УДК: 355.45:004.8 DOI: **10.33099/2311-7249/2026-55-1-167-178**

ШЕРСТЮК Євген Іванович,
Національний університет оборони України, Київ, Україна,
https://orcid.org/0009-0009-5111-7747

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ МІНІСТЕРСТВА ОБОРОНИ УКРАЇНИ В СИСТЕМІ КРИЗОВОГО РЕАГУВАННЯ

Метою статті *є розроблення структурної схеми інформаційної технології підтримки прийняття рішень для Міністерства оборони України в системі кризового реагування на основі аналізу теоретико-методологічних засад побудови інтегрованих систем інформаційної підтримки управлінських рішень у сфері оборони України та країн членів НАТО для забезпечення ефективного реагування на кризові ситуації в умовах сучасних безпекових викликів.*

Методи досліджень. *Для досягнення поставленої мети застосовано комплекс методів наукового пізнання: системний аналіз – для дослідження структури та взаємозв'язків компонентів системи інформаційної підтримки; порівняльний аналіз – для зіставлення вітчизняного та міжнародного досвіду впровадження систем підтримки прийняття рішень; метод експертних оцінок – для визначення вагових коефіцієнтів у математичних моделях; математичне моделювання – для формалізації процесів оцінювання надійності інформації та готовності системи.*

Отримані результати дослідження. *Здійснено аналіз основних нормативно-правових, інституційних і технологічних чинників, що визначають сучасний стан і перспективи розвитку таких систем. Визначено основні невідповідності між наявними практиками інформаційної підтримки та вимогами до сучасних систем підтримки прийняття рішень у сфері оборони. Наведено матрицю невідповідностей і окреслено шляхи вдосконалення інституційної архітектури, нормативної бази та технологічної модернізації. Запропоновано дві математичні моделі: інтегрований індекс надійності стосовно оцінювання достовірності інформації та індекс готовності системи для кількісної оцінки ступеня наближення поточної системи інформаційної підтримки до цільового стану. Показано важливість інтеграції штучного інтелекту та ситуаційних центрів як базових елементів інформаційної підтримки управлінських рішень в умовах гібридних загроз. Наведено структурну схему інформаційної технології підтримки прийняття рішень для Міністерства оборони України в системі кризового реагування.*

Наукова новизна *полягає у розробленні структурованого підходу до ідентифікації організаційних і технологічних розривів у системах підтримки прийняття рішень через впровадження спеціалізованої матриці невідповідностей. Уточнено та формалізовано нові кількісні показники (індекси), які дають змогу об'єктивно оцінювати як надійність вхідної інформації, так і рівень зрілості всієї системи інформаційної підтримки в умовах гібридних загроз.*

Теоретичне та практичне значення. *Отримані результати створюють концептуальну основу для модернізації ситуаційних центрів та проєктування систем підтримки прийняття рішень нового покоління. Впровадження запропонованих методичних підходів сприятиме підвищенню точності, швидкості та узгодженості управлінських рішень у кризових ситуаціях, що є критично важливим для забезпечення національної безпеки України.*

Ключові слова: *система підтримки прийняття рішень, інформаційна підтримка, кризове реагування, ситуаційний центр, інформаційна технологія підтримки прийняття рішень, штучний інтелект, міжвідомча взаємодія, надійність інформації.*

Вступ

Постановка проблеми. У XXI столітті кризові ситуації стають дедалі складнішими та динамічнішими, істотно впливаючи на функціонування сектору безпеки та оборони. До таких ситуацій належать збройні конфлікти, терористичні акти, кіберінциденти, природні катастрофи, пандемії та інформаційні атаки. Їхньою характерною рисою є високий рівень невизначеності, обмежені часові рамки для реагування та необхідність ухвалення управлінських рішень на основі фрагментарної або суперечливої інформації. В таких умовах ефективність реагування значною мірою залежить від якості інформаційної підтримки процесів управління. Інформація має бути актуальною, достовірною, оперативною й структурованою відповідно до потреб користувачів.

Водночас, незважаючи на створення ситуаційних центрів в органах сектору безпеки та оборони, в Україні досі не існує єдиної методики їх функціонування, уніфікованої системи збору та

верифікації даних, а також загальнодержавного стандарту міжвідомчого обміну інформацією. Оцінювання достовірності інформації передбачає окрему оцінку джерела на надійність та змісту інформації на достовірність. Це ускладнює побудову цілісної системи інформаційної підтримки управлінських рішень, здатної забезпечити ефективне реагування на кризові виклики.

Аналіз останніх досліджень і публікацій. Зарубіжна практика, зокрема, досвід НАТО, США та Великобританії, демонструє ефективність впровадження систем підтримки прийняття рішень Системи підтримки прийняття рішень (Decision Support Systems (далі – DSS)) у сферах військового управління, прогнозування бойових дій, логістики та стратегічного планування [12]. Водночас, вітчизняні науковці, зокрема В. Бочарніков, О. Гудима, Є. Живило, В. Машталір, А. Павліковський, В. Пристайко, Ю. Руснак, С. Свєшніков та Ю. Стужук, досліджують проблематику побудови, функціонування та вдосконалення систем інформаційної підтримки управлінських рішень і ситуаційних центрів в органах сектору безпеки та оборони. Разом із тим, такі системи мають відповідати основним вимогам: оперативності, сумісності, надійності та захищеності [5; 6; 8; 9; 10; 11].

Досвід функціонування Ситуаційного центру Міністерства оборони України (далі – СЦ МО України), висвітлений у працях А. Павліковського, В. Бочарнікова, С. Свєшнікова та О. Гудими, демонструє, що ситуаційний центр (далі – СЦ) виступає моделлю завчасного виявлення та аналізу кризових ситуацій сектору безпеки та оборони [5; 7]. Водночас залишаються актуальними питання удосконалення математичних моделей прогнозування, інтеграції методів системного аналізу та забезпечення нормативно-правової бази функціонування мережі ситуаційних центрів.

Метою статті є розроблення структурної схеми інформаційної технології підтримки прийняття рішень для Міністерства Оборони України в системі кризового реагування на основі аналізу теоретико-методологічних засад побудови інтегрованих систем інформаційної підтримки управлінських рішень у сфері оборони України та країн членів НАТО для забезпечення ефективного реагування на кризові ситуації в умовах сучасних безпекових викликів.

Виклад основного матеріалу дослідження

У державах Північноатлантичного альянсу реалізація інтегрованих систем інформаційної підтримки управлінських рішень здійснюється в межах концепції «Командування, Контроль, Зв'язок, Комп'ютери, Добування, Спостереження та Розвідка» (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR)). Ці системи забезпечують об’єднання різнорідних джерел даних, формування ситуаційної обізнаності, проведення автоматизованого аналізу та підтримку ухвалення рішень на стратегічному, оперативному й тактичному рівнях.

У Збройних Силах США активно впроваджується система «Інструмент спільної підтримки прийняття рішень» (Joint Decision Support Tool (JDST)), яка дає змогу формувати та оцінювати альтернативні варіанти дій у режимі реального часу з використанням імітаційного моделювання та сценарного аналізу. У Великобританії функціонує «Система оперативної підтримки оборони» (Defence Operational Support System (DOSS)), що інтегрує оперативну інформацію, логістичні потоки й інструменти планування операцій.

Перелік стандартизованих інформаційних платформ НАТО містить такий інструментарій розвідки (NATO Intelligence Toolbox), як «Інтегроване командування та управління» (Integrated Command and Control (ICC)), «Логістичні функціональні зони послуг» (Logistics Functional Area Services (LOGFAS)), а також системи, створені на основі «Моделі даних спільного консультування, обміну інформацією командування та управління» (Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM)). Зазначені рішення ґрунтуються на стандартах «Угоди НАТО про стандартизацію» (STANAG) і забезпечують взаємосумісність національних систем DSS під час виконання коаліційних операцій [9].

Серед головних переваг інформаційних систем НАТО слід виокремити модульну архітектуру, що дає змогу адаптувати функціональні можливості відповідно до специфіки завдань конкретної місії та рівня командування. Високий рівень автоматизації суттєво зменшує час підготовки управлінських рішень і мінімізує вплив людського чинника. Згідно з оцінками стратегічного командування НАТО, що відповідає за адаптацію, модернізацію та підвищення боєздатності збройних сил Альянсу (Allied Command Transformation), застосування систем DSS із використанням елементів штучного інтелекту дає змогу скоротити цикл ухвалення рішень на 30–50 % порівняно з традиційними підходами до планування [7].

Накопичений досвід держав-членів НАТО засвідчує доцільність стратегічного впровадження цифрових платформ управління, інтегрованих з джерелами розвідданих, системами зв'язку й аналітичними модулями. Водночас цей досвід підкреслює необхідність формування єдиної архітектури даних, запровадження міжвідомчих протоколів взаємодії та забезпечення належного рівня підготовки персоналу для ефективної експлуатації таких рішень.

Практичний досвід застосування систем інформаційної підтримки управлінських рішень у реальних операціях підтверджує їхню високу ефективність як інструменту скорочення часу реагування та підвищення якості прийнятих рішень. Зокрема, під час багатонаціональних миротворчих операцій НАТО в Косово (KFOR), Афганістані (ISAF), а також у рамках операції «Unified Protector» у Лівії активно використовувалися інтегровані інформаційні системи планування, моделювання та розвідки. Вони забезпечували своєчасне інформування командного складу й автоматизоване оцінювання варіантів дій [9].

Дослідження, проведені після завершення зазначених операцій, засвідчили, що застосування таких систем не лише пришвидшує процес прийняття рішень, але й значно знижує кількість помилкових або суперечливих рішень завдяки автоматизованій верифікації даних, які надходять із різних джерел [7]. Під час операції «Enduring Freedom» в Афганістані особливу увагу надавали використанню інтелектуальних систем аналізу ризиків. Вони давали змогу оперативно виявляти аномальні патерни поведінки противника, прогнозувати зміну обстановки та забезпечувати ефективний розподіл ресурсів у режимі реального часу.

Системи DSS продемонстрували високу ефективність і в цивільних кризових ситуаціях. Наприклад, під час реагування на наслідки урагану «Катріна» у США централізовані платформи обробки інформації забезпечили координацію дій між військовими, урядовими та гуманітарними структурами. Це дало змогу точніше визначити пріоритети допомоги та оптимізувати логістичні маршрути [12].

Отже, досвід провідних країн НАТО підтверджує, що впровадження сучасних систем інформаційної підтримки управлінських рішень у сфері військового управління істотно підвищує здатність до адаптації в умовах криз та знижує ризики прийняття неефективних рішень у ситуаціях із високим рівнем невизначеності.

Україна має передумови для впровадження сучасних систем DSS, зокрема, через досвід створення СЦ і співпрацю з міжнародними партнерами у сфері безпеки. Водночас існує низка проблем, що ускладнюють повномасштабну інтеграцію таких систем. До них належать недостатня інтегрованість інформаційних систем різних органів управління, відсутність стандартизованих протоколів обміну інформацією, обмежений доступ до сучасних технологій і низький рівень підготовки персоналу.

Узагальнення результатів аналізу проблемного поля дає змогу виділити основні розриви між поточним станом системи інформаційної підтримки управлінських рішень МО України та її бажаною (цільовою) моделлю. Це дає змогу не лише чітко визначити об'єкт подальшого дослідження, а й сформувати структуровані напрями вдосконалення (табл. 1).

Таблиця 1

Аналіз стану системи підтримки управлінських рішень Міністерства оборони України

№	Компонент/Функція	Наявний стан	Цільовий стан/Вимоги
1	Нормативно-правове забезпечення	Фрагментарне, без єдиного базового закону чи стандартів DSS	Єдина нормативна рамка з визначеним статусом DSS та процедурою взаємодії
2	Інституційна архітектура	Відсутність координаційного органу з повноваженнями інтеграції DSS	Встановлена вертикаль відповідальних органів, інтеграція на рівні МО України та РНБО України*
3	Інформаційна сумісність між відомствами	Відсутність уніфікованих стандартів форматів даних, різні інформаційні системи	Стандартизовані протоколи даних, єдине інформаційне середовище
4	Технологічна база (DSS, IAT, AI)	Локальні рішення, часто без інтеграції штучного інтелекту та моделювання сценаріїв	Використання інтелектуальних систем, прогнозних моделей, пояснюваного штучного інтелекту
5	Кадрове забезпечення та аналітична спроможність	Брак фахівців з роботи з великими даними, штучним інтелектом, геопросторовими даними	Система підготовки аналітиків DSS з профільною освітою
6	Рівень автоматизації процесів	Багато операцій виконується вручну або через розрізнені засоби	Автоматизоване оброблення даних, інтегровані інформаційно-аналітичні технології з уніфікованим інтерфейсом
7	Кіберзахищеність систем	Кіберзахисту фрагментарний, обмежена виявлюваність атак	Багаторівнева система кіберзахисту з активним моніторингом

* Рада національної безпеки та оборони України.

Для подолання зазначених перешкод доцільно розробити національну стратегію впровадження DSS, що передбачатиме чіткі стандарти взаємодії, програми підготовки фахівців і поетапне технічне переоснащення структур безпеки та оборони. Це уможливить ефективніше реагування України на сучасні виклики та забезпечення високого рівня національної безпеки.

У цій статті, під *інформаційною підтримкою управлінських рішень* слід розуміти систематизовану діяльність, спрямовану на забезпечення керівників усіх рівнів управління достовірною, актуальною та структурованою інформацією, необхідною для прийняття обґрунтованих управлінських рішень. Вона охоплює сукупність методів, засобів і технологій збору, обробки, аналізу, зберігання та подання інформації, що використовується в процесі управління [2]. Основна мета інформаційної підтримки полягає у зниженні рівня невизначеності під час ухвалення рішень, підвищенні

обґрунтованості та оперативності реагування в динамічному середовищі, особливо, в умовах кризових ситуацій. До основних елементів інформаційної підтримки належать [5]:

інформаційні джерела – канали отримання даних, зокрема системи спостереження, розвідки, оперативного моніторингу, а також відкриті джерела та внутрішні інформаційні бази;

технології збору інформації – інструменти для автоматизованого або напівавтоматизованого збирання, фільтрації та агрегування даних з різнорідних джерел у часі, наближеному до реального;

аналітичні системи – програмно-алгоритмічні комплекси, що забезпечують глибокий аналіз, оцінювання ризиків, моделювання сценаріїв розвитку подій, прогнозування результатів управлінських рішень;

інтерфейси візуалізації та подання інформації – інформаційні панелі, карти, звіти, адаптовані до потреб користувачів відповідно до рівня управління, що дають змогу швидко сприймати основні висновки та тенденції.

Ефективна інформаційна підтримка має бути орієнтована на потреби кінцевих користувачів – командирів, аналітиків, державних службовців. Надзвичайно важливим є дотримання принципів доступності, релевантності, повноти, оперативності та надійності інформації [3]. Отже, сучасна інформаційна підтримка управлінських рішень у системі кризового реагування має ґрунтуватись на інтегрованому підході, поєднуючи технології обробки великих обсягів даних, засоби штучного інтелекту, аналітичне моделювання та адаптивні інтерфейси, здатні підтримувати керівника в умовах багатофакторного вибору та обмеженого часу [1].

Формування ефективної інформаційної підтримки вимагає наявності структури, яка б визначала логіку руху інформаційних потоків, розподіл функцій між суб'єктами управління та послідовність етапів опрацювання інформації. Така структура інформаційної технології є основою для побудови єдиної цифрової системи управління, що відповідає сучасним вимогам оперативності, адаптивності та міжвідомчої координації (рис. 1).

Основними елементами технології є:

інформаційний простір – сукупність джерел і каналів даних про оперативну обстановку, моніторингові платформи, дані розвідки, геопросторову інформацію тощо;

центри обробки та аналізу – аналітичні вузли, що забезпечують первинну фільтрацію, верифікацію, інтеграцію даних і генерування інформаційних продуктів для управлінських рішень;

суб'єкти прийняття рішень – органи військового управління, органи виконавчої влади, органи цивільного захисту, які використовують інформаційні продукти відповідно до своєї компетенції;

зворотний зв'язок – механізм оцінки ефективності реалізованих рішень та оновлення вихідних даних для наступних управлінських циклів.

Наведена на рис. 1 технологія має функціонувати в умовах постійної невизначеності, високої динаміки подій і багаторівневої координації. Тому, важливо закладати в її основу принципи інформаційної сумісності, кіберстійкості, адаптивного аналізу та оперативного доступу до даних [2]. Використання такої структури сприяє підвищенню ефективності усіх етапів управлінського процесу – від збору інформації до реалізації та оцінювання рішень, здатну забезпечити стійкість системи до реагування у кризових ситуаціях.

В умовах кризового реагування особливе значення набувають ситуаційні центри – спеціалізовані організаційно-технічні структури, що забезпечують координацію, моніторинг, аналіз і оперативну підтримку прийняття управлінських рішень. Вони функціонують як основні вузли інтеграції інформаційних потоків і формують базу для розроблення сценаріїв реагування, оцінювання ризиків і прогнозування розвитку подій [3].Проведений аналіз засвідчує, що головними чинниками ефективності ситуаційних центрів є не лише рівень технологічної оснащеності, а й, передусім, їхнє функціональне включення до загальної системи оборонного управління та здатність здійснювати аналітичну трансформацію даних у релевантні управлінські продукти. Ситуаційні центри, що інтегрують засоби ситуаційного моделювання, методи прогнозування на основі багатофакторного аналізу та оперативної візуалізації даних, демонструють вищу здатність до своєчасного реагування на кризові виклики та прийняття рішень в умовах високої невизначеності [2]. На сучасному етапі актуальним є питання розроблення науково-обґрунтованих підходів до стандартизації функціоналу ситуаційних центрів, визначення їхньої ролі в системі управління оборонного відомства та оцінювання впливу аналітичних продуктів на якість рішень.

Дослідження [6] демонструє концептуальний підхід до формування організаційної структури СЦ МО України, що передбачає створення спеціалізованих підрозділів для моніторингу, аналізу та прогнозування. Функціонування СЦ МО України являє собою модель завчасного виявлення та аналізу кризових ситуацій сектору безпеки держави. Досвід України, зокрема функціонування СЦ МО України та регіональних ситуаційних підрозділів, що діють у межах координації з Головним ситуаційним центром при Раді національної безпеки та оборони України (далі – ГСЦ РНБО України), демонструє, що такі центри можуть стати основою для побудови національної системи кризового управління. Проте, ефективність їх діяльності, значною мірою, залежить від рівня автоматизації, оперативного доступу до баз даних, технічної інфраструктури та рівня підготовки персоналу. У контексті гібридних загроз і багатоаспектних криз СЦ мають розвиватися за напрямом інтеграції з цифровими платформами DSS, мати доступ до джерел розвідки на основі відкритих джерел (Open Source Intelligence (OSINT)), використовувати аналітику на основі штучного інтелекту (далі – ШІ) та підтримувати сценарне планування дій. Тому, СЦ виступають критичним елементом інформаційно-аналітичної підтримки управління, здатним забезпечити стабільність, адаптивність і стратегічну стійкість у період криз.

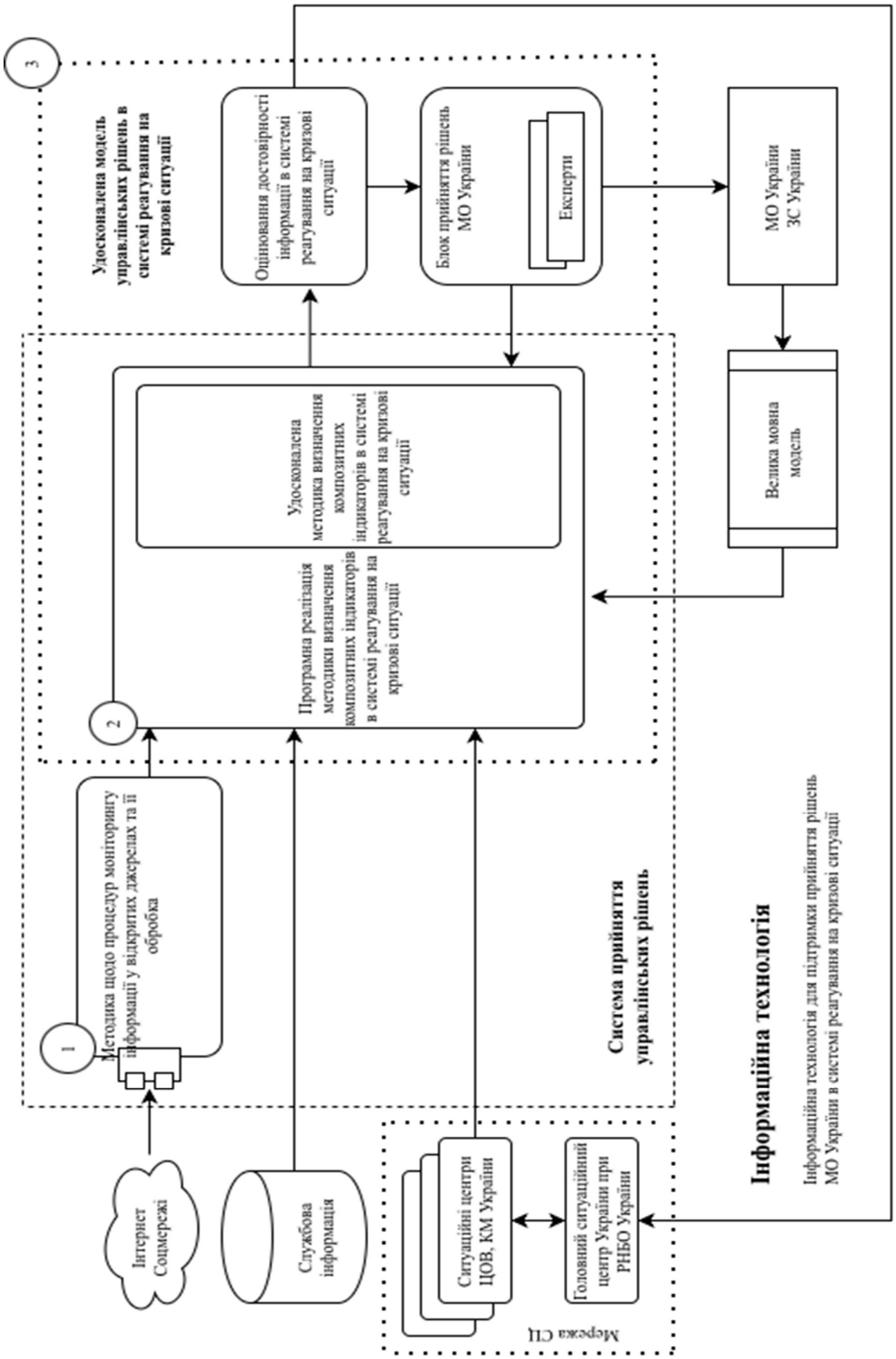

Рисунок 1 – Структурна схема інформаційної технології підтримки прийняття рішень Міністерства оборони України в системі кризового реагування

Інституціональна модель забезпечення інформаційної підтримки управлінських рішень у секторі оборони України формується в межах взаємодії уповноважених органів, закріплених у чинному законодавстві та стратегічних документах. До провідних суб'єктів належать Міністерство оборони України, Генеральний штаб Збройних Сил України, Головне управління розвідки Міністерства оборони України, Державна служба спеціального зв'язку та захисту інформації України, ГСЦ РНБО України, а також відомчі ситуаційно-аналітичні центри [6].

Нормативну базу функціонування цієї системи складають: Указ Президента України «Про удосконалення мережі ситуаційних центрів та цифрову трансформацію сфери національної безпеки і оборони» від 18 червня 2021 року № 260/2021, Постанова Кабінету Міністрів України «Питання мережі ситуаційних центрів» від 11 липня 2023 року № 705, а також Стратегія воєнної безпеки України від 25 березня 2021 року № 121/2021. У зазначених документах визначено механізми координації, напрями модернізації та цілі щодо підвищення оперативності ухвалення рішень у секторі безпеки та оборони [10; 11]. Проте, незважаючи на існуючі регламенти, спостерігається низка проблем: неузгодженість стандартів обміну інформацією між органами, дублювання функціональних повноважень, обмежений рівень автоматизації процесів аналітичної обробки даних. Крім того, зберігається фрагментарність цифрової інфраструктури, що ускладнює комплексне впровадження DSS-рішень.

У цьому контексті важливим кроком є розроблення нормативно-правового документу, який би регламентував порядок впровадження систем підтримки прийняття рішень з урахуванням сучасних IT-інструментів, зокрема ШІ, та передбачав механізми адаптації до змін середовища безпеки [6].

Нормативно-правова база інформаційної підтримки в оборонному секторі України залишається фрагментованою та потребує подальшої систематизації. Попри наявність окремих положень у стратегічних документах та відомчих актах, питання організації, стандартизації та технічного супроводу інформаційної підтримки не мають комплексного регламентування.

Чинне законодавство України, зокрема, Закони України (зі змінами) «Про національну безпеку» від 21 червня 2018 року № 2469-VIII, «Про оборону України» від 21 червня 2018 року № 2469-VIII, «Про інформацію» від 2 жовтня 1992 року № 2657-XII та «Про захист інформації в інформаційно-телекомунікаційних системах» від 05 липня 1994 року № 80/94-ВР, окреслює лише загальні межі управління інформаційними потоками та обміну даними. Водночас не існує єдиного акту, який би фіксував вимоги до DSS або ситуаційно-аналітичної інфраструктури в системі оборонного управління. На практиці це призводить до того, що запровадження окремих елементів інформаційної підтримки, зокрема, цифрові платформи, не супроводжується уніфікованими стандартами сумісності, інформаційної безпеки, правового режиму використання даних. Крім того, є правова невизначеність щодо відповідальності за аналітичні продукти DSS, їхнього статусу в процедурі ухвалення управлінських рішень та можливостей інтеграції з національною системою кібербезпеки.

У контексті євроатлантичної інтеграції України, постає необхідність гармонізації національного правового поля з відповідними стандартами НАТО та Європейського Союзу, зокрема, STANAG щодо обміну оперативною інформацією та забезпечення сумісності DSS у багатонаціональному середовищі. Для створення сучасної нормативної основи інформаційної підтримки є доцільним розроблення окремого законодавчого акту або рамкового підзаконного документа, що регулюватиме: статус систем DSS і ситуаційних центрів у структурі оборонного управління; вимоги до форматів даних, протоколів обміну та інформаційної безпеки; повноваження органів щодо створення, обслуговування та експлуатації аналітичної інфраструктури; юридичну значимість та обмеження використання результатів DSS у процесі ухвалення рішень; механізми контролю, відповідальності й міжвідомчої координації у сфері цифрової підтримки управління.

Особливого значення набуває розроблення типового положення про ситуаційний центр органу сектору безпеки і оборони [8], що визначає стандарти функціонування, організаційну структуру, повноваження та відповідальність ситуаційного центру. Запровадження такої нормативної бази створить передумови для цілісної архітектури управління у сфері оборони, підвищення якості рішень і адаптивності до сучасних викликів національної безпеки [9]. Україна вже має приклади реалізації ефективних рішень у сфері інформаційної підтримки. Найбільш показовим є функціонування СЦ МО України, який забезпечує оперативний моніторинг, аналітику, формування інформаційних продуктів і координацію дій між підрозділами.

До переваг слід віднести використання багатоджерельної інформації, впровадження інструментів візуалізації, оперативність передачі даних. Водночас залишаються проблеми з уніфікацією протоколів, автоматизацією процесів і кадровим забезпеченням, зокрема у сфері аналітики ШІ. Епізодичні приклади роботи ситуаційних груп у регіонах України, зокрема, під час криз у гуманітарній сфері або у відповідь на атаки по критичній інфраструктурі, засвідчують потенціал до масштабування. Але такі практики потребують інституціоналізації та системного супроводу.

Як підсумок зазначимо, що наразі доцільно створити єдиний стандарт архітектури систем DSS для цивільного й військового секторів та заснувати центр компетенцій з цифрового управління у секторі безпеки і оборони, також потрібна системна підготовка аналітиків, з акцентом на вміння роботи з цифровими платформами й ШІ та посилити інтеграцію відомчих інформаційно-комунікаційних систем із забезпеченням обміну інформацією в часі,

наближеному до реального. Отже, вітчизняна практика роботи СЦ створює основу для формування ефективної та стійкої системи інформаційної підтримки, адаптованої до сучасних викликів.

Інформаційно-аналітичні технології (далі – ІАТ) є базисом сучасних систем підтримки управлінських рішень, особливо в умовах багатофакторної динаміки кризових ситуацій. Вони перетворюють сировинні дані на релевантні знання, що є критично важливими для ухвалення обґрунтованих рішень у сфері оборонного управління [8]. Сучасні ІАТ поділяються за функціональним призначенням щодо:

збору даних – сенсорні мережі, супутниковий моніторинг, системи дистанційного зондування, інструменти вебскрейпінгу та краудсорсингові платформи;

обробки та зберігання великих даних (Big Data) – обчислювальні кластери, хмарні платформи, розподілені сховища;

аналітики – методи статистичного аналізу, машинне навчання, штучні нейронні мережі, алгоритми виявлення аномалій, обробка природної мови (Natural Language Processing (NLP));

візуалізації – інструменти бізнес-аналітики, геоінформаційні системи, що дають змогу інтерактивно представляти аналітичні висновки, моделі та сценарії;

інтеграція – сервіс-орієнтована архітектура (SOA), мікросервіси, програмні інтерфейси (API) для забезпечення з'єднання та обміну даними між різними компонентами DSS.

Окрему категорію становлять когнітивні технології, що базуються на ШІ та забезпечують автоматичну побудову сценаріїв, прогнозування ризиків і оцінювання альтернатив управлінських дій. Їх інтеграція у військове управління суттєво зменшує час реагування, підвищує точність рішень та знижує ризики, пов’язані з суб’єктивними факторами [5; 9]. У контексті сучасних викликів основними вимогами до ІАТ є масштабованість, стійкість до втрат зв’язку, відповідність вимогам інформаційної безпеки. Це зумовлює потребу побудови адаптивної архітектури ІАТ, що спирається на принципи модульності, відмовостійкості та міжвідомчої сумісності.

ШІ дедалі активніше інтегрується в системи підтримки управлінських рішень у сфері національної безпеки й оборони. Його використання забезпечує автоматизовану обробку великих обсягів даних, моделювання сценаріїв, оцінювання ризиків і ухвалення рішень у реальному часі [5; 9]. Головна перевага ШІ полягає у здатності виявляти приховані залежності в гетерогенних даних. Завдяки методам машинного та глибинного навчання створюються моделі, що здатні до самонавчання та адаптації до змін середовища без прямого втручання людини. На рівні оперативного управління, ШІ уможливлює прогнозування обстановки, виявлення аномалій, оцінювання ефективності варіантів дій та підвищення ситуаційної обізнаності. Це, в свою чергу, знижує когнітивне навантаження на командирів, скорочує цикл ухвалення рішень і підвищує синхронізацію дій між структурами. Разом із тим, інтеграція ШІ супроводжується низкою викликів: складність валідації результатів, прийнятих алгоритмами, упередженість даних, відсутність правового регулювання та етична невизначеність щодо розподілу відповідальності між людиною та машиною. Актуальним напрямом досліджень є розроблення моделей пояснюваного ШІ (Explainable AI, XAI), що забезпечують прозорість логіки прийнятих рішень. Це особливо важливо в оборонному управлінні, де наслідки помилок можуть бути критичними.

Отже, ШІ значно розширює аналітичні можливості систем інформаційної підтримки управління, підвищуючи їх адаптивність, швидкодію та обґрунтованість. Його впровадження вимагає не лише технічної інтеграції, а й належного нормативного, етичного та організаційного супроводу.

ІАТ дедалі активніше впроваджуються у практику військового управління, виступаючи інструментом забезпечення ситуаційної обізнаності, планування операцій та підтримки стратегічного ухвалення рішень. Їх застосування охоплює широкий спектр завдань – від тактичного аналізу бойових дій до стратегічного прогнозування безпекових сценаріїв [2]. У контексті оборонного планування ІАТ забезпечують:

оперативне оновлення даних про оперативну обстановку на театрі воєнних дій;

виявлення слабких місць у системах управління військами з використанням аналітичних алгоритмів;

прогнозування розвитку бойових дій залежно від змін оперативної ситуації та варіантів управлінських рішень;

консолідацію та інтеграцію розвідувальної, спостережної та зв’язкової інформації в уніфікованому цифровому середовищі.

Особливу роль відіграють геоінформаційні технології, що забезпечують просторову візуалізацію бойових порядків, маршрути логістики, зони ураження, а також інтегруються з прогнозними моделями в реальному часі. Крім того, системи ситуаційного моделювання на основі ШІ вже застосовуються в тактичному управлінні для генерації варіантів реагування на зміну оперативної обстановки.

Застосування ІАТ дає змогу скоротити час на обробку оперативної інформації, мінімізувати людський фактор у критичних ситуаціях та покращити точність управлінських дій у бойових умовах. Разом із тим, залишаються виклики, пов’язані з уніфікацією даних між підрозділами, сумісністю національних і союзницьких платформ, а також збереженням інформаційної безпеки в умовах кіберзагроз [5; 9]. У перспективі ІАТ мають стати основою інтелектуальної цифрової екосистеми оборонного управління, де дані, аналітика та рішення формуються в інтегрованому, багаторівневому форматі – від польового командира до стратегічного керівництва.

Ефективність системи інформаційної підтримки управлінських рішень значною мірою визначається якістю інформації, що надходить до особи, яка приймає рішення. Відповідно до стандартів НАТО та вітчизняної практики, оцінювання достовірності інформації здійснюється за двома незалежними параметрами: надійністю джерела та достовірністю змісту інформації. Для формалізації процесу оцінювання введемо такі позначення:

$i \in A, B, C, D$ – категорія надійності джерела;

$j \in 1, 2, 3, 4$ – категорія достовірності інформації;

$R_s(i)$ – коефіцієнт надійності джерела категорії i;

$R_c(j)$ – коефіцієнт достовірності інформації категорії j.

Значення коефіцієнтів встановлено на основі експертних оцінок (табл. 2).

Таблиця 2

Коефіцієнти надійності джерел та достовірності інформації

Категорія джерела	Характеристика	$R_s(i)$	Категорія інформації	Характеристика	$R_c(j)$
A	цілком надійне	0,95	1	підтверджена	0,95
B	зазвичай надійне	0,85	2	ймовірно правдива	0,85
C	досить надійне	0,65	3	можливо правдива	0,65
D	не завжди надійне	0,45	4	сумнівна	0,45

Інтегрований індекс надійності інформації RI визначається як зважена сума:

$$RI_{ij} = w_s \times R_s(i) + w_c \times R_c(j), w_s + w_c = 1 \quad (1)$$

де w_s та w_c – вагові коефіцієнти, що відображають відносну важливість оцінки джерела та змісту інформації відповідно.

Вибір вагових коефіцієнтів $w_s = 0{,}6$ та $w_c = 0{,}4$ обґрунтовується тим, що в умовах інформаційної війни та гібридних загроз надійність джерела є критично важливим фактором, оскільки навіть достовірна за змістом інформація з ненадійного джерела може бути елементом дезінформаційної операції [9]. Альтернативним підходом до визначення вагових коефіцієнтів є застосування методу аналізу ієрархій, що дає змогу врахувати думки декількох експертів. Матриця значень інтегрованого індексу RI наведена в табл. 3.

Таблиця 3

Матриця інтегрованого індексу надійності інформації RI_{ij}

Джерело \ Інформація	1 (R_c=0,95)	2 (R_c=0,85)	3 (R_c=0,65)	4 (R_c=0,45)
A (R_s=0,95)	0,950	0,910	0,830	0,750
B (R_s=0,85)	0,890	0,850	0,770	0,690
C (R_s=0,65)	0,770	0,730	0,650	0,570
D (R_s=0,45)	0,650	0,610	0,530	0,450

Для практичного застосування доцільно ввести порогові значення індексу:

$RI \geq 0{,}80$ — інформація придатна для прийняття критичних рішень;

$0{,}60 \leq RI < 0{,}80$ — інформація потребує додаткової верифікації;

$RI < 0{,}60$ — інформація не рекомендована для використання без підтвердження з альтернативних джерел.

Для кількісного оцінювання ступеня наближення поточної системи інформаційної підтримки до цільового стану пропонується індекс готовності системи (System Readiness Index, SRI). Припустимо, що система характеризується множиною компонентів $K = k_1, k_2, \ldots, k_n$, кожен з яких оцінюється за шкалою від 0 до 1, де 0 – повна невідповідність цільовому стану, 1 – повна відповідність. На основі матриці невідповідностей (табл. 1) визначено сім ключових компонентів ($n = 7$):

k_1 – нормативно-правове забезпечення;

k_2 – інституційна архітектура;

k_3 – інформаційна сумісність;

k_4 – технологічна база (DSS, IAT, AI);

k_5 – кадрове забезпечення;

k_6 – рівень автоматизації;

k_7 – кіберзахищеність.

Індекс готовності системи визначається за виразом:

$$SRI = \Sigma(m = 1to7) \times \alpha_m \times S_m, \text{ де } \Sigma\alpha_m = 1 \quad (2)$$

де S_m – оцінка стану m-го компонента ($0 \leq S_m \leq 1$);

α_m – ваговий коефіцієнт m-го компонента.

Вагові коефіцієнти визначено методом експертних оцінок з урахуванням пріоритетності компонентів для забезпечення ефективного функціонування системи інформаційної підтримки (табл. 4).

Таблиця 4

Вагові коефіцієнти компонентів системи інформаційної підтримки

№	Компонент	Позначення	Ваговий коефіцієнт α_m	Обґрунтування
1.	Нормативно-правове забезпечення	k_1	0,10	Базова умова функціонування
2.	Інституційна архітектура	k_2	0,15	Визначає координацію та управління
3.	Інформаційна сумісність	k_3	0,20	Критична для міжвідомчої взаємодії
4.	Технологічна база	k_4	0,20	Основа аналітичних можливостей
5.	Кадрове забезпечення	k_5	0,15	Людський фактор ефективності
6.	Рівень автоматизації	k_6	0,10	Швидкість обробки інформації
7.	Кіберзахищеність	k_7	0,10	Забезпечення безпеки системи
	Разом		1,00	

Інтерпретація значень індексу SRI:

$SRI \geq 0{,}80$ – система готова до ефективного функціонування;

$0{,}50 \leq SRI < 0{,}80$ – система потребує модернізації окремих компонентів;

$SRI < 0{,}50$ – система потребує комплексної трансформації.

Для завчасного виявлення потенційних загроз і кризових ситуацій доцільним є застосування прогнозних моделей, що базуються на аналізі часових рядів та ідентифікації аномальних патернів [4]. Такі моделі дають змогу оцінити ймовірність виникнення кризи та сформувати превентивні заходи реагування. Методологія побудови таких моделей, запропонована О. Гудимою [6], передбачає застосування байєсівських мереж, експертних оцінок та методів машинного навчання для формування інтегрованої системи раннього попередження. Прогнозна модель може бути наведена у вигляді:

$$P(Crisis|X) = P(X|Crisis) \times P(Crisis)/P(X) \quad (3)$$

де $P(Crisis|X)$ – ймовірність виникнення кризи за наявності ознак X;

$P(X|Crisis)$ – ймовірність спостереження ознак за умови кризи;

$P(Crisis)$ – апріорна ймовірність кризи;

$P(X)$ – повна ймовірність спостереження ознак.

Застосування такої моделі у поєднанні з індексами RI та SRI дає змогу формувати комплексну систему інформаційної підтримки управлінських рішень у кризових ситуаціях. Попри активний розвиток цифрових технологій у секторі національної безпеки й оборони, впровадження систем інформаційної підтримки управлінських рішень в Україні стикається з низкою комплексних проблем. Серед основних бар'єрів, що перешкоджають ефективному функціонуванню таких систем, можна виокремити:

фрагментарність нормативно-правового регулювання. Відсутність уніфікованого законодавчого підґрунтя, яке б визначало статус, повноваження, структуру та вимоги до систем DSS, обмежує їхню ефективність і ускладнює міжвідомчу взаємодію [12];

технічна несумісність між системами. Наявність різноформатних платформ, відсутність єдиних стандартів обміну даними та взаємодії ускладнює побудову інтегрованого інформаційного середовища в умовах кризового реагування. Це особливо актуально для взаємодії між Збройними Силами України, Службою безпеки України, Ради національної безпеки і оборони України, Державної служби України з надзвичайних ситуацій та іншими головними структурами;

кадровий дефіцит. Брак кваліфікованих аналітиків, фахівців із впровадження та супроводу ІАТ, а також експертів у сфері ШІ суттєво стримує як розбудову СЦ, так і ефективне використання сучасних рішень на всіх рівнях управління;

низький рівень автоматизації. Значна частина інформаційно-аналітичних процесів залишається ручною, що уповільнює реакцію на динамічні зміни в оперативному середовищі та знижує якість підтримки рішень;

кіберзагрози та вразливість ІТ-інфраструктури. Відсутність цілісної стратегії кіберзахисту, обмеженість у виявленні та протидії вторгненням, а також слабкі механізми автентифікації підвищують ризики уразливості ключових компонентів DSS [5; 9].

Сукупність наведених проблем створює складне середовище для повноцінного функціонування інформаційної підтримки управлінських рішень у сфері оборони. Для подолання цих викликів

необхідний системний, міжвідомчо скоординований підхід, що поєднує нормативне вдосконалення, розвиток технічної бази та людського капіталу. Для підвищення спроможностей систем інформаційної підтримки управлінських рішень в умовах криз необхідно реалізувати багатофакторну програму модернізації, яка передбачає такі напрями [12; 5; 9]:

удосконалення нормативно-правового середовища. Доцільно розробити спеціальний законодавчий акт або комплекс підзаконних документів, що регламентуватимуть статус, функції, повноваження та стандарти діяльності систем DSS;

створення єдиного міжвідомчого інформаційного середовища. Важливо забезпечити технічну сумісність платформ, розробити спільні протоколи обміну та впровадити централізований інформаційний хаб, який діятиме в режимі реального часу;

розвиток кадрового потенціалу. Необхідно впровадити цільові програми підготовки фахівців-аналітиків нового покоління з навичками роботи з великими даними, когнітивними системами та штучним інтелектом, а також стимулювати міжвідомчий обмін досвідом;

поглиблена інтеграція інструментів ШІ. Варто розширювати використання машинного навчання, систем прогнозного аналізу, когнітивної аналітики й пояснюваного ШІ у функціонуванні DSS;

зміцнення кіберстійкості. Потрібна побудова багаторівневої архітектури захисту: від захищеного зберігання даних до виявлення вторгнень, реагування на інциденти й аудит цифрової безпеки.

впровадження наведених математичних моделей. Застосування моделей інтегрованого індексу надійності інформації та індексу готовності системи забезпечить об’єктивне оцінювання якості інформаційних ресурсів та визначення пріоритетів модернізації.

Реалізація зазначених напрямів уможливить формування адаптивної, ефективної та безпечної архітектури інформаційної підтримки, здатної відповідати викликам сучасного та майбутнього безпекового середовища.

Висновки

У результаті дослідження встановлено, що ефективна система інформаційної підтримки управлінських рішень у системі оборонного управління України має ґрунтуватися на міждисциплінарному підході, що поєднує сучасні інформаційно-аналітичні технології, математичні моделі оцінювання, нормативну визначеність і механізми кризового планування.

Аналіз міжнародного досвіду підтверджує доцільність інтеграції Систем підтримки прийняття рішень (Decision Support Systems (DSS)) у структури військового управління для підвищення ситуаційної обізнаності, скорочення часу реагування та підвищення обґрунтованості рішень. Водночас в Україні необхідно усунути низку системних обмежень: фрагментарну правову базу, технічну роз'єднаність платформ, нестачу компетентного персоналу та зростаючі кіберзагрози.

Запропоновано математичні моделі, що ґуртуються на інтегрованому індексі надійності інформації RI для формалізації оцінювання достовірності інформації з урахуванням надійності джерела та змісту повідомлення, та індексі готовності системи SRI, що забезпечує кількісну оцінку ступеня наближення системи інформаційної підтримки до цільового стану. Практичні приклади застосування моделей підтверджують їх придатність для підтримки управлінських рішень.

Перспективними напрямами розвитку є нормативне оформлення діяльності ситуаційних центрів, створення єдиної інформаційно-технологічної інфраструктури міжвідомчого рівня, активне впровадження технологій штучного інтелекту, зокрема пояснюваного штучного інтелекту (eXplainable Artificial Intelligence (XAI)), а також формування кадрового резерву аналітиків нового покоління.

Отримані результати можуть стати концептуальною основою для модернізації ситуаційних центрів, розробки Систем підтримки прийняття рішень (DSS) нового покоління та формування політик у сфері цифрового оборонного управління.

Перспективи і напрями подальших досліджень: валідація запропонованих моделей на основі емпіричних даних функціонування ситуаційних центрів; розроблення методики визначення вагових коефіцієнтів на основі методу аналізу ієрархій; дослідження впливу інтеграції пояснюваного штучного інтелекту на якість управлінських рішень.

Конфлікт інтересів. Відсутній.

Фінансування дослідження не здійснювалося.

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

Використання засобів штучного інтелекту. Під час написання статті застосовувалися засоби ШІ для пошуку інформації, її оброблення, оформлення списку бібліографічних посилань, перекладу анотації. Використання засобів ШІ не призвело до порушення авторських прав й етичних норм наукового дослідження, а згенерований контент був перевірений і відповідає дійсності.

Список бібліографічних посилань

1. Конституція України : Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 10.04.2026). **2. Про національну безпеку України** : Закон України від 21.06.2018 №2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 10.04.2026). **3. Про оборону України** : Закон

України від 06.12.1991 № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 10.04.2026). **4. Питання мережі ситуаційних центрів** : Постанова Кабінету Міністрів України від 11.07.2023 № 705. URL: https://zakon.rada.gov.ua/laws/show/705-2023-%D0%BF#Text (дата звернення: 10.04.2026). **5. Павліковський А., Свєшніков С., Бочарніков В.** Ситуаційний центр стратегічного аналізу: аналітичні задачі і організаційні проблеми. *Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ*. 2025. Т. 2. С. 81–88. DOI: https://doi.org/10.33099/2304-2745/2024-3-83/81-88.
6. Гудима О.П. Удосконалення математичної моделі прогнозування та виявлення кризових ситуацій. *Наука і техніка Повітряних Сил Збройних Сил України.* 2021. № 1(42). С. 126–130. DOI: https://doi.org/10.30748/nitps.2021.42.16. **7. Гудима О.П.** Підхід до формування базової структури типового ситуаційного центру. *Débats scientifiques et orientations prospectives du développement scientifique.* 2022. URL: https://doi.org/10.36074/logos-08.07.2022.028. **8. Живило Є. О.** Ситуаційний центр Міністерства оборони України – модель завчасного виявлення та аналізу кризових ситуацій сектору безпеки держави. *Актуальні проблеми вітчизняної юриспруденції.* 2023. № 1. С. 56–60. DOI: https://doi.org/10.26565/1684-8489-2022-1-02.
9. Машталір В.В., Гудима О.П. Концептуальний підхід до формування моделі організаційної структури Ситуаційного центру Міністерства оборони України. *Сучасні інформаційні технології у сфері безпеки та оборони.* 2023. № 2(47). С. 31-40. DOI: https://doi.org/10.33099/2311-7249/2023-47-2-31-40. **10. Пристайко В.В.** Ситуаційні центри як ключовий інституційний механізм державного антикризового управління: зарубіжний досвід. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Державне управління.* 2019. Т. 30(69). № 3. DOI: https://doi.org/10.32838/2663-6468/2019.3/24.
11. Руснак Ю.І., Стужук Ю.В. Стратегічне інформаційне управління в системі безпеки та оборони: інтеграція та оптимізація. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки.* 2024. Т. 94. № 1. С. 86–96. DOI: https://doi.org/10.32453/3.v94i1.1584. **12. Delen D.** Decision Support and Business Intelligence Systems. 9th ed. Upper Saddle River, NJ : Pearson Education, 2010. 696 p.

INFORMATION TECHNOLOGY FOR DECISION SUPPORT FOR THE MINISTRY OF DEFENCE OF UKRAINE IN THE CRISIS RESPONSE SYSTEM

SHERSTIUK Yevhen, National Defence University of Ukraine, Kyiv, Ukraine,
https://orcid.org/0009-0009-5111-7747

Problem formulation. *The article addresses the lack of a unified, scientifically grounded methodology for information support of managerial decisions in Ukraine's defence sector, particularly in crisis response conditions. Despite the establishment of situational centres within the security and defence sector, no standardised data-collection and verification system, unified decision-support architecture, or common interoperability standards currently exist.* ***Purpose.*** *The article aims to develop a structural scheme for information technology to support decision-making in the Ministry of Defence of Ukraine's crisis response system, based on an analysis of the theoretical and methodological foundations of integrated information support systems in Ukraine's defence sector and in NATO member states.*

Research methods. *The study employs a set of scientific methods: systems analysis – to examine the structure and interrelations of information support components; comparative analysis – to contrast domestic and international experience in decision support system implementation; expert assessment – to determine weighting coefficients in mathematical models; mathematical modelling – to formalise the processes of information reliability evaluation and system readiness assessment.*

Literature review. *The analysis of international experience, particularly NATO, US, and UK practices, demonstrates the effectiveness of Decision Support Systems (DSS) in military management, operational forecasting, logistics, and strategic planning. Ukrainian scholars, including V. Bocharnikov, O. Hudyma, Ye. Zhyvylo, V. Mashtalir, A. Pavlikovskyi, V. Prystayko, Yu. Rusnak, S. Svieshnikov, and Yu. Stuzhuk, substantiate the necessity of developing nationally adapted decision support systems (DSS) and situational centres that meet the key requirements of timeliness, interoperability, reliability, and security. However, the gap between existing information support practices and modern DSS requirements remains significant and insufficiently studied.*

Research results. *The main regulatory, institutional, and technological factors determining the current state and development prospects of information support systems were analysed. Key gaps between existing practices and requirements for modern defence DSS were identified through a specially developed gap matrix. Two mathematical models are proposed: an integrated reliability index for assessing information credibility, and a system readiness index for quantifying the degree to which the current system approaches its target state. A structural scheme for information technology to support decision-making in the Ministry of Defence of Ukraine's crisis response system was developed.*

Research novelty *consists of developing a structured approach to identifying organisational and technological gaps in decision support systems by introducing a specialised gap matrix. New quantitative indicators (indices) have been formalised to enable the objective assessment of both the reliability of input information and the maturity of the entire information support system under hybrid threat conditions.*

Theoretical and practical significance. *The results provide a conceptual basis for modernising situational centres and designing next-generation decision support systems. Implementing the proposed methodological approaches will*

improve the accuracy, speed, and coherence of managerial decisions in crisis situations, which is critical to ensuring Ukraine's national security.

Conclusions and future work. *The developed structural scheme and mathematical models form a foundation for the practical modernisation of the Ministry of Defence situational centre and harmonisation with NATO standards. Further research should focus on empirical validation of the proposed indices and on the development of software to implement the described information technology.*

Keywords: *decision support system, information support, crisis response, situational centre, information technology for decision support, artificial intelligence, interagency interaction, information reliability.*

References

1. ***Konstytutsiia Ukrainy*** [online], (1996). Zakon Ukrainy № 254k/96-VR, 28 June. Available at: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text [Accessed: 10 April 2026]. **2.** ***Pro natsionalnu bezpeku Ukrainy*** [online], (2018). Zakon Ukrainy № 2469-VIII, 21 June. Available at: https://zakon.rada.gov.ua/laws/show/2469-19#Text [Accessed: 10 April 2026]. **3.** ***Pro oboronu Ukrainy*** [online], (1992). Zakon Ukrainy № 1932-XII, 06 December. Available at: https://zakon.rada.gov.ua/laws/show/1932-12#Text [Accessed: 10 April 2026]. **4.** ***Pytannia merezhi sytuatsiinykh tsentriv*** [online], (2023). Postanova Kabinetu Ministriv Ukrainy № 705, 11 July. Available at: https://zakon.rada.gov.ua/laws/show/705-2023-%D0%BF#Text [Accessed: 10 April 2026]. **5. Pavlikovskyi, A., Svieshnikov, S. and Bocharnikov, V.** (2025) Situational Centre for Strategic Analysis: Analytical Tasks and Organisational Problems, *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen NUOU*, Vol. 2, pp. 81–88. DOI: https://doi.org/10.33099/2304-2745/2024-3-83/81-88

6. Hudyma, O. P. (2021) Improvement of the Mathematical Model for Forecasting and Detection of Crisis Situations, *Nauka i tekhnika Povitrianykh Syl Zbroinykh Syl Ukrainy,* № 1(42), pp. 126–130. DOI: https://doi.org/10.30748/nitps.2021.42.16

7. Hudyma, O. P. (2022) Approach to the Formation of the Basic Structure of a Typical Situational Centre, *Débats scientifiques et orientations prospectives du développement scientifique*. DOI: https://doi.org/10.36074/logos-08.07.2022.028 **8. Zhyvylo, Ye. O.** (2023) The Situation Centre of the Ministry of Defence of Ukraine – A Model for Early Detection and Analysis of Crisis Situations in the State Security Sector, *Aktualni problemy vitchyznianoi yurysprudentsii,* № 1, pp. 56–60. DOI: https://doi.org/10.26565/1684-8489-2022-1-02

9. Mashtalir, V. V. and Hudyma, O. P. (2023) A Conceptual Approach to the Formation of the Organisational Structure Model of the Situation Centre of the Ministry of Defence of Ukraine, *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony,* № 2(47), pp. 31–40. DOI: https://doi.org/10.33099/2311-7249/2023-47-2-31-40 **10. Prystayko, V. V.** (2019) Situation Centres as the Key Institutional Mechanism of State Anti-Crisis Management: Foreign Experience, *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Derzhavne upravlinnia,* Vol. 30(69), № 3. DOI: https://doi.org/10.32838/2663-6468/2019.3/24

11. Rusnak, Yu. I. and Stuzhuk, Yu. V. (2024) Strategic Information Management in the Security and Defence System: Integration and Optimisation, *Zbirnyk naukovykh prats Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy. Seriia: viiskovi ta tekhnichni nauky,* Vol. 94, № 1, pp. 86–96. DOI: https://doi.org/10.32453/3.v94i1.1584

12. Delen, D. (2010) *Decision Support and Business Intelligence Systems*, 9th edn. Upper Saddle River, NJ: Pearson Education. 696 p.

Рукопис надійшов до редакції *24.02.2026*
Рукопис прийнято до друку після рецензування *08.04.2026*
Дата публікації *30.04.2026*