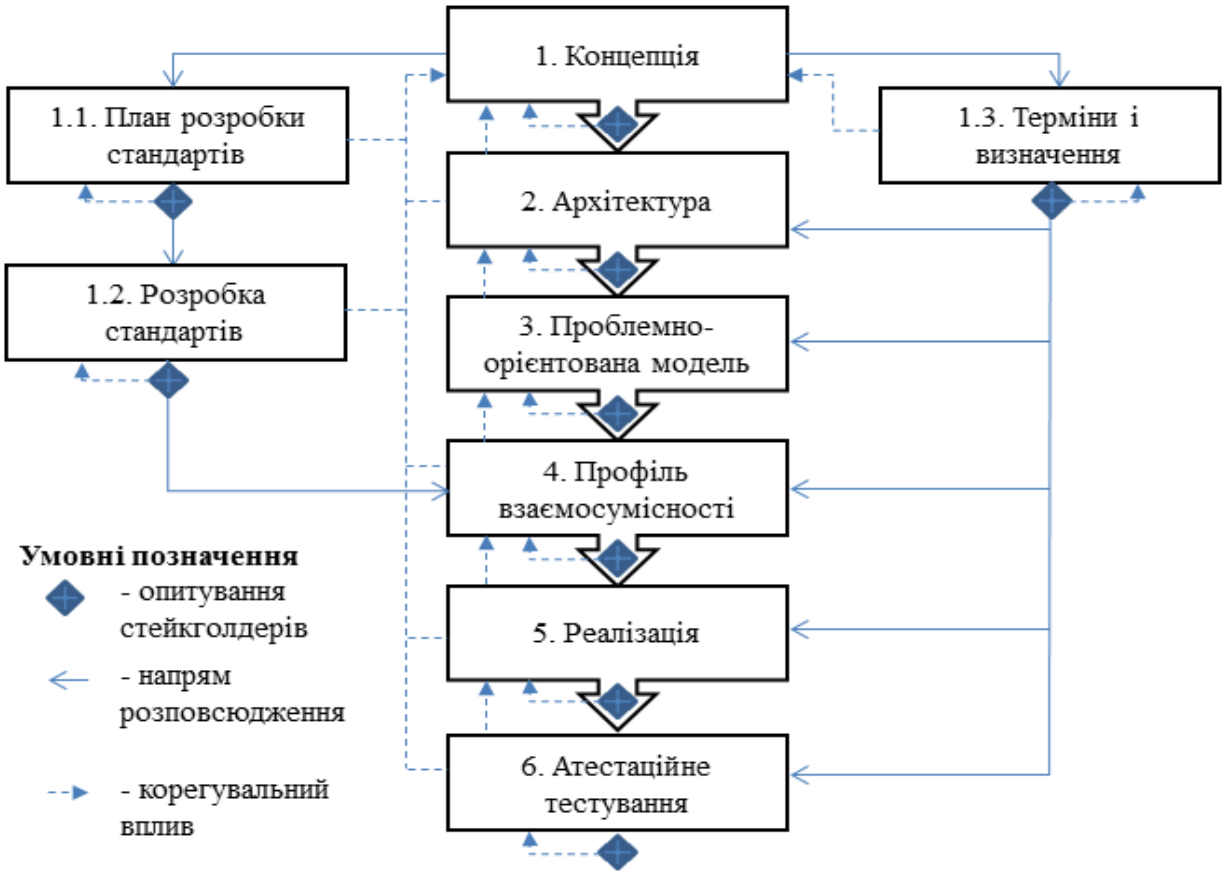


Рисунок 2. Основні етапи забезпечення інтероперабельності ситуаційних центрів України

Загалом забезпечення та верифікація інтероперабельності ситуаційного центру слід здійснювати щодо всіх компонентів (підсистем та елементів) надсистем, що мають зовнішні зв'язки із цими системами на правовому, організаційному, семантичному та технічному рівнях.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Таблиця 1. Рівні оцінювання інтероперабельності

№ рівня	Рівні сумісності	Опис
1	Відсутній	Взаємодія відсутня. Інтероперабельність неможлива та не планується.
2	Мінімальний	Кожна із систем має індивідуальну архітектуру. Інтероперабельність реалізується через специфічні процедури або за тимчасовою схемою.
3	Помірний	Заходів щодо поліпшення сумісності було вжито, але залишається значний потенціал для подальшого удосконалення інтероперабельності.
4	Кваліфікований	Зв'язки інтероперабельні. Відсутні лише деякі чинники повної сумісності.
5	Повна сумісність	Досягнуто максимального рівня інтероперабельності.

Висновок (Conclusion)

У статті досліджено проблематику забезпечення інтероперабельності ситуаційних центрів України як важливої передумови ефективного функціонування системи моніторингу та оцінювання стану воєнної безпеки. Проведений аналіз показав, що ситуаційні центри відіграють ключову роль у формуванні інформаційно-аналітичної підтримки процесів прийняття управлінських рішень у сфері національної безпеки, забезпечуючи збирання, оброблення, аналізування і поширення інформації про стан безпекового середовища. Водночас встановлено, що існуюча мережа ситуаційних центрів характеризується значною технічною, програмною та організаційною гетерогенністю, що ускладнює обмін інформацією між системами та знижує ефективність їхньої взаємодії.

У ході дослідження узагальнено теоретичні підходи до розуміння інтероперабельності інформаційних систем та обґрунтовано доцільність використання багаторівневої моделі забезпечення взаємосумісності, яка охоплює правовий, організаційний, семантичний і технічний рівні взаємодії. Визначено основні чинники, що впливають на рівень інтероперабельності ситуаційних центрів, зокрема відмінності у нормативно-правовому регулюванні, різнорідність інформаційно-комунікаційних технологій, відсутність уніфікованих стандартів обміну даними та недостатню координацію інформаційних процесів між суб'єктами сектору безпеки і оборони.

Обґрунтовано методичний підхід до верифікації інтероперабельності ситуаційних центрів України, який передбачає визначення вимог до взаємосумісності на різних рівнях функціонування систем, експертне оцінювання ступеня їх виконання та розрахунок показників інтероперабельної придатності й релевантності. Запропонована послідовність етапів оцінювання дозволяє визначати рівень інтероперабельності ситуаційного центру, встановлювати потенціал його взаємодії з іншими інформаційними системами та визначати напрями подальшого розвитку.

Рекомендації (Recommendations)

Отримані результати можуть бути використані під час формування та розвитку мережі ситуаційних центрів України, удосконалення системи інформаційно-аналітичного забезпечення державного управління у сфері безпеки і оборони, а також у процесі інтеграції національних інформаційних систем моніторингу безпеки з відповідними системами Європейського Союзу та НАТО. Реалізація запропонованих підходів сприятиме підвищенню ефективності обміну інформацією, покращенню координації між суб'єктами сектору безпеки і оборони та розвитку інтегрованої системи ситуаційної обізнаності держави.

Конфлікт інтересів (Conflict of Interest)

Одним із авторів статті є член редакційної колегії. Для уникнення конфлікту інтересів редакційний процес здійснював Олег Семененко.

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Використані джерела

1. European Commission. (2017). *New European interoperability framework: Promoting seamless services and data flows for European public administrations*. Publications Office of the European Union.
2. Janssen, M., & Estevez, E. (2013). Lean government and platform-based governance: Doing more with less. *Government Information Quarterly, 30*, S1–S8.
3. Turoff, M., Chumer, M., Van de Walle, B., & Yao, X. (2004). The design of a dynamic emergency response management information system. *Journal of Information Technology Theory and Application, 5* (4), 1–36.
4. Bui, T., & Sankaran, S. (2001). Decision support systems for situation management. *Communications of the ACM, 44* (1), 84–90.
5. Chen, D., Doumeingts, G., & Vernadat, F. (2008). Architectures for enterprise integration and interoperability: Past, present and future. *Computers in Industry, 59* (7), 647–659.
6. Vernadat, F. (2010). *Enterprise modeling and integration: Principles and applications*. Chapman & Hall.
7. Peristeras, V., & Tarabanis, K. (2004). *The connection, communication, consolidation, collaboration interoperability framework (C4IF) for information systems interoperability*. In Interoperability of Enterprise Software and Applications (pp. 61–72).
8. Горбулін, В., & Качинський, А. (2010). *Стратегічне планування: вирішення проблем національної безпеки*. НІСД.
9. Даник, Ю., Катеринчук, І., & Пічугін, М. (2016). *Інформаційна безпека держави: теорія та практика*. ЖНАЕУ.
10. *Нацгвардія України стала повноправним членом Асоціації FIEP*. https://nangu.edu.ua/news/38987-nacgvardiya-ukraini-stala-povnopravnim-chlenom-asociacii-fiep.
11. Ігнатьєв, А. М., & Купрієнко, Д. А. (2021). *Модель і методика верифікації інтероперабельності системи моніторингу прикордонної безпеки у контексті євроінтеграції України. Сучасні аспекти науки (с. 19–34)*. Т. IV. колективної моногр. (За ред. Є. О. Романенка, І. В. Жукової). ФОП КАНДИБА Т. П.
12. Осьмак, А. С. (2020). *Механізми забезпечення інтероперабельності сервісної діяльності органів публічної влади*. [Дис. докт. філософії, Національна академія державного управління при Президентові України].

References

1. European Commission. (2017). *New European interoperability framework: Promoting seamless services and data flows for European public administrations.* Publications Office of the European Union.
2. Janssen, M., & Estevez, E. (2013). Lean government and platform-based governance: Doing more with less. *Government Information Quarterly, 30*, S1–S8.
3. Turoff, M., Chumer, M., Van de Walle, B., & Yao, X. (2004). The design of a dynamic emergency response management information system. *Journal of Information Technology Theory and Application, 5* (4), 1–36.
4. Bui, T., & Sankaran, S. (2001). Decision support systems for situation management. *Communications of the ACM, 44* (1), 84–90.
5. Chen, D., Doumeingts, G., & Vernadat, F. (2008). Architectures for enterprise integration and interoperability: Past, present and future. *Computers in Industry, 59* (7), 647–659.
6. Vernadat, F. (2010). *Enterprise modeling and integration: Principles and applications.* Chapman & Hall.
7. Peristeras, V., & Tarabanis, K. (2004). *The connection, communication, consolidation,*

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

collaboration interoperability framework (C4IF) for information systems interoperability. In Interoperability of Enterprise Software and Applications (pp. 61–72).
8. Horbulin, V., & Kachynskyi, A. (2010). *Stratehichne planuvannia: vyrishennia problem natsionalnoi bezpeky.* NISD.
9. Danyk, Yu., Katerynchuk, I., & Pichuhin, M. (2016). *Informatsiina bezpeka derzhavy: teoriia ta praktyka.* ZhNAEU.
10. *Natshvardiia Ukrainy stala povnopravnym chlenom Asotsiatsii FIEP*. https://nangu.edu.ua/news/38987-nacgvardiya-ukraini-stala-povnopravnim-chlenom-asociacii-fiep.
11. Ihnatiev, A. M., & Kupriienko, D. A. (2021). *Model i metodyka veryfikatsii interoperabelnosti systemy monitorynhu prykordonnoi bezpeky u konteksti yevrointehratsii Ukrainy. Suchasni aspekty nauky (s. 19–34).* T. IV kolektyvnoi monohr. (Za red. Ye. O. Romanenka, I. V. Zhukovoi). FOP KANDYBA T. P.
12. Osmak, A. S. (2020). *Mekhanizmy zabezpechennia interoperabelnosti servisnoi diialnosti orhaniv publichnoi vlady*. [Dys. d-ra filosofii, Natsionalna akademiia derzhavnoho upravlinnia pry Prezydentovi Ukrainy].

Recommendations for Ensuring the Interoperability of Ukraine's Situation Centers

Oleksii Solomitskyi
Doctor Of Military Sciences, Profesor
Head Of Research Department
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: solosa1@gmail.com
ORCID: 0000-0001-8061-8895

Andrii Ignatiev
Candidate of Technical Sciences in Public Administration, Doctoral Student
National University of Defense of Ukraine
03049, Povitryanykh Sil Avenue, 28, Kyiv, Ukraine
e-mail: ertya1978@gmail.com
ORCID: 0000-0002-0482-6024

Maksym Kudrytskyi
Doctor Of Military Sciences
Head Of Research Department
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: kma_13@ukr.net
ORCID: 0000-0003-1554-4732

Volodymyr Koval
Candidate of Military Sciences, Senior Researcher
e-mail: vladimerkoval69@gmail.com
ORCID: 0000-0002-6209-6779

The Central Research institute
of the Armed Forces of Ukraine

ISSN (print): 2786-9318
ISSN (online): 2786-9326
Military Science. Vol. 4 No.1 (2026)

Denis Molchanov
Researcher
Research Laboratory
Department of Military Training
State University "Kyiv Aviation Institute"
03048, Medova Street, 1, Kyiv, Ukraine
e-mail: mdbua2@gmail.com
ORCID: 0009-0007-9268-2764

Abstract. The relevance of the study is обусловлена by the growing role of situation centers in the system of ensuring Ukraine's national and military security, as well as by the need for their effective interaction in the context of governance digitalization and integration into the European and Euro-Atlantic security space. The extensive network of situation centers operating within various state authorities and the security and defense sector requires coordinated technological, organizational, and legal solutions that enable information exchange, shared use of services, and a common understanding of data. The presence of significant heterogeneity in technical equipment, software, and information resources, as well as the absence of unified approaches to assessing the interoperability level of such systems, necessitates the development of scientifically grounded methodological recommendations for ensuring the interoperability of Ukraine's situation centers at both national and international levels. The study employs a set of general scientific and specialized methods, including system analysis, the structural and functional approach, methods of scientific abstraction and generalization, analysis of regulatory and legal acts and international experience in the functioning of security monitoring information and analytical systems, as well as expert evaluation methods. The methodological basis of the research is the concept of information systems interoperability, which involves the coordination of legal, organizational, semantic, and technical levels of interaction between monitoring systems and situation centers. As a result of the study, an approach to developing a verification model for the interoperability of Ukraine's situation centers has been substantiated. This approach involves the systematization of interoperability requirements at different levels, expert assessment of the compliance of situation centers with these requirements, and the determination of integral indicators of interoperability capability and relevance. A sequence of stages of the methodology for assessing the level of interoperability has been proposed, which makes it possible to quantitatively and qualitatively determine the degree of interaction among situation centers, with the Main Situation Center of Ukraine, and with the information and analytical systems of international partners. The obtained results create the prerequisites for improving the efficiency of the military security monitoring system, enhancing the information support of managerial decision-making, and forming a unified information space in the field of security and defense. The results of the research may be useful for public authorities, entities of the security and defense sector, research institutions, and analytical centers engaged in the development of situation centers, the digital transformation of the security governance system, the creation of security monitoring information and analytical systems, and the interoperability of information systems in the context of Ukraine's integration into the security structures of the EU and NATO.

Keywords: military security, situation centers, interoperability, information systems, military security monitoring, digital governance, information interoperability, security and defense sector, information and analytical systems.