**ISSN 2524-0056(Print)**
**ISSN 2519-481X(Online)**

**ВІЙСЬКОВИЙ ІНСТИТУТ**
**КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ**
**ІМЕНІ ТАРАСА ШЕВЧЕНКА**

**ЗБІРНИК НАУКОВИХ ПРАЦЬ**

# ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА

**Виходить 4 рази на рік**

**№ 77**

Згідно Наказу МОН №1188 від 24.09.2020, п. №156 Додатку 5 «Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка» включено до категорії «Б» за спеціальностями:

124 – «Системний аналіз»;
126 – «Інформаційні системи та технології»
254 – «Забезпечення військ (сил)»
255 – «Озброєння та військова техніка»

**КИЇВ – 2022**

УДК621.43
ББК 32-26.8-68.49
**Збірник наукових праць** Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, 2022. № 77. 184 с.



*Редакційна колегія прагне до покращення змісту та якості оформлення видання і буде вдячна авторам та читачам за висловлювання зауважень і побажань.*

Зареєстровано Міністерством юстиції України, свідоцтво про державну реєстрацію друкованого засобу масової інформації - серія КВ № 11541 – 413Р від 21.07.2006 р.

Відповідно до Наказу МОН України від 24.09.2020 № 1188 «Збірник наукових праць ВІКНУ імені Тараса Шевченка» внесено до категорії «Б» (технічні науки).

Затверджено на засіданні Вченої ради ВІКНУ від 15.12.22 р., протокол № 4.

Відповідальні за макет:
Литвиненко Н.І.,
Солодєєва Л.В.



Адреса редакції: 03189, м. Київ, вул. М. Ломоносова, 81, тел./факс +38 (044) 521 – 33 – 82
Наклад 50 прим.
Ел.адреса редактора: lenkov_s@ukr.net
Офіційний сайт журналу: http://miljournals.knu.ua/

**ЗМІСТ**

## ВІЙСЬКОВА ТЕХНІКА І ТЕХНОЛОГІЇ ПОДВІЙНОГО ПРИЗНАЧЕННЯ



## ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ



## ЗАГАЛЬНІ ПИТАННЯ

## CONTENTS

### MILITARY EQUIPMENT AND TWO-DESTINATION TECHNOLOGIES



### INFORMATION TECHNOLOGIES



### GENERAL QUESTIONS

УДК 621.396.967

д.тех.н., доц**. Глухов С.І.** (ВІКНУ)
к.т.н., с.н.с. **Гахович С.В.** (ВІКНУ)
к.т.н., с.н.с. **Охрамович М.М.** (ВІКНУ)
д. філос. з інформ. техн. **Коваль М.О.** (ВІКНУ)
к.пед.н. **Кравченко О.І.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2022/77-01

# МОДЕЛЬ ЦИФРОВОГО ТИПОВОГО ЕЛЕМЕНТУ ЗАМІНИ З КОМПЛЕКСНИМ ВИКОРИСТАННЯМ ДЖЕРЕЛ ДІАГНОСТИЧНОЇ ІНФОРМАЦІЇ

***У статті приведено порядок організації дослідження контролю технічного стану в сучасній радіоелектронній техніці, яка виконана на елементній базі четвертого та п'ятого поколінь. Показано комплексне використання декількох методів контролю працездатності цифрових типових елементів заміни, що містять мікроконтролери та здійснено розрахунок значень вихідних перемінних узагальненого модуля який відповідає дійсним фізичним об'єктам і може бути використаний у математичної моделі цифрового типового елементу заміни. Для скорочення кількості контрольних точок, в якості джерела діагностичної інформації використано параметри енергодинамічного процесу, що виникають у шині живлення цифрових елементів при їх перемиканні із одного логічного стану в інший. Це дає змогу зменшити кількість контрольних точок до однієї (шини живлення), одержуючи при цьому діагностичну інформацію про технічний стан кожного логічного елемента.***

***Робота розділена на чотири етапи, які включають в себе:***

***- аналіз внутрішньої структури та виділення підсистем у типовому елементі заміни;***

***- декомпозицію типового елемента заміни та виділення груп перемінних;***

***- синтез структурно-функціональної моделі цифрового типового елемента заміни;***

***- моделювання процесу взаємодії розробленої математичної моделі узагальненого модуля мікроконтролера з зовнішнім середовищем, аналіз ступеня адекватності моделі дійсним фізичним об'єктам.***

***Таким чином, запропоновано структурно-функціональну модель цифрового типового елементу заміни, в якому передбачено комплексне використання двох джерел діагностичної інформації: вихідних реакцій та характеристик енергодинамічного процесу в шині живлення цифрового ТЕЗ.***

***Ключові слова: енергодинамічний метод діагностування, радіоелектронна техніка, математична модель, джерело діагностичної інформації, типовий елемент заміни.***

**Вступ.** Процес підготовки і організації контролю технічного стану в сучасній радіоелектронній техніці (РЕТ), яка виконана на елементній базі четвертого і п'ятого поколінь, досить складний. Ця складність обумовлена, зокрема, використанням у складі нової техніки цифрових типових елементів заміни (ТЕЗ), які містять інтегральні схеми (ІС) та мікроконтролери.

Для ухвалення рішення про технічний стан ТЕЗ і локалізації дефектів необхідно провести технічне діагностування з перевіркою працездатності і визначення причин виникнення дефектів. Процес проведення діагностування цифрових ТЕЗ складається у вимірі й аналізі параметрів вихідних сигналів функціональних елементів, чи підсистем або деякого узагальнюючого сигналу в цілому. Для виміру й аналізу параметрів вихідних сигналів функціональних елементів і підсистем організують додаткові виходи, що називаються контрольними точками. Набір значень параметрів, що відображають якість інформації про технічний стан ТЕЗ, однозначно зв'язаний з кількістю контрольних точок, установлених на ньому. З ускладненням ТЕЗ збільшується число параметрів контролю, по яких приймають

рішення про технічний стан. Вибір найбільш інформативних параметрів дозволяє значною мірою скоротити число контрольних точок.

**Аналіз останніх досліджень.** На теперішній час існуючі методи контролю технічного стану цифрових елементів поодинці не дозволяють домогтися прийнятних результатів визначення технічного стану цифрових ТЕЗ з високою достовірністю за припустимий час. Це пов'язано з тим, що елементи, які складають цифровий ТЕЗ, мають велику кількість активних елементів на кристалі обмеженої площі, складну внутрішню структуру і високу ймовірність виникнення кратних дефектів, обмежену кількість виводів і контрольних точок [1, 2]. Тому, з метою досягнення прийнятних характеристик діагностування, сьогодні перспективним є комплексне використання декількох методів контролю працездатності цифрових ТЕЗ, що містять мікроконтролери.

Для скорочення числа контрольних точок при діагностуванні цифрових ТЕЗ, доцільно використовувати в якості джерела діагностичної інформації параметри енергодинамічного процесу (ЕДП), що виникають у шині живлення цифрових елементів при їх переключенні із одного логічного стану в інший. Це дозволяє зменшити кількість контрольних точок до однієї (шини живлення), одержуючи при цьому діагностичну інформацію про технічний стан кожного логічного елемента (ЛЕ) [1-3].

**Мета статті.** В статті пропонується нова структурно-функціональна модель цифрового ТЕЗ в якій передбачається комплексне використання двох джерел діагностичної інформації (ДІ): вихідних реакцій (ВР) та характеристик енергодинамічного процесу в шині живлення цифрового ТЕЗ.

**Виклад основного матеріалу.** Побудову означеної структурно-функціональної моделі проведемо в чотири етапи, використовуючи при цьому відомі підходи [3]:

1) аналіз внутрішньої структури та виділення підсистем у ТЕЗ;
2) декомпозиція ТЕЗ та виділення груп перемінних;
3) синтез структурно-функціональної моделі цифрового ТЕЗ;
4) моделювання процесу взаємодії розробленої математичної моделі (ММ) узагальненого модуля мікроконтролера з зовнішнім середовищем, аналіз ступеня адекватності моделі дійсним фізичним об'єктам.

**На першому етапі** виділяються підсистеми у цифровому ТЕЗ. З урахуванням характеристик енергодинамічнного процесу (ЕДП) внутрішню структуру ТЕЗ можна представити сукупністю трьох підсистем – інформаційної, керуючої і енергоживлення [4]. За допомогою інформаційної підсистеми здійснюється передача, опрацювання і збереження даних. Керуюча підсистема виконує допоміжні функції (аналізує інформаційні потоки згідно алгоритму опрацювання через модулі інформаційної підсистеми, генерує керуючі сигнали, які необхідні для роботи інформаційної підсистеми, а також формує сигнали для зв'язку ТЕЗ із зовнішнім середовищем). Підсистема енергозабезпечення призначена для живлення складових елементів цифрового ТЕЗ (логічних елементів з рівнями, що відповідають напругам живлення $U_{\text{жив}}$, причому $U_{\text{жив}} = \{U_{\text{жив }1}, ..., U_{\text{жив }i}, ..., U_{\text{жив }p}\}$, де $p$– число шин живлення, для яких характерні відповідні струми споживання при протіканні ЕДП, причому $I_{\text{жив}} = \{I_{\text{жив }1}, ..., I_{\text{жив }i}, ..., I_{\text{жив }p}\}$.

Вхідні діяння (ВД), що надходять на керуючу та інформаційну підсистеми ТЕЗ поділимо на два класи: керуючі та інформаційні. Під інформаційними вхідними діяннями $D^S$ і керуючими вхідними діяннями $D^U$ будемо розуміти сигнали, які утворюють відповідні множини багатомірних вхідних перемінних, причому

$$D^S = \{ D_1^S, \ldots, D_i^S, \ldots, D_\xi^S \}, \qquad D^U = \{ D_1^U, \ldots, D_i^U, \ldots, D_\Psi^U \},$$

де $\xi$, $\Psi$ – число вхідних інформаційних та керуючих шин відповідно.

Множину $D^U$ розділимо на дві підмножини $\{I\}$ і $\{D^C\}$ так, що

$$D^U = \{I\} \cup \{D^C\}.$$

Підмножину $\{I\}$ утворюють керуючі сигнали ТЕЗ причому

$$I = \{I_1, ..., I_i, ..., I_\mu\}, \qquad I_i \in (0, 1, T),$$

де μ – число керуючих сигналів, за допомогою яких цифровий ТЕЗ виконує керування зовнішніми пристроями чи, навпаки, зовнішні пристрої здійснюють безпосередній вплив на процес обробки даних у ТЕЗ. Ці сигнали подаються і знімаються, як правило, зі спеціально призначених входів і виходів [5, 6]; T - байдуже або невизначене значення сигналу.

Підмножину $D^C$ утворюють команди мікроконтролерів, причому

$$D^C = \{D_1^C, ..., D_i^C, ..., D_c^C\}, \quad D_i^C = \{C_{i1}, ..., C_{ij}, ..., C_{ig}\}, \qquad C_{ij} \in (0, 1, T),$$

де $c$ – число команд в системі команд мікроконтролера; $g$ – розрядність $i$-ої команди.

Множина $D^C$ задає множину функцій $\Phi$, причому $\Phi = \{\Phi_1, ..., \Phi_j, ..., \Phi_\tau\}$,

де τ – число функцій, які реалізує цифровий ТЕЗ; $\Phi_j$ - функція, згідно якій вхідній перемінній $D_i^S$ ставиться у відповідність вихідна перемінна $D_i^Z$ [1, 5]. Вихідні реакції ТЕЗ на вхідні діяння утворюють множину багатомірних вихідних перемінних $D^Z$, причому

$$D^Z = \{D_1^Z, ..., D_i^Z, ..., D_r^Z\}, \quad D_i^Z = \{Z_{i1}, ..., Z_{ij}, ..., Z_{is}\}, \qquad Z_{ij} \in (0, 1, T),$$

де $r$ – число вихідних шин; $S$ – розрядність $i$-ої вихідної шини.

Множина $D^Z$ утворюється з множини $D^S$ за рахунок функціональних перетворень вхідних перемінних, за допомогою яких здійснюється переключення точно визначених елементів. У цьому випадку справедливим є наступний вираз:

$$D^Z = F(D^S, D^U). \qquad (1)$$

Шина живлення з відповідними $U_{\text{жив}}$ є невід'ємною частиною цифрового ТЕЗ та, як правило, загальною для всіх його елементів. У цьому випадку справедливим є наступний вираз:

$$I_{\text{жив}} = F(D^Z, D^S, D^U). \qquad (2)$$

Вираз (2) показує аналітичну залежність $I_{\text{жив}}$ від інформаційних та керуючих ВД і вихідних реакцій мікроконтролерів. Аналіз виразів (1) і (2) показує, що контроль технічного стана цифрового ТЕЗ можна здійснити по двом джерелами діагностичної інформації: характеристиками ЕДП і ВР.

**На другому етапі** здійснюється декомпозиція цифрового ТЕЗ на рівні, які залежать від глибини представлення внутрішньої структури, та виділення груп перемінних. У зв’язку з необхідністю обліку великої кількості внутрішніх зв'язків і складності структури сучасного ТЕЗ найбільш раціонально будувати багаторівневу ієрархічну модель. Декомпозиція цифрового ТЕЗ на структурні рівні необхідна для спрощення розрахунків (дозволяє скоротити розглянуту множину припустимих $D^S$ і $D^U$). Також, це дає можливість, в залежності від наявної інформації про об’єкт діагностування (ОД) у розробника тестової послідовності (ТП), використовувати моделі різного рівня, що значно спрощує побудову та упорядкування ТП [7, 8].

За допомогою теорії графів представимо цифровий ТЕЗ як сукупність взаємопов’язаних елементів – ЛЕ, мікроконтролерів, які розташовані на ньому, а мікроконтролери представимо у вигляді сукупності функціонально-завершених вузлів (частин мікроконтролера, що виконують деякі операції над вхідними даними), які далі будемо називати *модулями*.

Перший ієрархічний рівень – це рівень ТЕЗ. На ньому представлені найбільш загальні властивості ТЕЗ: найменування мікроконтролерів, які розміщені на ньому; зв'язки між мікроконтролерами (можливість здійснення обміну даними); статистика відмов; розмір мінімального повного тесту та інша інформація загального характеру. Ці властивості представимо у вигляді орієнтованого зваженого по вершинам графа $G(V, X)$, де вершини $V^m \in V \ (m = \overline{1, \nu})$ – це мікроконтролери, а ребра $X^n \in X$ – зв'язки між ними. Напрямок ребра показує можливу послідовність обміну даними.

Вага вершини – це мінімальна кількість тестових послідовностей, які необхідні для повного тесту при контролі технічного стана мікроконтролера, яку представляє дана вершина. Для логічної завершеності додаємо дві вершини, які відповідають входу та виходу і мають відповідно мінімальний та максимальний номери. Це полегшує процес визначення першого та останнього елемента в тестовій послідовності. Дана модель представлена на рис. 1.

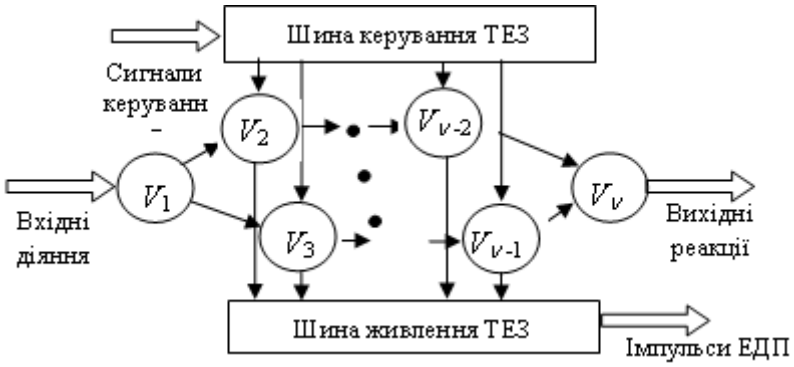



Рисунок 1– Модель цифрового ТЕЗ як сукупність взаємопов’язаних логічних елементів

Модель рівня ТЕЗ може знаходитись в одному з $N$ станів, якій відповідає подачі на відповідний мікроконтролер об'єкта діагностування сигналу "вибір кристала". Перехід з стана $s^i$ до стана $s^j$ здійснюється відповідно з наступним виразом:

$$s^i \xrightarrow{n^j = f(N^i)} s^j, \qquad n^j \in N,$$

де $s^i$ – теперішній стан моделі; $s^j$ – наступний стан моделі; $N^i$ – множина вершин, в які можливо здійснити перехід з вершин $n^i$; $n^j$ – вершина графа, яка належить множині $N^i$ і находиться як функція над цією множиною; $f(N^i)$ – функція над множиною $N^i$, яка визначається критерієм вибору.

Таким чином, представлений графічний рівень цифрового ТЕЗ дозволяє визначити порядок тестування мікроконтролерів, які розміщенні на ньому, та використовувати структурні підходи для синтезу ТП.

Другий ієрархічний рівень – це рівень мікроконтролера. На цьому рівні необхідно надати інформацію про модулі, з яких складається мікроконтролер, логічні зв'язки між модулями, розмір мінімального повного тесту модуля. Цю інформацію представимо орієнтованим зваженим по вершинам графом, вершини якого $V_n^v \in V^v \quad (n = \overline{1, N})$ – це модулі мікроконтролера, а орієнтовані ребра $X^\chi \in X$ вказують на зв’язок між ними. Вага кожної вершини показує кількість наборів даних, які необхідні для мінімального повного тесту відповідного модуля. Додатково вводяться дві вершини, які відповідають входу та виходу з мінімальним та максимальним номерами відповідно. Дана модель представлена на рис. 2.

Модель рівня складового елемента може знаходитись в одному з $L$ станів, якій відповідає подачі на відповідний модуль об'єкта діагностування керуючого сигналу. Перехід з стана $s_n^i$ до стана $s_n^j$ здійснюється відповідно наступному виразу:

$$s_n^i \xrightarrow{l^j = f(L^i)} s_n^j, \qquad l^j \in L^i,$$

де $s_n^i$ – теперішній стан моделі; $s_n^j$ – наступний стан моделі; $L^i$ – множина вершин, в які можливо здійснити перехід з вершин $l^i$; $l^j$ – вершина графа, яка належить множині $L^i$ і находиться як функція над цією множиною; $f(L^i)$ – функція над множиною $L^i$, яка визначається критерієм вибору.

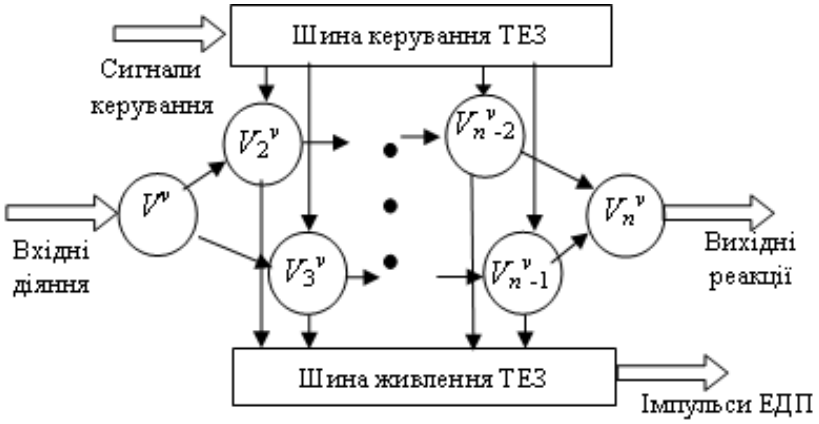



Рисунок 2– Модель цифрового ТЕЗ з мікроконтролером та логічними зв'язки між модулями

Даний рівень дозволяє використовувати для побудові ТП структурно-функціональні підходи на рівні ЛЕ, визначити послідовність перевірки модулів.

Останній ієрархічний рівень – це рівень модуля мікроконтролера. Для отримання математичної моделі розглянемо функціональні залежності стана модуля від вхідних діянь та конструктивного виконання модуля.

**На третьому етапі** здійснюється синтез математичної моделі для цифрового ТЕЗ. Виходячи з ієрархії розробленої моделі, розглянемо перемінні, які діють на зовнішніх виводах модуля, отримаємо вираз для узагальненого модуля мікроконтролера.

У загальному випадку на кожний модуль надходять інформаційні і керуючі діяння та подаються відповідні рівні напруги живлення, а сам модуль може мати декілька вихідних шин даних і живлення. Обмежимося розглядом модулів з однією вихідною шиною даних і живлення. Модулі з декількома вихідними шинами і шинами живлення будемо розділяти на деяку сукупність модулів з однією вихідною шиною даних і шиною живлення.

За конструктивно-схемотехнічним рішенням всі модулі можна розділити на асинхронні і синхронні [9, 10]. У *асинхронних* модулів ВР на інформаційні ВД з'являється через термін $t_s$ (затримка при поширенні сигналу в схемі). У *синхронних* модулів термін появи ВР на інформаційні ВД залежить як від терміну $t_s$, так і від часу $t_c$ (час надходження на відповідні входи цих модулів синхронізуючих імпульсів $\gamma_c$, $\gamma_c \in$ J). Синхросигнал $\gamma_c$ представляє собою одиничний (нульовий) імпульс, що надходить у точно визначені (дискретні) моменти часу $t_i \in T$ ($T$ – множина дискретних моментів часу). Сигнал, що обробляється у мікроконтролері, послідовно проходить через вказані модулі.

За реакцією на ВД всі модулі можна розділити на комбінаційні і послідовні [10]. *Модулі комбінаційного типу* – це такі модулі, ВР яких залежить тільки від ВД, що діють у даний момент часу $t_i$, і не залежить від ВД, що діяли у попередній момент часу $t_{i-1}$. До таких модулів відносяться схеми, які не містять елементів пам'яті (мультиплексори, арифметично-логічні пристрої, багаторозрядні зрушувачі та ін.). *Модулі послідовного типу* – це такі модулі, ВР яких залежить як від ВД, що діють на його входах у даний момент часу $t_i$, так і ВД, що надійшли на його входи у $n$ попередніх моментів часу $t_j$, $j = \overline{(i-n), i}$. До таких модулів відносяться схеми, які містять елементи пам'яті (регістри, лічильники та ін.).

Загальні перемінні модулів обох типів розділимо на наступні групи:

1) множина інструкцій $J = \{J_1, \ldots, J_i, \ldots, J_d\}$, $J_i = \{\Omega_{i1}, \ldots, \Omega_{ij}, \ldots, \Omega_{iu}\}$, $\Omega_{ij} \in (0, 1, T)$, ($d$ – кількість керуючих інструкцій; $u$ – розрядність керуючої шини модуля);

2) множина багатомірних вхідних перемінних $D^x = \{D_1^x, \ldots, D_i^x, \ldots, D_k^x\}$, $D_i^x = \{X_{i1}, \ldots, X_{ij}, \ldots, X_{ib}\}$, $X_{ij} \in (0, 1,$ T), ($k$ – кількість зовнішніх шин мікроконтролера чи вихідних шин модуля комбінаційного типу; $b$ – розрядність $i$-ої шини ВД, яка являє собою зовнішню шину мікроконтролера або вихідну шину модуля комбінаційного типу);

3) множина багатомірних вхідних перемінних $D^Y = \{ D_1^Y, ..., D_i^Y, ..., D_h^Y \}$, $D_i^Y = \{ Y_{i1}, ..., Y_{ie}, ..., Y_{ir} \}$, $Y_{ie} \in (0, 1, \text{Т})$, ($h$ – кількість шин, які відповідають перемінній стана модуля послідовного типу; $r$ – розрядність $i$-ої шини ВД, яка відповідає вихідній перемінній стана модуля послідовного типу).

Перемінні модуля комбінаційного типу розділимо на наступні групи:

1) множина багатомірних вихідних перемінних $D^z_{\text{комб}} = \{Z_1^k, ..., Z_i^k, ..., Z_v^k\}$, $Z_i^k \in (0, 1, \text{Т})$, ($v$ – розрядність вихідної шини модуля комбінаційного типу);

2) значення напруги шини живлення $U_{\text{комб}}$, для якої характерним є те, що при протіканні ЕДП струм споживання $I_{\text{комб}}$ залежить від виду тестових діянь і технології виготовлення мікроконтролера (транзисторно-транзисторна логіка (ТТЛ), емітерно-зв'язана логіка (ЕЗЛ) та ін.).

Перемінні модуля послідовного типу розділимо на наступні групи:

1) множина багатомірних вихідних перемінних $D^z_{\text{посл}}$, якій відповідає перемінна стана $D^z_{\text{посл}} = \{Z_1^{\text{п}}, ..., Z_i^{\text{п}}, ..., Z_f^{\text{п}}\}$, $Z_i^{\text{п}} \in (0, 1, \text{Т})$, ($f$ – розрядність вихідної шини модуля послідовного типу);

2) значення напруги шини живлення $U_{\text{посл}}$, для якої характерним є те, що при протіканні ЕДП струм споживання $I_{\text{посл}}$ залежить від виду тестових діянь, внутрішнього стана модуля, технології виготовлення мікроконтролера (ТТЛ, ЕЗЛ та ін.).

Для отримання єдиної та однозначної залежності ВР від інформаційних ВД об'єднаємо всі зовнішні інформаційні вхідні шини і всі внутрішні шини в одну з узагальненою розрядністю $H$ таким чином, що

$$\{D^x\} \cup \{D^Y\} = \{D^I\} = \{I_1, ..., I_i, ..., I_H\}, \quad H = \sum_{i=1}^{k} b_i + \sum_{i=1}^{h} r_i, \quad I_i \in (0, 1, \text{Т}).$$

Об'єднання (узагальнення) декількох однорідних шин в одну припустимо. В цьому випадку зберігаються фізичний зміст процесів, що описуються, і коректність ММ, а також здійснюється перехід від однієї форми представлення вхідних перемінних до іншої [11].

В узагальненому модулі вихідна перемінна $D^w$ описується наступним виразом:

$$D^w = \{w_1, ..., w_i, ..., w_\gamma\}, \quad w_i \in (0, 1, \text{Т}),$$

де γ – розрядність вихідної шини.

Для модуля комбінаційного типу $D^w = D^z_{\text{комб}}$, для модуля послідовного типу $D^w = D^z_{\text{посл}}$. В узагальненому модулі при протіканні ЕДП значенню напруги $U_{\text{узаг}}$ шини живлення відповідає струм споживання $I_{\text{узаг}}$. При цьому для модуля комбінаційного і послідовного типів $I_{\text{узаг}} = I_{\text{комб}} \cup I_{\text{посл}}$.

Таким чином, ММ $l$-го узагальненого модуля має наступний вид:

$$\text{М}^l_F = F(T, D^I, D^w, \Phi^w, I_{\text{узаг}}, \text{J}),$$

де $\Phi^w$ – множина функцій, що визначають значення $D^w$ відповідного типу модуля при відомих $T$, $J$ і $D^w$. Допоміжним параметром, який характеризує складність розробленої функціональної моделі мікроконтролера, являється формат множини функцій $\Phi^w$ перемінних J, $D^w$, $D^I$, що визначає їх розмірність, тобто $\Phi^w = \langle D^I, D^w, \text{J} \rangle$ [12].

Зважаючи на те, що шина живлення є загальною для всіх елементів, які складають мікроконтролер, можна стверджувати, що при урахуванні характеристик ЕДП в об'єкті діагностування буде справедливим наступний вираз:

$$I_{\text{узаг}} = F(\Phi_i^w(D^I(\text{J}_i))).$$

Математична модель мікроконтролера, яка представлена на рисунку 2, має наступний вид:

$$\text{М}_F^{\text{віс}} = F(\sum_l \text{М}_F^l, D^C, \Phi, D^S, D^Z),$$

де $l$ – кількість модулів в мікроконтролері.

Таким чином, узагальнена ММ цифрового ТЕЗ (див. рисунок 1) може бути представлена в наступному вигляді [13]:

$$\text{М}_F^{\text{тез}} = F(\sum_k \text{М}_F^{k,\text{віс}}, I), \quad (3)$$

де $k$ – кількість ВІС на ТЕЗ.

**На четвертому етапі** здійснюється моделювання процесу взаємодії, розробленої узагальненої ММ модуля мікроконтролера з зовнішнім середовищем і аналіз ступеня адекватності ММ цифрового ТЕЗ реальним фізичним об'єктам. Для цього розглянемо взаємодію модулів комбінаційного і послідовного типів з зовнішнім середовищем.

Аналізуючи вираз (1), можна стверджувати, що для модуля комбінаційного типу при виконанні будь-якої заданої інструкції $\text{J}_i \in \text{J}$ значення вихідної перемінної $D^w(\text{J}_i)$ у момент часу $t_i \in T$ буде визначатись наступним виразом:

$$D^w(\text{J}_i) = \Phi_i^w(D^I(\text{J}_i)), \qquad i = \overline{1,d}, \quad (4)$$

де $D^I(\text{J}_i)$ – значення в даний момент часу $t_i \in T$ підмножини перемінних вхідних діянь, що беруть участь у виконанні інструкції $\text{J}_i$; $\Phi_i^w$ – функція, визначена інструкцією $\text{J}_i$.

Для визначення ВР і реакції в шині живлення модуля послідовного типу в момент часу $t_i \in T$ крім зовнішньої складової ВД $D_i^x$ необхідно визначити значення внутрішньої складової вхідного діяння $D_i^Y$. Перемінна $D_i^Y$ відповідає значенню вихідної перемінної $D^w$, визначеної на попередньому такті в момент часу $t_{i-1} \in T$, тобто

$$D^{Yt_i} = D^{wt_{i-1}}.$$

У цьому випадку значення $D^{wt_{i-1}}$ визначається згідно з виразом (4). Зі зміною інструкції змінюється функція, яку виконує модуль, тобто $\text{J}_i \to \Phi_i^w$. Будемо вважати, що всі функції з множини $\Phi^w$ в модулі здійснюються роздільно [13].

Перемінні стану $\{D_1^Y, ..., D_i^Y, ..., D_h^Y\}$ модуля змінюються тільки під дією синхросигналів $\gamma_c$ з множини J. Таким чином, при наявності у керуючому діянні синхросигналу $\gamma_c$ значення перемінної $D^Y$ визначається згідно з формулою (4), що відповідає значенню $D^{Yt_i}$, визначеному в модулі після надходження синхросигналу $\gamma_c$. Якщо перемінною $D^{Yt_i}$ керують декілька синхросигналів $\gamma_c$, то в тактовий момент часу $t_i \in T$ можна реалізувати тільки один синхросигнал. Для однозначного визначення перемінної $D^Y$ синхросигнал потрібно реалізувати після того, як були змінені всі інші перемінні керуючого сигналу J і ВД $D^I$. При відсутності синхросигналу $\gamma_c$ йому присвоюється нейтральне значення, яке показує, що значення перемінної стана $D^Y$ не змінюється, тобто $D^{Yt_{i+1}} = D^{Yt_i}$. [14].

Розрахунок значень вихідних перемінних модулів виконується наступним чином. Для послідовного з'єднання модулів комбінаційного і послідовного типів при ВД, який містить в собі синхросигнал, значення вихідних перемінних комбінаційних модулів визначається, виходячи зі значень перемінних стана заданих в момент $t_i$, тобто до реалізації синхросигналу. При цих же ВД значення вихідних перемінних послідовних модулів визначаються після реалізації синхросигналу. Значення вихідних перемінних комбінаційних модулів, які

визначені після реалізації синхросигналу, визначаються на наступному ВД, в якому всім синхросигналам призначено нейтральні значення, а перемінним стана $D^{Y\,t_i}$ – значення, які установилися на попередньому вхідному наборі. В загальному випадку значення вихідних перемінних модулів ТЕЗ визначаються за допомогою послідовних вхідних даних (ВД), які складаються з двох наборів. В першому наборі реалізуємо синхросигнал, інструкцію $J_i$, яка визначає функцію $\Phi_i^w$ модуля, і визначає значення перемінної стана. В другому наборі за допомогою вхідних перемінних $D^I$ визначаємо значення перемінних стана $D^Y$.

**Висновки.** Показаний розрахунок значень вихідних перемінних узагальненого модуля відповідає дійсним фізичним об'єктам і може бути використаний для моделювання процесу взаємодії в ММ цифрового ТЕЗ. Як видно вираз (3) є узагальнюючим і справедливим для будь якого ТЕЗ. Таким чином, розроблена узагальнена математична модель цифрового ТЕЗ з урахуванням ЕДП відображає реальні фізичні процеси, які протікають в ТЕЗ, універсальна і може бути використана в якості базової моделі для розгляду типових дефектів, розробки загальних правил та методики побудови тесової послідовності і розробки методу контролю технічного стану цифрових ТЕЗ з урахуванням ЕДП.

ЛІТЕРАТУРА:


1. Василишин В.І., Женжера С.В., Чечуй О.В., Глушко А.П. Основи теорії надійності та експлуатації радіоелектронних систем. Харків: ХНУПС, 2018, 268 с.
2. Багринцев В.Т. Компьютерная электроника и микропроцессоры: Учебное пособие / В.Т. Багринцев, В.В. Багринцев, В.А. Ульшин. - Луганск: Изд-во "Ноулидж", 2010, 376 с.:
3. Вишнівський В.В. Аналіз методів форсованих випробувань для отримання залежності зміни діагностичного параметра від часу напрацювання напівпровідникових РЕК / В. В. Вишнівський, В.В. Василенко, В.В. Кузавков // Системи управління, навігації та зв'язку. – П.: ПНТУ. – 2015. – Вип. 1(33). – С. 18-21.
4. Вишнівський В.В. Проблема побудови та впровадження автономних автоматизованих систем діагностування радіоелектронного озброєння / В.В. Вишнівський, В.В. Кузавков, Г.І. Гайдур // Науковий журнал Інформаційна безпека Східно український національний університет ім. Володимира Даля. – Луганськ, 2014. – Вип. № 4(16). – С. 151-157.
5. Волошин, О. Ф. Моделі та методи прийняття рішень : навч. посіб. для студ. вищ. навч. закл. / О. Ф. Волошин, С. О. Мащенко. - 2-ге вид., перероб. та допов. - К. : Видавничо-поліграфічний центр "Київський університет", 2010. - 336 с.
6. Жердєв М.К. Концептуальні засади методу діагностування сучасних цифрових типових елементів заміни по форматним частотам перехідного процесу в шині живлення/М.К. Жердєв, В.О. Савран // Збірник наукових праці Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2016.- Вип.52. – С 20-32.
7. Жердєв М.К. Узагальнення результатів форсованих випробувань радіоелектронних компонентів / М.К. Жердєв, В.В. Кузавков // Збірник наукових праць Військового інституту Київського національного університету ім. Т. Шевченка. – К., 2015. – № 49. – С. 40-48.
8. Жиров Г.Б. Узагальнена діагностична модель цифрової ВІС для енергостатичного методу діагностування /Г.Б. Жиров // Вісник КНУ ім. Тараса Шевченка. – Сер. Військово-спеціальні науки. – К.: Київ. ун-т, 2005. – Вип. 11. – С. 55-60.
9. Надійність систем з надлишковістю: методи, моделі, оптимізація: [монографія] / Б. П. Креденцер [та ін. ; під наук. ред. д-ра техн. наук, проф. Б. П. Креденцера; Нац. техн. ун-т України "Київ. політехн. ін-т". - К.: Фенікс, 2013. - 341 с.
10. Ланецкий Б. Н. Адаптивное управление техническим состоянием и надежностью сложных технических систем в условиях ресурсных ограничений / Б. Н. Ланецкий, В. В. Лукьянчук // Системи озброєння і військова техніка. – Х. : ХУПС, 2011. – Вип. 2 (26). – С. 149–151.

11. Зубарєв В.В., Ковтуненко А. П., Раскин Л. Г. Математические методы оценки и прогнозирования технических показателей эксплуатационных свойств радиоэлектронных систем .Киев. Книжное изд-во НАУ, 2007. 296 с.

12. Кулик І. В. Засоби автоматизованої оцінки показників ефективності стратегій технічного обслуговування і ремонту систем радіоелектронного комплексу: автореф. дис. ... канд. техн. наук : 05.12.17 Львів, 2013. 20 с.

13. Шкуліпа П.А. Шляхи і методи підвищення ефективності автономних автоматизованих систем технічного діагностування радіоелектронних пристроїв спеціального призначення / П.А. Шкуліпа, М.К., Жердєв, С.В. Лєнков, Ю.О. Гунченко // Журнал «Сучасна спеціальна техніка», 2012. – № 3 (30). – С 69 – 74.

14. Шкуліпа П.А. Основні напрямки розвитку автоматизованих систем технічного діагностування об'єктів радіоелектроніки / П.А. Шкуліпа // Вісник Хмельницького національного університету. Технічні науки. – Хмельницький, 2012. – № 6.– С. 192 – 194.

REFERENCES:

1. Vasilishin V.I., Zhenzhera S.V., Chechuj O.V., Glushko A.P.(2018), "Osnovi teoriyi nadijnosti ta ekspluataciyi radioelektronnih sistem. [Basics of the theory of reliability and operation of radio electronic systems ], Harkiv, HNUPS, 268 p.

2. Bagrincev V.T., Bagrincev V.V., Ulshin V.A., "Kompyuternaya elektronika i mikroprocessory: Uchebnoe posobie" [Computer Electronics and Microprocessors: Study Guide], Lugansk, Izd-vo Noulidzh, 376 p.

3. Vyshnivskyi V.V., Vasylenko, V.V., Kuzavkov V.V." Analiz metodiv forsovanykh vyprobuvan dlia otrymannia zalezhnosti zminy diahnostychnoho parametra vid chasu napratsiuvannia napivprovidnykovykh REK" [Analysis of forced test methods to obtain the dependence of the diagnostic parameter change on the operating time of semiconductor RECs], Management, navigation and communication systems. PNTU. Issue 1(33). pp. 18-21.

4. Vishnivskij V.V. Problema pobudovi ta vprovadzhennya avtonomnih avtomatizovanih sistem diagnostuvannya radioelektronnogo ozbroyennya / V.V. Vishnivskij, V.V. Kuzavkov, G.I. Gajdur // Naukovij zhurnal Informacijna bezpeka Shidno ukrayinskij nacionalnij universitet im. Volodimira Dalya. – Lugansk, 2014. – Vip. № 4(16). – S. 151-157.

5. Voloshin, O. F., Mashenko S. O., (2010) "Modeli ta metodi prijnyattya rishen : navch. posib. dlya stud. vish. navch. zakl" [Decision-making models and methods: teaching. manual for students higher education closing ], Vidavnicho-poligrafichnij centr , Kiyivskij universitet, 336 p.

6. Zhierdev M.K., Savran V.O.,(2016) Kontseptualni zasady metodu diahnostuvannia suchasnykh tsyfrovykh typovykh elementiv zaminy po formatnym chastotam perekhidnoho protsesu v shyni zhyvlennia [Conceptual foundations of the method of diagnosing modern digital typical replacement elements by the format frequencies of the transition process in the power bus], Collection of scientific works of the Military Institute of Taras Shevchenko Kyiv National University.K. VIKNU, Issue 52, pp. 20-32.

7. Zherdiev, M.K., Kuzavkov, V.V. (2015), "Uzahal'nennia rezul'tativ forsovanykh vyprobuvan' radioelektronnykh komponentiv" [Summary of results of the forced test of radio-electronic components], Zbirnyk naukovykh prats' Vijs'kovoho instytutu Kyivs'koho natsional'noho universytetu imeni Tarasa Shevchenka, No. 49, Kyiv, pp. 40-48.

8. Zhyrov H.B.(2005),"Uzahalnena diahnostychna model tsyfrovoi VIS dlia enerhostatychnoho metodu diahnostuvannia" Generalized diagnostic model of digital VIS for the energy-static method of diagnosis], Bulletin of KNU named after Taras Shevchenko. Sir Military special sciences. K.: Kyiv. University, No.11 pp 55-60.

9. Kredencer B. P.(2013) "Nadijnist sistem z nadlishkovistyu: metodi, modeli, optimizaciya" [Reliability of systems with redundancy: methods, models, optimizatio], Nac. tehn. un-t Ukrayini "Kiyiv. politehn. in-t, Feniks, 341 p.

10. Laneckij B. N., Lukyanchuk V.V., (2011) “Adaptivnoe upravlenie tehnicheskim sostoyaniem i nadezhnostyu slozhnyh tehnicheskih sistem v usloviyah resursnyh ogranichenij”, [Adaptive control of the technical condition and reliability of complex technical systems under resource constraints], Sistemi ozbroyennya i vijskova tehnika, HUPS, Vip. 2 (26) pp. 149–151.

11. Zubaryev V.V., Kovtunenko A. P., Raskin L. G. (2007) “Matematicheskie metody ocenki i prognozirovaniya tehnicheskih pokazatelej ekspluatacionnyh svojstv radioelektronnyh sistem” [ Mathematical methods for assessing and predicting the technical indicators of the operational properties of radio electronic systems ], Knizhnoe izd-vo NAU, Kiev. 296 p.

12. Kulik I. V. (2013), Means of automated evaluation of indicators of effectiveness of strategies of technical maintenance and repair of systems of radio-electronic complex. Extended abstract of candidate’s thesis. Lviv: ONTU [in Ukrainian].

13. Shkulipa P.A., Zherdyev M.K., Lyenkov S.V., Gunchenko Yu.O. (2012) “Shlyahi i metodi pidvishennya efektivnosti avtonomnih avtomatizovanih sistem tehnichnogo diagnostuvannya radioelektronnih pristroyiv specialnogo priznachennya ” [Ways and methods of increasing the efficiency of autonomous automated systems technical diagnostics of special purpose radio electronic devices], Zhurnal Suchasna specialna tehnika, № 3 (30). pp 69 – 74.

14. Shkulipa P.A. (2012) “Osnovni napryamki rozvitku avtomatizovanih sistem tehnichnogo diagnostuvannya ob’yektiv radioelektroniki” [The main directions of the development of automated systems for technical diagnostics of radio electronics objects], Visnik Hmelnickogo nacionalnogo universitetu. Tehnichni nauki, Hmelnickij, № 6. pp.192 – 194.

**Doctor of Technical Sciences Hlukhov S.V.,**
**PhD Gakhovych S.V.,**
**PhD Okhramovych M.M.,**
**PhD Koval M.O.,**
**PhD Kravchenko O.I.**

## MODEL OF A DIGITAL STANDARD REPLACEMENT ELEMENT WITH INTEGRATEDUSE OF DIAGNOSTIC INFORMATION SOURCES

***The paper presents the procedure for organizing the study of technical condition control in modern radio-electronic equipment, which is made on the element base of the fourth and fifth generations. The complex use of several methods of performance control is shown in digital standard replacement elements containing microcontrollers and calculated values of the output variables of the generalized module that correspond to real physical objects and could be used in the mathematical model of a digital standard replacement element. To reduce the number of test points in the diagnosis of digital standard replacement elements, as a source of diagnostic information used the parameters of the energy-dynamic process that occur in the power bus of digital elements when they switch from one logical state to another. This makes it possible to reduce the number of control points to one (power bus), while obtaining diagnostic information about technical condition of each logical element.***

***The study is divided into four stages, which include:***

***- analysis of the internal structure and allocation of subsystems in a typical replacement element;***

***- decomposition of a typical replacement element and allocation of groups of variables;***

***- synthesis of the structural and functional model of a digital typical replacement element;***

***- simulation of the process of interaction of the developed mathematical model of the generalized microcontroller module with the external environment, analysis of the degree of adequacy of the model to real physical objects. In summary, the structural-functional model of a digital typical replacement element, which provides for the integrated use of two sources of diagnostic information: output reactions and characteristics of the energy-dynamic process in the power bus digital thesis.***

***Keywords: energy-dynamic diagnostic method, radio-electronic equipment, mathematical model, source of diagnostic information, typical replacement element.***

УДК 358:623.3

д.т.н., проф. **Довгополий А.С.** (ЦНДІ ОВТ ЗСУ)
д.т.н., проф. **Коцюруба В.І.** (НУОУ)
к.т.н., с.н.с. **Кривцун В.І.** (НАСВ, м. Львів)

DOI: https://doi.org/10.17721/2519-481X/2022/77-02

# МОДЕЛЮВАННЯ ПРОЦЕСІВ ВИЯВЛЕННЯ ВИБУХОНЕБЕЗПЕЧНИХ ПРЕДМЕТІВ ІНДУКЦІЙНИМ МЕТОДОМ НА ОСНОВІ РЕЗУЛЬТАТІВ ЕКСПЕРИМЕНТАЛЬНИХ ДОСЛІДЖЕНЬ

***З початком ведення неоголошеної війни російської федерації проти України у 2014 році, а у подальшому широкомасштабного вторгнення у лютому 2022 року дуже гостро постало питання розвідки та розмінування місцевості від вибухобезпечних предметів як під час виконання ведення бойових дій так і при відсутності їх. Досвід війни показує, що противник незважаючи на міжнародні конвенції щодо заборони певних видів мінної зброї, застосовує весь свій наявний арсенал мін та саморобні вибухові пристрої, які часто встановлюються на невилучаємість. Окрім мін та саморобних вибухових пристроїв територія України, де ведуться бойові дії або звільнені забруднена великою кількість різних боєприпасів, які не розірвалися.***

***Аналіз виконання завдань щодо розвідки та розмінування інженерними підрозділами ЗС України показує, що основним способом на сьогоднішній день залишається ручний, який є вкрай небезпечним для життя особового складу. З метою забезпечення виконання цих завдань ведеться робота щодо створення вітчизняних засобів дистанційної розвідки та розмінування. Однією і складових таких засобів є пошукові елементи вибухонебезпечних предметів, які працюють на різних фізичних принципах. Окрім теоретичних положень одним із важливих його етапів є проведення експериментального дослідження. В статті на основі раніше розроблених теоретичних положень наведено моделювання процесів виявлення вибухонебезпечних предметів індукційним методом під час проведення однофакторного експерименту з метою обґрунтування окремих показників ефективності елементів пошуку вибухонебезпечних предметів дистанційно-керованих комплексів розмінування.***

***Ключові слова: бойові дії; вибухонебезпечні предмети; розмінування; дистанційно-керований комплекс розмінування, експериментальні дослідження, індукційний метод, фактори, показники.***

**Вступ.** Аналіз ведення бойових дій у війні російської федерації проти України показує масове застосування мінно-вибухових загороджень як підрозділами ЗС України так і противником. Всупереч вимогам міжнародних конвенцій із заборони окремих видів мін противник застосовує весь наявний спектр мінної зброї, саморобні вибухові пристрої, фугаси, міни-пастки. Тактика дій противника передбачає під час відступу мінування як об’єктів інфраструктури так і жилих будівель і приміщень, в наслідок чого гинуть не тільки військові але і цивільне населення. Встановлення мінних полів, вузлів загороджень, групи та окремих мін, а також саморобних вибухових пристроїв та керованих фугасів призводить не тільки до знищення техніки та особового складу, а й до затримки військ, що наступають та примушення рухатись противника у вигідному напрямку [1-3]. В цих умовах під час наступальних (контрнаступальних) дій підрозділи ЗС України стикаються з проблемою подолання мінно-вибухових загороджень. Під час заняття районів розташування виникає питання щодо перевірки місцевості на наявність вибухонебезпечних предметів (ВНП).

Ще одним небезпечним наслідком ведення бойових дій є забруднення території боєприпасами, які не розірвалися. Війна російської федерації проти України призвела до того, що Україна стала однією з найбільш забруднених ВНП країн світу. Тільки станом на березень 2022 року за інформацією асоціації саперів України орієнтовне забруднення території України ВНП складає більше 82,5 тисяч квадратних кілометрів, за іншою інформацією ця цифра доходить до третини території країни [4,5]. Щодня ця територія збільшується та надходять повідомлення про підрив як цивільного населення так і військових. З початком російської

агресії в 2014 році Україна стала займати лідируючі позиції у світі за кількістю втрат цивільного населення від підриву на ВНП [6-8]. Зрозуміло, що на сьогоднішній день ситуація значно погіршилася, дані втрат уточняються.

Таким чином, Україна стикнулася з проблемою розвідки та розмінування у великих масштабах як під час ведення бойових дій так і в мирний час. Вирішення зазначеної проблеми можливо за рахунок створення перспективних дистанційно керованих (роботизованих) комплексів розмінування.

**Постановка проблеми.** Аналіз ведення бойових дій в війнах та конфліктах сучасності, миротворчих операціях та війні рф проти України показує, що темпи розвитку мінної зброї значно перевищують темпи розвитку протимінних засобів. Провідні країни світу забруднення територій ВНП вже кілька десятиліть сприймають це як загальносвітову проблему та вживають ряд заходів щодо її вирішення. Насамперед це створення міжнародних стандартів з розвідки та розмінування місцевості від ВНП та дистанційних (роботизованих) засобів виконання таких завдань [7-14]. Проте, питання забезпечення якості та безпеки виконання завдань очищення місцевості на сьогоднішній день в повному обсязі так і не вирішено, що і обумовлює подальше поширене застосування ручного способу розмінування, який є вкрай витратним та небезпечним. Завдання по подоланню МВЗ, перевірки місцевості на ВНП та розмінування в основному виконуються підрозділами інженерних військ, які на своєму оснащенні мають відповідні засоби розвідки та розмінування.

Досвід виконання цих завдань підрозділами ЗС та ДСНС України показує, що засоби розвідки місцевості та знищення ВНП, які знаходяться на їх оснащенні, застарілі, в наслідок чого ручний спосіб розмінування залишається основним. В наслідок такого стану щодня приходять відомості про втрати особового складу підрозділів інженерних військ, які виконують бойові завдання з розвідки місцевості на наявність ВНП та їх знищення, пророоблення проходів в МВЗ, супроводу колон тощо.

Отже, враховуючі все вище зазначене, у практиці розмінування значно загострюється потреба підвищення якості, оперативності та безпеки процесів, пошуку, виявлення, знищення або знешкодження ВНП. З метою забезпечення безпеки особового складу саперів та забезпечення вимог до процесу розвідки і розмінування актуальним питанням є створення дистанційно керованих (роботизованих) комплексів розмінування з обґрунтуванням відповідних параметрів. Однією з складових таких комплексів є пошуковий пристрій, в якості якого можуть використовуватися міношукачі, зокрема індукційні, які перебувають на озброєнні інженерних підрозділів.

Частково вирішити усунення вказаних невідповідностей можливо за рахунок впровадження експериментально підтверджених параметрів перспективних дистанційно керованих комплексів розмінування, які будуть оснащуватися індукційними пошуковими пристроями (міношукачами).

**Аналіз останніх досліджень і публікацій** [15-22] показав, що в них піднято та розглянуто часткові наукові задачі. Так відомі праці [15-21] присвячені висвітленню результатів наукових досліджень, спрямованих на моделювання процесів та обґрунтування вимог до засобів пошуку та виявлення ВНП різними методами, розглядаються аспекти дистанційного знищення ВНП. Проте, отримані результати, як правило, були перевірені методами математичного моделювання, без підтвердження їх натурними експериментами.

Проведений аналіз відомих доступних досліджень і публікацій дозволив дійти висновку, що задача проведення експериментальних досліджень можливості використання перспективних засобів пошуку та виявлення ВНП за допомогою дистанційно-керованих рухомих платформ (ДКРП) оснащеними індукційними пошуковими пристроями із врахуванням характеру мінування та типажу ВНП, що застосовуються під час ведення бойових дій, на сьогодні вирішена не у повному обсязі. Отже, підняте питання залишається актуальним і вимагає проведення подальших досліджень.

**Мета статті** полягає у висвітлені результатів однофакторного експерименту, на основі якого проведено моделювання та підтверджена доцільність використання переносних

індукційних імпульсних засобів пошуку ВНП, встановлених на ДКРП для побудови перспективних дистанційно-керованих комплексів розмінування (ДККР).

**Виклад основного матеріалу дослідження.** В роботі [23] була запропонована методика проведення експериментальних досліджень показників ефективності дистанційно-керованих комплексів розмінування. На основі цієї методики був проведений однофакторний експеримент із застосуванням в якості пошукового елементу індукційного імпульсного міношукача типу ИМП-2 (ПР-507).

Матеріально-технічним забезпеченням випробування були: дослідні ДКРП; макети учбових протитанкових мін типу ТМ-62М та протипіхотних мін типу ПМН-2; пошукове обладнання для розмінування: індукційний імпульсний міношукач типу ИМП-2 (ПР-507), прилади для вимірювання просторових параметрів (відстані, глибини встановлення); лінійка металева, штангенциркуль; ПЕОМ із осцилографом; пристрій фото- та відео-фіксації.

Загальна схема дослідження наведена на рис. 1.

Основними показниками, які досліджувалися були: $y_1$ – амплітуда сигналу ($A$, мВ); $y_2$ – період ($T$, мкс); $y_3$ – частота ($f$, Гц); $y_4$ – повздовжня ширина зони захвату ($l_y$,см); $y_5$ – поперекова ширина зони захвату ($l_x$, см). Задача полягала у визначенні висоти доцільного розташування пошукового обладнання над рівнем міни.

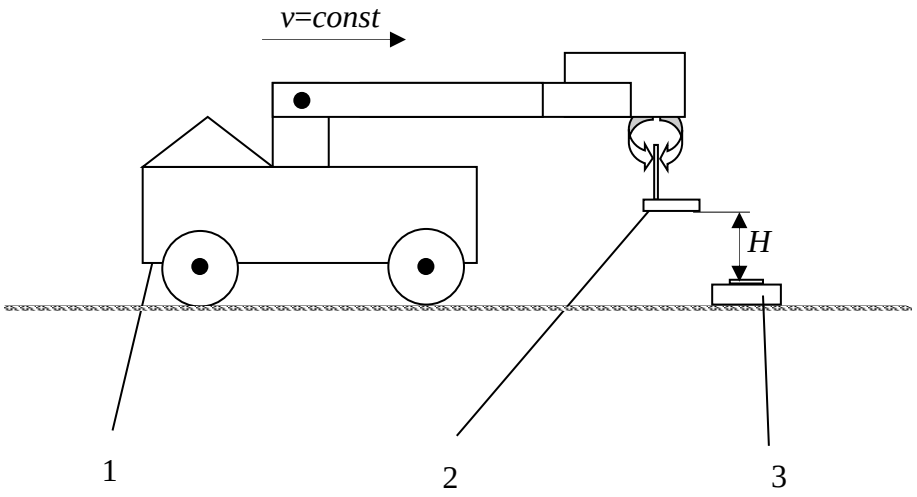



Рисунок 1 – Схема дослідження: 1 – ДКРП; 2 – антенний пристрій пошукового обладнання; 3 – міна або ВНП

В якості дистанційно-керованої рухомої платформи в умовах лабораторних випробувань використовувалась платформа ДКРП-1 (рис. 2).

Для проведення однофакторного експерименту (лабораторних випробувань) пошукове обладнання готувалось для роботи з одним коліном із додатковим дообладнанням пошукових елементів типу ИМП-2 (рис. 3) гвинтовим кріпленням із шайбою.

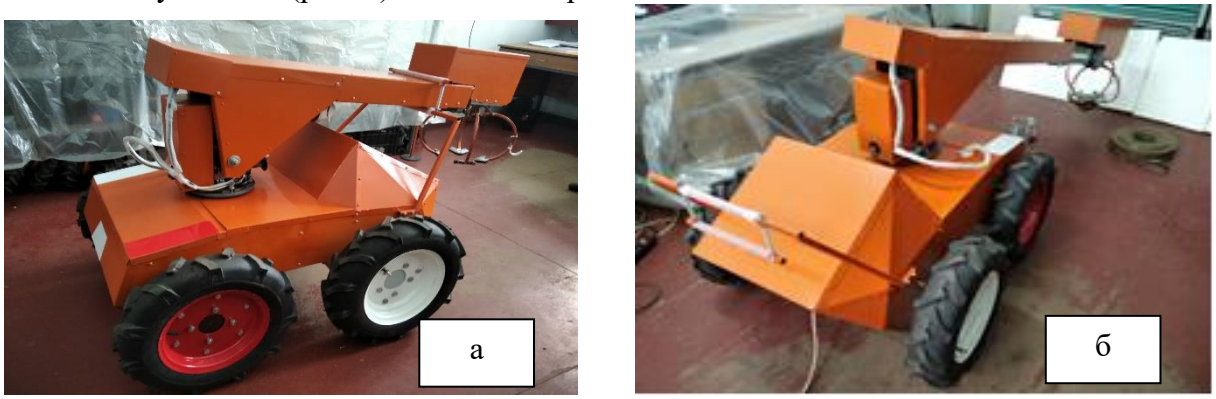



Рисунок 2 – Дистанційно керована рухома платформа ДКРП-1 (лабораторні випробування): а – транспортне положення; б – робоче положення

Утримання пошукового елементу під час проведення однофакторного експерименту (лабораторних випробувань) здійснювалось за допомогою захоплюючого пристрою (грейфера) маніпулятору.

**Результати проведення однофакторного експерименту**

Під час експерименту була визначена динаміка зміни значень обраних показників періоду (*T*), частоти (*f*) та амплітуди (*A*) сигналу при застосуванні різних типів інженерних мін та ВНП, зафіксовані за допомогою осцилографа.

Рисунок 3 – Варіант кріплення пристроїв для проведення експериментальних досліджень індукційного імпульсного типу ИМП-2 (ПР-507)

При проведенні експериментальних досліджень встановлено, що при використанні індукційного імпульсного методу виявлення ВНП під час збудження вторинного магнітного поля та фіксації його прийомною антеною пошукового елементу реєструються зміни параметри всіх трьох раніше вказаних показників: амплітуди (*A*), періоду (*T*) та частоти (*f*) сигналу.

На відміну від міношукача типу ИМП (індукційного з постійним магнітним полем) даний тип міношукача ИМП-2 (ПР-507) є більш чутливим до металевих предметів малої маси. Тому досліди проводились із використанням макетів як протитанкової міни типу ТМ-62М (в металевому корпусі) так і протипіхотної міни типу ПМН, що містить незначну кількість металу.

***Реагування на протитанкову міну типу ТМ-62М***

Динаміка зміни амплітуди сигналу (*A*) залежно від висоти над відкрито розташованою міною (*H*) та наближення до її центру ($l_y$) при повздовжньому переміщенні пошукового елемента та наведена у таблиці 1.

Значення показника амплітуди сигналу (*A*, В) залежно від висоти над відкрито розташованою протитанковою міною (*H*, см) та наближення до її центру ($l_y$, см) при повздовжньому переміщенні пошукового елемента.

Таблиця 1

| Висота над міною *H*, см | Наближення до центру міни ($l_y$, см) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | -30 | -20 | -10 | 0 | 10 | 20 | 30 | 40 | 50 | 60 |
| 10 | 0 | 1,54 | 1,32 | 1,36 | 1,315 | 1,27 | 1,36 | 1,45 | 0 | 0 |
| 15 | 0 | 0 | 1,36 | 1,45 | 1,45 | 1,45 | 1,455 | 1,46 | 0 | 0 |
| 20 | 0 | 0 | 1,47 | 1,37 | 1,41 | 1,45 | 1,465 | 1,48 | 0 | 0 |
| 25 | 0 | 0 | 0 | 1,49 | 1,535 | 1,58 | 0 | 0 | 0 | 0 |

Синтез результатів статистичних досліджень щодо значень показника амплітуди сигналу ($A$) наведено на рис. 4. Аналіз отриманих результатів показав, що при відсутності вторинного магнітного поля, що утворюється при наявності металевих предметів в межах первинного імпульсного магнітного поля, значення показника амплітуди сигналу ($A$) є відносно малим та дорівнює 24...27 мВ.

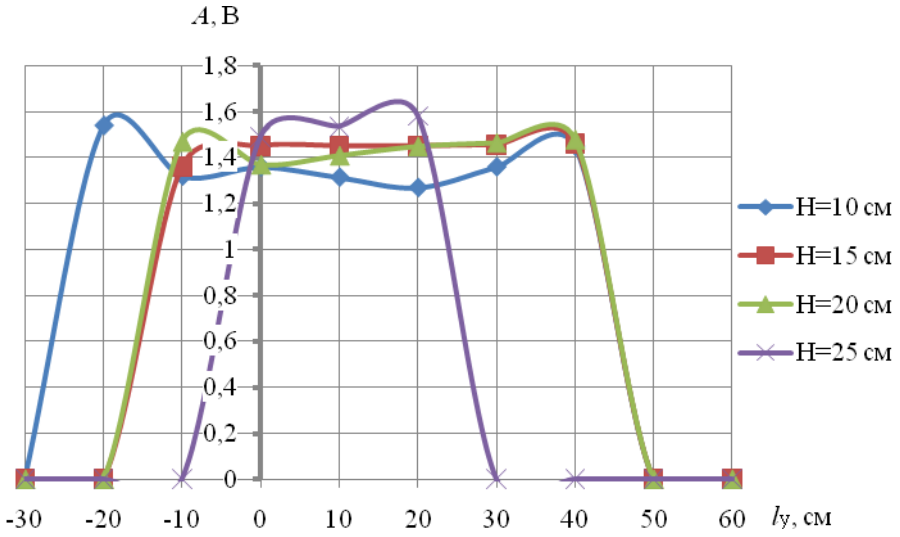



Рисунок 4 – Залежність значення показника амплітуди сигналу ($A$, В) від висоти над відкрито розташованою протитанковою міною ($H$, см) та наближення до її центру ($l_y$, см) при повздовжньому переміщенні пошукового елемента

При наближенні пошукового елементу до центра протитанкової міни типу ТМ-62М на відстань $l_y \approx$ –25...-20 см фіксується різке збільшення амплітуди до 1,25...1,63 В. При подальшому переміщені та при розташуванні пошукового елементу безпосередньо над центром міни зафіксовано незначні зниження амплітуди на 0,5...1,0 В. При наближенні до дальньої межі зони фіксації вторинного магнітного поля (відстань $l_y \approx$ + 20...40 см) показник амплітуди сигналу відновлюється до попереднього максимального значення. Після проходження відстані +25...+45 см (для різної висоти розташування пошукового елементу відносно поверхні міни) відмічається різке зменшення амплітуди до рівня не збудженого стану.

Динаміка зміни періоду сигналу ($T$) залежно від висоти над відкрито розташованою міною ($H$) та наближення до її центру ($l_y$) при повздовжньому переміщенні пошукового елемента та наведена у таблиці 2. Значення показника періоду сигналу ($T$, мкс) залежно від висоти над відкрито розташованою протитанковою міною ($H$, см) та наближення до її центру ($l_y$, см) при повздовжньому переміщенні пошукового елемента.

Таблиця 2

| Висота над міною $H$, см | Наближення до центру міни ($l_y$, см) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | -30 | -20 | -10 | 0 | 10 | 20 | 30 | 40 | 50 | 60 |
| 10 | 0 | 88 | 70 | 73 | 72 | 71 | 68 | 65 | 0 | 0 |
| 15 | 0 | 0 | 248 | 63 | 66,5 | 70 | 226 | 382 | 191 | 0 |
| 20 | 0 | 0 | 279 | 76 | 72 | 68 | 189,5 | 311 | 0 | 0 |
| 25 | 0 | 0 | 41,58 | 126 | 94,5 | 63 | 0 | 0 | 0 | 0 |

Синтез результатів статистичних досліджень щодо значень показника періоду сигналу ($T$) наведено на рис. 5.

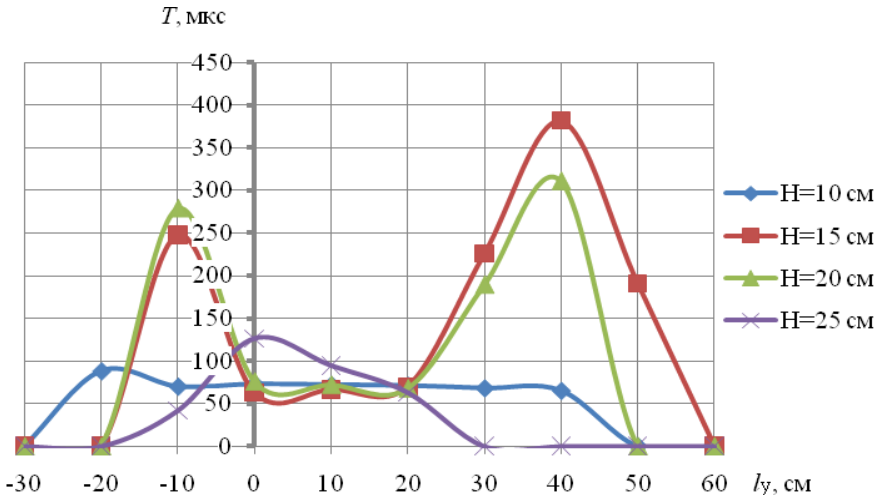



Рисунок 5 – Залежність значення показника періоду сигналу ($T$, мкс) від висоти над відкрито розташованою протитанковою міною ($H$, см) та наближення до її центру ($l_y$, см) при повздовжньому переміщенні пошукового елемента

Динаміка зміни частоти сигналу ($f$) залежно від висоти над відкрито розташованою міною ($H$) та наближення до її центру ($l_y$) при повздовжньому переміщенні пошукового елемента та наведена у таблиці 3. Значення показника частоти сигналу ($f$, кГц) залежно від висоти над відкрито розташованою протитанковою міною ($H$, см) та наближення до її центру ($l_y$, см) при повздовжньому переміщенні пошукового елемента.

Таблиця 3

| Висота над міною $H$, см | Наближення до центру міни ($l_y$, см) | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | -30 | -20 | -10 | 0 | 10 | 20 | 30 | 40 | 50 | 60 |
| 10 | 0 | 11,4 | 14,3 | 13,7 | 13,9 | 14,1 | 14,7 | 15,4 | 0 | 0 |
| 15 | 0 | 0 | 4,0 | 15,9 | 15,0 | 14,3 | 4,4 | 2,6 | 5,2 | 0 |
| 20 | 0 | 0 | 3,6 | 13,2 | 13,9 | 14,7 | 5,3 | 3,2 | 0 | 0 |
| 25 | 0 | 0 | 24,1 | 7,9 | 10,6 | 15,9 | 0 | 0 | 0 | 0 |

Синтез результатів статистичних досліджень щодо значень показника частоти сигналу ($f$) наведено на рис. 6.

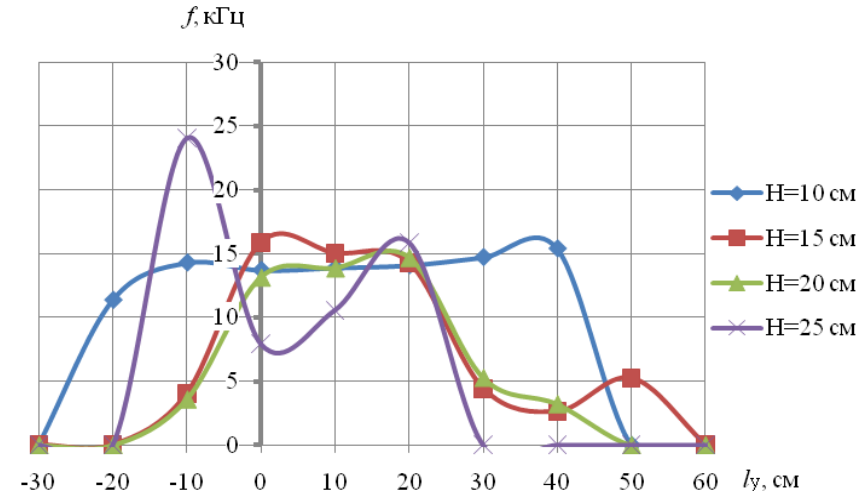



Рисунок 6 – Залежність значення показника частоти сигналу ($f$, кГц) від висоти над відкрито розташованою протитанковою міною ($H$, см) та наближення до її центру ($l_y$, см) при повздовжньому переміщенні пошукового елемента

Результати розрахунків (рис. 6) показали, що за зміною значення показника періоду сигналу (*T*) фіксація факту наявності протитанкової міни типу ТМ-62М можлива при розташуванні пошукового елементу на висоті відносно поверхні відкрито розташованої міною *H,* = 15...20 см та наближення до її центру ($l_y$,) при повздовжньому переміщенні пошукового елемента від -20 см до +40...50 см.

При наближенні до центру міни на тих же висотах розташування пошукового елементу відносно поверхні міни та при повздовжньому проходженні над нею від -10 см до +20 см зафіксовано зменшення значення періоду у шість разів до *T* = 50мкс. Вказаний провал показника може бути прив'язаний до геометричних розмірів ВНП.

Зроблені висновки щодо повздовжніх параметрів зони гарантованого виявлення, що підтверджені результатами статистичних досліджень щодо динаміки зміни значення показника частоти сигналу (*f*) залежно від висоти над відкрито розташованою міною (*H*) та наближення до її центру (*ly*) при повздовжньому переміщенні пошукового елемента.

В цілому, аналіз отриманих результатів статистичних досліджень значень показників сигналу при виявлені протитанкових мін типу ТМ-62М (аналогічних мін в металевих корпусах) під час здійснення пошуку за допомогою міношукача типу ИМП-2 (ПР-507) дозволив дійти висновку щодо можливості створення образів мін за обраними показниками. При цьому, ширина смуги зони реєстрації появи вторинного магнітного поля від металевого предмету може бути прийнята рівною 0,5 м (50 см).

Для оцінювання достовірності одержаних результатів експериментальних досліджень визначені значення дисперсії та середньоквадратичного відхилення за основним показником – амплітуди сигналу (*A*) для всієї вибірки дослідів (*n* = 40) в межах зони гарантованого виявлення ВНП аналогічні ПТМ типу ТМ-62М.

Встановлено, що значення математичного очікування вказаного показника для всієї вибірки дослідів дорівнює 150,33 мВ. При цьому, середньоквадратичне відхилення $\sigma$ = 5,99 мВ. Розрахунки показали, що середня відносна похибка дорівнює 4,2%.

Виходячи з того, що *n* > 30 дослідів, середню похибку визначають як

$$m = \pm \frac{\sigma}{\sqrt{n}} = \pm \frac{5,99}{\sqrt{40}} = \pm 0,95 \ .$$

Отже, можна стверджувати, що із довірчою ймовірністю не нижче ніж 0,95 середнє значення показника амплітуди сигналу $A = 150,33 \pm 0,95$ мВ в межах всієї зони гарантованого виявлення ПТМ типу ТМ-62М пошуковим пристроєм даного типу.

***Реагування на протипіхотну міну типу ПМН-2 (мало металоємна)***

Аналогічно як і в попередніх дослідженнях процесу використання міношукача типу ИМП-2 (ПР-507) підтверджено, що при використанні індукційного імпульсного методу виявлення ВНП під час збудження вторинного магнітного поля навіть від протипіхотної міни із малим вмістом металу та фіксації його прийомною антеною пошукового елементу реєструються зміни параметри всіх показників: амплітуди (*A*), періоду (*T*) та частоти (*f*) сигналу. Однак, за таких умов ефективна реєстрація відкрито розташованого на поверхні підлоги макета протипіхотної міни із масою металевого елементу 2...4 грами виявилась можливою лише при розташуванні пошукового елементу відносно поверхні міни на висоті до 10 см. Отже, зміна значень показників реєструвалась лише на вказаній висоті (*H*).

Динаміка зміни амплітуди сигналу (*A*) залежно від висоти над відкрито розташованою міною (*H*) та наближення до її центру ($l_y$) при повздовжньому переміщенні пошукового елемента та наведена у таблиці 4. Значення показника амплітуди сигналу (*A*, В) залежно від висоти над відкрито розташованою протипіхотною міною (*H*, см) та наближення до її центру ($l_y$, см) при повздовжньому переміщенні пошукового елемента.

Таблиця 4

| Висота над міною *H*, см | Наближення до центру міни ($l_y$, см) | | | | |
|---|---|---|---|---|---|
| | -20 | -10 | 0 | 10 | 20 |
| 10 | 0 | 0,114 | 1,45 | 0,123 | 0 |

Синтез результатів статистичних досліджень щодо значень показника амплітуди сигналу ($A$) наведено на рис. 7.

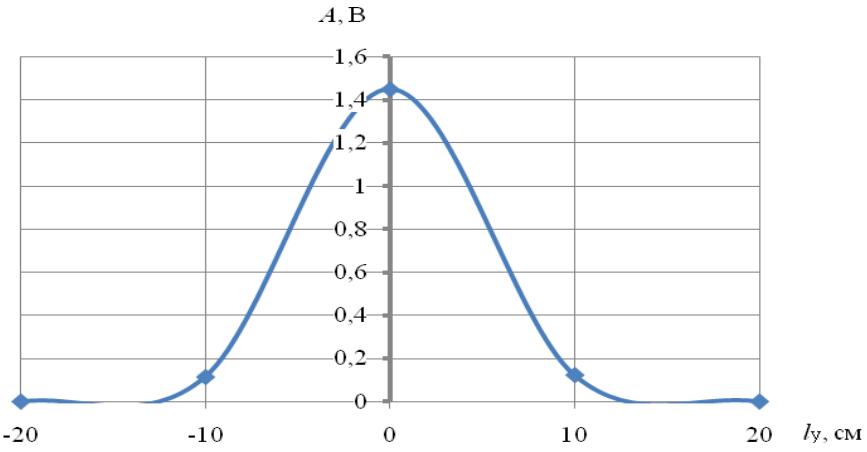



Рисунок 7 – Залежність значення показника амплітуди сигналу ($A$, мВ) від висоти над відкрито розташованою протипіхотною міною ($H$, см) та наближення до її центру ($l_y$, см) при повздовжньому переміщенні пошукового елемента

Динаміка зміни періоду сигналу ($T$) залежно від висоти над відкрито розташованою міною ($H$) та наближення до її центру ($l_y$) при повздовжньому переміщенні пошукового елемента та наведена у таблиці 5. Значення показника періоду сигналу ($T$, мкс) залежно від висоти над відкрито розташованою протипіхотною міною ($H$, см) та наближення до її центру ($l_y$, см) при повздовжньому переміщенні пошукового елемента.

Таблиця 5

| Висота над міною $H$, см | Наближення до центру міни ($l_y$, см) | | | | |
|---|---|---|---|---|---|
| | -20 | -10 | 0 | 10 | 20 |
| 10 | 0 | 0 | 68 | 454 | 0 |

Синтез результатів статистичних досліджень щодо значень показника періоду сигналу ($T$) наведено на рис. 8.

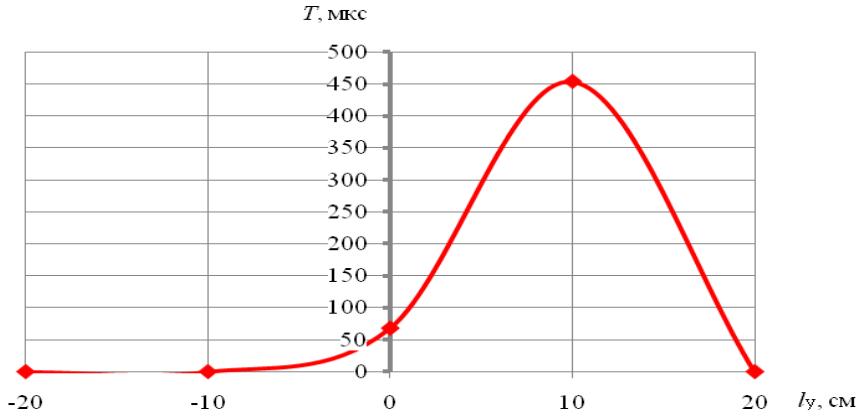



Рисунок 8 – Залежність значення показника періоду сигналу ($T$, мкс) від висоти над відкрито розташованою протипіхотною міною ($H$, см) та наближення до її центру ($l_y$, см) при повздовжньому переміщенні пошукового елемента

Динаміка зміни частоти сигналу ($f$) залежно від висоти над відкрито розташованою міною ($H$) та наближення до її центру ($l_y$) при повздовжньому переміщенні пошукового елемента та наведена у таблиці 6. Значення показника частоти сигналу ($f$, кГц) залежно від

висоти над відкрито розташованою протипіхотною міною ($H$, см) та наближення до її центру ($l_y$, см) при повздовжньому переміщенні пошукового елемента.

Таблиця 6

| Висота над міною $H$, см | Наближення до центру міни ($l_y$, см) | | | | |
|---|---|---|---|---|---|
| | -20 | -10 | 0 | 10 | 20 |
| 10 | 0 | 0 | 14,7 | 2,2 | 0 |

Синтез результатів статистичних досліджень щодо значень показника частоти сигналу ($f$) наведено на рис. 9.

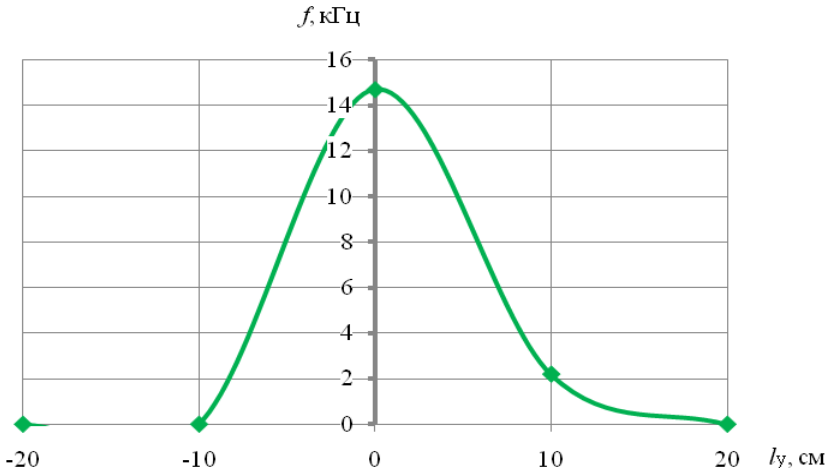



Рисунок 9 – Залежність значення показника частоти сигналу ($f$, кГц) від висоти над відкрито розташованою протипіхотною міною ($H$, см) та наближення до її центру ($l_y$, см) при повздовжньому переміщенні пошукового елемента

Аналіз отриманих результатів статистичних досліджень (рисунки 7-9) показав, що ширина смуги зони реєстрації появи вторинного магнітного поля від протипіхотної міни із малим вмістом металу може бути прийнята близько 0,2 м (20 см). Така ширина відповідає геометричним розмірам пошукового елементу та повинна бути врахована під час обґрунтування темпу пошуку протипіхотних мін. При цьому, максимального значення над центром міни зафіксовано для показників: амплітуди сигналу $A$=1,42 В та частоти сигналу $f$ = 14,7 кГц. За умов відсутності фіксації збудження вторинного магнітного поля в межах зони пошукового елементу показник амплітуди знижується до значення 11,4...12,3 мВ, а значення показників періоду та частоти сигналу на осцилограмах взагалі не фіксуються.

Для оцінювання достовірності одержаних результатів експериментальних досліджень визначені значення дисперсії та середньоквадратичного відхилення за основним показником – амплітуди сигналу ($A$) для всієї вибірки дослідів ($n$ = 32) в межах зони гарантованого виявлення ВНП аналогічні ППМ типу ПМН-2 (мало металоємких).

Встановлено, що значення математичного очікування вказаного показника для всієї вибірки дослідів дорівнює 147,4 мВ. При цьому, середньоквадратичне відхилення $\sigma$ = 5,195 мВ. Розрахунки показали, що середня відносна похибка дорівнює 3,4%.

Виходячи з того, що $n$ > 30 дослідів, середню похибку визначають як

$$m = \pm \frac{\sigma}{\sqrt{n}} = \pm \frac{5{,}195}{\sqrt{32}} = \pm 0{,}92 \ .$$

Отже, можна стверджувати, що із довірчою ймовірністю не нижче ніж 0,95 середнє значення показника амплітуди сигналу $A = 147{,}4 \pm 0{,}92$ мВ в межах всієї зони гарантованого виявлення ППМ типу ПМН-2 (мало металоємких) пошуковим пристроєм даного типу.

**Висновки.** В результаті проведення однофакторного експерименту параметрів міношукача типу ИМП-2 (ПР-507) встановлено, що фіксація наявності ПТМ, ППМ, в тому

числі й з малим вмістом металу здійснюється за значеннями параметрів амплітуди ($A$), періоду ($T$) та частоти ($f$) сигналу. За визначеною динамікою зміни показників встановлено, що виявлення ПТМ типу ТМ-62М фіксується при $l_y$ від –25...–20 см до +25...+45 см (при різних значеннях висоти розташування міношукача над міною). При цьому, максимальне значення амплітуди знаходиться в межах $A$ = 1,25...1,63 В. Встановлено, що ширина смуги зони реєстрації сигналу при пошуку мін типу ТМ -6 2М може бути прийнятою 50 см.

Дослідження зміни обраних параметрів показників при використанні міношукача типу ИМП-2 для пошуку мало металомістких ППМ показали, що фіксація наявності мін даного типу можлива при розташуванні антенного пристрою над міною на висоті $H \leq 10$ см. Встановлено, що ширина зони гарантованого виявлення буде рівною до 20 см. При цьому, значення амплітуди $A$ = 1,42 В і частоти $f$ = 14,7 кГц та періоду сигналу $T$ = 450 мкс.

Достовірність отриманих результатів підтверджується розрахунками щодо визначення середньої очікуваної помилки під час проведення однофакторного експерименту. Встановлено, що її значення знаходиться в межах 3,4...4,2% та є допустимою для обраних умов проведення експерименту.

Напрямком подальших експериментальних досліджень є проведення багатофакторного експерименту з метою встановлення параметрів пошуку ВНП з використанням пошукових елементів типу міношукачів ИМП, ИМП-2.

ЛІТЕРАТУРА:


1. Ментус І. Е. Ефективність інженерних боєприпасів: навчальний посібник. Кам’янець-Подільський: ФВП ПДАТУ, 2008. 80 с.
2. Саламахин Т. М. Боевая эффективность инженерных боеприпасов и элементов системы заграждений: учебное пособие. М.: ВИА им. Куйбышева, 1983. 424 с.
3. Підсумковий звіт про виконання бойових завдань саперними підрозділами ЗС України в Ісламській Республіці Афганістан у складі Литовської групи з реконструкції провінції Гор (ГРП) за період з листопада 2010 р. по листопад 2011 р. К.: ГШ ЗСУ, 2012. 47 с.
4. Майже половину території України потрібно розміновувати внаслідок війни – ДСНС [Електронний ресурс]. Режим доступу:. https://www.unian.ua/war/viyna-v-ukrajini-rozminuvati-treba-mayzhe-polovinu-teritoriji-ukrajini-dsns-novini-vtorgnennya-rosiji-v-ukrajinu-11781951.html.
5. Скільки території України потребує розмінування [Електронний ресурс]. Режим доступу:. https://www.slovoidilo.ua/2022/03/22/novyna/bezpeka/skilky-terytoriyi-ukrayiny-potrebuye-rozminuvannya-oczinka-asocziacziyi-saperiv
6. ООН закликає активізувати зусилля з розмінування на сході України [Електронний ресурс]. Режим доступу: https://www.unian.ua/war/10502961-oon-zaklikaye-aktivizuvati-zusillya-z-rozminuvannya-na-shodi-ukrajini.html
7. Допомога в діяльності, пов’язаній з розмінуванням. Доповідь Генерального секретаря ООН Антоніу Гутерреш на 72 сесії Генеральної асамблеї 31 липня 2017 року. URL: https://www.kmu.gov.ua/news/250123740
8. Україна – п’ята в світі за кількістю жертв вибухів мін. URL: https://m.censor.net.ua/news/ 3161155/ ukraina_pyataya_v_mire_po_kolichestvu_ jertv_vzry vov_min_doklad (дата звернення: 05.03.2020).
9. Міжнародні стандарти протимінної діяльності: організація національної програми. URL: https://www.osce.org/ukraine/149431? download=true
10. Commercial mine clearance agencies. URL: https://en.wikipedia.org/wiki/Mine_clearance_agency#Commercial_mine_clearance_agencies.
11. Office of Weapons Removal and Abatement (WRA). URL: https://www.state.gov/t/pm/wra/.
12. Robots for Humanitarian Demining. https://www.researchgate.net/publication/321954778
13. Demining robots – home. http://www.natospsdeminingrobots.com/

14. Demining Robots: Finding the right machine - Armtrac Ltd. https://armtrac.net/demining-robots/demining-robots-finding-right-machine/

15. Коцюруба В. І., Шишанов М. О., Гусляков О. М, Даценко І. П., Гімбер С. М. Обґрунтування раціональної комбінації методів виявлення вибухонебезпечних предметів для пошукових пристроїв робототехнічних комплексів розмінування. Зб. наук. праць Центрального науково-дослідного інституту озброєння та військової техніки Збройних Сил України. Київ: ЦНДІ ОВТ ЗСУ, 2015. №4(59). С. 187-19.

16. Коцюруба В.І. Синтез структури пошукових пристроїв виявлення вибухонебезпечних предметів. Збірник наукових праць Харківського національного університету ПС. Харків: ХНУПС, 2016. №4(49). С. 97-99.

17. Денисенко А. Н., Коцюруба В. И. Математическая модель обнаружения взрывоопасных предметов индукционным методом. Артиллерийское и стрелковое вооружение. 2009. №4(33). С. 19-23.

18. Звержинский С.С., Парфенов И.В. Метод магнитометрического обнаружения взрывоопасных предметов // Наукоемкие технологии. № 5, 2001. С. 29-34.

19. Щербаков Г.Н. Обнаружение скрытых объектов: монография. М.: Арбат-Информ, 2004. - 144 с.

20. Щербаков Г. Н. Новые методы обнаружения скрытых объектов: монография. М.: ООО Эльф ИПР, 2011. 503 с.

21. Щербаков Г.Н. Методы обнаружения мин – применительно к проблеме гуманитарного разминирования. Актуальность, проблемы // Специальная техника, 2003. № 3. С. 24-31.

22. Мосов С. П., Гурак С. П. Роботи та БПЛА проти мін. Оборонний вісник. № 11, 2019.

23. Коцюруба В.І., Кривцун В.І., Ляшенко В.А. Планування експериментальних досліджень показників ефективності дистанційно-керованих комплексів розмінування. Збірник наукових праць державного науково-дослідного інституту випробувань та сертифікації озброєння та військової техніки / Чернігів: ДНДІ ВС ОВТ, 2022. №3(13). С. 68-81.

REFERENCES:

1. Mentus I. E. Effectiveness of engineering munitions: a study guide. Kamianets-Podilskyi: FVP PDATU, 2008. 80 p.

2. Salamakhin T. M. Combat effectiveness of engineering munitions and elements of the obstructed system: textbook. M.: VIA named after Kuibysheva, 1983. 424 p.

3. Final report on the execution of combat missions by sapper units of the Armed Forces of Ukraine in the Islamic Republic of Afghanistan as part of the Lithuanian Group for the Reconstruction of the Gore Province (HRP) for the period from November 2010 to November 2011. K.: General Staff of the Armed Forces of Ukraine, 2012. 47 p.

4. Almost half of the territory of Ukraine needs to be demined as a result of the war - DSNS [Electronic resource]. Access mode:. https://www.unian.ua/war/viyna-v-ukrajini-rozminuvati-treba-mayzhe-polovinu-teritoriji-ukrajini-dsns-novini-vtorgnennya-rosiji-v-ukrajinu-11781951.html.

5. How much territory of Ukraine needs demining [Electronic resource]. Access mode:. https://www.slovoidilo.ua/2022/03/22/novyna/bezpeka/skilky-terytoriyi-ukrayiny-potrebuye-rozminuvannya-oczinka-asocziaczyiy-saperiv

6. The UN calls for intensified demining efforts in eastern Ukraine [Electronic resource]. Access mode: https://www.unian.ua/war/10502961-oon-zaklikaye-aktivizuvati-zusillya-z-rozminuvannya-na-shodi-ukrajini.html

7. Assistance in demining activities. Report of UN Secretary General Antonio Guterres at the 72nd session of the General Assembly on July 31, 2017. URL: https://www.kmu.gov.ua/news/250123740

8. Ukraine is fifth in the world in the number of victims of mine explosions. URL: https://m.censor.net.ua/news/ 3161155/ ukraina_pyataya_v_mire_po_kolichestvu_ jertv_vzry vov_min_doklad (date of application: 03/05/2020).

9. International mine action standards: organization of the national program. URL: https://www.osce.org/ukraine/149431? download=true

10. Commercial mine clearance agencies. URL: https://en.wikipedia.org/wiki/Mine_clearance_agency#Commercial_mine_clearance_agencies.

11. Office of Weapons Removal and Abatement (WRA). URL: https://www.state.gov/t/pm/wra/.

12. Robots for Humanitarian Demining. https://www.researchgate.net/publication/321954778

13. Demining robots - home. http://www.natospsdeminingrobots.com/

14. Demining Robots: Finding the right machine - Armtrac Ltd. https://armtrac.net/demining-robots/demining-robots-finding-right-machine/

15. Kotsyruba V. I., Shishanov M. O., Guslyakov O. M., Datsenko I. P., Gimber S. M. Justification of a rational combination of methods for detecting explosive objects for search devices of robotic demining complexes. Coll. of science Proceedings of the Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine. Kyiv: TsNDI OVT ZSU, 2015. No. 4(59). P. 187-19.

16. Kotsyruba V.I. Synthesis of the structure of search devices for detecting explosive objects. Collection of scientific papers of the Kharkiv National University PS. Kharkiv: KhNUPS, 2016. No. 4(49). P. 97-99.

17. Denysenko A.N., Kotsyuruba V.I. Mathematical model of detection of explosive objects by induction method. Artillery and small arms. 2009. No. 4(33). P. 19-23.

18. Zverzhinsky S.S., Parfenov I.V. The method of magnetometric detection of explosive objects // Naukoemkie tehnologii. No. 5, 2001. P. 29-34.

19. Shcherbakov G.N. Detection of hidden objects: monograph. M.: Arbat-Inform, 2004. 144 p.

20. Shcherbakov G.N. New methods of detecting hidden objects: monograph. M.: OOO Elf IPR, 2011. 503 p.

21. Shcherbakov G.N. Mine detection methods - applied to the problem of humanitarian demining. Relevance, problems // Special technology, 2003. No. 3. P. 24-31.

22. Mosov S.P., Gurak S.P. Robots and UAVs against mines. Defense Herald. No. 11, 2019.

23. Kotsyruba V.I., Kryvtsun V.I., Lyashenko V.A. Planning of experimental studies of indicators of effectiveness of remote-controlled demining complexes. Collection of scientific works of the State Research Institute for Testing and Certification of Weapons and Military Equipment / Chernihiv: DNDI VS OVT, 2022. No. 3(13). P. 68-81.

**Doctor of Technical Sciences Dovhopoly A.S.,**
**Doctor of Technical Sciences Kotsiuruba V.I.,**
**PhD Krivtsun V.I.**

## IMULATION OF EXPLOSIVE OBJECTS DETECTION PROCESSES USING THE INDUCTION METHOD BASED ON THE RESULTS OF EXPERIMENTAL RESEARCH

***With the beginning of the undeclared war of the Russian Federation against Ukraine in 2014, and the subsequent large-scale invasion in February 2022, the issue of reconnaissance and demining of the area from explosive devices both during the conduct of hostilities and in their absence became very acute. The experience of the war shows that the enemy, despite international conventions on the prohibition of certain types of mine weapons, uses its entire available arsenal of mines and improvised explosive devices, which are often set to non-removable. In addition to mines and improvised explosive devices, a large number of unexploded ordnance contaminates the territory of Ukraine, where hostilities are conducted or released.***

***Analysis of the execution of reconnaissance and demining tasks by the engineering units of the Armed Forces of Ukraine shows that the main method today remains manual, which is extremely dangerous for the lives of personnel. In order to ensure the fulfillment of these tasks, work is underway to create domestic means of remote reconnaissance and demining. One of the components of such means are search***

***elements for explosive objects that work on different physical principles. In addition to theoretical provisions, one of its important stages is conducting an experimental study.***

***In the article, based on previously developed theoretical provisions, the modeling of the processes of detecting explosive objects by the induction method during a one-factor experiment is carried out with the aim of substantiating individual indicators of the effectiveness of elements of the search for explosive objects of remote-controlled demining complexes.***

***Keywords: hostilities; explosive objects; demining; remote-controlled demining complex, experimental studies, induction method, factors, indicators.***

УДК 355.424
**Караванов О. А.** (НАСВ, Львів)

DOI: https://doi.org/10.17721/2519-481X/2022/77-03

# МЕТОДИКА СИНТЕЗУ РОЗВІДУВАЛЬНО-ВОГНЕВИХ СИСТЕМ

***У статті запропоновано алгоритм синтезу розвідувально-вогневих систем. Який дозволяє обґрунтувати потребу у зразках озброєння для комплектування підсистем вогневого ураження та розвідки зазначених систем. Сутність алгоритму полягає у впорядкуванні етапів щодо визначення потреби у зразках озброєння для забезпечення ефективного функціонування розвідувально-вогневих систем. Перевагою алгоритму є те, що він дозволяє враховувати стійкість функціонування та можливості кожного зразка озброєння виходячи із завдань, які покладаються на розвідувально-вогневу систему. Означене забезпечує проведення оптимального розподілу озброєння і запобігає перевитраті ресурсів. При цьому алгоритм є універсальним і забезпечує роботу із всіма типами засобів вогневого ураження та розвідки, які знаходяться на озброєнні у ракетних військах і артилерії Збройних Сил України, враховуючи ті що модернізуються або розробляються, а також з тими, що надходять у якості допомоги від західних країн-партнерів. Крім того, що запропонований алгоритм забезпечує визначення потреби озброєння при створені нових розвідувально-вогневих систем, враховуючи заданий ступінь виконання завдань, він також дозволяє визначити ступінь виконання поставлених завдань з врахуванням наявних сил і засобів.***

***Алгоритм базується на удосконаленому методі нелінійного програмування (двох функцій, який дозволяє врахувати, як неоднорідність типів зразків озброєння та військової техніки, так і неоднорідність цілей. Удосконалення полягає у визначенні "ваги" типів засобів вогневого ураження в залежності від "ваги" цілей до ураження яких вони залучаються. А в подальшому використання в якості вагових коефіцієнтів нормованих часток від цієї "ваги". Це дозволяє обґрунтовувати потребу в зразках озброєння з урахуванням заданого рівня виконання поставлених завдань. Означений алгоритм дозволяє врахувати нелінійність функцій, які описують різні типи озброєння та цілей.***

***Ключові слова:розвідувально-вогнева система, озброєння та військова техніка, стійкість функціонування, метод двох функцій.***

**Вступ та постановка задачі.** В умовах сьогодення, коли проходить стратегічний зсув у бік широкомасштабних бойових дій, артилерія залишається головним чинником, який здатний кардинально впливати на хід військових конфліктів [1-3]. В той же час, не виникає сумнівів що найбільш ефективним є застосування артилерії у складі розвідувально-вогневих систем (РВС). Застосування таких систем дозволяє значно скоротити тривалість циклу виявлення-ураження і при цьому забезпечує підвищення рівня керованості силами (людьми) та засобами (озброєння та військова техніка (ОВТ)), стійкості функціонування усієї системи та якості виконання завдань. Тому питанням розвитку РВС приділяється значна увага як у нас в країні так і у країнах-членах блоку НАТО [4].

Аналізуючи військові (бойові) операції остатніх десятиліть, було встановлено, що частка завдань з вогневого ураження противника (ВУП), які виконувались із залученням РВС зросла до 90% [5, 6]. Масово створюються і застосовуються РВС в ході окупаційної війни, яку веде російська федерація на території України. В існуючих умовах для росіян "ідеальною формулою" стало створення РВС у складі БПЛА (передусім "Орлан-10") з самохідними артилерійськими установками (САУ) (як правило "МСТА-С") та реактивними системами залпового вогню (РСЗВ) "Смерч" і "Ураган" [3]. Значно більший спектр ОВТ, що залучається до створення РВС у ЗС України. Це пов’язано з тим, що залучаються як зразки ОВТ, які знаходяться на озброєнні в українській армії, модернізуються, нові зразки, так і озброєння, що надходить у якості допомоги від західних партнерів. Перелік таких зразків є досить широким. До основних засобів вогневого ураження, що надходять у якості допомоги, відносяться: САУ - М 109 Paladin, PzH 2000, Caesar, Krab, DANA, Zuzana; гармати – М777, FH-70; РСЗВ – HIMARS, M 270 MLRS, VAMPIRE RM-70. До основних засобів розвідки слід віднести: радіолокаційні станції - AN/TPQ-48, AN/TPQ-49, AN/TPQ-36, AN/TPQ-37, Arthur, SharpEye

(очікується надходження AN/TPQ-50, Cobra); БПЛА- А1-СМ Фурія, Лелека 100, Fly Eye, RQ-20, Puma, Валькірія, PD-1, PD-2, Bayraktar Mini UA, Spectator-M1.

Проведений аналіз застосування РВС свідчить про те, що реальні результати застосування РВС не завжди співпадають з очікуваними. Причиною цього є багато чинників, серед яких недостатнє знання командирами обстановки що склалася, несвоєчасна обробка та доведення необхідної інформації [7, 8]. Також до таких чинників відноситься використання сил і засобів «які є під рукою» і можна негайно залучити до виконання завдання замість тих, які більше підходять до виконання завдання [9], що може призвести до збоїв в циклі виявлення-ураження та привести до нераціональної витрати ресурсів.

Однак, основним чинником, який значно впливає на результат застосування РВС є те, що доволі часто можливості підсистем РВС (вогневого впливу, розвідки, управління) щодо виконання поставлених завдань не співпадають [10]. Тобто РВС не є збалансованою, що призводить до невиконання (або виконання не у повній мірі) поставлених завдань та перевитрат ресурсів. Причин незбалансованості є декілька.

По-перше, це неврахування стійкості функціонування зразків ОВТ при створені РВС.

По-друге, складність врахування ступеня придатності ОВТ до виконання завдань (засобів вогневого ураження – до ураження тієї чи іншої цілі, засобів розвідки – до ведення розвідки (забезпечення розвідувальними даними засобів ВУП)).

По-третє, складність у здійсненні оптимального комплектування РВС у відповідності до визначених завдань, адже функції залежності завданого збитку і витрачених зусиль є нелінійними. До того ж ці функції залежать як від характеристик ОВТ, так і від характеристик цілі, яку спочатку необхідно виявити, а потім уразити. При тому всьому необхідно забезпечити врахування як імовірного виграшу – програшу при залучені до виконання завдань одних типів ОВТ, так і врахування імовірного виграшу – програшу при залучені до виконання завдань інших типів ОВТ.

Отже можна зробити висновки, що існуючі проблеми викликані недосконалістю науково-методичного апарату щодо здійснення комплектування РВС зразками ОВТ в залежності від ступеня досяжності виконання поставлених завдань з врахування стійкості функціонування самих зразків ОВТ.

Таким чином, у практиці застосування РВС виникла потреба у пошуку такого підходу до підбору зразків ОВТ, який дозволив би враховувати стійкість функціонування зразків озброєння при визначенні їх оптимальної кількість для досягнення заданого рівня виконання завдань. Тому дане дослідження є актуальним.

**Аналіз останніх досліджень та публікацій.** У дослідженні [11] розглядається напівдинамічний підхід до моделювання наземного бою на тактичному рівні. Підхід передбачає розбиття бою на етапи. На кожному етапі запропоновано використовувати три моделі: математичну модель програмування для оптимізації розподілу сил, імітаційну модель Ланчестера для прогнозування того, чи будуть досягнуті цілі етапу в рамках такого розподілу, і модель для визначення ефективності ОВТ від одного етапу до наступного. Взаємодія зазначених моделей одна з одною відбувається у в рамках системи підтримки прийняття рішень. Однак такий не враховує стійкість функціонування зразків ОВТ та не забезпечує визначення потреби зразків озброєння у відповідності до визначених завдань.

У роботі [12] розроблений алгоритм, який передбачає оцінювання ефективності застосування ОВТ на основі лінійної функції кількості кожного типу озброєння. Цей підхід базується на використанні підходів теорії рішень, зокрема визначення індексу ефективності озброєння/ваги (the weapon effectiveness index/weighted) (WEI/WUV). Однак суттєвим обмеженням цього підходу є необхідність суб'єктивного вибору числових коефіцієнтів для представлення різних типів озброєння, які представлені лінійними функціями.

Робота [13] присвячена вирішенню проблеми залучення ОВТ до виявлення та знищення цілей у системі протиракетної оборони. Цей підхід базується на декомпозиції нелінійної функції, методах лінеаризації та імітаційному підході. Такий підхід дозволяє дещо врахувати

особливості різних типів озброєння, однак не враховується ступінь досяжності мети при виконанні завдань.

Праця [14] присвячена розробленню методики оптимального розподілу ресурсів між споживачами. Сутність методики полягає у застосуванні методу нелінійного програмування, так званого методу двох функцій, для розподілу неоднорідних, за можливостями, ресурсів між неоднорідними, за потребами, споживачами. Однак в дослідженні розглядається прядок розподілу інформації між споживачами і взагалі не приділено уваги розподілу неоднорідних типів ОВТ.

У статті [15] запропоновано методичний підхід оцінки "бойових потенціалів" шляхом використання коефіцієнту "бойового потенціалу", який застосовується до певного зразка озброєння. Однак такий підхід не розглядає можливість об'єднання різнотипних зразків ОВТ в одну систему.

Дослідження [16] присвячено обґрунтуванню потреби у засобах ВУП та цілерозподілу при застосуванні РВС. Застосований у роботі підхід дозволяє врахувати нелінійність функцій, які описують різні типи засобів вогневого ураження та цілей. Разом з тим, у ньому не врахована стійкість функціонування ОВТ та не здійснено обґрунтування необхідної кількості засобів розвідки для функціонування РВС.

Загалом, у означених дослідженнях зроблено суттєвий внесок у здійснення розподілу зразків озброєння для ураження цілей. Однак у них не враховується стійкість функціонування зразків ОВТ. Також недостатньо приділено уваги розподілу засобів розвідки виходячи із можливостей засобів ВУП. Зазначене може привести до не стійкого функціонування РВС та нераціонального використання зразків ОВТ, тобто перевитрат ресурсів.

Таким чином, необхідність проведення дослідження зазначених питань обумовлена потребою врахування оптимізації витрат на досягнення встановленого рівня функціональних завдань.

**Мета статті** є розроблення методики синтезу розвідувально-вогневих систем при їх застосуванні з урахуванням стійкості функціонування елементів, що можуть включатися до їх складу. Це дасть можливість приймати обґрунтовані рішення щодо оптимального комплектування РВС враховуючи обстановку, що склалась на даний момент; наявні засоби розвідки, вогневого ураження та управління, що забезпечить виконання бойових завдань із залученням мінімальної кількості необхідних ресурсів.

**Виклад основного матеріалу.** Зважаючи на умови функціонування та прийняті обмеження необхідно зауважити, що необхідно здійснити розподіл неоднорідних ресурсів між неоднорідними споживачами. Найбільш простими та точними методами, що дозволяють здійснити такий розподіл, є методи нелінійного програмування [17]. Одним із методів, що дозволяє здійснити розподіл з врахуванням неоднорідності ресурсів та споживачів, є метод двох функцій [16, 18–21].

Також зазначений метод дозволяє максимально вигідно створити РВС із наявних сил і засобів враховуючи їх стійкість функціонування із мінімально необхідним їх залученням враховуючи заданий ступень ураження противника.

Порядок комплексування РВС, враховуючи наявні сили і засоби, буде складатись із двох етапів. Перший етап полягає у здійсненні цілерозподілу між наявними засобами вогневого ураження, а другий етап у визначенні типу та кількості засобів розвідки відповідно до потреб засобів вогневого ураження.

Сутність методу полягає в знаходженні матриці призначень $\|\mu^0\|$, (де $\mu$ – індикатор призначення певного типу ресурсу за певним споживачем) і передбачає проведення зазначеної процедури двічі. На першому етапі необхідно буде розподілити засоби вогневого ураження (ресурси) між цілями (споживачі). На другому етапі слід розподілити засоби розвідки (ресурси) у відповідності до потреб засобів вогневого ураження (споживачі). Знаходження $\|\mu^0\|$ дозволяє встановити максимальне значення функції придатності певного типу ресурсів забезпечувати потреби певних споживачів (G) [16-21].

$$G = \sum_{m=1}^{N} \mathrm{B}_m \left( 1 - \prod_{g=1}^{K} \left( 1 - P_{gm} \right) \right), \tag{1}$$

де $m$ – індикатор номера споживача;

$N$ – кількість споживачів;

$B_m$ – коефіцієнт важливості певного споживача;

$g$ – індикатор номера ресурсу певного типу;

$N$ – кількість типів ресурсів;

$P_{gm}$ – імовірність забезпечення потреби споживачів.

З огляду на те, що дослідження проводиться відносно РВС можливо припустити, що імовірність забезпечення потреб споживачів (Р) є ніщо інше, як імовірність виконання завдань (імовірність ураження цілі, імовірність виконання завдань з розвідки цілі та ін.)

Також необхідно зауважити, що досліджуючи розподілення неоднорідних ресурсів між неоднорідними споживачами з точки зору створення РВС, доцільно враховувати умови, в яких буде відбуватись процес функціонування зазначеної системи. Зважаючи на те, що РВС комплектуються зразками ОВТ (елементами), можливо стверджувати, що на якість виконання поставлених завдань буде впливати технічний стан елементу. Разом з тим, виходячи з призначення РВС [22], свої завдання елементи РВС будуть виконувати у ході військової (бойової) операції, що в свою чергу передбачає функціонування в умовах вогневого впливу противника. Тобто, здатність елементів РВС виконувати визначені завдання, крім технічного стану буде залежати і від відмов елементів, які будуть виникати внаслідок вдалого вогневого впливу противника. Показником, який забезпечує врахування відмов елементу, що виникають внаслідок технічних несправностей та вогневого впливу противника, є імовірність безвідмовного функціонування зразка ОВТ (елементу) ( $P_g^e$ ) [23]:

$$P_g^e = 1 - e^{-(\lambda_d + \lambda_s)t} \tag{2}$$

де $\lambda_d$ – інтенсивність потоку відмов елементу, які виникають внаслідок технічних несправностей;

$\lambda_s$ – інтенсивність потоку відмов елементу, які будуть виникати внаслідок вдалого вогневого впливу противника;

$t$– час функціонування елементу.

Враховуючи все вище зазначене, визначення імовірності забезпечення потреби споживачів (Р) під час функціонування РВС буде здійснюватись у відповідності до виразу:

$$P_{gm} = P_{gm}^{v} P_g^e, \tag{3}$$

де $P_{gm}^{v}$ – імовірність виконя завдань елементом РВС.

Порядок визначення імовірності виконання завдань тим чи іншим зразком озброєння в артилерії ($P_v$) є загальновідомим і викладений у [24].

При умовах, коли на одному кроці проводиться закріплення одного типу ресурсів за одним споживачем, то індикатор призначення набуває значень від 1 до K.

$$\sum_{m=1}^{N} \mu_{gm} = 1, g = 1.....K.$$

За таких умов: складові матриці призначення набувають значень 1 або 0, імовірність не забезпечення потреби споживачів лежить у межах від 0 до 1, коефіцієнт важливості цілі більше 0.

$$\left.\begin{array}{l} \mu_{gm} \in \{1, 0\}, \\ 1 \geq \left( M_{gm} = 1 - P_{gm} \right) \geq 0, \\ B_m > 0. \end{array}\right\} \begin{array}{l} g = 1....K, \\ m = 1....N. \end{array}$$

Особливістю застосування методу двох функцій при розробленні методики синтезу РВС є те, що показники, які описують виконання завдань певним елементом, характеризуються своєю імовірністю виконання завдань, яка враховує імовірність безвідмовного функціонування цього елемента, заданою в матриці $\left\|P_{gm}\right\|_{KN}$ [18-21]. Отже, рішення про закріплення певного типу ресурсів повинно бути прийняте до виконання відносно кожного споживача. З цією метою, кожному типу ресурсу присвоюється номер *g (g=1…K)*, а подія щодо призначення певного типу ресурсів для забезпечення потреб *m-ного* споживача фіксується за допомогою індикатора $\mu_{gm}=1$, ($\mu_{gm}=0$) – в іншому випадку). За таких умов матриця призначень буде включати в себе відомості про залучення певного типу ресурсів для забезпечення потреб певного споживача.

Розглянутий підхід щодо закріплення певного типу ресурсів за певним споживачем є класичним методом двох функцій [18–21] і дозволяє розподілити означену кількість ресурсів між споживачами. Разом з тим, застосування даного методу є проблематичним щодо визначення потреби кількості ресурсів для виконання поставленого завдання. Тому для забезпечення можливості визначати потребу у необхідній кількості ресурсів для забезпечення заданого ступеню досягнення мети, в даному випадку пропонується використовувати замість вагових коефіцієнтів їх нормовані частки, як це викладену у [16,19].

Розробка алгоритму обґрунтування потреби у зразках озброєння при створенні і застосуванні РВС з врахуванням стійкості функціонування елементів, що будуть входити до складу такої системи.

Вхідними даними для цього алгоритму є кількість та характер цілей, кількість типів елементів (засобу ВУП і засоби розвідки) та кількість елементів за типами, встановлений рівень значення цільової функції (ступінь ураження цілей, ступінь викриття об’єктів противника).

Створення алгоритму обґрунтування комплексування РВС пропонується виконувати за двома етапами (блоками) :

- обґрунтування потреби у засобах вогневого ураження для ураження визначеної кількості цілей;
- обґрунтування потреби у засобах розвідки для забезпечення потреб засобів ВУП.

1. Обґрунтування потреби у засобах вогневого ураження для ураження визначеної кількості цілей.

Під час здійснення обґрунтування потреби у засобах вогневого ураження для ураження визначеної кількості цілей під поняттям "ресурси" слід розуміти типи засобів вогневого ураження, а під поняттям "споживачі"- цілі які необхідно уразити.

По-перше, визначається так звана "імовірність забезпечення потреби споживачів". В умовах нашого дослідження, на даному етапі це буде імовірність виконання завдань *g-тим* типом засобів вогневого ураження щодо ураження *m-ної* цілі ($P_{gm}$):

$$P_{gm} = P_{gm}^{v} P_{g}^{e}, \tag{4}$$

де $P_{gm}^{v}$ – імовірність ураження *m-ної* цілі *g-тим* типом засобів вогневого ураження;

$P_{g}^{e}$ – імовірність безвідмовного функціонування *g-того* типу засобів вогневого ураження;

Результати розрахунків заносяться у табл.1.

Таблиця 1

Вихідні дані для здійснення цілерозподілу

| Номер типу засобу вогневого ураження | Кількість засобів ВУП певного типу | Номер цілі | | |
|---|---|---|---|---|
| | | *1* | ... | *m* |
| | | "Вага" цілі | | |
| | | $B_1$ | … | $B_m$ |
| 1 | $z_1$ | $P_{11}$ | … | $P_{1m}$ |
| … | … | … | … | … |
| *g* | $z_g$ | $P_{g1}$ | … | $P_{gm}$ |

По-друге, необхідно визначити нормовані частки коефіцієнтів важливості усієї сукупності цілей [18–21]:

$$L_m^{(i)} = \frac{B_m^{(i)}}{\sum\limits_{m=1}^{N} B_m^{(i)}}, \tag{5}$$

де *i* – номер кроку обчислення;
*m* – кількість цілей на певному кроці обчислень.

По-третє, проводиться визначення елементів поточної матриці значень виграшу при ураженні певного типу цілі певним типом засобів ВУП з урахуванням програшу при неуражені інших цілей $\left\| \Omega_{gm}^{(i)} \right\|_{KN}$ [18–21]:

$$\Omega_{gt}^{(i)} = L_m^{i-1} P_{gm} - \sum_{m=1}^{N} \frac{L_m^{i-1} P_{gm}}{M_{gm}} a_m^{(i-1)}, \tag{6}$$

$$\text{де } a_m^{(0)} = \prod_{g=1}^{K} M_{gm}, m = 1....N, g \in K^{(i)}, \tag{7}$$

$K^{(i)}$ – множина номерів типів засобів ВУП, невикористаних до *i-го* кроку обчислень;
*g* – кількість типів засобів вогневого ураження на певному кроці обчислень.

По-четверте, проводиться закріплення засобу вогневого ураження певного типу за певною ціллю $(\mu_{gm}^{(i)} = 1)$ відповідно до умови $\Omega_{gm}^{(i)} = \max\limits_{g,m} \Omega_{gm}, g \in K^{(i)}$

По-п’яте, здійснюються обчислення поточного значення цільової функції [18–21]:

$$G^{(i)} = G^{(i-1)} + \max \Omega_{gm}^{(i)}, \tag{8}$$

де $G^{(0)} = 0$

Під час виконання наступної дії проводиться перевірка умови досягнення рівня значення цільової функції встановленому рівню $G^{(i)} \geq G_{set\ level}^{(i-1)}$.

У подальшому проводиться обчислення нових значень нормованих часток коефіцієнтів важливості $B^{(i)}$ та добутку імовірностей не ураження цілі $a_m^{(i)}$ [18–21]:

$$B_m^{(i)} = \begin{cases} B_m^{(i-1)}, \text{ якщо } \mu_{gm}^{(i)} \neq 1, \\ B_m^{(i-1)} M_{gm}^{i}, \text{ якщо } \mu_{gm}^{(i)} = 1 \end{cases}, \tag{9}$$

$$a_m^{(i)} = \frac{a_m^{(i-1)}}{M_{gm}^{(i)}}. \tag{10}$$

Реалізація методу двох функцій для здійснення оптимального розподілу засобів вогневого ураження між цілями наведено в табл.2.

Таблиця 2

Оптимальний варіант розподілу засобів вогневого ураження між цілями

| Номер кроку | Номер типу засобів ВУП | Кількість засобів ВУП певного типу | Номер цілі | | | Максимальне значення функції за кожен засіб ВУП | Закріплений засіб ВУП за ціллю | Максимальне значення цільової функції |
|---|---|---|---|---|---|---|---|---|
| | | | *1* | ... | *m* | | | |
| | | | "Вага" цілі | | | | | |
| | | | $B_1^{(0)}$ | … | $B_m^{(0)}$ | | | |
| | | | Нормована частка "ваги" цілі | | | | | |
| | | | $L_1^{(0)}$ | … | $L_m^{(0)}$ | | | |
| 1 | 1 | $z_1^{(1)}$ | $\Omega_{11}^{(1)}$ | … | $\Omega_{1m}^{(1)}$ | $\max\limits_{1,m} \Omega_{1m}^{(1)}$ | $\mu_{gm}^{(1)}$ | $\max \Omega_{gm}^{(1)}$ |
| | … | … | … | … | … | … | | |
| | *g* | $z_g^{(1)}$ | $\Omega_{g1}^{(1)}$ | … | $\Omega_{gm}^{(1)}$ | $\max\limits_{g,m} \Omega_{gm}^{(1)}$ | | |
| | $L_m^{(1)}$ | | Нормована частка "ваги" цілі на *1-му* кроці обчислень | | | Поточне значення цільової функції | | |
| | | | $L_1^{(1)}$ | … | $L_m^{(1)}$ | $G^{(1)} = \max \Omega_{gm}^{(1)}$ | | |
| …. | …. | | …. | …. | …. | …. | | |
| *i* | 1 | $z_1^{(i)}$ | $\Omega_{11}^{(i)}$ | … | $\Omega_{1m}^{(i)}$ | $\max\limits_{1,m} \Omega_{1m}^{(i)}$ | $\mu_{gm}^{(i)}$ | $\max \Omega_{gm}^{(i)}$ |
| | … | … | … | … | … | … | | |
| | *g* | $z_g^{(i)}$ | $\Omega_{g1}^{(i)}$ | … | $\Omega_{gm}^{(i)}$ | $\max\limits_{g,m} \Omega_{gm}^{(i)}$ | | |
| | $L_m^{(i)}$ | | Нормована частка "ваги" цілі на *i-тому* кроці обчислень | | | Поточне значення цільової функції | | |
| | | | $L_1^{(i)}$ | … | $L_m^{(i)}$ | $G^{(i)} = G^{(i-1)} \max \Omega_{gm}^{(i)}$ | | |

На підставі табличного рішення проводиться визначення матриці призначень $\left\| \mu_{gm} \right\|_{KN}$ варіант якої наведено в табл. 3.

Таблиця 3

Матриця призначень певного засобу вогневого ураження за певною ціллю

| Номер типу засобу ВУП | Кількість засобів ВУП певного типу | Номер цілі | | |
|---|---|---|---|---|
| | | 1 | … | $m$ |
| 1 | $z_1$ | $\mu_{11}$ | … | $\mu_{1m}$ |
| … | … | … | … | … |
| $g$ | $z_g$ | $\mu_{g1}$ | … | $\mu_{gm}$ |

2. Обґрунтування потреби у засобах розвідки для забезпечення потреб засобів ВУП.

Під час здійснення обґрунтування потреби у засобах розвідки для забезпечення потреб засобів ВУП під поняттям "ресурси" слід розуміти типи засобів розвідки, а під поняттям "споживачі"- типи засобів ВУП.

По-перше, визначається імовірність виконання *r-тим* типом засобів розвідки щодо забезпечення потреб *g-того* типу засобів ВУП ($P_{rg}$):

$$P_{rg} = P_{rg}^{v} P_r^{e}, \tag{11}$$

де $P_{rg}^{v}$ – імовірність виконання *r-тим* типом засобів розвідки завдань з ведення розвідки в інтересах *g-того* типу засобів вогневого ураження;

$P_r^{e}$ – імовірність безвідмовного функціонування *r-того* типу засобів розвідки;

По–друге, необхідно встановити "вагу" (пріоритет) певного типу засобів вогневого ураження ($B_g$). В межах даного дослідження пропонується "вагу" певного типу засобів вогневого ураження визначати у відповідності до "ваги" цілей, ураження яких покладено на цей тип засобів ВУП:

$$B_g = \sum_{m=1}^{N_g} B_{mg}, \tag{12}$$

де $N_g$– кількість цілей, що уражаються *g-тим* типом засобів вогневого ураження;

$B_{mg}$ – коефіцієнт важливості цілі до ураження якої залучений *g-тий* тип засобів ВУП.

$$B_{mg} = \frac{B_m}{L_m} L_{mg}, \tag{13}$$

де $L_{mg}$ – нормована частка *m-ної* цілі, яка припадає для ураження засобом *g-того* типу;

Результати проведених обчислень заносяться у табл.4.

Таблиця 4

Вихідні дані для здійснення розподілу засобів розвідки

| Номер типу засобу розвідки | Кількість засобів розвідки певного типу | Номер типу засобу ВУП ( кількість) | | |
|---|---|---|---|---|
| | | *1* | … | *g* |
| | | "Вага" типу засобів ВУП | | |
| | | $B_1$ | … | $B_g$ |
| 1 | $h_1$ | $P_{11}$ | … | $P_{1g}$ |
| … | … | … | … | … |
| $r$ | $h_g$ | $P_{r1}$ | … | $P_{rg}$ |

По-третє, необхідно розрахувати величину нормованих часток коефіцієнтів важливості усієї сукупності типів засобів ВУП [18–21]:

$$L_g^{(i)} = \frac{B_g^{(i)}}{\sum_{g=1}^{K} B_g^{(i)}}, \tag{14}$$

де $i$ – номер кроку обчислення;

$g$ – кількість певного типів засобів ВУП на певному кроці обчислень.

По-четверте, проводиться визначення елементів поточної матриці значень виграшу при виконанні завдань з ведення розвідки в інтересах певного типу засобів ВУП певними типом засобів розвідки з урахуванням програшу при невиконанні завдань з розвідки в інтересах інших типів засобів ВУП $\left\|\Omega_{rg}^{(i)}\right\|_{RK}$ [18–21]:

$$\Omega_{rg}^{(i)} = L_g^{i-1} P_{rg} - \sum_{g=1}^{K} \frac{L_g^{i-1} P_{rg}}{M_{rg}} a_g^{(i-1)}, \tag{15}$$

де $a_g^{(0)} = \prod_{r=1}^{R} M_{rg}, g = 1....K, r \in R^{(i)}$;

$R^{(i)}$ – множина номерів типів засобів розвідки, невикористаних до *i-го* кроку обчислень;

$r$ – кількість типів засобів розвідки на певному кроці обчислень.

По-п’яте, проводиться закріплення засобу розвідки певного типу за певним типом засобів ВУП ($\mu_{rg}^{(i)} = 1$) відповідно до умови $\Omega_{rg}^{(i)} = \max_{r,g} \Omega_{rg}, r \in R^{(i)}$

По-шосте, здійснюються обчислення поточного значення цільової Функції [18–21]:

$$G^{(i)} = G^{(i-1)} + \max \Omega_{rg}^{(i)}, \tag{16}$$

де $G^{(0)} = 0$

Під час виконання наступної дії проводиться перевірка умови досягнення рівня значення цільової функції встановленому рівню $G^{(i)} \geq G_{set\ level}^{(i-1)}$.

У подальшому проводиться обчислення нових значень нормованих часток коефіцієнтів важливості $B^{(i)}$ типів засобів ВУП та добутку імовірностей невиконання завдань з розвідки в інтересах інших типів засобів ВУП $a_g^{(i)}$ [18–21]:

$$B_g^{(i)} = \begin{cases} B_g^{(i-1)}, \text{ якщо } \mu_{rg}^{(i)} \neq 1, \\ B_g^{(i-1)} M_{rg}^{i}, \text{ якщо } \mu_{rg}^{(i)} = 1 \end{cases}, \tag{17}$$

$$a_g^{(i)} = \frac{a_g^{(i-1)}}{M_{rg}^{(i)}}. \tag{18}$$

Реалізація методу двох функцій для здійснення оптимального розподілу засобів розвідки між засобами ВУП наведено в табл.5.

Таблиця 5

Оптимальний варіант розподілу засобів розвідки між засобами ВУП

| Номер кроку | Номер типу засобів розвідки | Кількість засобів розвідки певного типу | Номер типу засобів ВУП | | | Максимальне значення функції за кожен засіб розвідки | Закріплений засіб розвідки за засобом ВУП | Максимальне значення цільової функції |
|---|---|---|---|---|---|---|---|---|
| | | | *1* | ... | *g* | | | |
| | | | "Вага" типу засобів ВУП | | | | | |
| | | | $B_1^{(0)}$ | … | $B_g^{(0)}$ | | | |
| | | | Нормована частка "ваги" типу засобів ВУП | | | | | |
| | | | $L_1^{(0)}$ | … | $L_g^{(0)}$ | | | |
| 1 | 1 | $h_1^{(1)}$ | $\Omega_{11}^{(1)}$ | … | $\Omega_{1g}^{(1)}$ | $\max\limits_{1,g} \Omega_{1g}^{(1)}$ | $\mu_{rg}^{(1)}$ | $\max \Omega_{rg}^{(1)}$ |
| | … | … | … | … | … | … | | |
| | *r* | $h_r^{(1)}$ | $\Omega_{r1}^{(1)}$ | … | $\Omega_{rg}^{(1)}$ | $\max\limits_{r,g} \Omega_{rg}^{(1)}$ | | |
| | $L_g^{(1)}$ | | Нормована частка "ваги" цілі на *1-му* кроці обчислень | | | Поточне значення цільової функції | | |
| | | | $L_1^{(1)}$ | … | $L_g^{(1)}$ | $G^{(1)} = \max \Omega_{rg}^{(1)}$ | | |
| …. | …. | | …. | …. | …. | …. | | |
| *i* | 1 | $h_1^{(i)}$ | $\Omega_{11}^{(i)}$ | … | $\Omega_{1g}^{(i)}$ | $\max\limits_{1,g} \Omega_{1g}^{(i)}$ | $\mu_{rg}^{(i)}$ | $\max \Omega_{rg}^{(i)}$ |
| | … | … | … | … | … | … | | |
| | *r* | $h_r^{(i)}$ | $\Omega_{r1}^{(i)}$ | … | $\Omega_{rg}^{(i)}$ | $\max\limits_{r,g} \Omega_{rg}^{(i)}$ | | |
| | $L_g^{(i)}$ | | Нормована частка "ваги" цілі на *i-тому* кроці обчислень | | | Поточне значення цільової функції | | |
| | | | $L_1^{(i)}$ | … | $L_g^{(i)}$ | $G^{(i)} = G^{(i-1)} \max \Omega_{rg}^{(i)}$ | | |

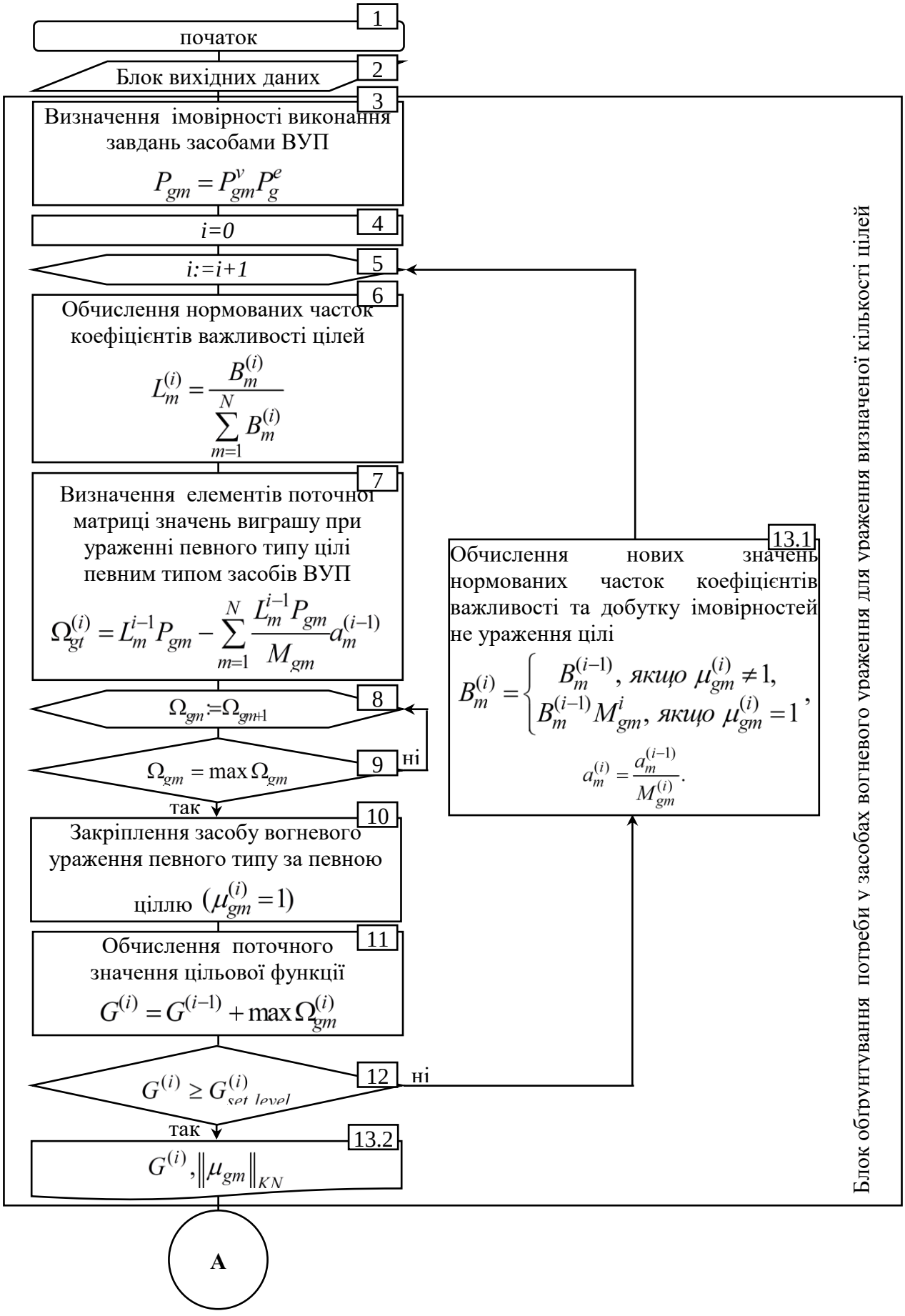
На підставі табличного рішення проводиться визначення матриці призначень $\left\| \mu_{rg} \right\|_{RK}$, варіант якої наведено в табл. 6.

Таблиця 6

Матриця призначень певного засобу розвідки за певним засобом ВУП

| Номер типу засобів розвідки | Кількість засобів розвідки певного типу | Номер типу засобів ВУП | | |
|---|---|---|---|---|
| | | 1 | … | *g* |
| 1 | $h_1$ | $\mu_{11}$ | … | $\mu_{1g}$ |
| … | … | … | … | … |
| *r* | $h_r$ | $\mu_{r1}$ | … | $\mu_{rg}$ |

Загальний вигляд блок схеми алгоритму обґрунтування потреби у зразках озброєння при створенні РВС який дозволяє врахувати стійкість функціонування елементів, що будуть входити до складу такої системи представлений на рис.1.


1
початок
2
Блок вихідних даних
3
Визначення імовірності виконання завдань засобами ВУП
$P_{gm} = P_{gm}^{v} P_{g}^{e}$
4
$i=0$
5
$i:=i+1$
6
Обчислення нормованих часток коефіцієнтів важливості цілей
$L_m^{(i)} = \frac{B_m^{(i)}}{\sum_{m=1}^{N} B_m^{(i)}}$
7
Визначення елементів поточної матриці значень виграшу при ураженні певного типу цілі певним типом засобів ВУП
$\Omega_{gt}^{(i)} = L_m^{i-1} P_{gm} - \sum_{m=1}^{N} \frac{L_m^{i-1} P_{gm}}{M_{gm}} a_m^{(i-1)}$
8
$\Omega_{gm} := \Omega_{gm+1}$
9
$\Omega_{gm} = \max \Omega_{gm}$
ні
так
10
Закріплення засобу вогневого ураження певного типу за певною ціллю $(\mu_{gm}^{(i)} = 1)$
11
Обчислення поточного значення цільової функції
$G^{(i)} = G^{(i-1)} + \max \Omega_{gm}^{(i)}$
12
$G^{(i)} \geq G_{set\ level}^{(i)}$
ні
так
13.1
Обчислення нових значень нормованих часток коефіцієнтів важливості та добутку імовірностей не ураження цілі
$B_m^{(i)} = \begin{cases} B_m^{(i-1)}, \text{ якщо } \mu_{gm}^{(i)} \neq 1, \\ B_m^{(i-1)} M_{gm}^{i}, \text{ якщо } \mu_{gm}^{(i)} = 1 \end{cases},$
$a_m^{(i)} = \frac{a_m^{(i-1)}}{M_{gm}^{(i)}}.$
13.2
$G^{(i)}, \left\| \mu_{gm} \right\|_{KN}$
A
Блок обґрунтування потреби у засобах вогневого ураження для ураження визначеної кількості цілей

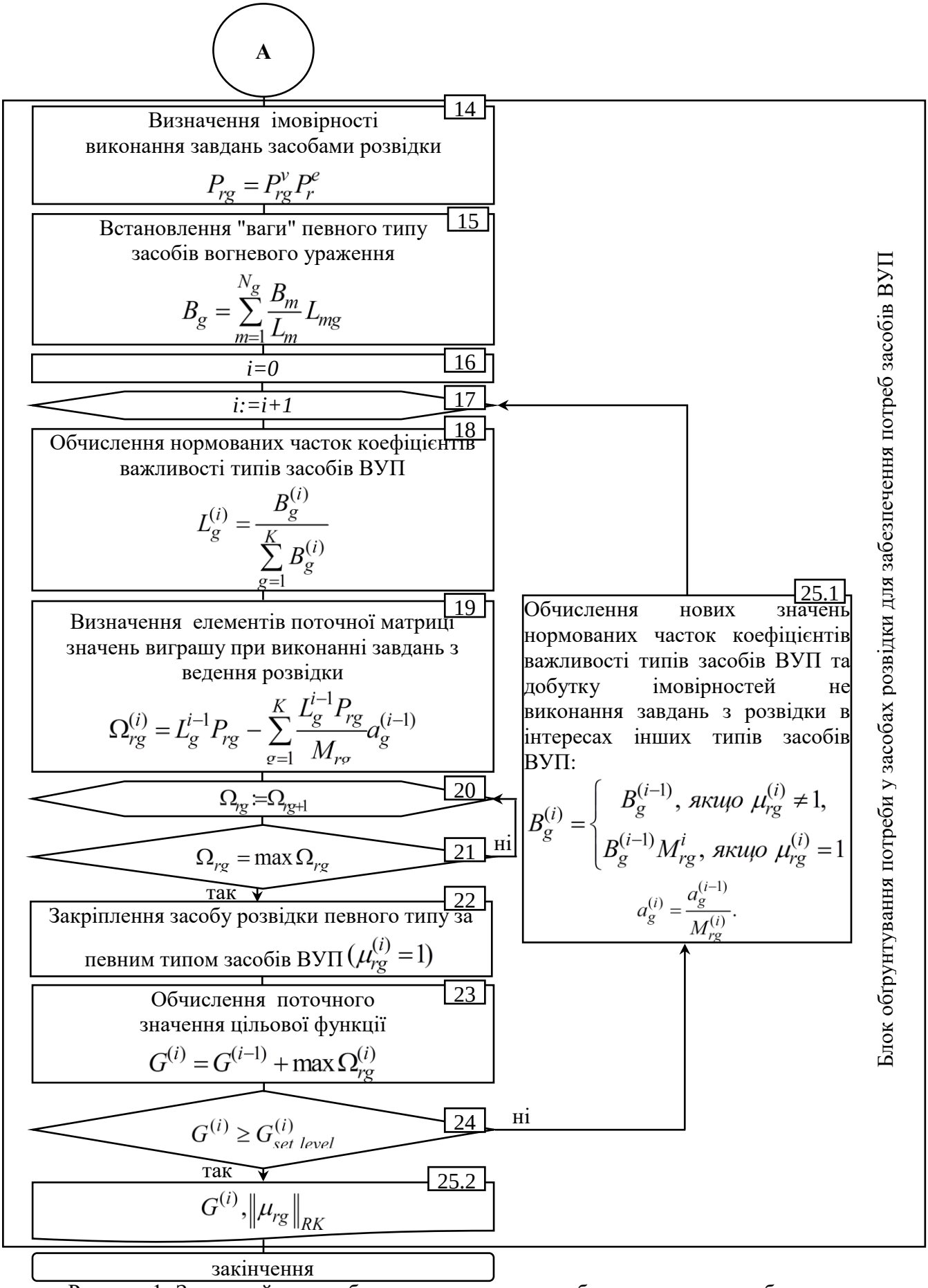



Рисунок 1- Загальний вигляд блок-схеми алгоритму обґрунтування потреби у зразках озброєння при створенні розвідувально-вогневої системи

Таким чином, запропоновано алгоритм обґрунтування потреби у зразках озброєння при створенні РВС (рис. 1), який дозволяє врахувати стійкість функціонування зразків ОВТ (2). Зазначений алгоритм складається з двох блоків та базується на застосуванні методу нелінійного програмування, зокрема методу двох функцій (табл.1-6), як під час вирішення завдань першого блоку, так і під час вирішення завдань другого блоку.

Зокрема застосування цього методу в алгоритмі дозволяє врахувати нелінійність функцій, що описують як цілі, так і різнотипні зразки озброєння різного призначення. Разом з тим, цей алгоритм дозволяє одночасно врахувати як можливий виграш при закріпленні певного типу засобу ВУП за ціллю та при закріпленні певних типів засобів розвідки за типами засобів ВУП, так і програш, якщо закріплення ресурсів здійснюється за іншими споживачами. Особливістю цього алгоритму є визначення "ваги" певного типу засобів ВУП в залежності від нормованої частки цілі, до ураження якої вони залучені (12). Використання нормованих часток від "ваги" чи то цілі на першому етапі (5), чи то типу засобів ВУП на другому етапі (14), дає можливість визначити ступінь досяжності мети при виконанні поставлених завдань.

Запропонований алгоритм є відносно простим у практичному використанні. Також, його перевагою є можливість враховувати стійкість функціонування зразків ОВТ та встановлений рівень значення цільової функції ( $G^{(i)}_{set\ level}$ ) (блоки 12, 24 рис.1).

Разом з тим необхідно зауважити, що:

по-перше, в цьому дослідженні величини імовірностей (імовірність безвідмовного функціонування елементів РВС ( $P^{e}_{g}$ ), імовірність ураження цілей елементами підсистеми ВУП ( $P^{v}_{gm}$ ), імовірність виконання завдань з розвідки елементами підсистеми розвідки ( $P^{v}_{rg}$ )) залежать від певних умов, які потребують постійного уточнення;

по-друге даний алгоритм можливо застосовувати тільки на етапі планування військової операції (бойових дій).

**Висновки.** Отже, запропоновано методику синтезу РВС, яка дозволяє обґрунтувати потребу у зразках ОВТ враховуючи їх стійкість функціонування при створені таких систем. Методика включає в себе два етапи. На першому етапі проводиться визначення приросту цільової функції (ефективності ВУП) та на його підставі визначення потреби у кількості засобів ВУП за типами відповідно до кількості та характеру цілей. На другому етапі проводиться визначення приросту цільової функції (ефективності виконання завдань з розвідки) та на його підставі формування необхідної кількості засобів розвідки для забезпечення потреб (можливостей) засобів ВУП. Застосування методу двох функцій у розглянутій методиці забезпечує врахування нелінійності функцій, що описують як різні типи цілей, так і різноманітні типи зразків озброєння. Разом з тим, особливістю методу двох функцій, що застосовується є те, що у якості вагових коефіцієнтів використовуються нормовані частки , ваги кожної цілі на першому етапі та ваги типу засобів ВУП на другому етапі. Також до особливостей слід віднести порядок розрахунку "ваги" певного типу засобів ВУП, яка визначається у відповідності до "ваги" цілей, які вони уражають. Це дозволяє визначати кількість ОВТ, що необхідно залучити до складу РВС, з урахуванням встановленого рівня досягнення поставленої мети створення РВС. Такий підхід дозволяє запобігти перевитраті ресурсів, тобто забезпечить комплектування РВС оптимальною (мінімально необхідною) кількістю ОВТ для виконання поставленого завдання враховуючи їх здатність до функціонування.

Зазначена методика може використовуватись штабами тактичного, оперативно-тактичного та стратегічного рівнів і застосовуватись на етапі планування військової операції (бойових дій). Вона дозволяє працювати з наявними та перспективними зразками ОВТ і забезпечує визначення їх потреби при створені нових РВС та визначення ступеня виконання поставлених завдань, враховуючи наявні сили і засоби.

Враховуючи те, що використання запропонованої методики обмежено етапом планування бойового застосування РВС, то перспективним напрямком є проведення досліджень щодо застосування зазначеної методики безпосередньо під час ведення бойових дій використовуючи підходи динамічного програмування.

ЛІТЕРАТУРА:


1. John Gordon IV, Igor Mikolic-Torreira, D. Sean Barnett, Katharina Ley Best, Scott Boston, Dan Madden, Danielle C. Tarraf, Jordan Willcox. [Електроний ресурс] *Army Fires Capabilities for 2025 and Beyond*. Santa Monica, CA: RAND Corporation, 2019. 248 p. Режим доступу: https://www.rand.org/pubs/research_reports/RR2124.html

2. Закордонні експерти про війну в Україні та її перспективи. [Електроний ресурс]. Режим доступу: https://armyinform.com.ua/2022/08/10/zakordonni-eksperty-pro-vijnu-v-ukrayini-ta-yiyi-perspektyvy/.

3. Вогневий вал: як побороти російську артилерію. [Електроний ресурс]. Режим доступу:https://www.bbc.com/ukrainian/features-61952663.

4. Daniel Jernigan. Closing the FIRES Gap; C.R.O.P.: A Baltic Fires Proposal. [Електроний ресурс] Field artillery journal 2021. Issue 4. Режим доступу: https://www.fieldartillery.org/news/closing-the-fires-gap-crop-a-baltic-fires-proposal.

5. Lingamfelter, L..Desert Redleg: Artillery Warfare in the First Gulf War. [Електроний ресурс] Lexington, Kentucky: University Press of Kentucky. 2020. 344 p. Режим доступу: http://doi:10.2307/j.ctvx0786x.

6. Harris C., Kagan, F. Russia's military posture: ground forces order of battle. [Електроний ресурс] Institute for the Study of War, 2018. 53 p. Режим доступу : https://www.jstor.org/stable/resrep17469

7. Perry, W. L., Darilek, R. E., Rohn, L. L., Sollinger, J. M. (Eds.). Operation IRAQI FREEDOM: Decisive War, Elusive Peace. [Електроний ресурс]. Rand Corporation, 2015. pp. 31–56.Режим доступу:
https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1214/RAND_RR1214.pdf .

8. Bensahel, N., Oliker, O., Crane, K., Brennan, R., Gregg, H., Sullivan, T., Rathmell, A. Chapter Two. Military Planning Efforts. After Saddam: Prewar Planning and the Occupation of Iraq. [Електроний ресурс]. RAND Corporation 2008. pp. 5–20. Режим доступу: https://www.jstor.org/stable/10.7249/mg642a.10?seq=1#metadata_info_tab_contents

9. Maistrenko, O., Ryzhov, Y., Khaustov, D., Tsbulia, S., Nastishin, Y.. Decision-Making Model for Task Execution by a Military Unit in Terms of Queuing Theory. [Електроний ресурс] Military Operations Research, 2021. №26 (1), pp.59–69. Режим доступу: https://doi.org/10.5711/1082598326159.

10. Maistrenko, O., Khoma, V., Karavanov, O., Stetsiv, S., Shcherba, A.. Devising a procedure for justifying the choice of reconnaissance-firing systems. [Електроний ресурс]. Eastern-European Journal of Enterprise Technologies, 2021. № 1 (3 (109)), pp. 60–71. Режим доступу: https://doi.org/10.15587/1729-4061.2021.224324

11. Ozdemirel, N. E., Kandiller, L.. Semi-dynamic modelling of heterogeneous land combat. [Електроний ресурс]. Journal of the Operational Research Society, 2006. № 57(1), pp. 38–51. Режим доступу: https://doi.org/10.1057/palgrave.jors.2601940.

12. Ben-Haim, Y. WEI/WUV for Assessing Force Effectiveness: Managing Uncertainty with Info-Gap Theory. [Електроний ресурс]. Military Operations Research, 2018. № 23(4), pp. 37–50. Режим доступу: https://www.jstor.org/stable/26553096

13. Uhm, H. S., Lee, Y. H. A Heuristic Algorithm for Weapon Target Assignment and Scheduling. [Електроний ресурс]. Military Operations Research, 2019. № 24(4), pp.53–62. Режим доступу: https://yonsei.pure.elsevier.com/en/publications/a-heuristic-algorithm-forweapon-target-assignment-and-scheduling.

14. О.В.Майстренко, О.В.Лихольот, М.О.Кольченко. Застосування методу двох функцій для вирішення завдань бойового забезпечення ракетних військ і артилерії. [Електроний ресурс]. Modern Information Technologies in the Sphere of Security and Defence, 2021. № 3(42), С. 5-16. Режим доступу: https://doi.org/10.33099/2311-7249/2021-42-3-5-16.

15. Шалигін, А., Нерубацький, В., Смик, С. Методичний підхід до оцінки бойових потенціалів безпілотних авіаційних комплексів, їх підрозділів і угруповань. [Електроний ресурс]. Наука і техніка Повітряних Сил Збройних Сил України, 2021. № 2(43), С. 73–79. Режим доступу: https://doi.org/10.30748/nitps.2021.43.10.

16. Maistrenko, O., Khoma, V., Lykholot, O., Shcherba, A., Yakubovskyi, O., Stetsiv, S., Kornienko, A., Saveliev A. Devising a procedure for justifying the need for samples of weapons and weapon target assignment when using a reconnaissance firing system. . [Електроний ресурс]. Eastern-European Journal of Enterprise Technologies, 2021. № 5(3 (113), pp. 65–74. Режим доступу: https://doi.org/10.15587/1729-4061.2021.241616.

17. Green, D. J., Moore, J. T., Borsi, J. J.. An Integer Solution Heuristic for the Arsenal Exchange Model (AEM). [Електроний ресурс]. Military Operations Research, 1997. № 3(2), pp. 5–15. Режим доступу: https://doi.org/10.5711/morj.3.2.5.

18. Ma, L., Wang, G.. A Solving Algorithm for Nonlinear Bilevel Programing Problems Based on Human Evolutionary Model. [Електроний ресурс]. Algorithms, 2020. №13 (10), 260 p. Режим доступу: https://doi.org/10.3390/a13100260.

19. Karavanov, O. One of decisions the weapon-target assignment (WTA) problem. [Електроний ресурс]. Débats Scientifiques Et Orientations Prospectives Du Développement Scientifique 2021. Vol. 2. Paris, pp. 87–90. Режим доступу: https://doi.org/10.36074/ logos-05.02.2021.v2.28.

20. Open'ko, P., Mirnenko, V. I., Tyurin, V. V., Myroniuk, M. Y., Doska, O.M., Bulay, A. M. Calculation Method Modification of Spare Parts Quantity to Restore Operability of Weapon Systems. Електроний ресурс]. Advances in Military Technology, 2021. №16 (1), pp.121–132. Режим доступу: https://doi.org/10.3849/aimt.01479

21. Основи моделювання бойових дій військ: підручник /А. В. Атрохов, І. Е. Вернер, В. І. Гавалко, В. І. Козаков. Київ: Вид. НАОУ, 2005. 484 с.

22. Майстренко О. В., Караванов О.А., Щерба А. А. Структурно-функціональний аналіз розвідувально-вогневої системи та декомпозиція її функцій та підсистем. *Військово-технічний збірник.* Львів 2021. №25 С.38-48. DOI: https://doi.org/10.33577/2312-4458.25.2021.38-48

23. Майстренко О. В., Караванов О.А., Лихольот О.В. Обґрунтування сукупності показників оцінювання стійкості функціонування розвідувально-вогневих систем. *Честь і закон*, Харків. 2022. №1(80) С.13-19. doi: https://doi.org/10.3849/aimt.01479

24. Використання теорії ймовірностей в артилерії: підручник / В. І. Макеєв, Ю. І. Пушкарьов, М. М. Ляпа та ін. Суми: Вид.Сумський державний університет, 2019. 494 с.

REFERENCES:

1. John Gordon IV, Igor Mikolic-Torreira, D. Sean Barnett, Katharina Ley Best, Scott Boston, Dan Madden, Danielle C. Tarraf & Jordan Willcox. (2019), "*Army Fires Capabilities for 2025 and Beyond"*. RAND Corporation. 248 p. www.rand.org/pubs/research_reports/RR2124.html (accessed 12 July 2022).

2. Закордонні експерти про війну в Україні та її перспективи. "Zakordonni eksperty pro viynu v Ukrayini ta yiyi perspektyvy. " [Foreign experts on the war in Ukraine and its prospects.] /armyinform.com.ua/2022/08/10/zakordonni-eksperty-pro-vijnu-v-ukrayini-ta-yiyi-perspektyvy/. (accessed 12 August 2022).

3. Вогневий вал: як побороти російську артилерію. "Vohnevyy val: yak poboroty rosiys′ku artyleriyu". [Fire shaft: how to defeat Russian artillery.] www.bbc.com/ukrainian/features-61952663. (accessed 01 August 2022).

4. Daniel Jernigan (2021) ″Closing the FIRES Gap; C.R.O.P.: A Baltic Fires Proposal. ″ Field artillery journal. Issue 4. www.fieldartillery.org/news/closing-the-fires-gap-crop-a-baltic-fires-proposal (accessed 20 July 2022).

5. Lingamfelter, L.. (2020) DesertRedleg: Artillery Warfare in the First Gulf War. Lexington, Kentucky: University Press of Kentucky. 344 p. doi:10.2307/j.ctvx0786x (accessed 05 July 2022).

6. Harris C., Kagan, F. (2018) Russia's military posture: ground forces order of battle. Institute for the Study of War. 53 p. www.jstor.org/stable/resrep17469 (accessed 04 May 2022).

7. Perry, W. L., Darilek, R. E., Rohn, L. L., Sollinger, J. M. (Eds.). (2015). ″Operation IRAQI FREEDOM: Decisive War, Elusive Peace.″ RAND Corporation. pp.31–56. www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1214/RAND_RR1214.pdf (accessed 23 May 2022).

8. Bensahel, N., Oliker, O., Crane, K., Brennan, R., Gregg, H., Sullivan, T., Rathmell, A. (2008). ″Chapter Two. Military Planning Efforts. After Saddam: Prewar Planning and the Occupation of Iraq.″ RAND Corporation, pp.5–20. www.jstor.org/stable/10.7249/mg642a.10?seq=1#metadata_info_tab_contents (accessed 20 May 2022).

9. Maistrenko, O., Ryzhov, Y., Khaustov, D., Tsbulia, S., Nastishin, Y. (2021), ″Decision-Making Model for Task Execution by a Military Unit in Terms of Queuing Theory.″ Military Operations Research, №26 (1), pp.59–69. doi.org/10.5711/1082598326159 (accessed 17 June 2022).

10. Maistrenko, O., Khoma, V., Karavanov, O., Stetsiv, S., Shcherba, A. (2021). ″Devising a procedure for justifying the choice of reconnaissance-firing systems.″ Eastern-European Journal of Enterprise Technologies, №1(3(109)), pp. 60–71. doi.org/10.15587/1729-4061.2021.224324 (accessed 17 May 2022).

11. Ozdemirel, N. E., Kandiller, L. (2006). ″Semi-dynamic modelling of heterogeneous land combat.″ Journal of the Operational Research Society, №57(1), pp.38–51. doi.org/10.1057/palgrave.jors.2601940 (accessed 28 May 2022).

12. Ben-Haim, Y. (2018). ″WEI/WUV for Assessing Force Effectiveness: Managing Uncertainty with Info-Gap Theory.″ Military Operations Research, №23(4), pp.37–50. www.jstor.org/stable/26553096 (accessed 17 June 2022).

13. Uhm, H. S., Lee, Y. H. (2019). ″A Heuristic Algorithm for Weapon Target Assignment and Scheduling.″ Military Operations Research, №24(4), pp.53–62. yonsei.pure.elsevier.com/en/publications/a-heuristic-algorithm-forweapon-target-assignment-and-scheduling (accessed 17 June 2022).

14. Maistrenko, O., Lykholot, O., Kolchenko, M. (2021). "Zastosuvannya metodu dvokh funktsiy dlya vyrishennya zavdan′ boyovoho zabezpechennya raketnykh viys′k i artyleriyi". [Application of the method of two functions to solve the tasks of combat support of missile troops and artillery.] Modern Information Technologies in the Sphere of Security and Defence, № 3(42). doi.org/10.33099/2311-7249/2021-42-3-5-16. (accessed 09 July 2022).

15. Shalygin, A., Nerubatsky, V., Smyk, S. (2021). "Metodychnyy pidkhid do otsinky boyovykh potentsialiv bezpilotnykh aviatsiynykh kompleksiv, yikh pidrozdiliv i uhrupovan′."[ A methodical approach to assessing the combat potential of unmanned aircraft systems, their units and groups.] Science and technology of the Air Force of the Armed Forces of Ukraine, №2(43), pp.73–79. doi.org/10.30748/nitps.2021.43.10 (accessed 16 July 2022).

16. Maistrenko, O., Khoma, V., Lykholot, O., Shcherba, A., Yakubovskyi, O., Stetsiv, S., Kornienko, A., & Saveliev A. (2021). "Devising a procedure for justifying the need for samples of weapons and weapon target assignment when using a reconnaissance firing system." Eastern-European Journal of Enterprise Technologies, №5(3 (113), pp.65–74. doi.org/10.15587/1729-4061.2021.241616 (accessed 12 August 2022).

17. Green, D. J., Moore, J. T., Borsi, J. J. (1997). "An Integer Solution Heuristic for the Arsenal Exchange Model (AEM)." Military Operations Research, №3(2), pp.5–15. doi.org/10.5711/morj.3.2.5 (accessed 15 August 2022).

18. Ma, L., Wang, G. (2020). "A Solving Algorithm for Nonlinear Bilevel Programing Problems Based on Human Evolutionary Model." Algorithms, №13(10), 260 p. doi.org/10.3390/a13100260 (accessed 11 July 2022).

19. Karavanov, O (2021). "One of decisions the weapon-target assignment (WTA) problem." Débats Scientifiques Et Orientations Prospectives Du Développement Scientifique. Vol.2. pp.87–90. doi.org/10.36074/ logos-05.02.2021.v2.28 (accessed 11 July 2022).

20. Open'ko, P., Mirnenko, V. I., Tyurin, V. V., Myroniuk, M. Y., Doska, O.M., Bulay, A. M. (2021). "Calculation Method Modification of Spare Parts Quantity to Restore Operability of Weapon Systems." Advances in Military Technology, №16 (1), pp.121–132. doi.org/10.3849/aimt.01479 (accessed 17 June 2022).

21. A. Atrokhov, I. Werner, V.Havalko & V. Kozakov. (2005). "Osnovy modelyuvannya boyovykh diy viys′k." [Basics of modeling military operations.] NAOU, Kyiv, 484 p.

22. Maistrenko O. V., Karavanov O. A.& Shcherba A. A. (2021) "Strukturno-funktsional′nyy analiz rozviduval′no-vohnevoyi systemy ta dekompozytsiya yiyi funktsiy ta pidsystem". [Structural and functional analysis of the reconnaissance fire system and decomposition of its functions and subsystems.] Military and technical collection, No. 25 pp.38-48 doi.org/10.33577/2312-4458.25.2021.38-48.

23. Maistrenko O. V., Karavanov O. A. & Lykholyot O. V. (2022), "Obgruntuvannya sukupnosti pokaznykiv otsinyuvannya stiykosti funktsionuvannya rozviduval′no-vohnevykh system." [Justification of the set of indicators for assessing the stability of the functioning of reconnaissance and fire systems.] Honor and Law,. No.1(80) pp/13-19 doi.org/10.3849/aimt.01479.

24. Makeev V. I., Pushkarev Yu. I.,. Lyapa M. M, and others (2019) "Vykorystannya teoriyi ymovirnostey v artyleriyi: pidruchnyk."[The use of probability theory in artillery]. Sumy State University, Sumy, 494 p.

**Karavanov O. A.**

**METHODS OF SYNTHESIS OF RECONNAISSANCE AND FIRE SYSTEMS**

***The article proposes an algorithm for the synthesis of reconnaissance and fire systems. Which allows you to justify the need for weapons samples for the completion of subsystems of fire damage and reconnaissance of the specified systems. The essence of the algorithm is to organize the stages of determining the need for weapons samples to ensure the effective functioning of reconnaissance and fire systems. The advantage of the algorithm is that it allows you to take into account the stability of functioning and the capabilities of each type of weapon based on the tasks that rely on the reconnaissance and fire system. This ensures the optimal distribution of weapons and prevents overspending of resources. At the same time, the algorithm is universal and ensures work with all types of means of fire damage and reconnaissance that are in service in the missile forces and artillery of the Armed Forces of Ukraine, taking into account those that are being modernized or developed, as well as those that come as aid from Western countries - partners. In addition to the fact that the proposed algorithm determines the need for weapons when creating new reconnaissance and fire systems, taking into account the given degree of task performance, it also allows determining the degree of performance of assigned tasks, taking into account the available forces and means.***

***The algorithm is based on an improved method of nonlinear programming (two functions), which allows you to take into account both the heterogeneity of types of weapons and military equipment, and the heterogeneity of targets. The improvement consists in determining the "weight" of the types of fire weapons depending on the "weight" of the targets to be hit they are involved. And in the future, normalized fractions of this "weight" are used as weighting coefficients. This makes it possible to justify the need for weapons samples taking into account the given level of performance of the assigned tasks. The defined algorithm allows taking into account the nonlinearity of the functions that describe different types of weapons and targets.***

***Keywords: intelligence-fire system, weapons and military equipment, stability of operation, method of two functions.***

УДК 355.02: 396

к.військ.н., доц. **Кацалап В.О.** (НУОУ)
**Омельянчук А.В.** (ГШ ЗСУ)
**Сивак О.В.** (ГШ ЗСУ)

DOI: https://doi.org/10.17721/2519-481X/2022/77-04

# ОБГРУНТУВАННЯ ПОКАЗНИКІВ ВІДМОВОСТІЙКОСТІ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ЦЕНТРУ ОПЕРАТИВНОГО КЕРІВНИЦТВА ЗБРОЙНИХ СИЛ УКРАЇНИ

***Сучасні підходи до обґрунтування показників відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України базуються на тому, що будь-який процес накопичення, збирання та зберігання інформації має незмінно циклічний характер. Ця його сутність обумовлює потребу обґрунтування показників, які дозволяють резервувати дані в автоматизованій системі управління. До таких показників відмовостійкості автоматизованої системи управління центру оперативного керівництва відносяться: цільова точка відновлення – RPO; цільовий час відновлення RTO; безперервності IT-сервісів. Наведені показники визначають ефективність інформаційного забезпечення автоматизованої системи управління, що полягає у забезпеченні керівництва своєчасною та достовірною інформацією.***

***Зазначене є особливо актуальним в умовах повномасштабної збройної агресії РФ проти України та потребує удосконалення підходів щодо забезпечення відмостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України. Розроблена у статті модель загроз безперервності надання IT-сервісів дозволяє порівняти класи загроз із частотою їх появи та типовими засобами захисту. На їх основі можливо порівнювати відповідні показники регламентного відновлення відносяться, зокрема резервне копіювання та архівування даних на віддаленому сервері (Crossite backup). Крім того, в роботі розглянуті підходи, що базуються на застосуванні фінансових показників ефективності процесів автоматизації (Total cost of ownership), які дозволяють оцінити сукупні витрати на інформаційні технології (обладнання, інструментальні засоби, процеси супроводу інформаційних систем.***

***Ключові слова: центр, оперативне керівництво, спеціальне програмне забезпечення, відмовостійкість, автоматизована система управління, автоматизовані інформаційні системи, Збройні Сили України.***

**Вступ.** У звіті Департаменту внутрішнього аудиту Міністерства оборони України [1] визначено, що автоматизована системи управління центру оперативного керівництва Збройних Сил України є елементом системи інформатизації Збройних Сил України та складовою частиною Єдиної автоматизованої системи управління військами (силами) і включає процеси створення, впровадження і застосування у різних сферах їх діяльності у мирний та воєнний час сучасних методів, систем і засобів одержання, оброблення, зберігання, передавання та використання інформації.

Процес побудови центру оперативного керівництва є основним елементом сучасної Єдиної автоматизованої системи управління Збройних Сил України та вимагає залучення значних відомчих, людських і матеріальних ресурсів, а досягнення очікуваного ефекту певною, мірою залежить від однакового трактування визначених завдань і розуміння їх складових.

Широкомасштабна агресія РФ проти України показала, що рівень відмовостійкості автоматизованої системи управління центру оперативного керівництва у Збройних Силах України, незважаючи на значне розширення ринку інформаційних послуг і продуктів, а також певний розвиток законодавчої бази щодо інформатизації та інформаційного забезпечення залишається на низькому рівні.

**Аналіз відомих досліджень та постановка задач.** В наукових публікаціях, присвячених проблемам відмовостійкості [2-6] розглядається, що використання інформаційних ресурсів спрощує процес прийняття рішень на застосування сил і засобів, які повинні системно реагувати на інформаційні впливи та інформаційні загрози. Базова функціональність таких систем обробки інформації досягається на основі реалізації у їх підсистемах розвідки та інформаційного забезпечення принципів управління, а однією із найважливіших умов дієздатності є потреба оцінювання інформаційних ресурсів, які генерує кожна із них.

В [3] зазначається, що принципові завдання побудови автоматизованих систем управління виконувались для реалізації концепції мережецентричних війн за умови коли сили і засоби розвідки оцінили декілька відомостей та провели класифікацію за джерелами з яких отримані дані. Іншими словами, без актуальної інформації будь-яка автоматизована система не спроможна виконати функціональні завдання за призначенням.

У статті [4] визначено, що у сучасній моделі ведення збройної боротьби є ряд небезпечних недоліків пов'язаних з надмірним адмініструванням процесу інформаційного забезпечення автоматизованих систем управління військами (силами). Але за умов неповних відомостей та даних про противника при малоефективній автоматизованій системі управління військами (силами), виникає ситуація коли кожне рішення буде недостатньо обґрунтованим у зв'язку з відсутністю інтегральних функцій щодо механізму нарощування взаємодії з іншими інформаційними системами.

Проведений аналіз робіт [7-10] присвячених обґрунтуванню показників відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України вказує на відсутність підходів, які дозволяють оцінювати шляхи надання відповідних протоколів обміну для забезпечення інформаційних систем логічною узгодженістю між іншими базами даних в існуючій автоматизованій системі управління військами (силами).

Зазначене вказує на необхідність обґрунтування показників відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України, що обумовлено відсутністю переліку функцій, щодо забезпечення передачі даних між інформаційно-телекомунікаційними мережами основних та резервних автоматизованих систем управління військами (силами).

**Метою статті** є обґрунтування показників відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України для подальшого визначення переліку функцій, що підлягають автоматизації за ступенем їх деталізації в системі управління військами (силами).

**Основні результати досліджень.** Основними проблемами центру оперативного керівництва Збройних Сил України вважаються застарілість або неефективне використання апаратного та програмного забезпечення, відсутність швидкісних захищених мереж передачі даних та централізованих сховищ даних, складність організації доступу до існуючих баз даних, відсутність єдиного формату обміну даними, і як наслідок – низька оперативність та недостовірність інформації.

Ефективне інформаційне забезпечення центру оперативного керівництва Збройних Сил України полягає у забезпеченні керівництва своєчасною та достовірною інформацією шляхом використання безперервних ІТ-сервісів.

Безперервність ІТ-сервісів є головною умовою, що застосовується при побудові центру оперативного керівництва Збройних Сил України, в який закладено комплекс заходів по забезпеченню постійної працездатності програмно-апаратних компонентів.

Це дозволяє зручно здійснювати планування та спрощує роботу користувачів по оформленню документів, що заощаджує час, але не може ефективно застосовуватися для забезпечення ситуаційної обізнаності під час ведення активних бойових дій. При розробці архітектури автоматизованої системи управління центру оперативного керівництва Збройних Сил України є потреба змістити акцент до ситуаційної обізнаності, як основи управління, а не резервування даних. Якщо переглянути архітектуру безперервності ІТ-сервісів, яка може розглядатись як сервіс на рівні оперативного командування або вище для резервування даних та планування ефективного використання, що в свою чергу задовольнить обрис вимог до автоматизованої системи управління центру оперативного керівництва Збройних Сил України.

Ключові характеристики, які визначають вимоги до безперервності ІТ-сервісів, наведені на (рис. 1).


Рисунок 1 – Цільова точка і цільовий час відновлення

На рис. 1 наведено зміст цільової точки відновлення та цільового часу відновлення для порівняння інтервалів часу в кожній із них.

RPO (*Recovery Point Objective*) – цільова точка відновлення – інтервал часу, що передує аварії, за який допускається втрата даних. Іншими словами, цей параметр показує, наскільки стан системи і даних може бути повернений назад при виникненні надзвичайної ситуації.

RTO (*Recovery Time Objective*) – цільовий час відновлення – інтервал часу після аварії, необхідний для відновлення стану системи і даних.

Відповідно, RTO показує час допустимого простою, а RPO – обсяг втрати даних. Теоретично значення RTO/RPO = 0 є найкращим: простій і втрата даних неприпустимі.

На практиці, досягнути RTO = 0 можливо у дуже обмеженому числі випадків, наприклад, коли можливе дублювання функціонально ідентичних апаратних компонент (блоків живлення, дисків, контролерів дискових масивів, мережевих портів).

У випадку більш масштабних аварій (наприклад, відмови серверу або системи) досягнути показника нульового RTO або неможливо фізично, або це може призвести до неприйнятного подорожчання чи ускладнення системи.

З цієї причини, на практиці під нульовим RTO доцільно розуміти час простою, що лежить в межах так званої еластичності функціональних процесів, що виражається в часових одиницях. Величина цієї еластичності може коливатися від декількох десятків секунд до декількох годин (табл. 1).

Таблиця 1

Типові значення часової затримки функціональних процесів

| **Функціональний процес** | **Типова тривалість затримки** |
|---|---|
| Системи масового обслуговування | 10-30 сек. |
| АРМ оператора оперативного управління | 1-5 хв. |
| АРМ оператора забезпечення (логістика) | 15-30 хв. |
| АРМ адміністративних процесів (персонал) | 1-2 год. |

Першим з кроків у проектуванні комплексу організаційно-технічних заходів, спрямованих на недопущення затримки, є визначення моделі загроз безперервності ІТ-сервісів і цільових параметрів RTO/RPO реагування на них. Типова модель загроз представлена в табл. 2.

Таблиця 2

Модель загроз безперервності надання ІТ-сервісів

| **Класи загрози** | **Опис** | **Частота** | **Типові засоби захисту** |
|---|---|---|---|
| А1. Локальні відмови | Некратні відмови устаткування та ПЗ, що призводять до непрацездатності однієї або декількох операційних систем. | Часто, до декількох разів на місяць. | Дублювання апаратних компонентів, холодний резерв, кластери, функції ОС центру оперативного керівництва (шар віртуалізації) |
| А2. Локальні катастрофи | Непрацездатність центру оперативного керівництва. Типові причини – відмова системи електроживлення або охолодження, локальна пожежа | Дуже рідко. Один раз в 3-5 років | Синхронний симетричний або асиметричний резервний центр оперативного керівництва (<50 км) |
| А3. Регіональні катастрофи | Одночасна непрацездатність всіх центру оперативного керівництва на відстані до 100 км. типові причини – масштабні порушення в роботі систем енергопостачання, повені, масові заворушення | Вкрай рідко. Один раз на/за кілька десятиліть | Асинхронний асиметричний резервний центр оперативного керівництва (>100км) |

| | | | |
|---|---|---|---|
| B1.<br>Руйнування даних на рівні логіки | Порушення логічної цілісності даних , викликане збоями ПЗ або помилками людини | Рідко.<br>Кілька разів на рік | Система резервного копіювання і відновлення |
| B2.<br>Вікно обслуговування | необхідність тимчасової зупинки IT-сервісів для проведення регламентного обслуговування устаткування і ПЗ | Часто.<br>До декількох разів на місяць. | Мобільність робочих навантажень |
| B3.<br>Зміни | Внесення змін в інфраструктуру або програмний ландшафт (модернізація обладнання, оновлення ПЗ, міграція центру оперативного керівництва, впровадження нових IT-сервісів) | Часто.<br>До декількох разів на місяць. | Процес управління змінами кошти на попереднє тестування змін |
| B4.<br>Складність | Мимовільна дестабілізація складних систем (наприклад, багатовузлових географічно розподілених кластерів) як результат непередбачуваного збігу обставин або викликані цією складністю помилки адміністрування | Рідко.<br>Кілька разів на рік | Спрощення архітектури, автоматизація сценаріїв адміністрування |

Аналіз результатів табл.1 показує, що із класу загроз найбільш розповсюдженими є локальні відмови, що призводять до непрацездатності однієї або кількох операційних систем декілька разів на рік. Що в порівнянні із руйнуванням даних на рівні логіки дозволяє системі самій адмініструвати копіювання і відновлюватись.

Тому показники відмовостійкості цільової точки відновлення та цільового часу відновлення RTO/RPO автоматизованої системи управління центру оперативного керівництва Збройних Сил України повинні мати оціночні характеристики, як для врахування самостійного, так і регламентного відновлення.

До основних показників регламентного відновлення відносяться:

резервне копіювання та архівування даних на віддаленому сервері (*Crossite backup*) з розміщенням їх;

різні способи реплікації даних на віддалену платформу з розміщенням їх на дискових масивах.

Наведені показники регламентного відновлення дозволяють прогнозувати сценарії можливих локальних і, тим більше, регіональних катастроф, які відрізняються від локальних відмов значно більшою масштабністю і варіативністю. На практиці неможливо передбачити всі можливі варіанти розвитку катастроф, які саме підсистеми IT-інфраструктури будуть

порушені і в якому порядку. З цієї причини реакція на катастрофу повинна визначатися чітким сценарієм дій, змістом і послідовністю враховуючи особливості конкретної ситуації.

Такий сценарій носить назву *DR-плану* (план відновлення у випадку фізичного знищення автоматизованої системи управління центру оперативного керівництва Збройних Сил України).

Типовий DR-план автоматизованої системи управління центру оперативного керівництва Збройних Сил України може включати в себе десятки і сотні послідовних і паралельних кроків щодо порядку залучення людських та технічних ресурсів. Кожен технічний або організаційний механізм захисту повинен бути приведений у дію відповідно до загального сценарію відновлення, з урахуванням конкретної ситуації і взаємодії з іншими механізмами. Одночасне спрацьовування великої кількості окремих механізмів захисту (як автоматизованих, так і ручних) без жорсткого регулювання, на практиці може призводити до взаємно деструктивних і блокуючих наслідків, у результаті чого вся система буде недієздатна.

Таким чином, адекватна реакція на катастрофічні події без DR-плану автоматизованої системи управління центру оперативного керівництва Збройних Сил України неможлива. Водночас, велика варіативність катастроф призводить до того, що неможливо створити універсальний DR-план автоматизованої системи управління центру оперативного керівництва Збройних Сил України, який би враховував всі можливі сценарії розвитку подій.

Виконання DR-плану автоматизованої системи управління центру оперативного керівництва Збройних Сил України завжди проводиться в контексті конкретної ситуації і особливості цієї ситуації, що напряму впливає на відповідні дії і їх послідовність, при виконанні DR-плану. На даному етапі розвитку технологій лише людина здатна на подібну корекцію і деталізацію DR-плану в реальному часі. Це означає, що виконання DR-плану центру оперативного керівництва Збройних Сил України без контролю людини неможливо. Водночас, необхідність участі людини у виконанні DR-плану центру оперативного керівництва Збройних Сил України не означає, що DR-план не піддається автоматизації. Навпаки, автоматизація є ефективною для рутинних "*атомарних*" процедур, які є складовими DR-плану центру оперативного керівництва Збройних Сил України.

Подібна автоматизація дозволяє людині сконцентруватися виключно на своїх функціях: загальній оцінці ситуації та прийнятті рішення про приведення в дію DR-плану центру оперативного керівництва Збройних Сил України та контроль за його виконанням, внесенням коригувань до послідовності дій при нештатних ситуаціях, взаємодії з іншими посадовими особами або організаціями.

IT-інфраструктура автоматизованої системи управління центру оперативного керівництва Збройних Сил України постійно піддається змінам. З цієї причини DR-план може з часом втрачати свою актуальність. Для цього його необхідно постійно уточнювати та періодично тестувати.

Основною проблемою при тестуванні DR-плану як елементу системи відмовостійкості центру оперативного керівництва Збройних Сил України є вплив на роботу продуктивних систем, що призводить до появи нових загроз безперервності IT. Виникає протиріччя, коли DR-план (а саме – необхідність його тестування), призначений для забезпечення безперервності IT, сам може стати загрозою для безперервності функціонування серверів.

З цієї причини максимальна ізоляція продуктивного і резервного дублювання, особливо на період тестування DR-плану центру оперативного керівництва Збройних Сил України, стає ключовою архітектурною вимогою. Ці вимоги потребують проведення аналізу інформаційних загроз відповідно до умов інформаційної технології які наведені в (табл. 2).

Наведені характеристики DR-плану центру оперативного керівництва Збройних Сил України дають можливість запропонувати для кожного класу загроз показники

відмовостійкості, як перелік функцій, що підлягають автоматизації за ступенем їх деталізації в системі управління військами (силами).

А1. Локальні відмови. Оптимальний метод захисту – автоматизовані засоби локальної відмовостійкості.

Дотримуючись принципу "*одне завдання - одне рішення*" доцільним є реалізація механізмів відмовостійкості на рівні рішення віртуалізації та автоматизації . Водночас, це не виключає використання обмеженої кількості специфічних для прикладного ПЗ засобів.

А2. Локальні катастрофи. Оптимальний метод захисту – синхронний резервний центр із частково автоматизованим DR-планом системи управління центру оперативного керівництва Збройних Сил України.

Основні і резервні функції, які підлягають автоматизації в центрі оперативного керівництва Збройних Сил України можуть бути застосовані в режимі "*активний-активний*", тобто кожен з них може нести корисне навантаження. При втраті одного з центрів з метою виключення деградації продуктивності DR-план повинен передбачати зупинку допоміжних додатків (наприклад, процесів розробки) і вивільнення додаткових ресурсів для продуктивного серверу системи. Повинні бути передбачені витрати на періодичне тестування DR-плану з мінімальним (нульовим) впливом на продуктивний сервер.

А3. Регіональні катастрофи. Оптимальний метод захисту – асинхронна або резервна автоматизована система управління центру оперативного керівництва Збройних Сил України. Асинхронна автоматизована система управління центру оперативного керівництва Збройних Сил України може бути асиметричною, тобто містити ресурси, необхідні тільки для зберігання баз даних і запуску на їх основі найбільш критичних масивів. Активація асинхронної автоматизованої системи управління центру оперативного керівництва Збройних Сил України дозволяє застосувати показники відмовостійкості цільової точки відновлення та цільового часу відновлення RTO/RPO, які необхідні для повернення до використання основної автоматизована система управління центру оперативного керівництва Збройних Сил України.

В1. Логічне руйнування даних. Оптимальний метод захисту – система резервного копіювання або відновлення. Слідуючи принципу "*одне завдання - одне рішення*" доцільним є реалізація механізмів резервного копіювання та відновлення на рівні операційних систем автоматизованої системи управління центру оперативного керівництва Збройних Сил України. Обов'язковим елементом системи повинна бути процедура періодичної перевірки можливості відновлення прикладних процесів з використанням резервної копії даних.

В2-В4. Обслуговування, зміни, складність. Оптимальними методами захисту – є мобільність робочих навантажень, процес управління змінами (включаючи інструменти попереднього тестування наслідків змін без впливу на продуктивний сервер системи), усунення зайвої складності або невиправданого автоматизму спрацьовування засобів захисту.

Аналіз наведених функцій показує, що кожна з них має певні особливості, реагування на які потребує впровадження на ряду з показниками відмовостійкості цільової точки відновлення та цільового часу відновлення RTO/RPO такого, як безперервності ІТ-сервісів автоматизованої системи управління центру оперативного керівництва Збройних Сил України.

Врахування додаткового показника відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України, зокрема безперервності ІТ-сервісів є необхідним, оскільки ІТ-інфраструктура автоматизованої системи управління залежить від технологій, які постійно удосконалюються та має відповідати вимогам:

захист від витоку інформації під час передачі її між основною та резервною автоматизованою системою управління центру оперативного керівництва Збройних Сил України;

можливість забезпечення взаємодії з існуючими автоматизованими системами, що функціонують в Збройних Силах України;

можливість взаємодії з інформаційними системами країн членів НАТО.

Реалізація наведених вимог буде можлива шляхом виконання запропонованого узагальненого алгоритму перевірки існуючої системи забезпечення безперервності ІТ-сервісів.

1. Забезпечення безперервності ІТ-сервісів:

захист ІТ-сервісів від загроз;

визначення найбільш важливих ІТ-сервісів за ступенем критичності на основі результатів аналізу взаємозалежностей ІТ-сервісів та їх впливу на функціональні-процеси;

визначення цільових RTO/RPO.

2. DR-план – розробка, оновлення і перевірка:

підготовка плану відновлення;

перевірка актуальності плану відновлення;

проведення тестової перевірки плану відновлення;

приведення до вимог автоматизованим DR-планом системи управління центру оперативного керівництва Збройних Сил України.

3. Підготовка персоналу до виконання DR-плану:

проведення періодичних тренувань по виконанню вимог автоматизованим DR-планом системи управління центру оперативного керівництва Збройних Сил України;

визначення залікового рівня підготовки персоналу.

4. Проведення тестової активації та передачі управління до резервної автоматизованої системи управління центру оперативного керівництва Збройних Сил України:

перевірка готовності резервної автоматизованої системи управління центру оперативного керівництва до активації;

перевірка суміжності в роботі резервної і основної автоматизованої системи управління центру оперативного керівництва.

5. Перевірка придатності резервних копій даних для відновлення ІТ-сервісів:

перевірка можливості фізичного зчитування резервних копій з носіїв;

тестова перевірка когерентності цих копій;

перевірка можливості відновлення ІТ-сервісів на випадок пошкодження даних;

проведення тестування придатності резервних копій для відновлення прикладних систем забезпечення безперервності ІТ-сервісів.

Врахування наведеного узагальненого алгоритму перевірки існуючої системи забезпечення безперервності ІТ-сервісів під час визначення показників відмово стійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України дозволить організувати безперебійну роботу критичних ІТ-систем в новітній Єдиній автоматизованій системі управління військами (силами).

Зазначене потребує в життєвому циклі функціонування автоматизованої системи управління центру оперативного керівництва Збройних Сил України розглядати технологічну та економічну складові. Технологічна з’являється на стадіях проектування та будівництва шляхом врахування цільової точки відновлення ІТ-сервісів.

З фінансової точки зору життєвий цикл створення та функціонування центру оперативного керівництва Збройних Сил України характеризується зростанням капітальних витрат, пік яких припадає на першу половину стадії будівництва, з виходом в рівноважну точку досягненні граничного терміну експлуатації коли вартість підтримання об’єкта в належному стані не виправдовується його цільове призначення. Ці умови потребують

проведення фінансових розрахунків щодо визначення сукупної вартості володіння (*Total cost of ownership – TCO*).

ТСО – є ключовим кількісним показником ефективності процесів автоматизації, який дозволяє оцінити сукупні витрати на інформаційні технології (обладнання, інструментальні засоби, процеси супроводу інформаційних систем, а також дії кінцевих користувачів), аналізувати їх і відповідно управляти витратами (бюджетом) для досягнення балансу доцільності та вартості прямих витрат.

Розрахунок прямих витрат під час створення та функціонування центру оперативного керівництва Збройних Сил України включає як обладнання його амортизацію, так і адміністрування інфраструктури, введення обладнання в експлуатацію, електрика, оплата праці працівників і послуг підрядників, навчання, зв'язок) в ТСО враховуються і непрямі витрати:

втрати від планових і позапланових збоїв в роботі обладнання та ПЗ;

втрати часу співробітників на самостійне управління користувацькими пристроями і додатками;

порушення інформаційної безпеки.

Ключовим принципом створення та функціонування центру оперативного керівництва Збройних Сил України, є системний підхід, який дозволяє оцінити вартість майбутньої та дає уявлення про ймовірні втрати в процесі експлуатації. Незважаючи на те, що більшість витрат можуть бути передбачені або спрогнозовані з високою точністю, деякі витрати носять імовірнісний характер, що тягне за собою ризик істотних відхилень дійсних витрат від очікуваних.

**Висновки.** Основою інтеграції існуючих та перспективних інформаційних систем є центри оперативного керівництва Збройних Сил України, які поєднані у єдиний інформаційний простір та створюють єдине інформаційне середовище з інтегрованою базою даних та єдиними сервісами обміну базами даних. Врахування запропонованого переліку функцій, які підлягають автоматизації за ступенем їх деталізації в системі управління військами (силами) дозволить здійснювати резервування передачі даних між інформаційно-телекомунікаційними мережами основних та резервних автоматизованих систем управління центрами оперативного керівництва Збройних Сил України. Врахування доцільних показників відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України, якими є цільова точка відновлення та цільовий час відновлення RTO/RPO підвищить оперативність функціональних процесів в кризових ситуаціях під час застосування конкретної моделі загроз безперервності надання ІТ-сервісів. Особливе місце в процесі відмовостійкості автоматизованої системи управління центру оперативного керівництва Збройних Сил України займає показник безперервності ІТ-сервісів. Тому, що врахування його характеристик дозволить удосконалювати ІТ-інфраструктуру автоматизованої системи управління, що є фундаментом єдиного інформаційного середовища Збройних Сил України. Впровадження показників, які характеризують фінансові розрахунки щодо визначення сукупної вартості створення та функціонування центру оперативного керівництва Збройних Сил України забезпечить додаткове прогнозування витрат на розвиток Єдиної автоматизованої системи управління військами (силами).

ЛІТЕРАТУРА:

1. Звіт Департаменту внутрішнього аудиту Міністерства оборони України № 234/4341 від 18.12.2020 [Електронний ресурс]: bihus.info. – Режим доступу: http://bihus.info/vijskovi-zlyly-600-mln-na-systemu-upravlinnya-armiyeyu-yaka-mozhe-vyyavytysya-vzagali-neprydatnoyu.

2. Про Положення про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України [Електронний ресурс]: указ [видано Президентом України 14 квітня 1999 р. № 379/99]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/379/99.

3. Про затвердження переліку пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 2015 року [Електронний ресурс]: постанова [видано Кабінетом Міністрів України 7 вересня 2011 р. № 942-2011-п (Із змінами)]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/942-2011-%D0%BF.

4. Уряд планує створити ситуаційний центр [Електронний ресурс]. – Режим доступу: http://defpol.org.ua/site/index.php/ru/arhiv/2010-01-06-09-33-10/8713-2012-02-08-12-24-20.

5. Коммерческие ЦОД в Украине: новый этап развития [Электронный ресурс]. – Режим доступа: http://www.sib.com.ua/arhiv_2010/2010_3/ statia_3_1_2010/statia_3_1_2010.htm.

6. Institute for Data Center Professionals [Electronic Resource]. – Mode of access: http://idcp.marist.edu.

7. Uptime Institute LLC [Electronic Resource]. – Mode of access: http://uptimeinstitute.com.

8. TIA/EIA-942. Telecommunications Infrastructure Standard for Data Centers. – SP–3-0092, 2005. – 151 p.

9. EN 50173-5. Information technology – Generic Cabling Systems – Part 5: Data Centres. – European Standards(EN), 2007. – 140 p.

10. Датацентр консалтинг: Denovo [Электронный ресурс]. – Режим доступа: http://www.de-novo.biz/chastnye-oblaka-i-korporativnye-tsody/datatsentr-konsalting.

REFERENCES:

1. Report of the Department of Internal Audit of the Ministry of Defense of Ukraine No. 234/4341 dated 18.12.2020 [Electronic resource]: bihus.info. – Access mode: http://bihus.info/vijskovi-zlyly-600-mln-na-systemu-upravlinnya-armiyeyu-yaka-mozhe-vyyavytysya-vzagali-neprydatnoyu.

2. About the Regulation on the Anti-Terrorist Center and its coordination groups under the regional bodies of the Security Service of Ukraine [Electronic resource]: decree [issued by the President of Ukraine on 14 April 1999 p. № 379/99]. – Access mode: http://zakon2.rada.gov.ua/laws/show/379/99.

3. On approval of the list of priority thematic areas of scientific research and scientific and technical development for the period until 2015 [Electronic resource]: resolution [issued by the Cabinet of Ministers of Ukraine on September 7, 2011 № 942-2011-п]. – Access mode: http://zakon4.rada.gov.ua/laws/show/942-2011-%D0%BF.

4. The government plans to create a situation center [Electronic resource]. – Access mode: http://defpol.org.ua/site/index.php/ru/arhiv/2010-01-06-09-33-10/8713-2012-02-08-12-24-20.

5. Commercial data center in Ukraine: new stage of development [Electronic resource]. – Access mode: http://www.sib.com.ua/arhiv_2010/2010_3/ statia_3_1_2010/statia_3_1_2010.htm.

6. Institute for Data Center Professionals [Electronic Resource]. – Mode of access: http://idcp.marist.edu.

7. Uptime Institute LLC [Electronic Resource]. – Mode of access: http://uptimeinstitute.com.

8. TIA/EIA-942. Telecommunications Infrastructure Standard for Data Centers. – SP–3-0092, 2005. – 151 p.

9. EN 50173-5. Information technology – Generic Cabling Systems – Part 5: Data Centres. – European Standards(EN), 2007. – 140 p.

10. Data center consulting: Denovo [Electronic Resource]. – Electronic Resource: http://www.de-novo.biz/chastnye-oblaka-i-korporativnye-tsody/datatsentr-konsalting.

**PhD Katsalap V.O.,**
**Omelianchuk A.V,.**
**Syvak O.V.**

# JUSTIFICATION OF INDICATORS OF FAILURE RESISTANCE OF THE AUTOMATED CONTROL SYSTEM OF THE CENTER OF OPERATIONAL MANAGEMENT OF THE ARMED FORCES OF UKRAINE

***Modern approaches to substantiating the failure-tolerance indicators of the automated control system of the operational command center of the Armed Forces of Ukraine are based on the fact that any process of accumulating, collecting and storing information is invariably cyclic in nature. This essence determines the need to justify the indicators that allow data to be backed up in the automated management system. Such indicators of fault tolerance of the automated control system of the operational management center include: target recovery point - RPO; target recovery time - RTO; continuity of IT-services. The given indicators determine the effectiveness of the information support of the automated management system, which consists in providing management with timely and reliable information.***

***This is especially relevant in the conditions of full-scale armed aggression of the Russian Federation against Ukraine and requires improvement of approaches to ensure the resilience of the automated control system of the operational command center of the Armed Forces of Ukraine.***

***The model of IT-service continuity threats developed in the article makes it possible to compare classes of threats with their frequency of occurrence and typical means of protection. Based on them, it is possible to compare the corresponding indicators of scheduled recovery, in particular backup and archiving of data on a remote server (Crossite backup).***

***In addition, the work considers approaches based on the application of financial indicators of the effectiveness of automation processes (Total cost of ownership), which allow to estimate the total costs of information technologies (equipment, tools, processes of supporting information systems.***

***Keywords: center, operational management, special software, fault tolerance, automated control system, automated information systems, Armed Forces of Ukraine.***

УДК: 519.24

д.т.н., проф. **Кошовий М.Д.** (НАКУ «ХАІ»)
**Пилипенко О.Т.** (НАКУ «ХАІ»)

DOI: https://doi.org/10.17721/2519-481X/2022/77-05

# ЗАСТОСУВАННЯ МЕТОДУ ЗРОСТАЮЧИХ ДЕРЕВ ДЛЯ ОПТИМІЗАЦІЇ ПЛАНІВ БАГАТОФАКТОРНИХ ЕКСПЕРИМЕНТІВ

***На сьогоднішній день проблематикою у світі є висока вартість виробництва та ресурсів, через це гостро стає питання оптимізації виробництва для зменшення використання ресурсів. Процес дослідження експерименту на початковому етапі дає змогу зменшити витрати ресурсів за рахунок детального аналізу. Для цього виявляють кроки, які можемо спростити, а це дає економію ресурсів під час виробництва або дослідження. Найчастіше експерименти є багатофакторними і пов'язані з пошуком оптимальних умов проведення, підбором найбільш раціонального обладнання та якісної сировини. Існує необхідність в підвищенні ефективності експериментальних досліджень. Ці дослідження дозволяють докладніше вивчити об'єкти, що дає можливість отримати більше інформації та забезпечує умови їх оптимізації.***

***В процесі дослідження об'єктів необхідно побудувати їх математичні моделі, які дають можливість визначити раціональне співвідношення параметрів. Планування експерименту дозволяє розрахувати максимально ефективний порядок виконання дослідів та вивчити вплив окремих факторів на критерії оптимізації. Застосування методів планування експериментів допомагає в отриманні максимальної кількості корисної інформації при мінімальних вартісних та часових витрат. В даній статті досліджується метод зростаючих дерев для оптимізації за вартісними витратами планів багатофакторних експериментів. Для підтвердження його працездатності та ефективності проводиться порівняльний аналіз з існуючими методами оптимізації. Метод натхненний еволюцією зростаючих дерев і включає етапи посадки і зростання. Розроблено алгоритм та програмне забезпечення, які реалізують даний метод. Програмна реалізація алгоритму виконана за допомогою framework Angular.***

***При дослідженні технологічних процесів була доведена працездатність та ефективність методу зростаючих дерев для оптимізації за вартісними витратами планів багатофакторних експериментів. Проведено його порівняння з бактеріальним методом оптимізації та методом, заснованим на використанні коду Грея. Об'єкт дослідження: процес оптимізації планів багатофакторних експериментів за вартісними витратами. Предмет дослідження: метод зростаючих дерев для оптимізації за вартісними витратами планів багатофакторних експериментів та програмне забезпечення, що його реалізує.***

***Ключові слова: метод зростаючих дерев, дослідження, багатофакторний експеримент, програмне забезпечення, алгоритм.***

**Вступ.** За збільшенням вартості ресурсів та товарів, питання оптимізації процесів виробництва стоїть досить гостро. Кожна компанія намагається вижити і тим самим оптимізувати свої витрати та зменшити вартість виробництва, збільшити потенціал та фінальну ефективність. Максимально оптимізувати процес виробництва від постанови задачі до реалізації готової продукції. Тому задача оптимізації за часовими та вартісними витратами планів багатофакторних експериментів для дослідження виробництва процесів є актуальною.

При цьому виникає завдання пошуку найбільш ефективного методу оптимізації планів багатофакторних експериментів.

Об'єкт дослідження: процес оптимізація планів багатофакторних експериментів за вартісними витратами.

Предмет дослідження: метод зростаючих дерев для оптимізації за вартісними витратами планів багатофакторних експериментів та програмне забезпечення, що його реалізує.

Мета дослідження: розробка методу зростаючих дерев та програмного забезпечення, що його реалізує; застосування методу при дослідженні технологічних процесів; оцінка ефективності методу.

**Аналіз останніх досліджень.** На сьогоднішній день існує значна кількість методів оптимізації планів багатофакторних експериментів [1]. Кожен метод має свої переваги, недоліки та специфіку використання. Більшість методів, які мають перевагу у знаходженні максимально наближеної до оптимальної матриці планування, при зростанні кількості факторів стикаються із проблемою зменшення точності рішення та збільшення обчислювальної потужності та загального часу розрахунку оптимального плану експеримента.

Широко відомі такі методи: повний перебір [2], аналіз перестановок [2], випадковий пошук [2], алгоритм оптимізації роєм часток [3], оптимізація бджолиним роєм [4], метод, заснований на застосуванні коду Грея [5], бактеріальний метод [6], алгоритм чорної дірки [7], алгоритм лева [8], метод стрибаючих жаб [9]. Основними недоліками перелічених методів є: обмежена кількість факторів для об'єкта дослідження, низька швидкодія, знаходження матриці планування, яка не наближена до оптимального значення.

В зв'язку з цим виникає потреба в розробці методу, який характеризується такими параметрами: використанням більше ніж п'яти факторів, отриманням оптимального плану експерименту, високою швидкодією. Таким чином, розглядається застосування методу зростаючих дерев для оптимізації за вартісними витратами плану багатофакторного експерименту для дослідження технологічного процесу гальванічного міднення друкованих плат.

**Основні матеріали дослідження.** Під час виробництва можливі такі причини браку друкованих плат: підгоряння, відслоювання гальванічного покриття, його нерівномірність. Тому виникає необхідність у виконанні попереднього експериментального дослідження технологічного процесу, у побудові адекватної математичної моделі, вибору критерія та методу оптимізації, що дозволить зменшити кількість бракованої продукції.

Операції гальванічної металізації друкованих плат можна описати математичними моделями на основі статистичних методів планування експерименту [10]. Доцільність такого підходу пояснюється складністю досліджуваних процесів, швидкістю отримання математичних моделей, відсутністю детального вивчення хіміко-фізичних закономірностей, які потребують значних вартісних та часових витрат.

Як вихідні показники запропоновані параметри, які характеризують нерівномірність покриття провідників гальванічними опадами.

Ці параметри визначають за такими формулами [11]:

$$\Delta h = supH - infH;$$
$$\Delta h_{\text{ср}} = \frac{1}{n}\sum_{i=1}^{n}\Delta h_i;$$
$$\Delta h_i = supH_i - infH_i;$$
$$H_i \subseteq H;\ i = \overline{1,n}$$

де $\Delta h$ - максимальний розкид висоти провідників, $\Delta h_{ср}$ - середній розкид,

$H_i$ - підмножина множини H, елементами якої є висота провідників, що визначається у характерних локальних місцях n друкованої плати.

Показник $R_z$ визначається згідно з методикою вимірювання параметрів шорсткості поверхні. При цьому вимірюють на профілограмі відстані $h_{imax}$ від п'яти найбільших максимумів профілю до базової лінії та відстані $h_{imin}$ від п'яти найбільших мінімумів профілю до базової лінії, мм.

$$R_z = \frac{1}{5V_B}\left(\sum_{i=1}^{5} h_{imax} - \sum_{i=1}^{5} h_{imin}\right) * 10^3,$$

де $R_z$ - параметр шорсткості поверхні провідників друкованої плати,

$V_в$ - вертикальне збільшення профілографа.

Метою експериментального дослідження операції гальванічного міднення друкованих плат є побудова математичних моделей, які характеризують зв'язок окремих її параметрів $X_i$ з показниками якості $\Delta h$, $\Delta h_{ср}$, $R_z$:

$$\Delta h = f_1(X_1, X_2, X_3, X_4);$$

$$\Delta h_{\text{ср}} = f_2(X_1, X_2, X_3, X_4);$$

$$R_z = f_3(X_1, X_2, X_3, X_4).$$

Фактори, що впливають на результат: $X_1$ – концентрація $CuSO_4$ в електроліті гальванічної ванни, г/л; $X_2$ – концентрація $H_2SO_4$ в розчині, г/л; $X_3$ – густина струму в гальванічній ванні, А/дм$^2$ ; $X_4$ – час обробки плат в цій ванні. Для оптимізації плану повного факторного експерименту $2^4$ за вартісними витратами був застосований метод зростаючих дерев.

**Алгоритм реалізації методу зростаючих дерев.** Алгоритм зростаючих дерев натхненний еволюцією зростаючих дерев і включає етапи посадки і росту. На етапі посадки саджанці випадково рівномірно розташовуємо в області пошуку, створюючи рівномірний сад. Етап росту реалізуємо за допомогою операторів схрещування, розгалуження, щеплення.

Метод зростаючих дерев базується на використанні графів типу дерева. Граф типу дерева - це зв’язковий ациклічний граф, який відомий своєю простотою та ефективністю [12].

Суть оптимізації плану багатофакторного експерименту методом зростаючих дерев полягає в наступному.

Крок 1. Вибір кількості факторів.

Крок 2. Введення значення вартості переходів для кожного з факторів.

Крок 3.1. Генерація початкової матриці в залежності від кількості факторів.

Крок 3.2. Визначення послідовності проведення розрахунків матриць.

Крок 4. Розрахунок вартості початкової матриці.

Крок 5.1. Підстановка рядка на початок матриці.

Крок 5.1.1. Підрахунок вартості переходу між вибраним рядком та наступним.

Крок 5.1.2. Пошук мінімальної різниці вартості переходу вибраного рядку з рядком, який не був ще використаний у матриці.

Крок 5.1.3. Усі рядки з матриці були використані.

Крок 5.1.4. Замінюємо початковий рядок матриці на наступний, який не був використаний, і проводимо розрахунок.

Крок 5.2. Усі рядки матриці були підставлені на початок матриці та проведені за такою схемою.

Крок 6.1. Розрахунок вартості всіх отриманих матриць.

Крок 6.2. Проводимо порівняння вартості отриманих матриць.

Крок 7. На основі отриманих результатів обираємо матрицю з мінімальною сумарною вартістю.

Крок 8. Порівняння та аналіз початкової матриці з оптимальною, яка була розрахована за допомогою методу зростаючих дерев.

Крок 9. Виведення отриманих результатів на екран.

Програмна реалізація алгоритму виконана за допомогою framework Angular на мові розробки TypeScript [13], який є надбудовою над мовою програмування JavaScript. Переваги використання Angular полягає у тому, що він побудований на основних принципах об'єктно-орієнтованого програмування (ООП). Методологія ООП заснована на представленні програми у вигляді сукупності взаємодіючих об'єктів, кожен із яких є екземпляром певного класу, а класи утворюють ієрархію спадкування.

Схема алгоритму роботи методу зростаючих дерев представлена на рис. 1.

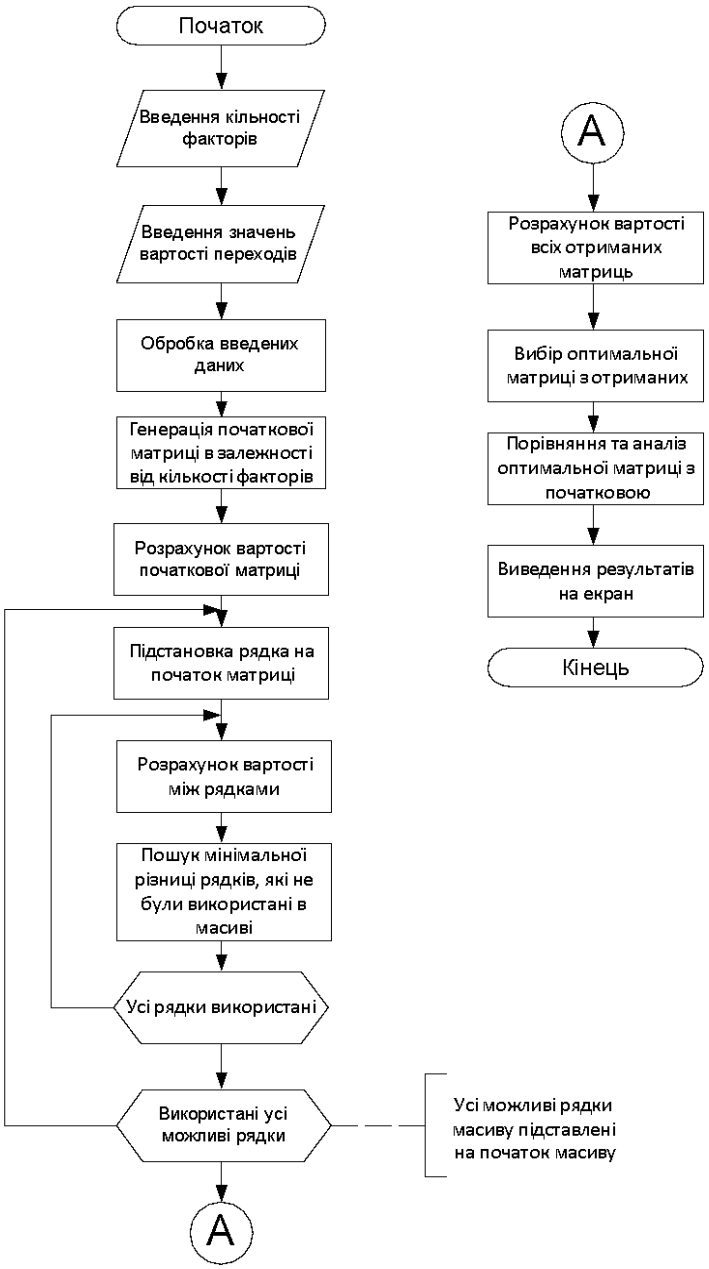



Рисунок 1 – Схема реалізації методу зростаючих дерев

**Результат оптимізації.** Була проведена оптимізація планів багатофакторних експериментів методами зростаючих дерев, бактеріальної оптимізації, методом, що ґрунтується на використанні коду Грея. Виконано порівняльний аналіз отриманих планів експерименту.

Вартості змін значень рівнів факторів наведені в табл. 1.

Таблиця 1

Вартість змін значень рівнів факторів, ум. од.

| Фактор | Вартість змін значень рівнів, ум. од. | |
|---|---|---|
| | з «-1» до «+1» | з «+1» до «-1» |
| $X_1$ | 18.85 | 7.45 |
| $X_2$ | 8.65 | 4.45 |
| $X_3$ | 0.19 | 0.18 |
| $X_4$ | 1.15 | 0.77 |

У табл. 2 приведена початкова матриця багатофакторного експерименту.

Таблиця 2

Початкова матриця багатофакторного експерименту

| Номер досліду | Фактори | | | |
|---|---|---|---|---|
| | $X_1$ | $X_2$ | $X_3$ | $X_4$ |
| 1 | - | - | - | - |
| 2 | + | - | - | - |
| 3 | - | + | - | - |
| 4 | + | + | - | - |
| 5 | - | - | + | - |
| 6 | + | - | + | - |
| 7 | - | + | + | - |
| 8 | + | + | + | - |
| 9 | - | - | - | + |
| 10 | + | - | - | + |
| 11 | - | + | - | + |
| 12 | + | + | - | + |
| 13 | - | - | + | + |
| 14 | + | - | + | + |
| 15 | - | + | + | + |
| 16 | + | + | + | + |

Плани багатофакторних експериментів, отриманих методом, що ґрунтується на використанні коду Грея та бактеріальної оптимізації, представлені в табл. 3.

Таблиця 3

План багатофакторного експерименту, що ґрунтується на використанні коду Грея, та план, отриманий методом бактеріальної оптимізації

| Метод, заснований на коді Грея | | | | | Бактеріальний метод | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Номер досліду | Фактори | | | | Номер досліду | Фактори | | | |
| | $X_1$ | $X_2$ | $X_3$ | $X_4$ | | $X_1$ | $X_2$ | $X_3$ | $X_4$ |
| 1 | - | - | - | - | 1 | + | + | + | + |
| 2 | - | - | - | + | 2 | + | + | - | + |
| 3 | - | - | + | + | 3 | + | + | + | - |
| 4 | - | - | + | - | 4 | + | + | - | - |
| 5 | - | + | + | - | 5 | + | - | + | + |
| 6 | - | + | + | + | 6 | + | - | - | + |
| 7 | - | + | - | + | 7 | + | - | + | - |
| 8 | - | + | - | - | 8 | + | - | - | - |
| 9 | + | + | - | - | 9 | - | + | + | + |
| 10 | + | + | - | + | 10 | - | + | - | + |
| 11 | + | + | + | + | 11 | - | + | + | - |
| 12 | + | + | + | - | 12 | - | + | - | - |
| 13 | + | - | + | - | 13 | - | - | + | + |
| 14 | + | - | + | + | 14 | - | - | - | + |
| 15 | + | - | - | + | 15 | - | - | + | - |
| 16 | + | - | - | - | 16 | - | - | - | - |

Для знаходження мінімальної вартості проведення експерименту було проведено оптимізацію початкового плану ПФЕ методом зростаючих дерев. План отриманого багатофакторного експерименту наведено у табл. 4.

Таблиця 4

Оптимальний план багатофакторного експерименту, отриманий методом зростаючих дерев

| Номер досліду | Фактори | | | |
|---|---|---|---|---|
| | $X_1$ | $X_2$ | $X_3$ | $X_4$ |
| 1 | + | + | - | - |
| 2 | + | + | + | - |
| 3 | + | + | + | + |
| 4 | + | + | - | + |
| 5 | + | - | - | + |
| 6 | + | - | + | + |
| 7 | + | - | + | - |
| 8 | + | - | - | - |
| 9 | - | - | - | - |
| 10 | - | - | + | - |
| 11 | - | - | + | + |
| 12 | - | - | - | + |
| 13 | - | + | - | + |
| 14 | - | + | + | + |
| 15 | - | + | + | - |
| 16 | - | + | - | - |

Вартісні витрати на реалізацію експерименту за початковим планом складають 252.61 ум. од., за оптимальним планом – 25.87 ум. од. Порівняно з початковим планом, виграш становить 9.76 разів. А у порівнянні з планом експерименту, отриманим з використанням коду Грея, вартість реалізації якого дорівнює 40.37 ум. од., отримуємо виграш 1,56 разів. Порівнюючи з вартістю реалізації плану експерименту, отриманого бактеріальним методом, що складає 34.30 ум.од., виграш становить 1.33 рази.

Результати порівняння ефективності методу зростаючих дерев з іншими методами представлені в табл. 5.

Таблиця 5

Результати порівняння ефективності методу зростаючих дерев з іншими методами

| Метод оптимізації | Вартість, ум.од. |
|---|---|
| Початковий метод | 252.61 |
| Код Грея | 40.37 |
| Бактеріальний метод | 34.30 |
| Метод зростаючих дерев | 25.87 |

**Висновки.** Для оптимізації планів багатофакторного експерименту за вартісними витратами розроблено метод зростаючих дерев. Для реалізації методу було розроблено програмне забезпечення за допомогою framework Angular на мові розробки TypeScript [13]. У порівнянні з методом, отриманим з використанням коду Грея, та бактеріальним методом, була доведена працездатність та ефективність методу зростаючих дерев.

За результатами дослідження метод зростаючих дерев дає виграш у вартості в 9.76 разів у порівнянні з початковим планом експерименту. У порівнянні з планом експерименту, отриманим з використанням коду Грея, маємо виграш в 1.56 разів, а у порівнянні з бактеріальним методом перевага складає 1.33 рази.

ЛІТЕРАТУРА:


1. Кошовий М. Д., Бурлєєв О. Л., Пампуха А. І. Аналіз методів оптимального планування багатофакторного експерименту за вартісними та часовими показниками. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – №75. С. 94-107. DOI: https://doi.org/10.17721/2519-481X/2022/75-10.
2. Кошевой Н. Д., Костенко Е. М. Оптимальное по стоимостным и временным затратам планирование эксперимента: монография. Нац. аэрокосм. ун-т им. Н. Е. Жуковского «Харьк. авиац. ин-т». – Х.: ХАИ; Полтава: Шевченко Р. В., 2013. – 316 с. ISBN 978-966-8798-89-4.
3. Кошевой Н. Д., Беляева А. А. Применение алгоритма оптимизации роем частиц для минимизации стоимости проведения многофакторного эксперимента. Радіоелектроніка, інформатика, управління. - 2018. - № 1. - С. 41-49. DOI: 10.15588 / 1607-3274-2018-1-1.
4. Карпенко А. П. Популяционные алгоритмы глобальной поисковой оптимизации. Обзор новых и малоизвестных алгоритмов. Информационные технологии. 2012. № 7. С. 1-32.
5. Koshevoy N. D., Kostenko E. M., Pavlyk A. V., Koshevaya I. I., Rozhnova T. G. Research of multiple plans in multi-factors experiments with a minimum number of transitions of levels of factors. Radio Electronics, Computer Science, Control. 2019. no 2, P.53-59. DOI: 10.15588/1607-3274-2019-2-6.
6. Кошовий М. Д., Пилипенко О. Т. Застосування методу бактеріальної оптимізації для мінімізації витрат часу при проведенні багатофакторного експерименту. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2021. – №72. С. 25-31. DOI: https://doi.org/10.17721/2519-481X/2021/72-04.
7. A. Hatamlou, Black hole: A new heuristic optimization approach for data clustering, Information sciences, 2013 - vol. 222, pp. 175–184,.
8. M. Yazdani, F. Jolai, Lion optimization algorithm (loa): a nature-inspired metaheuristic algorithm, Journal of computational design and engineering, 2016 - vol. 3, no. 1, pp. 24–36.
9. Koshevoy N. D., Muratov V. V., Kirichenko A. L., Borisenko S. A. Application of the “jumping frogs” algorithm for research and optimization of the technological process. Radio Electronics, Computer Science, Control. 2021. no1(1). – P. 57 – 65. DOI: 10.15588/1607-3274-2021-1-6.
10. Адлер Ю. П. Планирование эксперимента при поиске оптимальных условий (программное введение в планирование эксперимента) / Ю.П. Адлер, Е. В. Маркова, Ю. В. Грановский. – М. : Наука, 1971. – 283 с.
11. Кошевой Н. Д. Автоматизация экспериментальных исследований: моногр. / Н.Д. Кошевой, В.А. Гаевой. – Х.: Факт, 2001. – 112 с.
12. Харари Ф. Теория графов / Ф. Харари. – М.: Мир, 1973. – 302 с.
13. Введение в typescript [Електронний ресурс]. – 2021. URL: https://metanit.com/web/typescript.

REFERENCES:


1. Koshoviy M. D., Burleev O. L., Pampuha A. I. Analiz metodiv optimalnogo planuvannya bagatofaktornogo eksperymentu za vartisnimi ta chasovimi pokaznikami [Analysis of methods of optimal planning of a multifactorial experiment by cost and time indicators]. Zbirnik naukovih prats Viyskovogo Institutu Kyivskogo natsionalnogo universitetu Imeni Tarasa Shevchenka. – K.: VIKNU, 2022. – No. 75. pp. 94-107.

2. Koshevoy N. D. and Kostenko E. M. Optimalnoe po stoimostnyim i vremennyim zatratam planirovanie eksperimenta [Optimal cost and time planning of the experiment]: monografiya. Nats. aerokosm. un-t im. N. E. Zhukovskogo «Khark. aviats. in-t». – Kh.:KhAI; Poltava: Shevchenko R. V., 2013. – 316 pp. ISBN 978-966-8798-89-4.

3. Koshevoy N. D. and Belyaeva A. A. Primenenie algoritma optimizatsii roem chastits dlya minimizatsii stoimosti provedeniya mnogofaktornogo eksperimenta [Application of the Particle Swarm Optimization Algorithm to Minimize the Cost of Conducting a Multivariate Experiment]. Radioelektronika, informatyka, upravlinnia. - 2018. - № 1. - pp. 41-49. DOI: 10.15588 / 1607-3274-2018-1-1.

4. Karpenko A.P. Populyatsionnyie algoritmyi globalnoy poiskovoy optimizatsii. Obzor novyih i maloizvestnyih algoritmov [Population algorithms for global search optimization. Overview of new and little-known algorithms]. Informatsionnyie tehnologii. 2012. № 7. P. 1-32.

5. Koshevoy N. D., Kostenko E. M., Pavlyk A. V., Koshevaya I. I. and Rozhnova T. G. Research of multiple plans in multi-factors experiments with a minimum number of transitions of levels of factors. Radio Electronics, Computer Science, Control. 2019. № 2, P. 53-59. DOI: 10.15588/1607-3274-2019-2-6.

6. Koshevoy N. D. and Pylypenko O.T. Zastosuvannya metodu bakterialnoyi optimizatsiya dlya minimizatsIyi vitrat chasu pri provedeni bagatofaktornogo eksperymentu [Application of the bacterial optimization method to minimize time spent in multifactorial experiments]. Zbirnik naukovih prats Viyskovogo Institutu Kyivskogo natsionalnogo universitetu Imeni Tarasa Shevchenka. – K.: VIKNU. – 2021. No. 72. – pp. 25-31. DOI: https://doi.org/10.17721/2519-481X/2021/72-04

7. A. Hatamlou, Black hole: A new heuristic optimization approach for data clustering, Information sciences, 2013 - vol. 222, pp. 175–184,.

8. M. Yazdani and F. Jolai, Lion optimization algorithm (loa): a nature-inspired metaheuristic algorithm, Journal of computational design and engineering, 2016 - vol. 3, no. 1, pp. 24–36.

9. Koshevoy N. D., Muratov V. V., Kirichenko A. L. and Borisenko S. A. Application of the “jumping frogs” algorithm for research and optimization of the technological process. Radio Electronics, Computer Science, Control. 2021. no1(1). – P. 57-65. DOI: 10.15588/1607-3274-2021-1-6.

10. Adler Y.P., Markova E.V. and Granovskiy Y. V. Planirovanie eksperimenta pri poiske optimalnyih usloviy (programmnoe vvedenie v planirovanie eksperimenta) [Experiment design in search of optimal conditions (software introduction to experiment design)]. - M.: Nauka, 1971 – P. 283

11. Koshevoy N. D. and Gaevoy V. A. Avtomatizatsiya eksperimentalnyih issledovaniy [Automation of experimental research]: monografiya. H.: Fakt, 2001 - P. 112.

12. Harari F. Teoriya grafov [Graph theory]. – M.: Mir, 1973. – P. 302.

13. Vvedenie v typescript [Introduction to typescript]. – 2021. URL: https://metanit.com/web/typescript.

**Doctor of Technical Science, Koshovyi M. D.,**
**Pylypenko O.T.**

# APPLICATION OF THE GROWING TREES METHOD FOR OPTIMIZING PLANS OF MULTIFACTOR EXPERIMENTS

***Nowadays, the high cost of production and resources is the problem in the world, because of this, the issue of optimizing production to reduce the use of resources becomes acute. The research of the experiment at the initial stage makes it possible to reduce resource costs due to detailed analysis. For this we identify steps that we can simplify, which saves resources during production or research. Most often, experiments are multifactorial and related to the search for optimal conditions, selection of the most rational equipment and high-quality raw materials. There is a need to increase the effectiveness of experimental research. These researches allow us to study objects in detail, which provides the ability to obtain more information and offers conditions for their optimization.***

***In the process of researching objects, it is necessary to build their mathematical models, which allow us to determine a rational ratio of parameters. Experiment planning allows for calculating the most effective order of performing experiments and studying the influence of individual factors on optimization criteria. The use of experimental planning methods helps in obtaining the maximum amount of useful information with minimal cost and time spent. This article examines the growing tree method for cost optimization of multifactor experimental plans. To confirm its functionality and effectiveness, a comparative analysis is conducted with existing optimization methods. The method is inspired by the evolution of growing trees and includes the stages of planting and growth. An algorithm and software that implement this method have been developed. The software implementation of the algorithm is made with the help of the framework Angular. In the study of technological processes, the functionality and effectiveness of the method of growing trees for cost optimization of plans of multifactor experiments has been proven. It has been compared with the bacterial optimization method and the method based on the use of the Gray code. The object of research: the process of optimization of plans of multifactor experiments according to its cost.***

***The subject of study: growing tree method for cost optimization of multifactor experimental plans and software implementing it.***

***Keywords: growing tree method, research, multifactor experiment, software, algorithm.***

**УДК 355/358**

к.т.н. **Максименко Ю.А.** (ВА м. Одеса)
к.т.н., доц. **Маміч В.В**. (ВА м. Одеса)
д.н. з держ.упр., проф. **Попов С.А.** (ВА м. Одеса)
**Шаршаткін Д.Ю.** (ВА м. Одеса)

DOI: https://doi.org/10.17721/2519-481X/2022/77-06

# АНАЛІЗ ФУНКЦІОНУВАННЯ СИСТЕМИ АНАЛІТИЧНОЇ РОЗВІДКИ НАТО

***Для успішного ведення сучасного бою, за поглядами сучасних військових вчених, необхідно, насамперед, знати противника, його сили, засоби і характер дій. Для забезпечення цими даними командирів і штабів усіх ступенів існує найважливіший вид бойового забезпечення дій військ – розвідка. Досвід ведення бойових дій свідчить, що тільки там, де розвідка ведеться активно і цілеспрямовано, бойові завдання вирішуються успішно і з найменшими втратами. Навпаки, погано організована розвідка завжди була головною причиною невдалих бойових дій військ. У теперішній час значно виріс обсяг завдань, які вирішує розвідка. Натомість терміни їх виконання суттєво скоротилися. Підвищилися вимоги щодо часу передавання даних і точності визначення координат об'єктів (цілей) противника. Аналітична розвідка - компонент розвідувальної діяльності, що складається з виявлення, оцінювання, прогнозування різних соціальних процесів, подій, заходів на основі відомостей, переважно одержуваних з відкритих джерел, а також видобуваються розвідкою інших видів (агентурною, технічною та ін.). Аналітична розвідка ділиться на оперативну (ту, що обслуговує поточні потреби) і стратегічну (яка формує стійкі уявлення). Оперативно досліджує короткочасні феномени (мають місце, недавні або скоро очікувані) - для забезпечення відповідної невідкладної діяльності. Стратегічна виявляє те, що вкрай неочевидно, настає не скоро, змінюється повільно, вимагає довготривалих, масштабних заходів. Аспекти аналітичної розвідки: збір і зіставлення різних відомостей з метою виявлення тенденцій, суперечностей, дезінформації, помилкової інтерпретації, маніпуляційних заходів, неявних подій, прихованої діяльності, а також формування загальних уявлень про різні істотних суб'єктах і феномени; оцінювання суб'єктів, подій, дій, намірів; прогнозування подій, дій, намірів; планування заходів, подій. Інформаційне забезпечення конкретних відкритих і таємних операцій; участь у розробці стратегій забезпечення національної безпеки, національного розвитку, глобального розвитку. Актуальним питанням сьогодення стало широке впровадження сучасних інформаційних технологій, на думку вчених, воно є безумовною вимогою сучасних бойових дій.***

***Ключові слова: аналітична розвідка, соціальні процеси, інформаційне забезпечення, інтерпретація, маніпуляція, феномени,загальні уявлення, компонент,стратегічна розвідка.***

**Вступ та постановка задачі.** За поглядами воєнних фахівців НАТО механізм здійснення розвідувальної діяльності іншими словами називають розвідувальним циклом. Основною проблемою проведення розвідувальних процедур є використання розвідувального циклу - послідовності дій, за допомогою яких інформація отримується, зводиться, перетворюється на розвідувальну інформацію і стає доступною для користувачів. У загальному вигляді розвідувальний цикл являє собою комплекс заходів, що складається з етапів, які виконуються на різних рівнях із різною швидкістю. Ці етапи передбачають виконання дій, які, фактично, визначають суть розвідки: націлювання, добування, обробку й доведення. Деякі заходи перекривають один одного і часто проводяться одночасно, а не послідовно. Кожен етап підвищує цінність інформації. На початковому етапі не зрозуміло не тільки що робити, але і що взагалі відбувається. Далі усвідомлюється, що відбувається і уявлення структуруються. Ви вже дещо розумієте. Цінність вашої інформації підвищилася. Після чого ви формулюєте проблему, ставите завдання й прикидаєте план дій. Цінність інформації ще збільшилася. Далі починається збір потенційно корисної інформації та її накопичення [1]. Цінність інформації ще збільшується. І так у міру наближення до фінішу ви збільшуєте цінність вашої інформації. Але дійшовши до останнього пункту робота не закінчується. Як тільки споживач починає використовувати інформацію, надану вами, його обізнаність збільшується, а це вносить відповідні корективи в його дії і в його інформаційні потреби. Споживач коригує свої запити і розвідувальний цикл повторюється. Мало того, на

етапі усвідомлення або планування, збору або обробки інформації, на її поширення або використання також можуть бути внесені відповідні корективи. І розвідувальний цикл повториться. У цьому полягає одна з найважливіших проблем сучасної розвідувальної діяльності - циклічність і безперервність [2].

**Аналіз останніх досліджень і публікацій**. Питання аналізу функціонування системи аналітичної розвідки НАТО розглянуті у нижче переліченої наукової літератури:

Методичні рекомендації з розробки розвідувальних оцінок (за стандартами провідних країн-членів НАТО). – К.: ГУР МО України, 2018. – 118 с.; Курносов Ю. Аналітика як інтелектуальна зброя. – М.: Ритм, 2015, - 613 с.; Оленович І.Ф., Сбітнев А.І. та ін.; Методологія дослідження складних систем військового призначення, Київ, вид. НАОУ, 2003, 400 с.; Артюшин Л.М., Зиатдинов Ю.К., Харченко А.В. Під ред. И.А. Попова; Великі технічні системи, проектування та керування. – Харків: Факт, 1997. – 400 с.;

Тактична розвідка в бойових прикладах за досвідом проведення АТО:

посібник. – Київ: МОУ ГУР, 2017. – 160 с.; Тактика в бойових прикладах (з досвіду антитерористичної операції): навч.-метод. посіб./колектив авторів; за заг. ред. А. М. Сиротенка. – К.: НУОУ ім. І. Черняховського, 2017. – 140 с.; Військовий стандарт 01.101.004. Видання 2. Воєнна розвідка. Розвідувально-інформаційна діяльність. Терміни та визначення. – К. : Міністерство оборони України, 2015. – 26 с.; Процеси розвідувальної діяльності. Стандарт НАТО. Союзницька об'єднана настанова AJP–2.1 (видання B, варіант 1)/ Управління стандартизації НАТО, 2016. – 80 с.; Основи розвідувально-інформаційної діяльності: настанова Штабу розвідки Міністерства оборони Великобританії. – К.: ГУР МО України, 2015. – 51 с. [3].

Відповідно до поширених підходів наукових публікацій розвідувальний цикл має шість основних етапів: націлювання або планування, добування, обробка, оцінка, поширення, отримання висновків. **Планування, націлювання -** передбачає встановлення вимог до розвідувальних даних, планування зусиль щодо збору інформації та постановку завдань добувним підрозділам. Ці вимоги є ключовими для розвідки. Щоб зробити цей процес більш ефективним, передбачено два напрями керівництва діями зовнішнє і внутрішнє: зовнішнє керівництво здійснюють командири (командувачі) на кожному рівні: встановлюють параметри вимог до розвідданих і визначають цілі; внутрішнє керівництво здійснює начальник органу управління розвідки у кожній ланці штабу інтегрованої розвідки; з**бирання, добування -** процес виконання заходів та дій, спрямованих на отримання розвідувальної інформації шляхом виявлення об'єктів противника. Активні дії щодо добування інформації ведуться за допомогою спостереження і рекогносцировки, що становить основну частину зібраної інформації [4].

Добуваючи розвідувальну інформацію, необхідно підтримувати взаємозв'язок з іншими видами розвідки для оптимізації зібраних розвідданих; **обробка** перетворення добутої розвідувальної інформації в розвідувальні відомості шляхом аналізу, оцінювання надійності та достовірності, інтерпретації розвідувальних відомостей в дані. У результаті обробки інформації можуть з'явитися додаткові вимоги до збору та передачі розвідувальних даних. **Оцінка -** підготовка розвідувальної оцінки забезпечує розуміння оперативної обстановки і є основою планування. Об'єднана розвідувальна оцінка оперативної обстановки фокусує зусилля розвідки, сприяє виробленню розуміння оперативної обстановки, допомагає реалізувати план з виявлення можливостей для рішучих дій. **Поширення -** етап, суть якого полягає у вчасному наданні розвідувальної оцінки в потрібній формі відповідними засобами споживачам у найбільш зручний для них спосіб. На етапах оцінювання та поширення слід дотримуватись встановленого режиму секретності згідно з вимогами замовника. Знання, поширене через тиждень, рівноцінне незнанню. Немає цінності в зібраних даних і ситуаційній обізнаності, якщо вони не були використані для виконання місії або оцінювання нанесеної шкоди противнику; **Отримання висновків -** завершальний етап розвідувального циклу, який полягає в отриманні висновків, рекомендацій, зворотній реакції від споживача інформації.

**Мета статті** полягає у аналізі функціонування системи аналітичної розвідки НАТО, з метою. використання елементів розвідувального циклу, який прийнятий у країнах-членах НАТО, при плануванні розвідки, що застосовуються у Збройних Силах України [5].

**Виклад основного матеріалу.** У польовому статуті армії США FM 2-0 (2004) INTELLIGENCE OPERATIONS так сформульовано поняття «розвідувальний процес»: Розвідувальний процес охоплює всі елементи операційного процесу (планування, підготовка, виконання та оцінка) і може виконуватися кілька разів для підтримки кожного елемента. Незважаючи на те, що він розроблений аналогічно операційному процесу, процес розвідки включає в себе аспекти і дії, специфічні для функції розвідувальної діяльності: Планування і безпосереднє виконання всіх кроків процесу розвідки тісно пов'язані з плануванням и виконання оперативної діяльності; Етапи збору, обробки і поширення а також аналітична діяльність розвідувального процесу відповідають завданням оперативної діяльності; Безперервна оцінка розвідувальної інформації є частиною загальної діяльності командування в оперативному процесі. Розвідувальні операції зазвичай включають п'ять функцій, які складають процес розвідки: **планування, підготовка, збір, обробка та виробництво.** Крім того, в п'яти функціях інтелектуального процесу виконуються три спільні завдання: **аналізувати, поширювати і оцінювати.**

Три загальні завдання обговорюються після виконання останньої функції. Функції розвідувального процесу не обов'язково є послідовними; це те, що відрізняє **процес** розвідки від **циклу** розвідки. Розвідувальний процес генерує інформацію про загрози і ситуації, яка дозволяє командиру і штабу розробити план, захопити і зберегти ініціативу, створити і використовувати раптовість і досягати успіху [6].

Відповідно до польового статуту FM 2-0 2019 року процес розвідки армії складається з **чотирьох етапів (планування і управління, збір, виробництво і поширення) і двох безперервних заходів (аналіз і оцінка)** [7].

Командири керують процесом розвідки. Процес розвідки підтримує всі дії оперативного процесу (планування, підготовка, виконання та оцінка) і може виконуватися кілька разів на кожному етапі боя (операції). Хоча розвідувальний процес і розроблений аналогічно оперативному процесу, він включає в себе дії, специфічні для розвідувально-бойових дій: Планування і безпосереднє виконання етапів розвідувального процесу тісно пов'язані з планом діяльності командування; Етапи збору, обробки і поширення, а також аналітична діяльність розвідувального процесу відповідають задуму боя (операції); Оцінка, яка є безперервною, є частиною загальної діяльності з оцінки операційного процесу.

Об'єднані розвідка, спостереження та рекогносцировка (JISR) – це синхронізація та інтеграція можливостей та заходів операцій та розвідки, спрямовані на надання своєчасної інформації для підтримки прийняття рішень. «Процес циклу JISR» – це комбінована функція розвідки та операцій, що вимагає широкої координації та співпраці між співтовариством на багатьох рівнях. JISR НАТО інтегрує можливості Альянсу та національних систем розвідки, спостереження та рекогносцировки (ISR), політику, процедури та системи для надання інформаційної підтримки лідерам, командирам та особам, які приймають рішення, від політичних і стратегічних сфер до тактичного рівня включно.

JISR-процес виконується в п'ять послідовних кроків: вимоги (task), збір (collect), обробка (process), використання (exploit) і поширення (disseminate), які мають абревіатуру TCPED [8].

На JISR-процес покладається місія забезпечити командира всіма специфічними даними, інформацією і ситуаційною обізнаністю, що стосується збору інформації в процесі проведення операції. Така архітектура процесу дає змогу інтегрувати наявні розвідувальні спроможності в загальну схему маневру операції. Розвідка є лише частиною операції, а пріоритети операції в цілому, місце та діяльність розвідки в підтримці операції визначає командир. Надання "**вимог"** (tasking) є першим кроком JISR-процесу, який полягає в чітких вимогах до збору у вигляді інструкцій і наказів для координації та контролю JISR-засобів. На цьому кроці задіються функції персоналу штабу з управління вимогами до розвідки (IRM) та

визначають оптимальні джерела розвідки з огляду на операційну необхідність, ризики застосування, обмежену наявність інструментів. Малоймовірно, що особовий склад розвідки колись матиме достатню кількість людей або ресурсів, аби задовольнити всім запитам. Ведення розвідки має бути заздалегідь сплановано й організовано настільки надійно, наскільки це можливо в межах наявних обмежень. Для її успішного ведення мають бути визначені пріоритети процесу розвідки, враховуючи, що вимоги не завжди відповідають наявним спроможностям. Третій крок – "**обробка**" (process) полягає в конвертації зібраних даних у встановлені, зручні формати, які дозволяють візуалізацію, подальше використання, зберігання і поширення оброблених даних. Головною вимогою виконання цього кроку є побудова єдиної інформаційної мережі, завдяки якій добиваються ефекту синергії, коли ефективність від сумісної дії об'єднаних у мережу сил за сукупним результатом перевищує сумарну ефективність від застосування тих же сил та засобів окремо. Поширення оброблених даних в єдиній мережі є важливим для обробки даних з інших джерел розвідки, які в цей же час задіяні в цій або суміжній зоні відповідальності. Горизонтальні зв'язки сприяють поширенню розуміння, що є істотним для оптимізації застосування різних джерел розвідки. Кожне джерело у співпраці з іншими може відкоригувати власний збір даних і поліпшити якість інформації в результаті їх обробки. П'ятий крок JISR-процесу – "**поширення**" (dissemination) включає своєчасне постачання JISR-результатів авторизованим запитувачам в необхідному форматі обумовленими каналами комунікації [9]. Важливо, щоб поширювана ситуаційна обізнаність була стислою і наочною для уникнення переобтяження командира.

Інтеграція розвідувального і операційного циклів JISR-процес не підміняє розвідувальний цикл, скоріше він є частиною процесу інтеграції розвідки в операції. Через синхронізацію та інтеграцію розвідувальних і операційних процесів командири та їх штаби мають змогу визначати пріоритети, надавати вимоги та розподіляти наявні засоби в кожній конкретній операції. JISR в рамках Агентства зв'язку та інформації НАТО (NCI).

У структурі Агентства NCI **Об'єднана служба розвідки, спостереження та рекогносцировки** (JISR SL, Joint Intelligence, Surveillance and Reconnaissance Service Line) є під елементом Директората прикладних служб (DAS, Directorate of Application Services). В даний час в JISR SL налічується близько 80 співробітників у трьох різних місцях Агентства – Брюсселі, Монсі (Бельгія) та Гаазі (Нідерланди). Програма JISR SL спрямована на постійну підтримку необхідності своєчасно збирати, обробляти, використовувати та поширювати дані та інформацію тим, хто повинен знати. JISR SL несе відповідальність перед своїми клієнтами за планування, координацію та проведення заходів по повному управлінню життєвим циклом на підтримку циклу JISR та пов'язаних з ними послуг, включаючи: стратегію, політику, доктрину та концепції; стандартизацію та сумісність; аналіз вимог Концепції розробки та експериментування (CD&E, Concept Development and Experimentation; проектування та розробка; процеси, процедури, тактика та методи; придбання, впровадження та інтеграція системи; операції з впровадження та обслуговування (O&M, Transition and Service Operations). Основна увага JISR полягає в тому, щоб забезпечити глобальну сумісність у межах НАТО JISR та з зовнішніми спільнотами за інтересами (COIs,Communities of Interest). JISR SL значно підвищує операційну ефективність та ефективність своїх клієнтів завдяки широкому спектру узгоджених служб JISR, що підтримується добре навченим, високоосвіченим та унікально досвідченим персоналом, у чотирьох ключових сферах СВП: служби розвідувальних програм, служби спостереження та рекогносцировки, електронні війни та датчики, геопросторові служби [4]. Результати розвідувальних операцій, за поглядами командування НАТО, можуть представляти в різного роду звітах. Вони стандартизовані в НАТО і узагальнені в STANAG 2022 Intelligence Reports (Угоди про стандартизацію, Standardization Agreements), який містить перелік усіх доповідей НАТО про розвідку та детальну інформацію про те, де можна знайти формат кожного звіту. Принципи, що застосовуються при оформленні звітів: чіткість, актуальність та стислість [10].

У країнах-членах НАТО використовуються такі стандартні формати звітів та повідомлень розвідувальних даних, щоб гарантувати співпрацю з країнами-партнерами, у всіх

можливих випадках, де письмові повідомлення та інформація веб-розвідки повинні відповідати форматам. Прикладами таких повідомлень є: розвідувальні повідомлення (INTREP), підсумкові розвідувальні звіти (INTSUM), додаткова доповідь з розвідки (SUPINTREP), тематичні звіти (Thematic Reports) [11].

Intelligence Report (INTREP) – розвідувальний звіт. INTREP – це стандартизований звіт, який, виходячи зі своєї важливості, поширюється без урахування конкретного графіку. Він готується у всіх ешелонах, коли спостерігаються факти, що впливають на можливості противника, або коли відбулася зміна можливостей противника. Він передається вищим, нижчим та сусіднім підрозділам на розсуд командира, який складає звіт. Він надсилається спонтанно, без урахування конкретного графіку часу, якомога швидше після отримання інформації, яка вимагає невідкладної уваги командира. Кожен раз, коли дозволяє час, INTREP включає в себе тлумачення інформації про яку повідомляється, розвідувальним органом, що створює джерело інформації. Перше слово звіту - INTREP. Для цього звіту не передбачений будь-який формат, але він повинен відповідати узгодженим стандартам НАТО. Він може бути надісланий у вигляді вільного тексту зі структурованим заголовком та колонтитулом у відповідності до формату, визначеного в Директиві звітування про Bi-MNC (Посібник з бойової інформації багатонаціональних сил, Battlefield Information **– M**ulti **N**ational **C**orps), або у вигляді форматованого повідомлення, що відповідає правилам ADatP-3 (основний стандарт НАТО для публікації даних який визначає правила побудови повідомлень, Allied Data Publication). З метою спрощення процесу були розроблені подальші повідомлення, які містять конкретні структуровані дані, що стосуються питань морської, сухопутної чи повітряної діяльності, які складають основу MARINTREP, LANDINTREP або AIRINTREP [12].

Intelligence Summary (INTSUM) - підсумковий розвідувальний звіт INTSUM - це стислий, періодичний підсумок розвідки про поточну ситуацію противника в зоні відповідальності командира, розроблений для оновлення розвідувальної інформації та для висвітлення важливих подій протягом звітного періоду. Тому він повинен містити будь-яку інформацію, яка відповідає вимогам розвідки будь-якого командира, до штабу якого він розповсюджується, і повинен містити висновки, засновані на оцінці та інтерпретації цієї інформації. Поширення INTSUM повинно включати всіх тих, чиї обов'язки та інтереси можуть впливати на зміст звіту. Формат INTSUM повинен відповідати узгодженим стандартам НАТО. Він може бути надісланий як вільний текст із заголовком та колонтитулом у форматі, визначеному в Директиві звітування про Bi-MNC, або у вигляді відформатованого повідомлення, що дотримується правил ADatP-3. Supplementary Intelligence Report (SUPINTREP) - додатковий звіт про розвідку. Цей звіт може час від часу формуватися, за спеціальним запитом або під час підготовки до спеціальної операції. Він призначений для надання детальних оглядів та аналізу всіх даних розвідувальної інформації про один або кілька конкретних об'єктів, які були зібрані протягом певного часу. Поширення SUPINTREP регулюється його змістом. Для цього звіту не існує узгодженого формату НАТО, за винятком вимоги, що слово «SUPINTREP» повинно з'являтися на початку кожного звіту. Директива про звітність Bi-MNC містить формат звіту про вільний текст із заголовком та колонтитулом [13].

Electronic Data Dissemination - електронне поширення даних. Все частіше розвідувальна інформація поширюється в електронному вигляді. Це знімає вимогу до створення письмових або відформатованих повідомлень і має перевагу в тому, що дозволяє отримувати розвідку передбачуваним реципієнтом майже в реальному часі.

Сьогодні НАТО перебуває у найбільш складній і непрогнозованій ситуації в аспекті безпеки з часів холодної війни – більш зухвала Росія, кібер і гібридні загрози, криза і нестабільність на Близькому Сході і у Північній Африці, продовження існування терористичної загрози. У відповідь на це динамічне середовище загроз члени Альянсу фундаментально адаптують підходи НАТО до забезпечення розвідувальної діяльності на допомогу керівництву у прийнятті рішень.

Найбільш значна реформа відбулась у 2017 році, коли Альянс створив у штаб-квартирі НАТО новий Об'єднаний відділ розвідки і безпеки (JISD). Моїм завданням, як першого

помічника Генерального секретаря відповідального за цей Відділ, було виробити бачення, створити професійні кадри і започаткувати широкомасштабні реформи з поліпшення якості і корисності розвідувальної інформації, яка надається вищому політичному і військовому керівництву НАТО. Ця робота передбачала тісну співпрацю з іншими керівниками розвідувальних служб НАТО, особливо з SHAPE J2 (розвідувальне управління в штабі Верховного головнокомандувача Об'єднаних збройних сил НАТО в Європі, або Командування ОЗС НАТО з питань операцій). Один з нових засобів НАТО, система Спостереження Альянсу за поверхнею, яка складається з повітряних, наземних і допоміжних елементів – забезпечить всепогодне, постійне спостереження за великими територіями на суші і на морі в режимі часу, наближеному до реального, що покращить ознайомлення із ситуацією на театрі. Фото Northrop Grumman [14].

Основна мета полягала в тому, щоб зробити розвідувальну інформацію якомога більш корисною для наших клієнтів. Наша розвідувальна інформація мала бути високоякісною, зосередженою на пріоритетах керівництва, і надана в потрібний час тим, кому вона необхідна. Генеральний секретар постійно наголошує, що діяльність розвідки повинна забезпечувати краще ознайомлення з обстановкою і інформацію, потрібну для прийняття політичних рішень. Задля цього необхідно було максимально наблизити оцінку інформації до Північноатлантичної ради, Військового комітету і вищого керівництва Альянсу. Створення JISD також стало першим прикладом створення в штаб-квартирі спільного Цивільно-військового відділу НАТО [8]. Об'єднати раніше відокремлені цивільні і військові штаби розвідників було нелегким завданням. В той час дехто побоювався зіткнення професійних культур і підходів до розвідки. Насправді, це було зовсім не так. Об'єднання окремих розвідувальних підрозділів дозволило нам здійснювати цілісну оцінку розвідданих, посилити нашу ефективність, уникнути дублювання зусиль і спиратись на сильні сторони як цивільної, так і військової організації, розвиваючи при цьому нову культуру співробітництва. Більше того, це дозволило JISD результативно протистояти гібридним, кібер і терористичним загрозам, які дедалі частіше постають перед країнами - членами альянсу НАТО, посиливши нашу спроможність аналізувати ці питання універсального характеру. Задля забезпечення JISD здатності допомагати при підготовці ґрунту для прийняття рішень в Альянсі, ми постаралися краще узгодити сфери нашої уваги і часові рамки з планами керівництва, засіданнями і місіями. Справжня сила розвідки Альянсу полягає в тому, що вона забезпечує спільні інформаційні рамки для прийняття рішень, чим підсилює солідарність в Альянсі. Хоча це здається не простою справою, мій досвід вказує на те, що насправді фундаментальних розбіжностей набагато менше, ніж можна було б очікувати. Справді, деякі дуже важливі рішення Північноатлантичної ради могли бути прийняті лише на основі розвідувальної інформації, яка була доступна для усіх членів Альянсу. Це стосується відповіді НАТО на порушення Росією Договору про ядерні сили середньої дальності, а також вислання країнами-членами Альянсу понад 150 російських шпигунів після спроби Москви убити колишнього російського агента Сергія Скрипаля за допомогою нервово-паралітичної речовини у Сполученому Королівстві в березні 2018 року (британська громадянка Дон Стерджесс пізніше померла після контакту з цією речовиною). Ми також доповнювали довгострокові стратегічні оцінки більш актуальною інформацією про обстановку [8]. На основі глибоких знань і досвіду наших аналітиків ми можемо здійснювати швидку попередню оцінку для наших клієнтів. Нові внутрішні формати обміну розвідданими в штаб-квартирі НАТО, такі як засідання відповідних зацікавлених сторін на високому рівні, радикально збільшили частотність і відповідність розвідувальної інформації, яку отримує вище керівництво. Ніколи до цього розвідувальна інформація не була більш актуальною і релевантною для прийняття рішень в НАТО. Як стратегічний лідер в сфері розвідки, я повинен не обмежуватись баченням лише JISD. «Розвідувальне підприємство НАТО» виходить далеко поза межі штаб-квартири НАТО і зв'язане з численними критично важливими функціями в обох Стратегічних командуваннях. Через те, що ці функції розмножувались «органічно», без спільного загального плану, має місце проблема загальної цілісності. Члени Альянсу погодились з тим, що спільний підхід

покращив би обмін розвідданими, координацію продуктів, посилив би можливості виявлення і попередження, і поліпшив би менеджмент і управління [9]. У тісній співпраці з Командуванням ОЗС НАТО з питань операцій (АСО) і Командуванням ОЗС НАТО з питань трансформації (АСТ) ми розпочали спільно визначати і впроваджувати ряд основних проектів з реформування. З роками ми напрацювали робочі відносини довіри між інституціями. Зокрема, тісне партнерство з АСО забезпечило значні досягнення щодо попередження і настороженості, де ми доклали особливих зусиль до створення більш ефективної архітектури, поліпшивши цілісність механізмів і усунувши недоліки. Нова система краще пристосована до нинішніх комплексних загроз і ми зараз працюємо з членами Альянсу над тим, щоб вона діяла належним чином у разі реальної кризи [10]. Двотижневі випробування «Юніфайд віжн» 18 відбулись у червні 2018 року на територіях НАТО в Європі і Північній Америці задля перевірки оперативної сумісності багатонаціональних і колективних Об'єднаних сил і засобів розвідки, спостереження і виявлення. Виробництво продукту зараз регулярно координується між штаб-квартирою і Стратегічними командуваннями. Знову-таки, ми усуваємо дублювання, спрямовуємо наші зусилля на забезпечення наших лідерів більш цілісною розвідувальною картиною. Поза лаштунками, ряд функцій має важливе значення для менеджменту, обміну і обробки розвідданих. Лише після того, як менеджмент технічних функцій буде цілковито оптимізований і забезпечений належними кадрами, розвідка НАТО досягне свого повного потенціалу. Задля запобігання витоку інформації і використанню наших слабких місць нашими супротивниками, члени Альянсу не можуть обійтись без безпеки. Безпека сприяє довірі, а довіра сприяє обміну розвідданими. Було дуже розумно включити Офіс безпеки НАТО (NOS) до Об'єднаного відділу. Об'єднання функцій розвідки і безпеки під одним дахом забезпечує щоденну взаємодію між ними. Серед багатьох інших важливих функцій NOS нині займається ретельним спостереженням, перевірками на допуск і бере участь в усіх реформах розвідки. Для максимального використання нашого потенціалу ми розширюємо наші засоби і можливості. Додаткова інформація, отримана з відкритих джерел, буде використовуватись на підтримку ретельного і вчасного аналізу [11]. Ми нині підсилюємо наші наявні можливості і засоби для пошуку у величезних масивах даних в мережі Інтернет. Для того щоб грати на випередження, до цього необхідно додати підтримку з боку передових методів аналізу і штучного інтелекту. Ще один новий засіб, система Спостереження Альянсу за поверхнею, яка складається з безпілотних літальних апаратів, наземних і допоміжних елементів, забезпечить всепогодне, постійне спостереження за великими територіями на суші і на морі в режимі часу, наближеному до реального, що покращить ознайомлення з ситуацією на театрі. Задля удосконалення обміну і оброблення розвідданих в НАТО ми також фундаментально переглядаємо технічну базу і оперативну сумісність систем ІТ і управління даними. За майже три роки після створення цього Відділу цивільно-військова співпраця в галузі розвідки в НАТО стала стандартною практикою. Ми прямуємо в напрямі спільної культури праці, а оцінювання стають більш цілісними і виконуються швидше. Попит на високоякісні розвіддані як ніколи високий, і вони відіграють дедалі більшу роль у виробленні політики і прийнятті рішень. Проте ще не всі завдання розв'язані. Реформи необхідно поглиблювати. Усе ще має місце різниця в культурі. Військові, які зосереджені на плануванні і операціях, як правило більше схильні до підходу за принципом «потрібно ділитись». Деякі цивільні розвідувальні організації дотримуються набагато більш стриманого підходу до своєї інформації, наголошуючи на принципі «потрібно знати». Такі глибоко укорінені традиції важко подолати. Загрози безпеці важко вловити. Альянсу необхідно постійно бути в курсі нових подій і стежити за ними з відповідною швидкістю. І Росія, і Китай роблять великі інвестиції в свої звичайні збройні сили, розробляючи і демонструючи при цьому нові передові ядерні озброєння і ракетні системи. Обидві країни активно працюють над новими і проривними технологіями, що може мати далекосяжні наслідки для членів Альянсу. Гібридні і кіберзагрози вже стали новою нормою. Інші країни і недержавні гравці також розвивають нові сили і засоби. Тому наступними роками важливість розвідки в НАТО буде лише зростати [12]. На початку 2017 року НАТО створила новий підрозділ – «Об'єднаний відділ розвідки і безпеки» (JISD).

Це найбільш значна реформа в історії розвідки Альянсу. У відповідь на зміну загроз, викликану зухвалою поведінкою Росії і зростанням тероризму і нестабільності на сході, члени Альянсу фундаментально переглядають підходи НАТО до організації і аналізу розвідувальної діяльності та інформації. У нинішньому глобалізованому, гіперзв'язаному, багатополярному світі НАТО необхідно водночас відстежувати і оцінювати численні і різноманітні загрози: звичайні військові, розповсюдження зброї масового знищення, засоби гібридної війни, комп'ютерні атаки і міжнародний тероризм – це лише декілька найскладніших. У географічному сенсі НАТО почала дивитись більш широко, від центральної Африки до Північної Кореї і від Арктики до Близького Сходу. Забезпечення необхідними розвідданими повинно відповідати надшвидким темпам змін [13]. Більше того, межа між цивільним і військовим, між війною і миром дедалі більше розмивається. Це також робить необхідною кращу інтеграцію цивільної і військової розвідки в НАТО в єдину ефективну структуру, здатну забезпечити Північноатлантичну раду і Військовий комітет НАТО цілісною розвідувальною картиною. Ці міркування підштовхнули лідерів Альянсу до початку фундаментальної реформи розвідки НАТО на саміті у Варшаві в липні 2016 року. Ключовим елементом цієї реформи стало створення нового підрозділу в штаб-квартирі НАТО, який складається з двох частин: розвідки (з об'єднаними напрямами цивільної і військової розвідки) і безпеки (Офіс безпеки НАТО). Роль НАТО в протидії тероризму розширюється і Альянсу потрібно глибше розбиратись в обстановці в цій сфері [14]. Розвідка повинна не відставати від розвитку політичних і військових пріоритетів. Регіональна увага НАТО розширюється і перед Альянсом постають посилені загрози, які продукує гібридна сфера, кіберпростір і тероризм. Розвідка повинна більше уваги зосереджувати на цих транснаціональних питаннях і розвивати для цього необхідні сили і засоби. Загроза гібридної війни зараз займає таке високе місце, що міністри оборони країн Альянсу поставили перед нами завдання створити спеціальний підрозділ в штаб-квартирі НАТО для системного вивчення цього питання. Нова секція гібридного аналізу була створена в JISD в липні 2017 року. Вона відповідає за аналіз усього спектра гібридних дій, на основі цивільних і військових, закритих і відкритих джерел. Це як з'єднувати між собою лініями крапки, відображення потреби у цілісній картині. Дедалі більш важливу роль в цьому відіграватиме комп'ютерна безпека. Так само, із розширенням ролі НАТО в протидії тероризму, Альянсу потрібне більш глибоке знання обстановки в цій сфері. Для цього ми створили нову Групу розвідки з питань тероризму, яка зосередиться на забезпеченні стратегічної розвідувальної інформації з усього світу. Секція безпеки цього відділу також приділяє велику увагу тероризму. Офіс безпеки НАТО продовжує забезпечувати безпеку штаб-квартири НАТО і персоналу НАТО, залученого до виконання місій. Він також розробляє стандарти безпеки задля захисту закритої інформації і систем, і забезпечення виконання цих вимог установами НАТО, країнами - членами НАТО і країнами-партнерами. Його включення в склад нового відділу надає додаткові можливості досягнення більшої синергії в нашій роботі, особливо між розвідкою і контррозвідкою. Створений у 2006 році Центр узагальнення розвідувальної інформації НАТО (NIFC) – це організація під військовим управлінням, що спонсорується США, заснована Військовим комітетом НАТО на основі Меморандуму про розуміння між 26 із 29 країн - членів НАТО і однією країною-партнером. Центр сприяє обміну і узагальненню розвідувальної інформації, допомагає заповнювати білі плями в розвідданих і підтримує планування і виконання поточних операцій. Це один із елементів надзвичайно складної мережі дійових осіб і структур, з яких складається розвідка НАТО [15].

Дивлячись уперед, ми повинні розширювати наш фокус уваги і розглядати розвідувальну діяльність НАТО загалом. Лише частка професіоналів-розвідників НАТО працюють саме у JISD; більшість з них розкидана по усій Командній структурі НАТО. Надзвичайно складна мережа дійових осіб і структур також охоплює Центр узагальнення розвідувальної інформації НАТО в Моулсворті у Великій Британії, Центри передового досвіду в різних сферах, і низку комітетів (військових, цивільних, з питань безпеки), що представляють національні розвідслужби. Нинішній ландшафт розвідки НАТО «органічно»

розвивався роками без якогось спільного генерального плану. Хоча ця спадщина є багатим ресурсом, спільне планування і координація усієї діяльності залишається складним завданням. Розвідувальну діяльність НАТО можна зробити більш ефективною і цілісною в різні способи – синхронізуючи зусилля, усуваючи дублювання і повністю оптимізуючи ресурси. Альянс повинен стимулювати спільну діяльність із стратегічного планування на майбутнє і визначати пріоритети для діяльності загалом. «Єдина НАТО» має бути нашим керівним принципом. Рухаючись цим шляхом ми збережемо наш ентузіазм і позитивну динаміку [16].

**Висновки**. Таким чином, одним із пріоритетних напрямів удосконалення аналітичної розвідки є створення ефективної системи розвідки Збройних Сил України відповідно до стандартів НАТО. Цілями подальшого розвитку та ефективної роболти системи воєнної розвідки є**:** посилення спроможності органів військового управління розвідки та військових частин розвідки ЗС України для здобування розвідувальної інформації; проведення спеціальних заходів в інтересах застосування ЗС України та інших складових сил оборони.

**Напрямок подальших досліджень.** Відмічено, що пріоритетними завданнями подальших досліджень повинні бути заплановані наступні**:** забезпечення підготовки особового складу органів аналітичної розвідки та військових частин розвідки ЗС України до виконання завдань за стандартами НАТО; забезпечення розвитку спроможності щодо здобування розвідувальних відомостей в інтересах застосування ЗС України та інших складових сил оборони з урахуванням принципів і стандартів НАТО; автоматизація процеси збору і обробки розвідувальної інформації та створення АСУ розвідки з урахуванням принципів і стандартів НАТО; забезпечення органів воєнної розвідки достатніми матеріально-технічними засобами технічної розвідки з урахуванням принципів і стандартів НАТО; розвиток та придбання новітніх високотехнологічних засобів розвідки, в тому числі космічної та геопросторової розвідки;упровадження захищених каналів передачі інформації [16]. На сьогодні вже проведено роботу із зазначених напрямків, а саме:щодо переведення на нові штати розвідувальних рот бригад; практично завершено переведення на нові штати розвідувальних батальйонів; триває перехід на уніфіковані організаційно-штатні структури органів управління, решти частин та підрозділів розвідки ЗС України; просувається робота щодо формування розвідувального органу ГШ ЗС України (Головне управління розвідувального забезпечення).

ЛІТЕРАТУРА:

1. https:// bintel.org.ua/nukma/rozviduvalnij-proces-nato/

2. Настанова з тактичної розвідки/ Командування СВ ЗС України. – Київ : МОУ, 2017. – 127 с.

3. Тактична розвідка в бойових прикладах за досвідом проведення АТО : посібник. – Київ : МОУ ГУР, 2017. – 160 с.

4. Тактика в бойових прикладах (з досвіду антитерористичної операції): навч.-метод. посіб./колектив авторів; за заг. ред. А. М. Сиротенка. – К. : НУОУ ім. І. Черняховського, 2017. – 140 с.

5. https://www.nato.int/docu/review

6. Військовий стандарт 01.101.001. Видання 2. Воєнна розвідка. Терміни та визначення. – К. : Міністерство оборони України, 2011. – 24 с.

7. Військовий стандарт 01.101.004. Видання 2. Воєнна розвідка. Розвідувально-інформаційна діяльність. Терміни та визначення. – К. : Міністерство оборони України, 2015. – 26 с.

8. Левченко О. В. Методика оцінки противника у бою : навчальний посібник/ О. В. Левченко. – К. : НАОУ, 2001. – 76 с.

9. https://www.nato.int/docu/review

10. Методичні рекомендації з розробки розвідувальних оцінок (за стандартами провідних країн-членів НАТО). – К. : ГУР МО України, 2018. – 118 с.

11. Варенко В. М. Інформаційно-аналітична діяльність : навчальний посібник. – К. : Університет “Україна”, 2014. – 417 с.

12. Захарова І. В. Основи інформаційно-аналітичної діяльності : навчальний посібник. – К. : “Видавництво “Центр учбової літератури”, 2013. – 336 с.

13. Процеси розвідувальної діяльності. Стандарт НАТО. Союзницька об’єднана настанова AJP–2.1 (видання B, варіант 1)/ Управління стандартизації НАТО, 2016. – 80 с.

14. Основи розвідувально-інформаційної діяльності: настанова Штабу розвідки Міністерства оборони Великобританії. – К. : ГУР МО України, 2015. – 51 с.

15. https://defpol.org.ua/index.php/produkty-tsentru/49-shliakh-ukrainy-do-nato/1084

REFERENCES:

1. https://bintel.org.ua/nukma/rozviduvalnij-proces-nato/

2. Instruction on tactical intelligence/Command of the Defense Forces of the Armed Forces of Ukraine. - Kyiv: MOU, 2017. - 127 p.

3. Tactical intelligence in combat examples based on the experience of anti-terrorist operation: manual. – Kyiv: MOU HUR, 2017. – 160 p.

4. Tactics in combat examples (from the experience of an anti-terrorist operation): teaching method. manual/team of authors; in general ed. A. M. Syrotenko. - K.: NUOU named after I. Chernyakhovsky, 2017. – 140 p.

5. https://www.nato.int/docu/review

6. Military standard 01.101.001. Edition 2. Military intelligence. Terms and definitions. - K.: Ministry of Defense of Ukraine, 2011. - 24 p.

7. Military standard 01.101.004. Edition 2. Military intelligence. Intelligence and information activities. Terms and definitions. - K.: Ministry of Defense of Ukraine, 2015. - 26 p.

8. Levchenko, O.V. Methodology for assessing the enemy in battle: study guide/ O.V. Levchenko. - K.: NAOU, 2001. - 76 p.

9. https://www.nato.int/docu/review

10. Methodological recommendations for the development of intelligence assessments (according to the standards of leading NATO member countries). - K.: GUR Ministry of Defense of Ukraine, 2018. - 118 p.

11. Varenko V. M. Information and analytical activity: study guide. - K.: "Ukraine" University, 2014. - 417 p.

12. Zakharova I. V. Fundamentals of information and analytical activity: a study guide. - K.: "Centre of Educational Literature" Publishing House, 2013. - 336 p.

13. Intelligence activity processes. NATO standard. Allied Joint Instruction AJP–2.1 (edition B, version 1)/ NATO Standardization Office, 2016. – 80 p.

14. Basics of intelligence and information activities: instruction of the Intelligence Staff of the Ministry of Defense of Great Britain. - K.: GUR Ministry of Defense of Ukraine, 2015. - 51 p.

15. https:// defpol.org.ua/index.php/produkty-tsentru/49-shliakh-ukrainy-do-nato/1084

**PhD Maksimenko Yu.A.,**
**PhD Mamich V.V.,**
**Doctor of Science from public administration, Popov S.A.,**
**Sharshatkin D.Yu.**

# ANALYSIS OF THE FUNCTIONING OF THE NATO ANALYTICAL INTELLIGENCE SYSTEM

***For the successful conduct of a modern battle, according to the views of modern military scientists, it is necessary, first of all, to know the enemy, his forces, means and nature of actions. In order to provide commanders and staffs of all levels with this data, there is the most important type of combat support for military operations - intelligence. The experience of conducting military operations shows that only where reconnaissance is conducted actively and purposefully, combat tasks are solved successfully and with the least losses. On the contrary, poorly organized intelligence has always been the main cause of unsuccessful military operations. Nowadays, the volume of tasks solved by intelligence has grown significantly. Instead, the terms of their implementation were significantly reduced. The requirements for the time of data transmission and the accuracy of determining the coordinates of enemy objects (targets) have increased. Analytical intelligence is a component of intelligence activity, consisting of detection, assessment, forecasting of various social processes, events, activities based on information, mainly obtained from open sources, as well as obtained by intelligence of other types (agency, technical, etc.). Analytical intelligence is divided into operational (which serves current needs) and strategic (which forms stable insights). Proactively investigates short-term phenomena (occurring, recent or soon expected) to ensure appropriate immediate action. Strategic reveals what is extremely unobvious, does not come soon, changes slowly, requires long-term, large-scale measures. Aspects of analytical intelligence: collection and comparison of various information in order to identify trends, contradictions, misinformation, misinterpretation, manipulative measures, implicit events, hidden activities, as well as the formation of general ideas about various significant subjects and phenomena; assessment of subjects, events, actions, intentions; forecasting events, actions, intentions; planning of activities, events. Information provision of specific open and secret operations; participation in the development of strategies for ensuring national security, national development, and global development. Wide implementation of modern information technologies has become an urgent issue today, according to scientists, it is an absolute requirement of modern warfare.***

***Keywords: analytical intelligence, social processes, information provision, interpretation, manipulation, phenomena, general ideas, component, strategic intelligence.***

УДК 355:001.89 (477) **Мацьовитий В. Л.** (ЦВСД НУОУ)

DOI: https://doi.org/10.17721/2519-481X/2022/77-07

# РОЗВИТОК ІНТЕГРОВАНОЇ СИСТЕМИ НАУКОВОЇ І НАУКОВО-ТЕХНІЧНОЇ ДІЯЛЬНОСТІ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

***У статті розглянуто особливості функціонування систем наукової та науково-технічної діяльності наукових установ Міністерства оборони України в контексті європейського досвіду держав-членів НАТО (далі – NINTD), перспективи законодавчої та нормативно-правової бази щодо Коротко викладено організацію військових досліджень:***

***бачення наукових установ Міністерства оборони України та Командування Об'єднаних сил щодо основних питань організації НІНТД, використання різних моделей організації та проведення досліджень у військовій науці, контролю якості наукової продукції, її комплексної оцінки та ступеня секретність наукової інформації;***

***деякі аспекти особливостей функціонування систем управління суб'єктами НІНТД, основні принципи та підходи до створення та розвитку національних наукових систем у сфері військової науки. Аналіз основних особливостей функціонування систем наукової та науково-технічної діяльності наукових установ Міністерства оборони України в контексті європейського досвіду держав-членів НАТО.***

***У статті використано систему загальнонаукових та спеціальних методів теоретичного та емпіричного дослідження: аналіз наукових публікацій, представлених у зарубіжній періодиці, та відкритих матеріалів з досліджуваної проблематики в мережі Інтернет, систематизація наукових джерел, узагальнення та системний підхід.***

***Аналіз існуючої системи наукових установ Збройних Сил України переконливо свідчить про наявність низки проблемних організаційно-технічних питань та функціонування системи наукової та науково-технічної діяльності Збройних Сил України, які суттєво знизити його ефективність. Насамперед це пов'язано з недосконалістю нормативно-правової бази, організаційно-штатної структури наукових підрозділів, системи їх комплексного забезпечення. Крім того, вжиті заходи системою керівництва Збройних Сил України та управління військами (силами) призвели до необхідності вдосконалення вертикалі управління науковими установами Збройних Сил України. В таких умовах виникає необхідність розробки обґрунтованих рекомендацій щодо підвищення ефективності діючої системи наукових установ Збройних Сил України на основі відповідного науково-методичного апарату.***

***Ключові слова: Збройні Сили; наукові дослідження; модель організації воєнно-наукових досліджень; організація наукової і науково-технічної діяльності; система воєнно-наукових досліджень.***

**Вступ.** В умовах сучасних загроз з урахуванням продовження реалізації Російською Федерацією стратегії ведення бойових дій в нових формах, особливої уваги потребує питання оцінювання ефективності функціонування існуючої системи наукових установ Збройних Сил України. Актуальність даного питання обумовлене необхідністю забезпечення органів військового управління військ (сил) результатами наукових досліджень, які дозволяють прийняти обґрунтовані рішення щодо:

- подальшого розвитку Збройних Сил України;
- удосконалення форм і способів застосування військ (сил);
- створення дієвої системи їх підготовки та всебічного забезпечення;
- приведення організаційно-штатних структур та чисельності у відповідність до визначених функцій та завдань;
- забезпечення необхідного рівня укомплектованості наукових установ фахівцями вищої кваліфікації;
- прийняття на озброєння нових (модернізованих) зразків озброєння та військової техніки.

**Аналіз останніх досліджень і публікацій**. На сьогоднішній день на шляху України до

Європейського наукового простору та необхідності приведення вітчизняної законодавчої бази щодо воєнної науки у відповідність до прийнятих міжнародних стандартів, а також до умов, що склалися на цей час в Україні, а саме до нових викликів, пов'язаних з війною розв'язаною Російською Федерацією проти України (введенням воєнного стану в державі), особливої уваги потребують питання подальшого удосконалення існуючої наукової системи (моделі) організації наукової і науково-технічної діяльності в системі Міністерства оборони України з урахуванням принципів та підходів держав-членів і партнерів НАТО (далі – НІНТД).

Існуюча модель організації НІНТД в системі Міністерства оборони України є абстрактною, яка по собі виявляє причинно-наслідкові взаємозв'язки між системою управління, наукових установ та консультативно-дорадчих органів в процесі їх функціонування в рамках загальної системи НІНТД. Головною метою побудови даної моделі є вироблення політики Міністерства оборони України у сфері НІНТД та розв'язання проблем щодо узгодженості рішень з найбільш важливих питань розвитку воєнної науки та пріоритетних завдань і перспектив розвитку Збройних Сил України, тощо. Загалом, по своїй суті, зазначений процес являється формальним описом об'єкта моделювання – сучасної системи НІНТД Міністерства оборони України, який по собі відображає напрями, тобто наші погляди на існуючі у цій сфері проблемні питання (суттєві недоліки) та наше бачення щодо можливих шляхів їх вирішення.

Тому питання напрямків удосконалення існуючої моделі організації НІНТД в системі Міністерства оборони України мають розглядатися через призму системного аналізу складових сучасної системи НІНТД (системи управління, наукових установ та консультативно-дорадчих органів), аналізу причинно-наслідкових зв'язків між ними тощо. Основним завданням у цьому аспекті є винайдення оптимальних підходів:

до питань щодо напрямків удосконалення існуючої моделі організації НІНТД в системі Міністерства оборони України з урахуванням принципів та підходів держав-членів і партнерів НАТО, а також запозичення їх передового досвіду щодо питань організації наукових досліджень у сфері оборони держави;

до питань щодо структури удосконаленої моделі організації НІНТД, автоматизації впровадження результатів моделювання за рахунок цифровізації процесів розв'язання завдань воєнної науки, поєднання логіки та поглядів на проблеми, що розв'язуються в Міністерстві оборони та Генеральному штабі Збройних Сил України;

до питань щодо шляхів удосконалення нормативно-правового забезпечення організації НІНТД в системі Міністерства оборони України та визначення основних нормативно-правових документів для внесення змін і доповнень.

У першу чергу, це сприятиме розробленню проєкту удосконаленої системи (моделі) організації НІНТД в системі Міністерства оборони України з урахуванням принципів та підходів держав-членів і партнерів НАТО, а також пропозицій щодо внесення змін та доповнень в існуючу нормативно-правову базу з питань організації ННТД в системі Міністерства оборони України [1-4].

Разом з тим, розглядаючи проблематику внесення змін та доповнень до нормативно-правових документів з питань НІНТД в системі Міністерства оборони України, необхідно зазначити, що на сьогодні ключовим стало переопрацювання питань щодо планування НІНТД, врахування при цьому заходів оборонної реформи, передбачених Стратегічним оборонним бюлетенем України та Державною цільовою оборонною програмою розвитку Збройних Сил України до 2026 року, Державною цільовою програмою розвитку озброєння та військової техніки на період до 2026 року [2,6]. Також визначено, що основним нормативним документом для внесення змін та доповнень, має стати Положення про організацію наукової і науково-технічної діяльності в системі Міністерства оборони України, затвердженого наказом Міністерства оборони України від 27.07.2016 року № 385 і зареєстрованого в Міністерстві юстиції України 22.08.2016 року за №1172/29302 (із змінами і доповненнями, внесеними наказами Міністерства оборони України від 11.12.2019 року № 635, від 31.08.2020 року № 306) – саме його розділ щодо організації планування НІНТД в системі Міністерства оборони

України і лише в контексті щодо зміни у підходах до нього, структуризації та розширення (уточнення за потреби окремих питань) та доповнення окремими пунктами щодо сумісності процесів планування з оборонним плануванням в Міноборони і Збройних Силах України на основі спроможностей та підходів до організації НІНТД в державах-членах і партнерах НАТО [5] .

Таким чином, актуальним є вирішення питання розвитку інтегрованої системи ННТІД у ЗС України для забезпечення наукового супроводження формування та реалізації заходів державної політики у воєнній сфері, підвищення спроможностей Збройних Сил України для захисту територіальної цілісності і недоторканості України, ведення всеохоплюючої оборони та вирішення актуальних потреб підготовки, забезпечення та застосування військ (сил) Збройних Сил України.

**Метою статті** є аналіз основних особливостей функціонування систем наукової і науково-технічної діяльності наукових установ Збройних Сил України в контексті європейського досвіду держав-членів НАТО для розв'язання визначених завдань роботи, а саме: проведення аналізу існуючої моделі організації НІНТД в системі Міністерства оборони України, обґрунтувати напрями удосконалення моделі організації НІНТД в системі Міністерства оборони України з урахуванням принципів та підходів держав-членів і партнерів НАТО та розроблення пропозицій щодо внесення змін та доповнень в існуючу нормативно-правову базу з питань організації НІНТД в системі Міністерства оборони України, в процесі дослідження проведення порівняльного аналізу систем наукових досліджень у сфері оборони України та державах-членах і партнерах НАТО.

У статті використано систему загальнонаукових і спеціальних методів теоретичного та емпіричного дослідження: аналіз наукових публікацій викладених у періодичних іноземних виданнях та відкритого матеріалу з досліджуваної проблематики в Інтернеті, систематизація наукових джерел, узагальнення та системний підхід.

**Виклад основного матеріалу**. У загальному комплексі завдань розвитку Збройних Сил України значна увага приділялася підвищенню ефективності та функціонування системи воєнно-наукових досліджень у Збройних Силах України.

Водночас деякі запровадженні останніми роками заходи призвели до негативних наслідків. Останнім часом основні повноваження щодо управління науково і науково-технічною діяльністю перебрало на себе Міністерство оборони України, і це управління інтегроване з управлінням військовою освітою, як наслідок за багатьма напрямками, зв'язок між виробниками воєнно-наукової продукції та її основним споживачем – Збройні Сили України, майже втрачено .

Аналіз свідчить, що впродовж останніх років простежується певне нехтування вітчизняною наукою в тому розумінні, що відповіді на питання будівництва Збройних Сил України дає, насамперед, досвід армій провідних країн світу, але не діяльність вітчизняних наукових установ. Зокрема, на сьогодні моделюванням не охоплюються низка питань щодо оборонного планування в державі, питань стратегії воєнної безпеки та загалом шляхів досягнення цілей державної політики у воєнній сфері, у тому числі і питань щодо державного замовлення на підготовку наукових кадрів вищої кваліфікації для наукових установ та ВВНЗ Збройних Сил України, що являється основним недоліком моделі. Крім того, моделюванням не охоплюються такі важливі питання сьогодення, як урахування принципів та підходів до організації ННТД в державах-членах і партнерах НАТО.

Тому, враховуючи вищевикладене, з метою розв'язання вищезазначених недоліків, постало завдання щодо винайдення обрису удосконаленої системи організації НІНТД в системі Міністерства оборони України, з характерними (притаманними лише їй, як стандартними та специфічними) вимогами.

На сьогодні, до основних стандартних вимог до систем віднесені:

адекватність – тобто, відповідність систем для проведення дослідження (розв'язання) поставлених завдань;

точність в отриманні результатів – відповідність ступеню отриманих результатів (з раніше встановленими та/або бажаними);

універсальність – можливість використання системи для розширення кола завдань дослідження;

доцільна економічність систем – адекватність отриманих результатів дослідження з фінансовими затратами на нього.

До основних специфічних вимог:

спроможність системи щодо найбільш повного розкриття проблематики стосовно організації НІНТД в Міноборони України, на основі як вітчизняного так і зарубіжного досвіду у цій сфері;

структура системи має формуватися із використанням єдиних підходів до організації НІНТД як в системі Міністерства оборони України так і у Збройних Силах України;

стиль і термінологія формулювань, які використаються для опису результатів моделювання, повинні бути зорієнтовані на визначений (затребуваний) кінцевий результат, мають мати одинакове розуміння проблематики щодо наукової діяльності як з боку замовників так і з боку виконавців.;

спроможність отримання та обробки як загальнодоступної наукової інформації так і інформації обмеженого доступу.

співпраці та взаємодії між замовниками і виконавцями досліджень.

Важливою умовою подальшого удосконалення системи наукових установ у воєнно-наукових досліджень є, координація НІНТД між замовниками і виконавцями в оборонній галузі, результативність якої значною мірою залежить від чіткої постановки завдань. Очевидно, що провідна роль тут належить замовникам досліджень.

У перспективі наука має функціонувати в середовищі, яке характеризується конкуренцією виконавців наукових досліджень. Це дозволить впровадити в організацію та планування наукової і науково-технічної діяльності елементів ринкових відносин між замовниками і виконавцями воєнно-наукової продукції дало б змогу досить швидко, протягом певних років, усунути серйозні недоліки існуючої системи наукових досліджень наукових установ і поставити її на вивільнення формалізму.

Система управління науковою і науково-технічною діяльністю у Збройних Силах України є складовою системи управління Збройних Сил України і забезпечує в даний час виконання завдань науковими установами.

Розвиток Збройних Сили потребує проведення досліджень за багатьма напрямками на стратегічному, оперативному і тактичному рівнях за наступними темами, а саме:

з воєнно-політичних проблем – оцінка та прогноз загроз у воєнній сфері, стратегічне оборонне планування розвитку спроможностей Збройних Сил України та інших складових сил оборони, наукове супроводження оцінки, прогнозування та процесів розвитку безпекового середовища довкола України на середньострокову та довгострокову перспективу та інші;

з воєнно-економічних проблем – наукове супроводження заходів формування системи управління ресурсами Міністерства оборони України, Збройних Сил України, інших складових сил оборони в контексті виконання процесів стратегічного оборонного планування на основі спроможностей;

з воєнно-теоретичних проблем – удосконалення системи управління, оптимізації та уніфікації організаційно-штатної структури та чисельності органів військового управління, уточнення повноважень їх керівників відповідно до стандартів НАТО;

з військово-технічних проблем – наукове супроводження заходів Державної цільової оборонної програми розвитку озброєння та військової техніки Збройних Сил;

з воєнно-історичних проблем – узагальнення історичного досвіду минулих війн та сучасних збройних конфліктів, застосування збройних сил держав світу, розвитку засобів, форм і способів ведення збройної [17].

Збереження наявного наукового потенціалу потребує концентрації наукових колективів і кадрів у системі існуючих науково-дослідних установ із врахуванням їхнього наявного і перспективного наукового потенціалу.

Забезпечення незалежного оцінювання спроможностей науково-дослідних установ і підрозділів ВВНЗ може забезпечити незалежний (позавідомчий) науково-організаційний підрозділ урядового підпорядкування (на зразок національного центру досліджень Польщі). Для оцінювання необхідно введення на державному рівні наукометричної методики оцінювання наукової і науково-технічної діяльності, а також створення наукометричної бази і забезпечення відкритого доступу до рейтингу вчених і установ.

Враховуючи те, що у перспективній структурі Збройних Сил України будуть розділені функції підготовки і застосування між Генеральним штабом Збройних Сил України і видами Збройних Сил, при цьому функції підготовки видів будуть покладені на командувачів видів Збройних Сил, доцільно передбачити розвиток системи науково-дослідних установ (підрозділів ВВНЗ), що виконують дослідження за тематиками розвитку виду у підпорядкуванні командувачів видів Збройних Сил.

На стратегічному рівні проводити розвиток науково-дослідних установ за напрямком забезпечення проведення досліджень ефективності застосування Збройних Сил і їх угруповань у сучасних військових конфліктах, та розробки і наукового супроводження доктрин і стратегій розвитку і застосування Збройних Сил і видів Збройних Сил.

Напрямки військово-технічної науки можливо об’єднувати шляхом єдиної координації наукових досліджень однією з науково-дослідних установ, яка буде визначатись провідною за результатами незалежного оцінювання її спроможностей. Визначення пріоритету необхідно здійснювати на конкурсній основі при незалежному оцінюванні.

На майбутнє вдосконалення системи управління науковою і науково-технічною діяльністю доцільно спрямувати на забезпечення управління науковими дослідженнями наукових і науково-випробувальних установ та ВВНЗ в умовах комерціалізації виконання наукових досліджень. Окрема необхідно проводити управління дослідженнями за напрямком прогнозу складу системи наукових досліджень Збройних Сил України, місця і змісту досліджень у системі досліджень НАТО.

Додаткового вивчення потребують питання управління із інформаційного забезпечення науково-дослідних робіт на всіх рівнях їх проведення.

Як висновок, можна сказати, що система управління науковою і науково-технічною діяльністю у Збройних Силах України забезпечує в даний час виконання завдань системою військової науки.

Розвиток Збройних Сили потребує проведення досліджень за багатьма напрямками на стратегічному, оперативному і тактичному рівнях.

Збереження наявного наукового потенціалу потребує концентрації наукових колективів і кадрів у системі існуючих науково-дослідних установ із врахуванням їхнього наявного і перспективного наукового потенціалу.

Незалежне оцінювання спроможностей наукових установ у Збройних Силах України може забезпечити незалежний (позавідомчий) науково-організаційний підрозділ.

Враховуючи те, що у перспективній структурі Збройних Сил України будуть розділені функції застосування, підготовки, забезпечення між Міністерством оборони, Генеральним штабом Збройних Сил України і видами Збройних Сил, доцільно передбачити відповідний розвиток системи НІНТД.

Окремо хотілось сказати про необхідність проведення досліджень за напрямком прогнозу складу системи наукових установ Збройних Сил України, місця і змісту досліджень у системі досліджень НАТО.

Підважуючи підсумки ми бачимо, що на шляху України до Європейського наукового простору та необхідності приведення вітчизняної законодавчої бази щодо воєнної науки, у відповідність до прийнятих міжнародних стандартів, а також до умов, що склалися в Україні, а саме до викликів, пов’язаних з війною, розв’язаною Російською Федерацією проти України,

особливої уваги потребують питання щодо удосконалення існуючої системи (моделі) з організації наукової і науково-технічної діяльності наукових установ в системі Міністерства оборони України з урахуванням принципів та підходів держав-членів і партнерів НАТО [3,4].

Щодо бази даних стосовно принципів та підходів у питаннях стосовно організації систем воєнно-наукових досліджень в державах-членах НАТО**,** визначені такі принципи: безперервність, єдність, гнучкість та реальність.

Також визначено, що усі зазначені принципи віднесені до проблематики планування у сфері НІНТД. Принцип безперервності передбачає процес планування ННТД, як безперервний у часі, принцип єдності передбачає, що планування воєнно-наукових досліджень в структурних підрозділах Міністерств оборони країн-членів НАТО повинно мати системний характер, а робота з питань планування повинна здійснюватися у єдиному напрямку щодо забезпечення розвитку сил оборони держав тощо. Принципи гнучкості та реальності полягають у чіткому їх реагуванні на виклики, воєнні загрози державам та на непередбачувані воєнні обставини.

За результатами даного наукового дослідження визначено, що існуюча система являється абстрактною військовою моделлю, основним призначенням якої є моделювання результатів функціонування системи управління, системи наукових установ Збройних Сил України та систем консультативно-дорадчих органів Міністерства оборони і Збройних Сил України, з метою формування та/або вироблення (надання) вихідної інформації (пакету документів відповідного типу) за наступною проблематикою: політика Міністерства оборони України у сфері безпеки і оборони держави; розв’язання проблем розвитку воєнної науки і технологій; розвиток військової освіти; управління та планування НІНТД в системі Міністерства оборони України.

Так, мабуть кожна провідна країна світу ставить перед собою питання, чи необхідно взагалі проводити оборонні дослідження і розробки та яка повинна бути їх роль у національній оборонній політиці. Це питання є фундаментальним й викликане тим міркуванням, що багато потреб збройних сил можуть бути задоволені ринком, уникаючи при цьому необхідності несення витрат та ризиків.

Крім того, для підвищення якості та ефективності наукової і науково-технічної діяльності у наукових установах потрібно створити перспективну інформаційну систему (інтегроване науково-інформаційне середовище) наукової і науково-технічної діяльності, яка буде будуватися навколо процесів наукової і науково-технічної діяльності, що дозволить забезпечити, а саме:

електронний документообіг щодо наукової і науково-технічної діяльності Збройних Сил України;

швидку та зручну комунікацію представників наукових установ щодо наукової і науково-технічної діяльності Збройних Сил України;

автоматизований збір (отримання, реєстрації, обліку, збереження) інформації щодо наукової і науково-технічної діяльності Збройних Сил України;

створення внутрішнього інформаційного ресурсу та швидкий доступ представників наукових установ до необхідної інформації щодо наукової і науково-технічної діяльності Збройних Сил України (рис. 1).

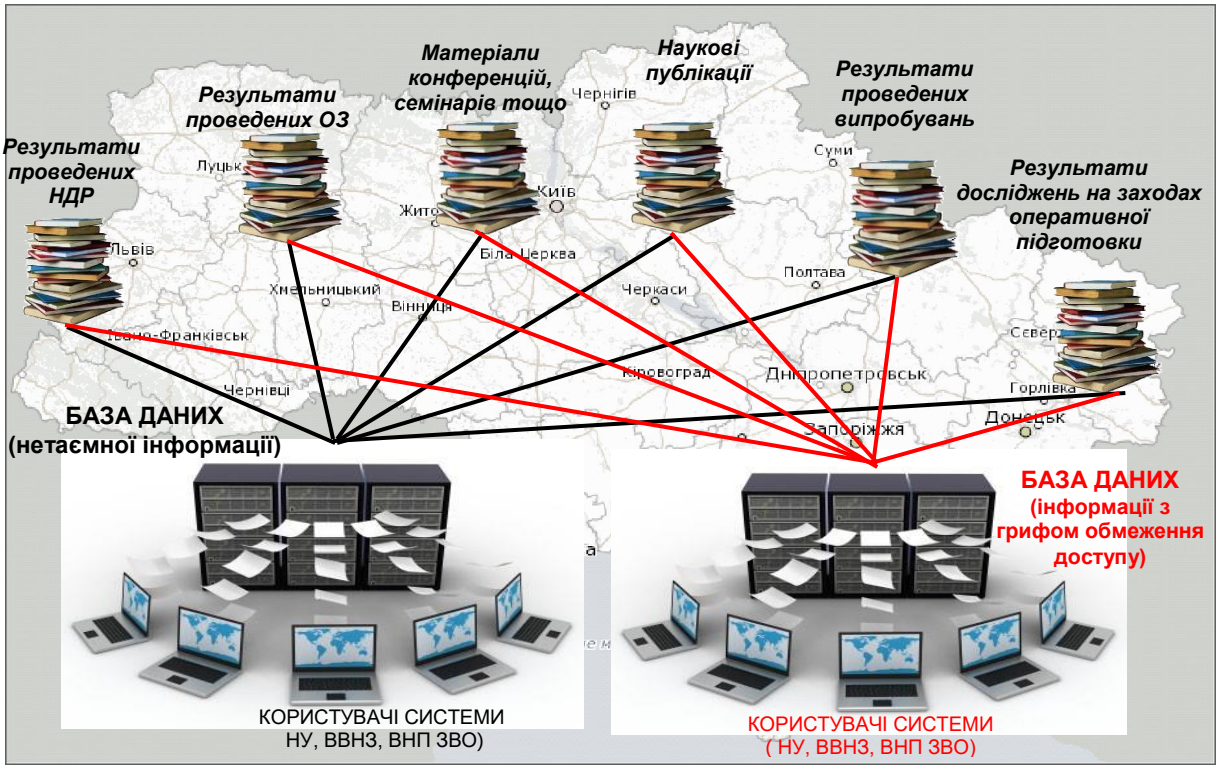



Рисунок 1 – Інтегроване науково-інформаційне середовище

Інформаційна система забезпечення наукової і науково-технічної діяльності повинна мати окремий контур для доступу до інформації з обмеженим доступом. Щодо контуру для роботи з відкритою інформацією, то вочевидь більшість інформаційних потреб військового науковця може забезпечити Національний депозитарій академічних текстів. У цьому не накопичуються лише матеріали виконаних оперативних завдань. Іноді оперативні завдання за обсягом досліджень дорівнюють науково-дослідним роботам.

Разом з тим, розглядаючи зазначену модель у військово-технічній транскрипції, модель представляє собою умовно сформоване інформаційне наукове середовище, яким охоплюється уся сфера діяльності суб'єктів НІНТД з питань планування, створення, накопичення, збереження та перетворення і споживання інформації. Іншими словами, це сукупність технічних і програмних засобів зберігання, обробки і передачі (поширення) результатів моделювання. За своїм масштабом, дане інформаційне середовище має усі притаманні риси загальнодержавного ієрархічного рівня, тобто може слугувати однією із складових перспективної моделі розвитку держави [15].

**Висновки.** Проведений аналіз функціонування існуючої системи наукових установ Збройних Сил України переконливо свідчить про наявність низки проблемних питань організаційного та технічного характеру та функціонуванням системи наукової і науково-технічної діяльності Збройних Сил України, які значно знижують її ефективність.

Насамперед, це пов'язано з недосконалою законодавчою та нормативно-правовою базою, організаційно-штатною структурою наукових підрозділів, системою їх всебічного забезпечення. Крім того, проведені заходи системи керівництва Збройних Сил України та управління військами (силами) призвели до необхідності удосконалення вертикалі управління науковими установами Збройних Сил України.

У таких умовах виникає необхідність вироблення обґрунтованих рекомендацій щодо підвищення ефективності функціонування існуючої системи наукових установ Збройних Сил України на підставі відповідного науково-методичного апарату.

Виходячи з зазначеного, застосування системного підходу для вивчення організації функціонування системи НІНТД дає змогу значно розширити уявлення про її сутність і

тенденції розвитку, глибоко та всебічно розкрити зміст процесів, що відбуваються, виявити об'єктивні закономірності формування цієї багатоаспектної системи.

ЛІТЕРАТУРА:

1. Тимчасова інструкція з організації робіт у Міністерстві оборони України та Збройних Силах України щодо впровадження стандартів НАТО, затверджена заступником Міністра оборони України 09 вересня 2016 року.

2. Закон України "Про вищу освіту" від 01.07.2014 № 1556-VII (із змінами) // База даних «Законодавство України» / ВР України. URL: http://zakon4.rada.gov.ua/laws/show/1556-18/page (дата звернення: 14.12.2018).

3. Положення про науково-інформаційну діяльність у Збройних Силах України, затверджено наказом Міністерства оборони України від 27 вересня 2000 року № 315 (із змінами), втратило чинність.

4. Закон України "Про наукову і науково-технічну діяльність" від 26 листопада 2015 року № 848-VIII (із змінами) // База даних «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/848-19/page (дата звернення: 14.12.2018)

6. Положення про організацію наукової і науково-технічної діяльності у Збройних Силах України, затверджено наказом Міністерства оборони України від 27 липня 2016 року № 385 (зі змінами) / База даних «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/z1172-16 (дата звернення: 12.12.2018)

7. Статут наукової і технологічної організації НАТО [Електронний ресурс]. Режим доступу: 2145-17.1215. Капосльоз Г.В. Системи військово-наукових досліджень зарубіжних країн.– Київ: НУОУ, 2018.

8. Офіційний сайт МО США. [Електронний ресурс].Режим доступу 2243–21.2. Капосльоз Г.В. Системи військово-наукових досліджень зарубіжних країн.– Київ: НУОУ, 2018.

9. Заключний звіт про НДР шифр "Сирена-М", м. Львів, АСВ, –С.74.

REFERENCES:

1. Tymchasova instruktsiia z orhanizatsii robit u Ministerstvi oborony Ukrainy ta Zbroinykh Sylakh Ukrainy shchodo vprovadzhennia standartiv NATO, zatverdzhena zastupnykom Ministra oborony Ukrainy 09 veresnia 2016 roku.

2. Zakon Ukrainy "Pro vyshchu osvitu" vid 01.07.2014 № 1556-VII (iz zminamy) // Baza danykh «Zakonodavstvo Ukrainy» / VR Ukrainy. URL: http://zakon4.rada.gov.ua/laws/show/1556-18/page (data zvernennia: 14.12.2018).

3. Polozhennia pro naukovo-informatsiinu diialnist u Zbroinykh Sylakh Ukrainy, zatverdzheno nakazom Ministerstva oborony Ukrainy vid 27 veresnia 2000 roku № 315 (iz zminamy), vtratylo chynnist.

4. Zakon Ukrainy "Pro naukovu i naukovo-tekhnichnu diialnist" vid 26 lystopada 2015 roku № 848-VIII (iz zminamy) // Baza danykh «Zakonodavstvo Ukrainy» / VR Ukrainy. URL: http://zakon.rada.gov.ua/laws/show/848-19/page (data zvernennia: 14.12.2018)

5. Polozhennia pro orhanizatsiiu naukovoi i naukovo-tekhnichnoi diialnosti u Zbroinykh Sylakh Ukrainy, zatverdzheno nakazom Ministerstva oborony Ukrainy vid 27 lypnia 2016 roku № 385 (zi zminamy) // Baza danykh «Zakonodavstvo Ukrainy» / VR Ukrainy. URL: http://zakon.rada.gov.ua/laws/show/z1172-16 (data zvernennia: 12.12.2018)

6. Ofitsiinyi sait MO SShA. [Elektronnyi resurs].Rezhym dostupu 2243–21.

7. Kaposloz H.V. Systemy viiskovo-naukovykh doslidzhen zarubizhnykh krain.– Kyiv:

NUOU, 2018.
8. Zakliuchnyi zvit pro NDR shyfr “Syrena-M” , m. Lviv, ASV, – p.74.

**Matsovytyi V. A.**

## DEVELOPMENT OF AN INTEGRATED SCIENTIFIC AND SYSTEM SCIENTIFIC AND TECHNICAL ACTIVITIES IN THE ARMED FORCES OF UKRAINE

***The article considers the peculiarities of the functioning of the systems of scientific and scientific-technical activities of scientific institutions of the Ministry of Defense of Ukraine in the context of European experience of NATO member states (hereinafter - NINTD), prospects of legislation and regulations on the organization of military research briefly outlined:***

***vision of scientific institutions of the Ministry of Defense of Ukraine and the Joint Forces Command on the main issues of NINTD organization, use of various models of organization and conduct of research in military science, quality control of scientific products, its comprehensive evaluation and degree of secrecy of scientific information;***

***some aspects of the peculiarities of the functioning of management systems of NINTD subjects, basic principles and approaches to the creation and development of national research systems in the field of military science.***

***Purpose. analysis of the main features of the functioning of systems of scientific and scientific-technical activity of scientific institutions of the Ministry of Defense of Ukraine in the context of the European experience of NATO member states. The article uses a system of general scientific and special methods of theoretical and empirical research: analysis of scientific publications presented in foreign periodicals and open material on the researched issues on the Internet, systematization of scientific sources, generalizations and systematic approach. The analysis of the existing system of scientific institutions of the Armed Forces of Ukraine convincingly shows the existence of a number of problematic organizational and technical issues and the functioning of the system of scientific and scientific-technical activities of the Armed Forces of Ukraine, which significantly reduce its effectiveness. First of all, this is due to the imperfect legal and regulatory framework, organizational and staffing structure of scientific units, the system of their comprehensive support. In addition, the measures taken by the system of leadership of the Armed Forces of Ukraine and the management of troops (forces) have led to the need to improve the vertical management of scientific institutions of the Armed Forces of Ukraine. In such conditions, there is a need to develop sound recommendations for improving the efficiency of the existing system of scientific institutions of the Armed Forces of Ukraine on the basis of the relevant scientific and methodological apparatus.***

***Keywords: functioning of the existing system, scientific institutions, scientific research and scientific and technical (experimental) developments, the model of organization of military research; organization of scientific and scientific-technical activities; system of military research; policies, principles, approaches to solving organizational problems in the field of military science.***

УДК 004.056.5

д.т.н., проф. **Кобозєва А.А.** (ОНПУ)
д.т.н., проф. **Маєвський Д.А.** (ОНПУ)
**Кирилюк В.О.** (ОНПУ)

DOI: https://doi.org/10.17721/2519-481X/2022/77-08

# МЕТОД ВИЯВЛЕННЯ ПОРУШЕННЯ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ, ЗАСНОВАНИЙ НА СПЕКТРАЛЬНОМУ РОЗКЛАДАННІ СИМЕТРИЗОВАНОЇ МАТРИЦІ БЛОКУ

***В роботі розглядається важлива науково-практична задача підвищення ефективності виявлення порушень цілісності інформації, зокрема цифрових зображень, що є її поширеним представленням, яка стає сьогодні одною з основних для фахівців в області інформаційної та кібербезпеки. Невиявлені своєчасно несанкціоновані зміни інформації можуть привести до негативних, катастрофічних наслідків як для окремих людей, підприємств, банків, фірм, так і для людства в цілому, коли йдеться про інформацію, що становить державну таємницю, містить дані зі сфери військової галузі, атомної енергетики, хімічної промисловості тощо, що визначає актуальність задачі, яка розглядається. Основним результатом роботи є удосконалений універсальний метод виявлення порушення цілісності цифрового зображення, готовий до практичної реалізації, теоретичний базис якого заснований на аналізі власних значень та власних векторів симетричних блоків матриці зображення, що ставляться у відповідність оригінальним блокам. В роботі обгрунтований спосіб симетризації матриці блоку, що дозволяє значно (більше, чим на 23%) скоротити обчислювальні і, як наслідок, часові витрати на експертизу зображення в порівнянні з часовими витратами методу-прототипу. Доведено, що для більшості отриманих симетричних блоків, що ставляться у відповідність блокам оригінального ЦЗ, кут між власним вектором, що відповідає максимальному власному значенню блока, і нормованим вектором модулів власних значень дорівнює певному значенню, яке не залежить від конкретики оригінального зображення, але є чутливим до його змін, що дало можливість забезпечити універсальність методу та підвищити його ефективність у сенсі точності виявлення порушення цілісності зображення більше, ніж на 5%, в порівнянні з аналогом. Значимість отриманих результатів полягає в забезпеченні за рахунок використання запропонованого методу підвищення ефективності процесу виявлення порушень цілісності зображення за критеріями обчислювальних (часових) витрат на експертизу одного зображення та точності виявлення***.

***Ключові слова***: ***цифрове зображення, порушення цілісності, власний вектор, власне значення.***

**Вступ.** Стрімкий розвиток інформаційних технологій, проникнення їх у всі сфери людської діяльності привів сучасне суспільство до стану, при якому несанкціоновані зміни інформації – порушення її цілісності можуть привести до негативних наслідків як для окремих людей, підприємств, банків, фірм, так і до катастроф для людства в цілому, якщо несанкціоновані зміни відбудуться з інформацією, що становить державну таємницю, містить дані зі сфери військової галузі, атомної енергетики, хімічної промисловості тощо, що може поставити під загрозу життя людей в усьому світі [1] і що є критично актуальним для нашої держави сьогодні, під час повномасштабного вторгнення Росії в Україну.

Питання виявлення порушень цілісності інформації – одного з критеріїв її захищеності, зокрема цифрових зображень (ЦЗ), що є її поширеним представленням, стає сьогодні одним з основних для фахівців в області інформаційної та кібербезпеки [2,3]. Ці порушення можуть проводитися різними способами, мати різні цілі. Так організація прихованого

(стеганографічного) каналу зв'язку, де порушення цілісності контейнера є результатом вбудови в нього додаткової інформації, може сприяти безпосередньо витоку секретної інформації, привести до матеріального, репутаційного збитку підприємств, фірм, банків, до наслідків державного масштабу [4]; застосування засобів графічних редакторів (Adobe Photoshop, Gimp та ін.) дозволяє, навіть не маючи спеціальної кваліфікації, обробляти, змінювати ЦЗ, цифрові відео, результатом чого може стати, зокрема усунення зі сцени ЦЗ (кадрів відео) окремих предметів, персонажів чи їх штучне додавання, що кардинально змінить зміст цифрового контенту та наслідки від його використання [5], може виявитися критичним при застосуванні таких контентів в судових справах, засобах масової інформації тощо. Тільки своєчасне виявлення неоригінальності цифрового контенту дозволить тут уникнути негативних наслідків, що говорить про актуальність і важливість розробки, модифікації, удосконалення відповідних методів, спрямованих на виявлення порушення цілісності інформаційного контенту, зокрема ЦЗ.

**Аналіз останніх досліджень і публікацій.** Методи виявлення порушення цілісності ЦЗ розподіляються на дві великі групи: активні і пасивні (або «сліпі») [6,7]. Активні методи, більшість із яких використовують електронний цифровий підпис або цифрові водяні знаки, потребують інформацію про оригінальне ЦЗ, на відміну від пасивних, для яких така інформація не потрібна. На сьогоднішній день саме пасивні експертні методи займають провідні позиції для розв'язку задачі, що розглядається [7-9], хоча організація «сліпого» детектування результатів порушення цілісності ЦЗ є більш складною. Всі пасивні методи в свою чергу, залежно від інформації, що є в наявності у експерта, можна розподілити на спрямовані (налаштовані на конкретні збурні дії, які враховують особливості, властивості тих збурень, що є результатом таких дій) та універсальні (налаштовані на виявлення наявності відмін досліджуванного контента від оригінального незалежно від того, яким чином ці зміни були отримані). Спрямовані методи, як правило, є більш ефективними при виявленні тої дії, на яку вони налаштовані, ніж універсальні в тих самих умовах застосування. Але, враховуючи те, що на практиці обізнаність експерта про можливі збурні дії не завжди присутня, наявний у експерта арсенал програмних засобів є обмеженим та принципово не може (у випадку спрямованих методів) забезпечити «готовність» до всіх збурних дій, надзвичайно актуальним на сьогодні є наявність, розробка, удосконалення саме універсальних методів для розв'язку задачі, що розглядається. І хоча розробки в цьому напрямку ведуться [10,11], при цьому найчастіше – в межах стеганоаналізу [12,13], на сьогоднішній день універсальні методи виявлення порушення цілісності ЦЗ майже відсутні, а зусилля вчених найчастіше спрямовані на виявлення результатів конкретних збурних дій: зміни яскравості [14], розмиття ЦЗ чи його частини [15], накладання шуму [16], результатів стеганоперетворення конкретними стеганоалгоритмами [17,18] тощо. Математичний базис таких методів формується з врахуванням особливостей, які вносять саме ці конкретні збурні дії в параметри оригінального ЦЗ. Так в [14] знайдене формальне представлення результату корекції яскравості ЦЗ у вигляді корекції максимального сингулярного числа $\sigma_1$ його матриці яскравості $Y$, яке і використане в відповідному експертному методі. В [19] запропонований метод виявлення результатів штучного підвищення різкості в ЦЗ, розглянутий конкретний фільтр, що використовується для цієї операції в графічному редакторі AdobePhotoshop – «Інтелектуальна різкість». Для відокремлення ЦЗ, що піддалися обробці таким фільтром, від таких, що не піддалися, використовується оцінка відношення кількості близьких пар кольорів до загальної кількості пар кольорів, яка специфічно змінюється при застосуванні згаданого фільтра, для якої імпірічно визначене порогове значення. В [17,18.] запропоновані стеганоаналітичні методи, спрямовані на виявлення результатів стеганоперетворення LSB-методом. Ці методи не тільки налаштовані на конкретний стеганографічний метод, а ще й накладають обмеження на

величину пропускної спроможності прихованого каналу зв'язку, що піддається експертизі. Існує ціла низка методів, які застосовуються для аналізу ЦЗ у форматі Jpeg, заснованих на виявленні «ефекту подвійного квантування», що виникає в гістограмах частотних коефіцієнтів зображення при первісному та повторному його збереженні в Jpeg, які мають значне поширення в силу широкого використання цього формату сьогодні для збереження ЦЗ [9,20], але очевидно, що «форматоорієнтованість» значно обмежує область застосування таких методів для експертизи цілісності і не дає можливості віднести їх до групи універсальних.

Одним з невеликої кількості існуючих універсальних пасивних методів виявлення порушення цілісності ЦЗ є метод, запропонований в [11]. Основою методу є доведена для більшості $l \times l$-блоків оригінального ЦЗ, отриманих шляхом стандартної розбивки його матриці, рівність:

$$\angle\left(u_1, \overline{\sigma}\right) \approx \angle\left(v_1, \overline{\sigma}\right) \approx \angle\left(n^{\circ}, e_1\right), \qquad (1)$$

де $u_1, v_1$ – ортонормовані сингулярні вектори (СНВ) блоку, що відповідають найбільшому сингулярному числу $\sigma_1$; $\overline{\sigma} = \sigma / \|\sigma\|$, де $\sigma = (\sigma_1, \sigma_2, ..., \sigma_i)^T$, $\sigma_1 \geq \sigma_2 \geq ... \geq \sigma_i \geq 0$ – сингулярні числа (СНЧ) блоку; $n^{\circ} = \left(1/\sqrt{l}, 1/\sqrt{l}, ..., 1/\sqrt{l}\right)^T \in R^l$ – *n*-оптимальний вектор простору $R^l$, $\angle\left(u_1, \overline{\sigma}\right)$, $\angle\left(v_1, \overline{\sigma}\right)$, $\angle\left(n^{\circ}, e_1\right)$ – величини кутів між векторами $u_1$ і $\overline{\sigma}$, $v_1$ і $\overline{\sigma}$, $n^{\circ}$ і вектором стандартного базису $e_1 = (1, 0, ..., 0)$ простору $R^l$, що відповідає додатному напряму осі $Ox_1$, відповідно. Значимою перевагою цього методу є те, що він залишається ефективним, незалежно від конкретики та сили збурної дії, в результаті якої відбувається порушення цілісності ЦЗ, від формату зображення. Але орієнтованість його на аналіз властивостей СНЧ, СНВ блоків, для отримання яких використовується їх нормальні сингулярні розкладання, які є достатньо «дорогими» в обчислювальному сенсі, робить актуальним питання його удосконалення при збереженні всіх переваг, як і метода, запропонованого в [21].

Таким чином, на основі проведеного аналізу наукових джерел встановлено, що проблема виявлення порушень цілісності ЦЗ не є вирішеною остаточно. Абсолютна більшість існуючих пасивних методів, що займають провідні позиції для розв'язку задачі, що розглядається, мають значні недоліки, серед яких: орієнтованість здебільшого на конкретну збурну дію, на формат ЦЗ, величину збурення, що зазнає оригінальний контент в результаті збурної дії, значні часові витрати, залишаючи *актуальною* задачу підвищення ефективності процесу виявлення порушень цілісності ЦЗ.

**Мета роботи та задачі дослідження.** *Метою* роботи є підвищення ефективності виявлення порушень цілісності ЦЗ шляхом удосконалення універсального методу, запропонованого в [11].

Як показники ефективності далі розглядаються: обчислювальні (часові) витрати на експертизу одного ЦЗ; точність виявлення порушення цілісності [22] (*accuracy* (*ACC*)), яка визначається відповідно до формули:

$$ACC = (TP + TN)/(TP + FN + TN + FP), \qquad (2)$$

де *TP* (*True Positive*) – число правильно виявлених ЦЗ, цілісність яких була порушена; *TN* (*True Negative*) – число правильно виявлених оригінальних ЦЗ; *FP* (*False Positive*) – число оригінальних ЦЗ, помилково прийнятих за такі, цілісність яких була порушена; *FN* (*False Negative*) – число ЦЗ, цілісність яких була порушена, помилково визнаних оригінальними.

Для досягнення поставленої мети в роботі розв'язуються наступні *задачі*:

1. Обгрунтувати спосіб симетризації матриці блоку ЦЗ, що дасть можливість заміни формальних параметрів блоку (СНЧ, СНВ), що використовуються в процесі експертизи в [11], на власні вектори і власні значення, отримання яких є менш обчислювально затратним;

2. Обгрунтувати математично можливість використання симетризованих блоків матриці ЦЗ для експертизи його цілісності;

3. Розробити удосконалення методу [11] та його алгоритмічну реалізацію;

4. Провести оцінку ефективності запропонованої алгоритмічної реалізації.

**Основний матеріал дослідження.** Нехай формальним представлення ЦЗ є $n \times n$-матриця $F$. У випадку кольорового зображення ця матриця може відповідати будь-якій кольоровій складовій (схема RGB) чи є матрицею яскравості (схема YUV). Матриця $F$ стандартним чином [23] розбивається на непересічні $l \times l$-блоки, довільний з яких позначимо $A$. Для матриці $A$, у якої відсутні кратні СНЧ, маємо єдине нормальне сингулярне розкладання [24]:

$$A = U \Sigma V^T = \sum_{i=1}^{l} \sigma_i u_i v_i^T , \qquad (3)$$

де $U, V$ – ортогональні $l \times l$-матриці, стовпці яких $u_i, v_i$, $i = \overline{1,l}$, є лівими і правими СНВ $A$ відповідно, при цьому ліві СНВ додатково є лексикографічно додатними; $\Sigma = diag\left(\sigma_1,..., \sigma_l\right), \sigma_1 \geq ... \geq \sigma_l \geq 0$ – СНЧ $A$. Права частина (3) представляє сингулярне розкладання $A$ у формі зовнішніх добутків [25].

Якщо матриця $A$ є симетричною, то всі її власні значення (ВЗ) є дійсними, при цьому для неї можливо побудувати єдине нормальне спектральне розкладання у випадку відсутності ВЗ з однаковими абсолютними значеннями:

$$A = W \Lambda W^T = \sum_{i=1}^{l} \lambda_i w_i w_i^T , \qquad (4)$$

де $W$ – ортогональна $l \times l$-матриця, стовпці якої $w_i$, $i = \overline{1,l}$, є лексикографічно додатними власними векторами (ВВ) $A$, $\Lambda = diag\left(\lambda_1,..., \lambda_l\right)$, $\lambda_1,..., \lambda_l$ – ВЗ $A$. Права частина (4) представляє спектральне розкладання $A$ у формі зовнішніх добутків [25].

Спектральне і сингулярне розкладання симетричної матриці пов'язані між собою [25]. При цьому очевидним є те, що обчислювальна складність процесу побудови сингулярного розкладання $A$, яке передбачає визначення елементів матриць $U, V$ і діагональної матриці $\Sigma$ і оцінюється як $O\left(l^3\right)$, приблизно вдвічі більше, ніж спектрального, де передбачається обчислення елементів лише матриці $W$ і діагональної матриці $\Lambda$ (таке ж саме співвідношення буде мати місце і для запитів до пам'яті). Таким чином, одним з шляхів удосконалення методу з [11], що очікувано сприятиме зменшенню часових витрат на експертизу ЦЗ, є побудова експертизи не на аналізі СНЧ і СНВ реальних блоків, а на аналізі ВЗ і ВВ для симетричних матриць блоків (якщо цю симетричність можливо буде забезпечити без втрати точності виявлення порушення цілісності $ACC$ та без виникнення обмежень на застосування відповідного методу). Дійсно, хоча обчислювальна складність будь-якого блокового методу, яким є і метод [11], визначається кількістю $l \times l$-блоків ЦЗ і для $n \times n$-матриці $F$ становить $C\left\lceil \frac{n}{l} \right\rceil \times \left\lceil \frac{n}{l} \right\rceil = O\left(n^2\right)$, де $C$ не залежить від $n$, незалежно від того, яка кількість операцій використовується для роботи з одним блоком, але кількість операцій обробки блоку

відіб'ється на коефіцієнті при $n^2$ і при застосуванні спектрального розкладання для матриці блоку цей коефіцієнт очевидно буде менше, чим при використанні сингулярного розкладання. Але в ЦЗ блок, як правило, не є симетричним. Розглянемо декілька можливих способів отримання симетричного виду блоку $B$, що буде ставитися у співвідношення реальному блоку $A$ ЦЗ при його експертизі:

$$A \quad \rightarrow \quad B = A^T A, \tag{5}$$

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1l} \\ a_{21} & a_{22} & \dots & a_{2l} \\ \dots\dots\dots & \dots\dots\dots & & \\ a_{l1} & a_{l2} & \dots & a_{ll} \end{pmatrix} \quad \rightarrow \quad B = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{l1} \\ a_{21} & a_{22} & \dots & a_{l2} \\ \dots\dots\dots & \dots\dots\dots & & \\ a_{l1} & a_{l2} & \dots & a_{ll} \end{pmatrix} \quad \vee \quad B = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1l} \\ a_{12} & a_{22} & \dots & a_{2l} \\ \dots\dots\dots & \dots\dots\dots & & \\ a_{1l} & a_{2l} & \dots & a_{ll} \end{pmatrix}, \tag{6}$$

$$A \quad \rightarrow \quad B = \frac{A + A^T}{2}. \tag{7}$$

Обчислювальна складність симетризації (5) визначається як $O\left(l^3\right)$, для (7) – $O\left(l^2\right)$. Використання одної з матриць $B$, що визначаються (6), взагалі не вимагає проведення жодної арифметичної операції для перерахування елементів $B$ відносно $A$, а може бути сформована лише за $O\left(l^2\right)$ операцій присвоювання, виконання яких вимагає меньшого часу, ніж будь-яка арифметична операція. На перший погляд, з точки зору часових витрат, перевагу треба віддати способу (6), але для кожного з варіантів (6) матриця $B$ несе в собі інформацію лише про нижній/верхній трикутник оригінальної матриці $A$, при цьому інформація про верхній/нижній трикутник губиться, а загалом губиться майже половина інформації про досліджуване ЦЗ, що є неприпустимим з урахуванням специфіки задачі, що розглядається в роботі. Передбаченим результатом цього, який підтверджено практично, є, на фоні зменшення часу експертизи, значне зменшення ефективності експертизи (*ACC*) в порівнянні з [11], що, з урахуванням вищенаведеного, робить пріоритетним спосіб (7) для симетризації блоку, який хоча дещо і спотворює інформацію про реальні значення матриці $A$, але зберігає її в цілому про блок $A$.

Враховуючи форму (3) сингулярного розкладання, з (7) для симетричної матриці $B$ маємо:

$$B = \frac{A + A^T}{2} = \frac{U\Sigma V^T + V\Sigma U^T}{2} = \frac{1}{2}\left( \sum_{i=1}^{l} \sigma_i u_i v_i^T + \sum_{i=1}^{l} \sigma_i v_i u_i^T \right) = \frac{1}{2} \sum_{i=1}^{i} \sigma_i \left( u_i v_i^T + v_i u_i^T \right) = \tag{8}$$

$$= \frac{1}{2}\left( \sigma_1 \left( u_1 v_1^T + v_1 u_1^T \right) + \sum_{i=2}^{l} \sigma_i \left( u_i v_i^T + v_i u_i^T \right) \right).$$

Як доведено в [26], для СНВ $u_1$, $v_1$ блоку оригінального ЦЗ, що відповідають максимальному СНЧ $\sigma_1$:

$$u_1 \approx n^\circ, \quad v_1 \approx n^\circ. \tag{9}$$

Підставимо (9) в (8):

$$B = \frac{1}{2}\left( \sigma_1 \left( n^{\circ}\left(n^{\circ}\right)^T + n^{\circ}\left(n^{\circ}\right)^T \right) + \sum_{i=2}^{l} \sigma_i \left( u_i v_i^T + v_i u_i^T \right) \right) = \sigma_1 n^{\circ}\left(n^{\circ}\right)^T + \frac{1}{2}\sum_{i=2}^{l} \sigma_i \left( u_i v_i^T + v_i u_i^T \right). \quad (10)$$

Для симетричної матриці $B$ існує певний зв'язок між її сингулярним і спектральним розкладанням [25]. Якщо у відповідності до (4) позначити спектральне розкладання $B$: $B = \overline{U}\,\overline{\Lambda}\,\overline{U}^T$ ($\overline{\Lambda} = diag\left(\overline{\lambda}_1, \overline{\lambda}_2, ..., \overline{\lambda}_l\right)$ – матриця ВЗ, $\overline{U} = \left(\overline{u}_1, \overline{u}_2, ..., \overline{u}_l\right)$ – ортогональна матриця ВВ), то сингулярне розкладання для $B$ виглядає: $B = \overline{U}\,\overline{\Sigma}\,\overline{V}^T$ ($\overline{\Sigma} = diag\left(\overline{\sigma}_1, \overline{\sigma}_2, ..., \overline{\sigma}_n\right)$ – матриця СНЧ, $\overline{V} = \left(\overline{v}_1, \overline{v}_2, ..., \overline{v}_l\right)$ – ортогональна матриця правих СНВ), де

$$\overline{\sigma}_i = \left|\overline{\lambda}_i\right|, \ \overline{v}_i = sign\left(\overline{\lambda}_i\right)\overline{u}_i. \quad (11)$$

З урахуванням (9) для $B$ при отриманні її сингулярного розкладання: $\overline{u}_1 \approx n^{\circ}$, $\overline{v}_1 \approx n^{\circ}$. Це означає, що для першого власного вектора $B$, що отримується при спектральному розкладанні $B$ і відповідає максимальному за модулем ВЗ, яке за теоремою Фробеніуса [27] є додатним: $\overline{u}_1 \approx n^{\circ}$.

Якщо б для $B$ будувалось спектральне розкладання у формі зовнішніх добутків, то ми б отримали:

$$B = \sum_{i=1}^{l} \overline{\lambda}_i \overline{u}_i \left(\overline{u}_i\right)^T = \overline{\lambda}_1 \overline{u}_1 \left(\overline{u}_1\right)^T + \sum_{i=2}^{l} \overline{\lambda}_i \overline{u}_i \left(\overline{u}_i\right)^T = \overline{\lambda}_1 n^{\circ}\left(n^{\circ}\right)^T + \sum_{i=2}^{n} \overline{\lambda}_i \overline{u}_i \left(\overline{u}_i\right)^T. \quad (12)$$

А якщо б для $B$ будувалось сингулярне розкладання у формі зовнішніх добутків, воно б мало вигляд:

$$B = \sum_{i=1}^{l} \overline{\sigma}_i \overline{u}_i \left(\overline{v}_i\right)^T = \overline{\sigma}_1 \overline{u}_1 \left(\overline{v}_1\right)^T + \sum_{i=2}^{l} \overline{\sigma}_i \overline{u}_i \left(\overline{v}_i\right)^T = \overline{\sigma}_1 n^{\circ}\left(n^{\circ}\right)^T + \sum_{i=2}^{l} \overline{\sigma}_i \overline{u}_i \left(\overline{v}_i\right)^T. \quad (13)$$

Враховуючи ортогональність ВВ, СНВ $B$, можна стверджувати, що серед власних векторів, як і серед лівих і правих СНВ $B$ є тільки по одному, що дорівнюють $n^{\circ}$. Це вектори, що відповідають найбільшому ВЗ/найбільшому СНЧ. Таким чином, перший доданок в правій частині (10) можна розглядати, як добуток першого (максимального) власного значення на відповідний власний вектор. Порівнюючи праві частини (10), (12) і (13), враховуючи (11), маємо:

$$\overline{\lambda}_1 = \overline{\sigma}_1 = \sigma_1. \quad (14)$$

Основою співвідношення (1) разом з (9) було в [26] співвідношення $\overline{\sigma} \approx e_1$, отримане з урахуванням того, що для блоків ЦЗ максимальне СНЧ є набагато більшим за всі інші СНЧ. Операція (7), усереднюючі значення яскравості пікселєй, розмиває блок, зменшуючи його високочастотну складову. Для СНЧ, враховуючи зв'язок між сингулярними тройками (блоку) матриці ЦЗ та її частотними коефіцієнтами, що полягає в тому, що сингулярні трійки, що відповідають максимальним/мінімальним/середнім СНЧ несуть в собі інформацію, головним чином, про низькочастотну/високочастотну/середньочастотну складову сигналу, це приводить до сукупного зменшення найменших і, можливо, середніх значень СНЧ, що, враховуючи (11), (14), приведе до того, що $\overline{\lambda}_1$ буде мати більшу абсолютну відокремленість

$$gap_{abs}(1,B) = \min_{i \neq 1} \left\| \left|\bar{\lambda}_1\right| - \left|\bar{\lambda}_i\right| \right\|, \tag{15}$$

ніж відокремленість $svdgap(1,A) = \min_{i \neq 1} \left|\sigma_1 - \sigma_i\right|$ СНЧ $\sigma_1$ в $A$. Наслідком цього, в свою чергу, буде те, що нормований вектор модулів власних значень $B$

$$\bar{\lambda} = \frac{\lambda}{\|\lambda\|}, \tag{16}$$

де $\lambda = \left(\bar{\lambda}_1, \left|\bar{\lambda}_2\right|, ..., \left|\bar{\lambda}_n\right|\right)^T$, буде ближче до $e_1$, чим нормований вектор $\bar{\sigma}$ СНЧ $A$, тобто:

$$\angle\left(\bar{\lambda}, e_1\right) < \angle\left(\bar{\sigma}, e_1\right). \tag{17}$$

Співвідношення (17) приведе до того, що для матриці $F$ ЦЗ буде більше блоків у вигляді $B$, для яких

$$\angle\left(\bar{u}_1, \bar{\lambda}\right) \approx \angle\left(n^\circ, e_1\right), \tag{18}$$

де $\bar{u}_1$ для матриці $B$ є ВВ, який відповідає максимальному власному значенню $\bar{\lambda}_1$, ніж блоків оригінальних $A$, для яких має місце (1).

Таким чином нами доведено

***Твердження 1***. Для більшості блоків у симетричному вигляді (7), що ставляться у відповідність блокам оригінального ЦЗ, має місце співідношення (18), при цьому (18) виконується для більшої кількості блоків, ніж співвідношення (1) для оригінальних блоків зображення.

Поняття «більшості блоків ЦЗ» на практиці візуалізується модою гістограми, що далі позначається $\Gamma_\lambda$, значень кутів $\angle\left(\bar{u}_1, \bar{\lambda}\right)$ $l \times l$-блоків цього зображення, яка для оригінального ЦЗ, дорівнює значенню кута $\angle\left(n^\circ, e_1\right)$ у відповідному просторі $R^l$. З доказу твердження 1 випливає, що при порушенні цілісності ЦЗ мода $\Gamma_\lambda$ може зсуватися з положення $\angle\left(n^\circ, e_1\right)$, що буде, разом з іншими характеристиками, вказівкою на неавторізовану зміну зображення. Крім зсуву моди $\Gamma_\lambda$ на порушення цілісності ЦЗ буде вказувати зміна характеру гістограми: в результаті збурної дії, навіть якщо мода $\Gamma_\lambda$ і залишиться в $\angle\left(n^\circ, e_1\right)$, значення в моді значно зменшиться, значна кількість блоків, що в оригінальному ЦЗ робили свій внесок в стовпець $\Gamma_\lambda$, що відповідає моді, в збуреному ЦЗ зробить внесок в інші стовпці. Оскільки відповідно до загальної формули для довільної симетричної матриці $M$ :

$$\max_j \left|\lambda_j(M) - \lambda_j(M + \Delta M)\right| \leq \|\Delta M\|_2, \tag{19}$$

де $M + \Delta M$ – збурена матриця, $\Delta M$ – матриця збурення, $\|\cdot\|_2$ – спектральна матрична норма [25], всі ВЗ симетричної $n \times n$-матриці $M$ є добре обумовленими, таким же буде і вектор $\bar{\lambda}$ (16) симетричного блоку $B$ (7), що ставиться у відповідність блоку $A$ ЦЗ. Чутливість (обумовленість) ВВ $\bar{u}_1$ симетричної довільної $M$ визначається формулою:

$$sin\ \theta_1 \le \frac{2\left\|\Delta M\right\|_2}{gap_{abs}(1, M)}, \qquad (20)$$

де $\theta_1$ – гострий кут між ВВ, що відповідають максимальним ВЗ в матрицях $M$ і $M + \Delta M$ Оскільки абсолютна відокремленість (15) максимального ВЗ для ЦЗ завжди є значною, такою, що набагато перевищує абсолютні відокремленості інших ВЗ, з (20) випливає нечутливість (добра обумовленість) $\bar{u}_1$ для блоку $B$ (7). Віходячи з (19), (20), можна стверджувати, що для тих блоків, що в оригінальному ЦЗ робили свій внесок в стовпець $\Gamma_\lambda$, який відповідає моді $\angle\left(n^\circ, e_1\right)$, і для яких в результаті збурної дії значення кута $\angle\left(\bar{u}_1, \bar{\lambda}\right)$ змінилося, ця зміна не може бути значною, залишаючи внесок таких блоків для збуреного ЦЗ в стовпці $\Gamma_\lambda$, що знаходяться в деякому незначному околі моди. Визначені зміни $\Gamma_\lambda$ при змінах зображення будуть тим більше, чим більше буде величина збурної дії, якій піддалося ЦЗ.

Отримані теоретичні висновки знайшли своє підтвердження на практиці, ілюстрація чого для конкретного ЦЗ наведена на рис.1, де очевидним є збільшення значення гістограми $\Gamma_\lambda$ в моді для випадку симетризованих блоків ЦЗ, яка відповідає значенню кута $\angle\left(n^\circ, e_1\right)$, що для $4 \times 4$ -блоків дорівнює 60 градусів (рис.1(б)), в порівнянні зі значенням в моді гістограми кутів між нормованим вектором СНЧ і лівим СНВ, що відповідає максимальному СНЧ, оригінальних блоків оригінального ЦЗ (рис.1(а)), а також видозміна $\Gamma_\lambda$ при порушенні цілісності ЦЗ (рис.1(в,г)).

Враховуючи все наведене вище, пропонується наступний удосконалений відносно [11] універсальний метод виявлення порушення цілісності ЦЗ, основні кроки якого наступні:

***Крок 1***. Матриця $F$ аналізованого ЦЗ розбивається стандартним чином на $l \times l$ -блоки, довільний з яких – блок $A$.

***Крок 2***. Кожному блоку $A$, отриманому на попередньому кроці, ставиться у відповідність симетричний блок $B = \frac{A + A^T}{2}$.

***Крок 3***. Для аналізованого ЦЗ будується гістограма $\Gamma_\lambda$ значень кутів $\angle\left(\bar{u}_1, \bar{\lambda}\right)$ в блоках $B$ з кроком $h$.

***Крок 4***. Для гістограми $\Gamma_\lambda$ визначається мода $A_\lambda$, а також значення $M_\lambda$ в моді.

***Крок 5***. Для аналізованого ЦЗ з використанням $\Gamma_\lambda$ обчислюється кількість $S_\lambda$ блоків, для яких:

$$\angle\left(\bar{u}_1, \bar{\lambda}\right) \in \left[\angle\left(n^\circ, e_1\right) - T, \angle\left(n^\circ, e_1\right) + T\right],$$

де $T$ – параметр, що визначається експериментально, характеризує радіус околa $\angle\left(n^\circ, e_1\right)$.

***Крок 6*** (*перевірка*).

*Якщо*

$$A_\lambda \notin \left\{\angle\left(n^\circ, e_1\right) - 1^\circ,\ \angle\left(n^\circ, e_1\right),\ \angle\left(n^\circ, e_1\right) + 1^\circ\right\},$$

*то*

для аналізованого ЦЗ цілісність порушена.

*Якщо*

$$\left(A_\lambda \in \left\{\angle\left(n^\circ, e_1\right) - 1^\circ,\ \angle\left(n^\circ, e_1\right),\ \angle\left(n^\circ, e_1\right) + 1^\circ\right\}\right) \& \left(S_\lambda / M_\lambda > P\right),$$

де $P$ – порогове значення, що визначається експериментально, характеризує видозміну гістограми в результаті збурної дії,

*то*

для аналізованого ЦЗ цілісність порушена.

*Якщо*

$$\left(A_\lambda \in \left\{\angle\left(n^\circ, e_1\right) - 1^\circ,\ \angle\left(n^\circ, e_1\right),\ \angle\left(n^\circ, e_1\right) + 1^\circ\right\}\right) \& \left(S_\lambda / M_\lambda \le P\right),$$

*то*

для аналізованого ЦЗ цілісність не порушена.

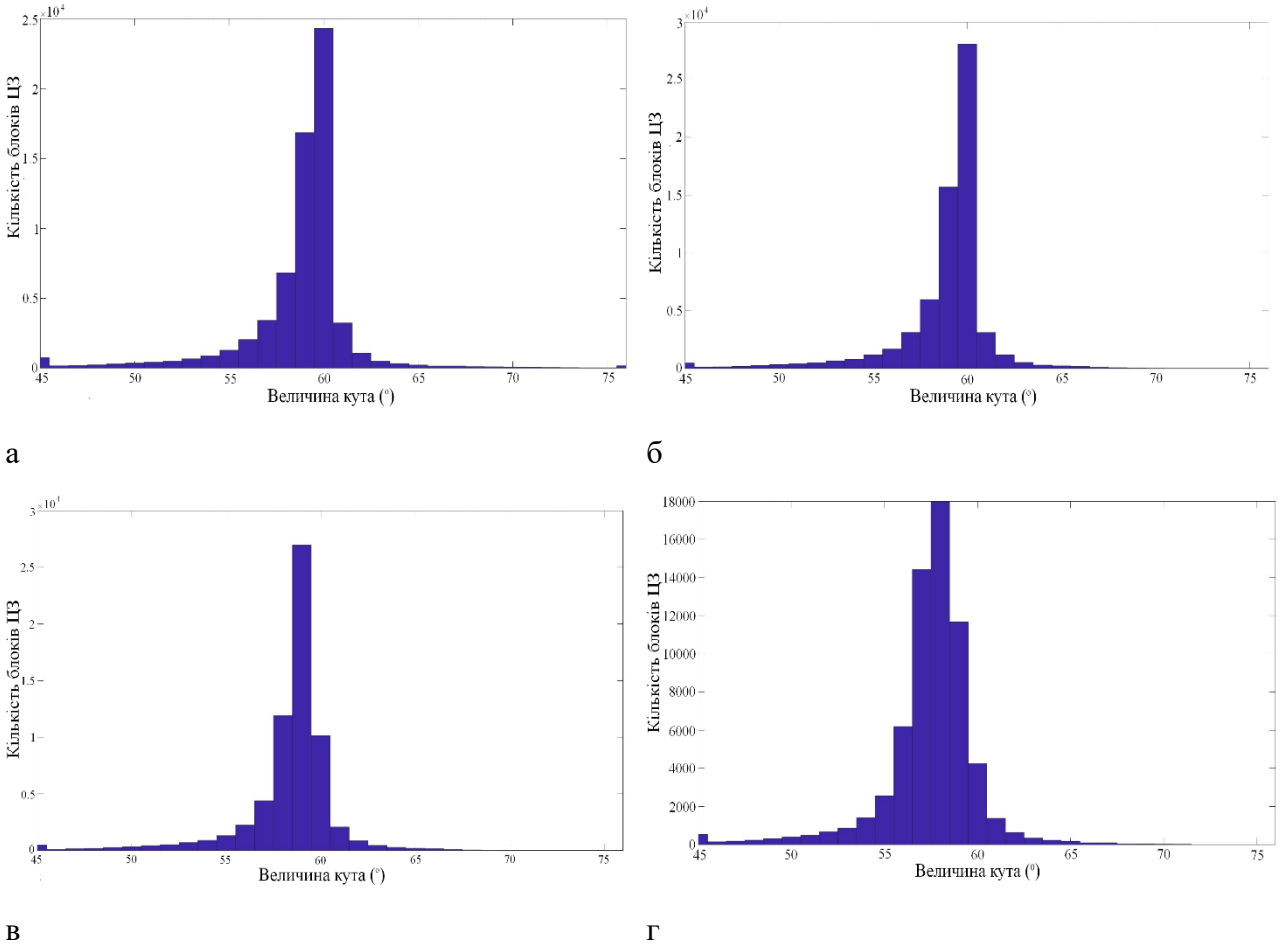



Рисунок 1 – Ілюстрація відмінностей відповідних гістограмм для конкретного ЦЗ

При його стандартному розбитті на $4 \times 4$-блоки: а – гістограма значень кутів між нормованим вектором СНЧ і лівим СНВ, що відповідає максимальному СНЧ, оригінальних

блоків оригінального ЦЗ; б – гістограма $\Gamma_\lambda$ для оригінального ЦЗ; в, г – $\Gamma_\lambda$ для ЦЗ, що піддалося збурній дії (мультиплікативний шум з $D = 0.001, 0.005$ відповідно).

Наслідком твердження 1 при реалізації удосконаленого методу буде збільшення показника $TN$ (2) та незбільшення показника $TP$ у порівнянні з первісним методом [11], що в результаті, виходячи з теоретичних міркувань, повинно привести до відносної порівнянності значень $ACC$ для цих двох методів.

Подальші результати обчислювального експерименту приводяться для алгоритмічної реалізації методу при наступних значення параметрів: $T = 15^\circ$, $P = 3.2$, $h = 1^\circ$, $l \in \{4,8,16,32\}$. В обчислювальному експерименті, метою якого була оцінка, в тому числі порівняльна, ефективності алгоритмічної реалізації удосконалено методу, було задіяно 500 оригінальних ЦЗ розміром $1024 \times 1024$ пікселя.

Результати есперименту, який проводився з використанням двох комп'ютерів (К1, К2) різної конфігурації (табл.1), що стосуються оцінки часових витрат, наведено на рис.2 для $l \in \{4,8,16,32\}$. Отримані результати ілюструють значну часову перевагу запропонованого удосконалення методу для кожного розміру блоку, яка монотонно зростає зі зменшенням їх кількості. Для $l = 32$ зменшення часу на експертизу одного ЦЗ складає 36.4% (для К1) і 30% (для К2) в порівнянні з аналогічним параметром первісного методу (рис.2(б)), середнє ж значення для зменшення часу по всьому експерименту ($l \in \{4,8,16,32\}$) становить 28.6% (пристрій К1), 23.7% (пристрій К2).

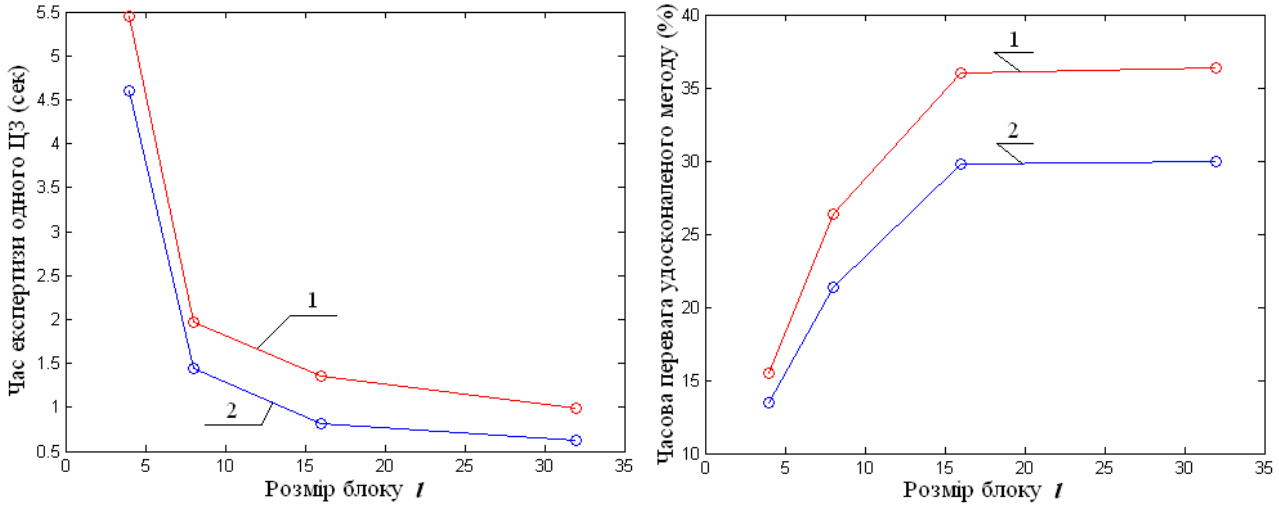
***Зауваження***. Треба зазначити, що наявні значні часові переваги удосконаленого методу відносно методу [11] досягаються не тільки в результаті меньшої обчислювальної складності безпосередньо спектрального розкладання симетризованих матриць блоків в порівнянні з сингулярним розкладанням оригінальних блоків, які відбуваються в ході експертизи, а й завдяки тому, що у вдосконаленому методі вдвічі зменшується кількість досліджуваних при експертизі об'єктів. Дійсно, в [11] будуються і досліджуються гістограми $\Gamma_U$, $\Gamma_V$ кутів $\angle(u_1, \bar{\sigma})$, $\angle(v_1, \bar{\sigma})$ для першого лівого і першого правого СНВ відповідно, тоді як в запропонованому методі лише $\Gamma_\lambda$, оскільки спектральне розкладання симетричної матриці зменшує кількість параметрів, що визначають відповідну матрицю, в порівнянні з сингулярним.

Таблиця 1.

Характеристики обчислювальних пристроїв К1, К2, використаних при тестуванні алгоритмічної реалізації удосконаленого методу виявлення порушення цілісності ЦЗ

| Пристрій | К1 | К2 |
|---|---|---|
| Ім'я пристроя | Aspire ES1-532G | LenovoIdeaPadGaming 3 15ACH6 |
| RAM | 4 ГБ | 16 ГБ |
| Відеокарта | NVIDIA GeForce 920mx | NVIDIA GeForce RTX 3050 Ti |
| Об'єм відеокарти | 2 ГБ | 4 ГБ |
| Процесор | IntelPentium N3710 | AMD Ryzen 5 5600H |
| Кількість ядер процесора | 4 | 6 |
| Кількість потоків процесора | 4 | 12 |

| | | |
|---|---|---|
| Базова швидкість | 1.6 Гц | 3.3 Гц |
| Накопичувач | SSD 512 ГБ | SSD 512 ГБ |




а б

Рисунок 2 – Порівняльна оцінка часових витрат експертизи ЦЗ: а – графіки залежності часу експертизи одного ЦЗ розміром $1024 \times 1024$ пікселя від розміру блоку $l$ (показники К1): 1 – метод [11], 2 – удосконалений метод; б – графік залежності часової переваги удосконаленого методу над методом [11] від розміру блоку на експертизу одного ЦЗ (%) на пристрої: 1 – К1; 2 – К2.

Результат будь-якої збурної дії $\Delta F$, спрямованої на ЦЗ з матрицею $F$, можна представити у вигляді [26]:

$$\overline{F} = F + \Delta F, \tag{21}$$

де $\overline{F}$ – матриця ЦЗ, цілісність якого порушена. З (21) випливає наявність нескінченної кількості різноманітних збурних дій, кожна з яких визначається своєю матрицею $\Delta F$. З урахуванням практичної неможливості розгляду всієї різноманітності збурень, а також того, що результат будь-якої збурної дії загалом може розглядатися як накладання деякого шуму [28], при моделюванні збурних дій в роботі були використані різноманітні шуми з різними параметрами. Результати оцінки, зокрема порівняльної, точності виявлення порушення цілісності $ACC$ (2) в таких умовах наведені в табл.2, де кращий результат в умовах конкретного значення $l$ і конкретної збурної дії для наочності виділений жирним шрифтом.

Для наочності порівняння ефективностей методів визначимо:

$$R = \frac{ACC_2 - ACC_1}{ACC_1} \cdot 100\ \%, \tag{22}$$

де $ACC_1$, $ACC_2$ – значення параметру $ACC$ для [11] і удосконаленого методу відповідно. Оцінка (22) знайшла своє відображення на рис.3, де очевидною є перевага удосконаленого методу для більшості збурних дій при різних розмірах блоків. Така перевага здебільшого пояснюється збільшенням параметру $TN$, що фігурує в (2). Це збільшення $TN$ склало: 13.6, 19.6, 29.8, 26.8% для $l = 4, 8, 16, 32$ відповідно. Максимально підвищення точності виявлення $ACC$ в

порівнянні з первісним методом склало 10.2%. І хоча для деяких збурних дій (гауссівський шум ($D = 0.0001, 0.001$)) при деяких значеннях $l$ спостерігалось зменшення $ACC$ (максимально це зменшення склало 6.2%), в цілому очевидним є підвищення точності виявлення порушення цілісності ЦЗ удосконаленим методом: середнє по експерименту значення $R$ є додатним і складає 5.42%.

Таблиця 2.

Значення $ACC$ в умовах різних збурних дій та різних розмірів, які використовуються при експертизі ЦЗ блоків

| Збурна дія | Розмір блоку $l$ | $ACC$ | |
|---|---|---|---|
| | | Метод [11] | Удосконалений метод |
| Мультиплікативний шум ($D = 0.005$) | 4 | 0.8611 | **0.9111** |
| | 8 | 0.8056 | **0.8722** |
| | 16 | 0.7611 | **0.8389** |
| | 32 | 0.7278 | **0.7889** |
| Гауссівський шум з нульовим математичним очікуванням ($D = 0.0001$) | 4 | 0.5722 | **0.5833** |
| | 8 | **0.5389** | 0.5167 |
| | 16 | 0.5222 | **0.5444** |
| | 32 | **0.5389** | 0.5278 |
| Гауссівський шум з нульовим математичним очікуванням ($D = 0.001$) | 4 | **0.8556** | 0.8056 |
| | 8 | 0.8056 | **0.8556** |
| | 16 | 0.7556 | **0.8056** |
| | 32 | 0.7222 | **0.7667** |
| Гауссівський шум з нульовим математичним очікуванням ($D = 0.01$) | 4 | 0.8667 | **0.9167** |
| | 8 | 0.8111 | **0.8722** |
| | 16 | 0.7611 | **0.8389** |
| | 32 | 0.7278 | **0.7889** |
| Пуассонівський шум | 4 | 0.8667 | **0.9111** |
| | 8 | 0.8111 | **0.8722** |
| | 16 | 0.7611 | **0.8389** |
| | 32 | 0.7278 | **0.7889** |

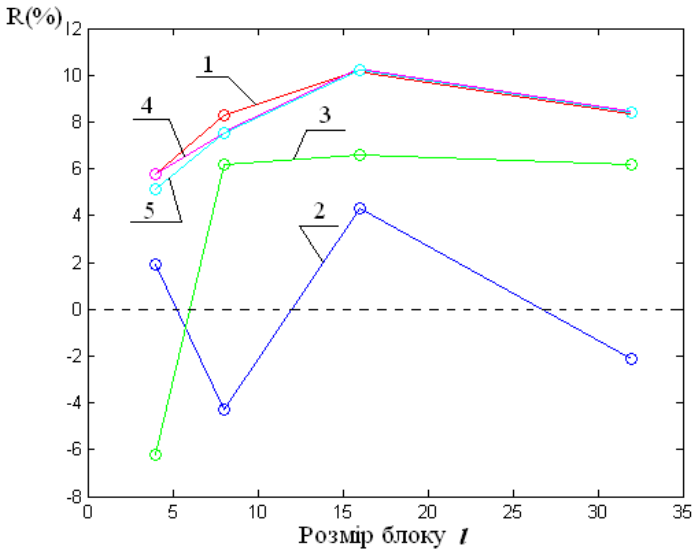



Рисунок 3 – Графіки залежності значення $R$ (22) від розміру блоку в умовах різних збурних дій: 1 – мультиплікативний шум ( $D = 0.005$ ); 2,3,4 – гауссівський шум з нульовим математичним очікуванням і $D = 0.0001$ , $D = 0.001$ і $D = 0.01$ відповідно; 5 – пуассонівський шум

Таким чином, по результатам тестування алгоритмічної реалізації удосконаленого універсального методу виявлення порушення цілісності ЦЗ можна стверджувати, що його ефективність перевищує ефективність методу [11] як по обчислювальній складності (часу експертизи одного ЦЗ), так і по точності виявлення.

**Висновки.** В роботі вирішено важливу та актуальну науково-практичну задачу підвищення ефективності виявлення порушень цілісності ЦЗ шляхом удосконалення універсального методу, запропонованого в [11].

Мета роботи була досягнута завдяки теоретично обгрунтованому вибору способу симетризації матриці $l \times l$-блоку ЦЗ з наступним доведенням того, що для більшості отриманих симетричних блоків, що ставляться у відповідність блокам оригінального ЦЗ, кут між лексикографічно додатним власним вектором, що відповідає максимальному власному значенню симетризованого блока, і нормованим вектором модулів власних значень дорівнює куту між *n*-оптимальним та першим вектором $e_1$ стандартного базису відповідного простору $R^l$. Найбільш важливим результатом роботи є удосконалений універсальний метод виявлення порушення цілісності ЦЗ, готовий до практичної реалізації. Властивості аналізуємих параметрів, зменшення їх кількості в симетричних блоках дають можливість підвищити показник правильно виявлених оригінальних ЦЗ і, як наслідок, точність виявлення в середньому більше, ніж на 5%; зменшити обчислювальну складність і, як наслідок, часові витрати на експертизу ЦЗ в середньому більше, ніж на 23%, в порівнянні з [11].

В даний момент зусилля авторів роботи сконцентровані на уточненні параметрів, що використовуються при алоритмічній реалізації методу, для підвищення показника *TP* з наступним підвищенням точності виявлення порушення цілісності ЦЗ.

ЛІТЕРАТУРА:

1. Информационное противоборство в современных условиях / Л.Г. Пирцхалава, В.А. Хорошко, Ю.Е. Хохлачева, М.Е. Шелест. К.: ЦП «Компринт», 2019. 226 с.

2. Uliyan, D.M., Jalab, H.A., Abdul Wahab, A.W., Sadeghi, S. Image region duplication forgery detection based on angular radial partitioning and Harris key-points / Symmetry. 2016. 8(7). 62.

3. Задірака, В.К. Сучасні методи розв’язання задач інформаційної безпеки / Вісник НАН України. 2014. 5. С. 65–69.

4. Mandal, P.C., Mukherjee, I., Paul, G., Chatterji, B.N. Digital image steganography: A literature survey / Information Sciences. 2022. 609. P. 1451–1488.

5. Борисенко, І.І. Виявлення цифрового фотомонтажу на основі аналізу контрастності зображення / Сучасний захист інформації. 2020. №2. С. 47–51.

6. Joglekar, N.P., Chatur, P.N. A compressive survey on active and passive methods for image forgery detection / International Journal of Engineering and Computer Science. 2015. 4(1). P. 10187–10190.

7. Shwetha, B., Sathyanarayana, S.V. Digital image forgery detection techniques: a survey / ACCENTS Transactions on Information Security. 2017. 2(5). P. 22–31.

8. Thakur, T., Singh, K., Yadav, A. Blind approach for digital image forgery detection / International Journal of Computer Applications. 2018. 179(10). P. 34–42.

9. Chu, X., Li, H. A Survey of Blind Forensics Techniques for JPEG Image Tampering / Journal of Computer and Communications. 2019. 7(10). P. 1–13.

10. Бобок, І.І Розвиток загального підходу до проблеми виявлення порушень цілісності цифрових зображень / Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2017. 2(34). С. 78–88.

11. Kobozeva, A.A., Bobok, I.I., Garbuz, A.I. General principles of integrity checking of digital images and application for steganalysis / Transport and Telecommunication Journal. 2016. 17(2). P. 128–137.

12. Lerch-Hostalot, D., Megias, D. Unsupervised steganalysis based on artificial training sets / Engineering Applications of Artificial Intelligence. 2016. 50. P. 45–59.

13. Bobok, I.I. Steganalysis method for detection of the hidden communication channel with low capacity / Telecommunications and Radio Engineering. 2018. 77(18). P. 1597–1604.

14. Лебедева, Е.Ю., Кобозева, А.А. Основы метода выявления клонированных участков изображения, подвергнутых коррекции яркости / Сучасна спеціальна техніка. 2013. 3(34). С. 17–24.

15. Li, H., Luo, W., Qiu, X., Huang, J. Image forgery localization via integrating tampering possibility maps / IEEE Transactions on Information Forensics and Security. 2017. 12(5). P. 1240–1252.

16. Трифонова, К.О. Метод виявлення порушення цілісності цифрового зображення шумом Перліна / Радіоелектроніка, інформатика, управління. 2017. 2. С. 134–142.

17. Khan, S., Khan, K., Ali, F., Kwak, K.-S. Forgery detection and localization of modifications at the pixel level / Symmetry. 2020. 12(1). 137.

18. Al-Jarrah, M.M, Al-Taie, Z.H., Abuarqoub, A. Steganalysis using LSB-focused statistical features / Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS’17). 2017. Article 54. P. 1–5.

19. Зоріло, В.В., Кіосєва, О.І., Зоріло, І.В. Модифікація алгоритму виявлення штучного підвищення різкості цифрового зображення / Інформатика та математичні методи в моделюванні. 2018. 8(2). С. 156–163.

20. Duan, X.T., Peng, T., Li, F.F., Wang, J. Blind separation of tampered images based on JPEG double compression properties / Journal of University of Jinan (Science and Technology). 2017. 31. P. 87–96.

21. Bobok, I.I., Kobozeva, A.A. Method for detecting of digital image integrity violations due to its block processing / Радіотехніка. 2019. 199. С. 130–141.

22. Geetha, S., Sindhu, S., Kamaraj, N. Close color pair signature ensemble adaptive threshold based steganalysis for LSB embedding in digital images / Transactions on Data Privacy. 2009. 1. P. 140–161.

23. Гонсалес, Р., Вудс, Р. Цифровая обработка изображений. М.: Техносфера, 2006. 1070 с.

24. Bergman, C., Davidson, J. Unitary embedding for data hiding with the SVD / Security, steganography and watermarking of multimedia contents VII, SPIE. 2005. 5681. P. 619–630.

25. Деммель, Д. Вычислительная линейная алгебра: теория и приложения. М.: Мир, 2001. 430 с.

26. Кобозева, А.А. Основы общего подхода к разработке универсальных стеганоаналитических методов для цифровых изображений / Праці Одеського політехнічного університету. 2014. 2. С. 136–146.

27. Гантмахер, Ф.Р. Теория матриц: монография. 5-е изд. М.: Физматлит, 2004. 559 с.

28. Srinivas, R., Panda, S. Performance analysis of various filters for image noise removal in different noise environment / International Journal of Advanced Computer Research. 2013. 3. P. 47–52.

REFERENCES:

1. Pirtskhalava, L.G., Khoroshko, V.A., Khokhlacheva, J.E., Shelest, M.E. (2019), “Informatsionnoe protivoborstvo v sovremennyh usloviyah” [Information Warfare in Modern Conditions], Komprint, Kyiv, 226 p.

2. Uliyan, D.M., Jalab, H.A., Abdul Wahab, A.W., Sadeghi, S. (2016), “Image region duplication forgery detection based on angular radial partitioning and Harris key-points”, Symmetry, 8(7), 62.

3. Zadiraka, V.K. (2014), “Suchasni metody rozvyazannya zadach informatsiynoy bezbeky” [Modern Methods for Solving the Tasks of Information Safety], Visnyk of the National Academy of Sciences of Ukraine, 5, pp. 65–69.

4. Mandal, P.C., Mukherjee, I., Paul, G., Chatterji, B.N. (2022), “Digital image steganography: A literature survey”, Information Sciences, 609. pp. 1451–1488.

5. Borysenko, I.I. (2020), “Vyyavlennya tsyfrovogo fotomontazhu na osnovi kntrstnosti zobrazhennya” [Detection of digital photomontage based on image contrast analysis], Modern Information Security, 2, pp. 47–51.

6. Joglekar, N.P., Chatur, P.N. (2015), “A compressive survey on active and passive methods for image forgery detection”, International Journal of Engineering and Computer Science, 4(1), pp. 10187–10190.

7. Shwetha, B., Sathyanarayana, S.V. (2017), “Digital image forgery detection techniques: a survey”, ACCENTS Transactions on Information Security, 2(5), pp. 22–31.

8. Thakur, T., Singh, K., Yadav, A. (2018), “Blind approach for digital image forgery detection”, International Journal of Computer Applications, 179(10), pp. 34–42.

9. Chu, X., Li, H. (2019), “A Survey of Blind Forensics Techniques for JPEG Image Tampering”, Journal of Computer and Communications, 7(10), pp. 1–13.

10. Bobok, I.I. (2017), “Rozvytok zagalnogo pidhodu do problem vyyavlennya porushen’ tsilisnosti tsyfrovyh zobrazhen” [Development of a general approach to the problem of detecting integrity violations of digital images] / Legal, Regulatory and Metrological Support of Information Security System in Ukraine, 2, pp. 78–88.

11. Kobozeva, A.A., Bobok, I.I., Garbuz, A.I. (2016), “General principles of integrity checking of digital images and application for steganalysis”, Transport and Telecommunication Journal, 17(2), pp. 128–137.

12. Lerch-Hostalot, D., Megias, D. (2016), “Unsupervised steganalysis based on artificial training sets”, Engineering Applications of Artificial Intelligence, 50, pp. 45–59.

13. Bobok, I.I. (2018), “Steganalysis method for detection of the hidden communication channel with low capacity”, Telecommunications and Radio Engineering, 77(18), pp. 1597–1604.

14. Lebedieva, E.J., Kobozieva, A.A. (2013), “Osnovy metoda vyyavleniya klonirovannyh uchastkov izobrazheniy, podvergnutyh korrektsii yarkosti” [Fundamentals of the method for detecting cloned image areas subjected to brightness correction], Modern Special Technics, 3, pp. 17–24.

15. Li, H., Luo, W., Qiu, X., Huang, J. (2017), “Image forgery localization via integrating tampering possibility maps”, IEEE Transactions on Information Forensics and Security, 12(5), pp. 1240–1252.

16. Tryfonova, K.O. (2017), “Metod vyyavlennya porushennya tsilisnosti tsyfrovogo zobrazhennya shumom Perlina” [A method of detecting a violation of the integrity of a digital image by Perlin noise], Radio Electronics, Computer Science, Control, 2, pp. 134–142.

17. Khan, S., Khan, K., Ali, F., Kwak, K.-S. (2020), “Forgery detection and localization of modifications at the pixel level”, Symmetry, 12(1), 137.

18. Al-Jarrah, M.M, Al-Taie, Z.H., Abuarqoub, A. (2017), “Steganalysis using LSB-focused statistical features”, Proceedings of the International Conference on Future Networks and Distributed Systems (ICFNDS’17), article 54, pp. 1–5.

19. Zorilo, V.V., Kioseva, O.I., Zorilo, I.V. (2018), “Modyfikatsiya algorytmu vyyavlennya shtuchnogo pidvyschennya rizkosti tsyfrovogo zobrazhennya” [Modification of algorithm for detecting artificial improvement of sharpness of the digital image], Informatics and Mathematical Methods in Simulation, 2, pp. 156–163.

20. Duan, X.T., Peng, T., Li, F.F., Wang, J. (2017), “Blind separation of tampered images based on JPEG double compression properties”, Journal of University of Jinan (Science and Technology), 31, pp. 87–96.

21. Bobok, I.I., Kobozeva, A.A. (2019), “Method for detecting of digital image integrity violations due to its block processing”, Radiotechnika, 199, pp. 130–141.

22. Geetha, S., Sindhu, S., Kamaraj, N. (2009), “Close color pair signature ensemble adaptive threshold based steganalysis for LSB embedding in digital images”, Transactions on Data Privacy, 1, pp. 140–161.

23. Gonzalez, R.C., Woods, R.E. (2006), “Tsifrovaya obrabotka izobrazheniy” [Digital Image Processing], Technosfera, Moscow, 1070 p.

24. Bergman, C., Davidson, J. (2005), “Unitary embedding for data hiding with the SVD”, Security, steganography and watermarking of multimedia contents VII, SPIE, 5681, pp. 619–630.

25. Demmel, D. (2001), “Vychislitelnaya linejnaya algebra: teoriya i prilozheniya” [Numerical Linear Algebra: Theory and Applications], Mir, Moscow, 430 p.

26. Kobozeva, A.A. (2014), “Osnovy obschego podhoda k razrabotke universalnyh steganoanaliticheskih metodov dlya tsifrovyh izobrazheniy” [A basis of common approach to the development of universal steganalysis methods for digital images], Odes’kyi Politechnichnyi Universytet. Pratsi, 2, pp 136–146.

27. Gantmacher, F.R. (2004), “Teoriya matrits: monografiya” [Matrix Theory], FizMatLit, Moscow, 559 p.

28. Srinivas, R., Panda, S. (2013), “Performance analysis of various filters for image noise removal in different noise environment”, International Journal of Advanced Computer Research, 3, pp. 47–52.

**Doctor of Technical Sciences, Kobozieva A.A.,**
**Doctor of Technical Sciences, Maevsky D.,A.**
**Kyryliuk V.O.**

## METHOD OF DETECTING VIOLATION OF DIGITAL IMAGE INTEGRITY BASED ON SPECTRAL DECOMPOSITION OF SYMMETRIZED BLOCK MATRIX

***The work considers an important scientific and practical task of increasing the effectiveness of detecting violations of the integrity of information, in particular digital images, which is its common representation, which is becoming one of the main ones for specialists in the field of information and cyber security today. Undetected, unauthorized changes to information in a timely manner can lead to negative, catastrophic consequences for individuals, enterprises, banks, firms, and for humanity as a whole, when it comes to information that constitutes a state secret, contains data from the military industry, nuclear energy, chemical industry, etc., which determines the relevance of the problem under consideration. The main result***

***of the work is an improved universal method for detecting violations of the integrity of a digital image, ready for practical implementation, the theoretical basis of which is based on the analysis of eigenvalues and eigenvectors of symmetric blocks of the image matrix, which correspond to the original blocks. The paper substantiates the method of symmetrization of the block matrix, which allows to significantly (by more than 23%) reduce computational and, as a result, time costs for image examination in comparison with the time costs of the prototype method. It is proved that for the majority of the obtained symmetric blocks that correspond to the blocks of the original CG, the angle between the eigenvector corresponding to the maximum eigenvalue of the block and the normalized vector of the modules of the eigenvalues is equal to a certain value that does not depend on the specifics of the original image, but is sensitive to its changes, which made it possible to ensure the universality of the method and increase its efficiency in the sense of the accuracy of detecting a violation of the integrity of the image by more than 5%, compared to the analogue. The significance of the obtained results lies in ensuring, due to the use of the proposed method, an increase in the efficiency of the process of detecting violations of the integrity of the image according to the criteria of computing (time) costs for the examination of one image and the accuracy of detection.***

***Keywords: digital image, integrity violation, eigenvector, eigenvalue.***

УДК 004.89

д.т.н., проф. **Лєнков С.В.** (ВІКНУ)
к.т.н., доц., **Джулій В.М** (ХмНУ)
**Солодєєва Л.В.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2022/77-09

# МЕТОД ПРОТИДІЇ ПОШИРЕННЮ ТА ВИЯВЛЕННЯ ШКІДЛИВОЇ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

***В роботі продено дослідження задачі виявлення та протидії поширенню у соціальних мережах шкідливої інформації, в тому числі «фейкових новин». Особливо гостро стоїть необхідність протидії поширенню у соціальних мережах таких новин, що породжують хвилі паніки, які виникають під час пандемії. На теперішній час – війна в Україні. Фейкові новини поширюються у соціальних мережах у шість разів швидше, ніж правдиві дописи. Російська пропаганда стала одним з головних елементів війни в Україні, її якісно закамуфльовано під вигляд матеріалів західних ЗМІ - DW, CNN або BBC. Основна складність виявлення та протидії поширенню шкідливої інформації в соціальних мережах безпосередньо слідує із використанням на сучасному етапі тенденцій розвитку інформаційно - технологічної сфери, а саме: збільшення швидкості поширення шкідливої інформації в соціальних мережах; швидкості виникнення нових джерел поширення шкідливої інформації; збільшення об'єму інформації, що містить шкідливі повідомлення; швидкості тиражування повідомлень в мережі; кількості сценаріїв привернення уваги аудиторії; рівня гетерогенності даних. За своєю архітектурою соціальні мережі є багатокомпонентними рішеннями, в архітектурі мережі знаходяться: компоненти, які здійснюють обробку контенту; компоненти, які забезпечують функції маркетингу, адміністрування, зберігання даних. Соціальні мережі не містять окремого компонента виявлення та протидії поширенню шкідливій інформації в мережі.***

***Проведений аналіз та дослідження оцінювання ефективності інформаційно-аналітичних систем та інформатизації процесів, показали, що проблема виявлення та протидії поширенню в соціальних мережах шкідливої інформації не може вважатися вирішеною і вимагає на даному етапі проведення нових досліджень та дозволяє визначити загальні вимоги до системи протидії, в основу реалізації якої, покладено модельно-методичний апарат. З метою підвищення ефективності системи протидії в Інтернет - мережах вирішена задача розробки відповідного підходу підвищення обґрунтованості прийнятого рішення на протидію поширенню та виявлення шкідливої інформації за рахунок збільшення числа параметрів, що враховуються при виборі інформаційного об'єкта впливу та дійових контрзаходів. Вирішення поставленої задачі, досягається за рахунок проведення ранжування контрзаходів та аналізу джерел мережі шкідливої інформації. Запропонований метод протидії та виявлення в соціальних мережах поширенню шкідливої інформації, ґрунтується на використанні запропонованих моделей, алгоритмів, забезпечує, на відміну від аналогів, аналіз інформації соціальних мереж; формування списків інформаційних об'єктів впливу для проведення протидії об'єктам, сортування інформаційних об'єктів; надання оператору системи протидії пропонованого та альтернативних варіантів з обґрунтуванням вибору. Розроблений метод виявлення та протидії поширенню шкідливої інформації в соціальних мережах відрізняється від існуючих, використанням запропонованих алгоритмів оцінки джерел повідомлень, аналізом та ранжуванням контрзаходів, в результаті підвищується обґрунтованість прийняття рішення про протидію поширенню шкідливої інформації та вибору***

***контрзаходу, відповідним чином скорочується час роботи оператора системи у процесі протидії поширенню шкідливої інформації у соціальних мережах.***

***Ключові слова: шкідлива інформація, соціальні мережі, контрзаходи, джерела повідомлень, метод протидії, інформаційна система.***

**Вступ.** На сучасному етапі, глибина проникнення у повсякденне життя людства, соціальних мереж є значною. Перевагою соціальних мереж є можливість оперативно висловлювати свою думку учасникам комунікації, значній кількості групі людей, публікувати медіа-, відео файли. Соціальні мережі є не лише засобом спілкування групи людей, а також інструментом поширення інформації в мережі, в тому числі шкідливої інформації. Очевидною проблемою інформаційної безпеки суспільства, сьогодення стала шкідлива інформація, також необхідно зазначити, що злочинні та терористичні угрупування беруть на озброєння, дедалі частіше, засоби інформаційного впливу, розробляють та пишуть стратегії, спрямовані на залучення нових адептів та розширення сфери впливу через соціальні мережі. Таким чином, однією зі складових надійного забезпечення інформаційної безпеки держави є проведення аналізу, виявлення, моніторинг та активна протидія розповсюдженню шкідливої інформації в соціальних мережах [1,2].

До шкідливої інформації, поширеної в соціальних мережах, частіше відносять «фейкові новини». Особливо гостро стоїть необхідність протидії поширенню у соціальних мережах таких новин, що породжують хвилі паніки, які виникають під час пандемії. На теперішній час – війна в Україні. Фейкові новини поширюються у соціальних мережах у шість разів швидше, ніж правдиві дописи. Російська пропаганда стала одним з головних елементів війни в Україні, її якісно закамуфльовано під вигляд матеріалів західних ЗМІ - DW, CNN або BBC.

**Аналіз останніх досліджень та постановка задачі.** Проблема виявлення та протидії поширенню у соціальних мережах шкідливої інформації, в тому числі «фейкових новин», має недостатньо науково-технічних рішень. Відомі підходи та засоби протидії виявлення в соціальних мережах шкідливої інформації не відповідають вимогам до адекватності, повноти, швидкості та точності прийнятих рішень. Дана ситуація зумовлена кількома причинами: система розділена на два не пов'язаних модулі – моніторинг та протидія, між якими знаходиться оператор. Соціальні мережі складаються з множини різнорідних повідомлень, які мають складну структуру, дана особливість повідомлень не в повній мірі враховується при виборі засобів протидії – джерело, тип повідомлення, а також інші характеристики. Необхідно обробляти надвеликі об’єми інформації в реальному масштабі часу і в стислий термін вибирати відповідний інструмент для проведення контрзаходу протидії поширенню шкідливої інформації, оператор системи протидії в ручному режимі не в змозі зупинити поширення шкідливої інформації в соціальній мережі [3,4].

На теперішній час, основна складність виявлення та протидії поширенню шкідливої інформації в соціальних мережах безпосередньо слідує із використанням на сучасному етапі тенденцій розвитку інформаційно - технологічної сфери, а саме: збільшення швидкості поширення шкідливої інформації в соціальних мережах; швидкості виникнення нових джерел поширення шкідливої інформації; збільшення об’єму інформації, що містить шкідливі повідомлення; швидкості тиражування повідомлень в мережі; кількості сценаріїв привернення уваги аудиторії; рівня гетерогенності даних. Таким чином, розглянуті тенденції поширення шкідливої інформації в Інтернет мережах, зумовлюють необхідність підвищення ефективності протидії та виявлення в соціальних мережах шкідливої інформації, враховуючи також при цьому, обґрунтованість та оперативність [5,6].

Швидкість змін в інформаційному полі суспільства є досить великою, уповільнена та невірна реакція з боку органів безпеки держави може призвести до катастрофи суспільства.

Адаптація до змін в інформаційному полі держави, потребує на сучасному етапі значних і швидких коригувань у сфері захисту інформаційного поля держави. Необхідно бути більш здатним краще протидіяти та відновлюватися після кризи, більш обізнаними щодо характеру та потенціалу кризових ситуацій.

Під категорію шкідливої інформації, з погляду забезпечення державної безпеки підлягають наступні види інформації: інформація, включена до державного списку екстремістських матеріалів [2]; інформація, що ідентифікується як заборонена до поширення в державі [7]; персональні дані; інформація для службового користування; конфіденційна інформація. Забороняється поширення інформації в Інтернет мережі, спрямованої на пропаганду війни, розпалювання релігійної, національної, расової ненависті та ворожнечі, інформації, за поширення якої передбачено адміністративну, кримінальну відповідальність.

За своєю архітектурою соціальні мережі є багатокомпонентними рішеннями, в архітектурі мереж знаходяться: компоненти, які здійснюють обробку контенту; компоненти, які забезпечують функції маркетингу, адміністрування, зберігання даних. Соціальні мережі не містять окремого компонента виявлення та протидії поширенню шкідливій інформації [8,9].

Проведений аналіз та дослідження оцінювання ефективності інформаційних систем та інформатизації процесів, показали, що проблема виявлення та протидії в соціальних мережах шкідливої інформації не може вважатися вирішеною і вимагає на даному етапі проведення нових досліджень.

Протидія поширенню шкідливої інформації у соціальних мережах є важливим елементом інформаційної безпеки особистості, суспільства, держави, проте більшість систем, на теперішній час не враховує простір функціональності системи виявлення та протидії поширенню шкідливою інформації, системи розділені на два модулі: моніторинг та протидія, необхідна автоматизація процесу протидії. Соціальні мережі мають складну структуру, параметри повідомлень та джерел не в повній мірі враховуються під час вибору засобів протидії та виявлення шкідливої інформації. При розробці методу протидії поширенню шкідливої інформації в Інтернет мережі, необхідно: в повній мірі, враховувати кількість повідомлень на сторінці, характеристики джерела, зворотній зв'язок від джерела та аудиторії повідомлень; підтримувати дві стадії роботи системи протидії: налаштування, експлуатація; ранжувати контрзаходи з урахуванням коефіцієнтів складності [1,10].

**Дослідження задач побудови систем протидії поширенню та виявлення шкідливої інформації в соціальних мережах.** Проведений порівняльний аналіз досліджень в області протидії та виявлення шкідливої інформації в соціальних мережах дозволив визначити загальні вимоги до системи протидії, в основу реалізації, покладено модельно-методичний аппарат [1,2,5, 7-9]. Розглянемо необхідний фундамент функціональності системи протидії поширенню та виявлення шкідливої інформація в соціальних мережах (рис. 1).

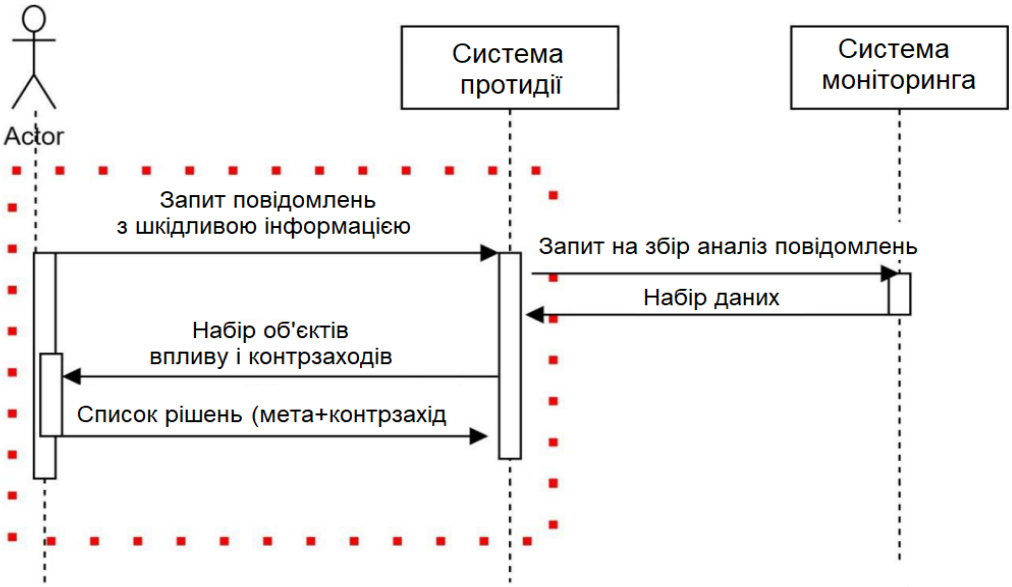



Рисунок 1 – Фундамент функціональності системи протидії поширенню та виявлення шкідливої інформації у соціальних мережах

Система протидії (рис. 1) може бути центральним елементом у процесі виявлення шкідливих повідомлень в соціальних мережах. Процеси у системі протидії та виявлення шкідливих повідомлень в Інтернет мережі можуть бути автоматизовані з використанням запропонованих алгоритмів і відповідних програмних компонентів.

Вимоги до системи протидії розділимо на дві групи: функціональні та не функціональні. Функціональні вимоги можуть бути реалізовані шляхом проектування та розробки архітектури компонентів, програмних прототипів. Функціональні вимоги - функції, які має виконувати система протидії. Не функціональні вимоги можуть бути реалізовані шляхом розробки відповідних моделей та алгоритмів. Не функціональні вимоги описують цільові характеристики системи: оперативність, вимоги щодо обґрунтованості та ресурсоспоживання.

Функціональні вимоги до системи виявлення та протидії поширенню шкідливої інформації в соціальних мережах: формування задачі на збір повідомлень; аналіз повідомлень для системи моніторингу; аналіз джерел повідомлень в отриманому наборі даних; налаштування доступних заходів виявлення та протидії поширенню шкідливоїінформації в інформаційно-аналітичній системі; сортування та ранжування об'єктів впливу на отриманому наборі даних; вибір засобів впливу для протидії; сортування та ранжування доступних контрзаходів з бази даних контрзаходів для відповідного набору отриманих даних; генерація звітів про роботу системи виявлення та протидії в адаптованому вигляді, для адміністратора системи; генерація звітів про отримані результати у адаптованому вигляді, для експерта з інформаційної безпеки організації.

Задача дослідження полягає у розробці: моделей - шкідливої інформації, джерела повідомлень та соціальної мережі; алгоритмів проведення аналізу джерел поширення шкідливої інформації у соціальних мережах та проведення ранжування контрзаходів; методу виявлення та протидії поширенню шкідливої інформації у соціальних мережах з урахуванням вимог до обґрунтованості; архітектури компонентів інформаційно-аналітичної системи протидії поширеню шкідливої інформації в соціальних мережах.

**Метод протидії поширенню та виявлення шкідливої інформації в соціальних мережах.** Протидія поширенню шкідливої інформації може здійснюватися на основі проведеного аналізу та дослідження джерел повідомлень [1,5,7,10]. Об'єктом деструктивного

впливу шкідливої інформації є користувачі соціальних мережі. Кожен користувач залишає відповідний слід під час перегляду повідомлення в мережі і може залишити відповідну реакцію. Таким чином, алгоритм оцінки джерел повідомлень, повинен враховувати зворотній в'язок від користувачів шкідливої інформації в соціальній мережі, у процесі інформаційного обміну. Множина $ACTIVITY$ включає всі ознаки зворотнього зв'язку від користувачів шкідливої інформації соціальної мережі (1):

$$ACTIVITY\{countrepost, countLike, countComment, countView\}, \quad (1)$$

де $countrepost$ – кількість посилань на джерело («репостів»), $countLike$ - кількість позначок, $countComment$ – кількість коментарів, $countView$ – кількість переглядів. До множини $SOURCE\{sourceID, messageURL\}$ входить ідентифікатор джерела, адреса повідомлень у соціальній мережі.

Таким чином, необхідно знайти кортеж атрибутів, на основі елементів множини $ACTIVITY$ і відношення *R*, які характеризуть $SOURCE$ (2).

$$R(SOURCE, MESSAGE) - < index_{active}, index_{viewability}, index_{impact} >, \quad (2)$$

де $index_{active}$ - індекс активності, $index_{viewability}$ - індекс перегляду, $index_{impact}$ - індекс впливу джерела повідомлень.

Значення індексів перегляду, активності, впливу джерела повідомлень знаходиться в діапазоні від 0 до 2, до значень індексів застосовується нормування – порівняльна нормалізація, ідеальне значення є максимум.

Розглянемо алгоритм оцінки джерел повідомлень соціальної мережі:

1. На вхід алгоритму подається кортеж: $< sourceID, messageURL, repostCount, likesCount, commentCount, viewCount >$.

2. Обчислення індексу активності джерел повідомлень соціальної мережі: формуються хеш-таблиці (key-value) - <sourceID, urlCOUNTER>, <messageURL, likesCount>, <messageURL, commentCount>, <messageURL, repostCount>; в наступній хеш-таблиці сумуються показники commentCount, repostCount, likesCount для messageURL, формується, в даному випадку кортеж $< message.SourceID, activityIndex >$; значення з кортежу $< message.SourceID, activityIndex >$ сумуються, результат ділиться на показник *urlCOUNTER* з першої хеш-таблиці, таким чином формується набір індексів активності джерел повідомлень, до яких застосовується нормування.

3. Обчислення індексу перегляду джерел повідомлень соціальної мережі: формуються хеш-таблиці (key-value), $\{SourceID : urlCOUNTER, messageURL : viewCount\}$. Значення viewCount всіх $messageURL$ сумуються і отриманий результат ділиться на $urlCOUNTER$. В результаті формується кортеж $< SourceID, viewIndex >$. Індекси переглядів нормуються.

4. Обчислення індексу впливу джерела повідомлень соціальних мереж: для кожного джерела повідомлень перемножуються індекси переглядів та активності, в результаті отримаємо значення індексу впливу, також для нього використаємо порівняльне нормування. На виході алгоритму оцінки джерел повідомлень соціальної мережі формується кортеж $< sourceID, activityIndex, viewIndex, impactIndex >$.

Алгоритм оцінки джерел повідомлень соціальної мережі в процесі інформаційного обміну враховує зворотній зв'язок, його кількісні характеристики від аудиторії поширення шкідливої інформації, перетворює їх у якісні індекси.

Алгоритм сортування об'єктів впливу соціальної мережі. В основі існуючих рішень, методів протидії поширенню шкідливої інформації в соціальних мережах лежать підходи виявлення із шкідливою інформацією інформаційних об'єктів. Розглянуті підходи опираються

на концепцію - «виявлення-протидія» інформаційних об'єктів [3,10]. Інформаційні об'єкти, які містять джерела шкідливої інформації в соціальних мережах - мільйони. Інформаційні об'єкти можливо поділити за індексами активності та потенціалом джерела, таким чином, можна застосувати фільтр у процесі вибору інформаційного об'єкта протидії та задати пріоритет. Алгоритм сортування інформаційних об'єктів впливу соціальної мережі пов'язаний із алгоритмами оцінкою джерел повідомлень та ранжування за потенціалом, отримує вхідні дані з них, сортує інформаційні об'єкти впливу за пріоритетом на виході. Цільова функція об'єктів впливу за пріоритетом задається наступною формулою:

$$f(S) \to l_{pr}^{s} = l_{p}^{s} + l_{i}^{s} = [0,4], \tag{3}$$

де $S$ – джерело повідомлень, $l_{pr}^{s}$ - пріоритет джерела повідомлень, $l_{p}^{s}$ - потенціал, $l_{i}^{s}$ - індекс впливу.

Правила вибору об'єкта впливу *Target:* $\left\{source \in TARGET \mid I_{pr}^{s} \cong \max\right\}$; $\left\{message \in TARGET \mid I_{pr}^{s} \cong \min\right\}$, де $TARGET$ - множина інформаційних об'єктів впливу.

Алгоритм сортування об'єктів впливу соціальної мережі наведено на рис. 2. На вхід алгоритму сортування об'єктів (рис. 2) передається набір кортежів $< messageURL, sourceID, potentialIndex, activityIndex, viewIndex, impactIndex >$. На першому етапі роботи алгоритму обчислюється середнє арифметичне індексу впливу всіх джерел повідомлень, виділяються об'єкти з низьким та високим пріоритетом. Формуються кортежі з індексом пріоритету $1 \le l_{pr}^{s} \le 3$ $< messageURL, sourceID, potentialIndex, activityIndex, viewIndex, impactIndex >$.

Результат роботи алгоритму - набір кортежів та два списки: набір кортежів *Priority_Medium*, передається оператору для вибору та додаткової оцінки інформаційного об'єкта впливу між адресою сторінки в соціальній мережі та адресою повідомлення; *Priority_High* – цілі *Target*, *sourceID* є інформаційним об'єктом впливу, для прийняття заходів протидії мають високий пріоритет; *Priority_Low* – цілі *Target*, *messageURL* є інформаційним об'єктом впливу, для прийняття заходів протидії мають низький пріоритет. Алгоритм сортування інформаційних об'єктів впливу соціальної мережі формує пріоритетні списки для протидії поширенню шкідливої інформації.

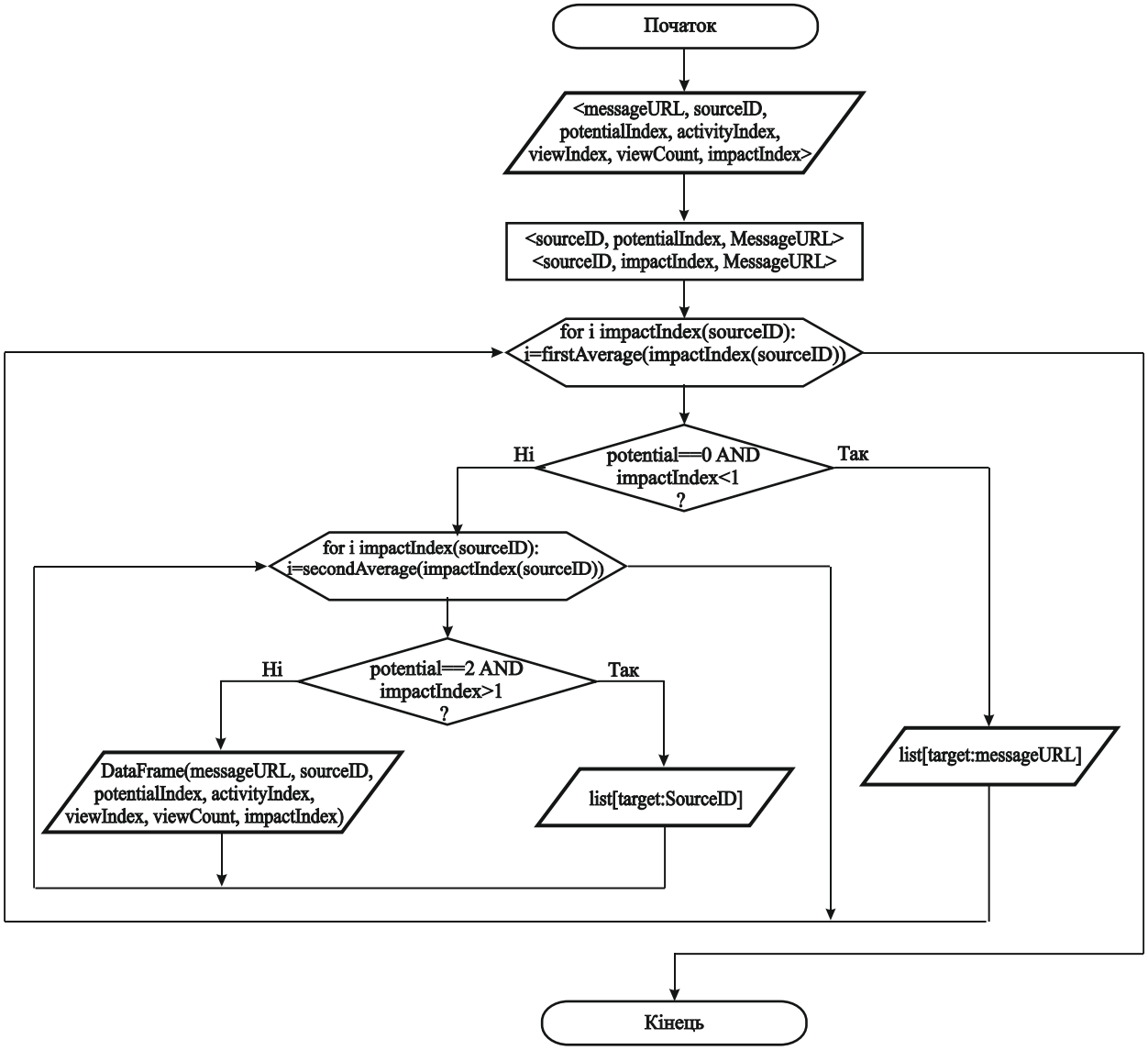



Рисунок 2 – Алгоритм сортування об'єктів впливу соціальної мережі

Метод протидії поширенню в соціальних мережах шкідливої інформації вирішує задачу інформаційної підтримки процесу ухвалення рішень та включає: проведення аналізу зібраної та обробленої інформації; вироблення, на основі проведеного аналізу повідомлень, варіантів рішень; проведення оцінки отриманих варіантів, вибір найкращого варіанта; надання обраного та альтернативних варіантів, особі, яка приймає рішення, з обґрунтуванням вибору.

Метод протидії, відповідно до життєвого циклу інформаційних систем, поділяється на два етапи: налаштування та експлуатацію. На стадії формування вхідних даних та налаштування системи протидії надаються: списки доступних у системі контрзаходів, їх коефіцієнти; списки інформаційних загроз; списки доступних агентів реалізації; формується список ранжованих контрзаходів. Стадія експлуатації включає: аналіз об'єктів впливу та їх сортування; отримання інформації від системи моніторингу; формування пар ціль-контрзахід; запуск протидії.

На рисунках 3 та 4 наведено загальне представлення методу протидії в соціальних мережах поширенню та виявлення шкідливої інформації.

Стадія налаштування методу протидії та формування вихідних даних включає:

1. Налаштування системи запитів. Оператор, відповідно до інформаційно-ознакової моделі загроз [7], формує список інформаційних загроз та їх ознак. Після отримання від

оператора інформаційних загроз та їх ознак, формується перелік загроз та ознак (табл. 1). Списки загроз та їх ознак, отриманих в результаті виконання налаштування системи запитів, зберігаються у загальному сховищі даних.

Таблиця 1

Список загроз та їх ознак

| Загроза | Шкідлива інформація у соцмережах | Інформаційні ознаки |
|---|---|---|
| $T_1$ | Наркотики купити | $a_1$ |
| | Наркотики рецепт виготовлення | $a_2$ |
| $T_2$ | Вибуховий пристрій набір для збирання з інструкцією | $b_1$ |
| $T_3$ | Секретний алгоритм захисту телефонних дзвінків | $c_1$ |

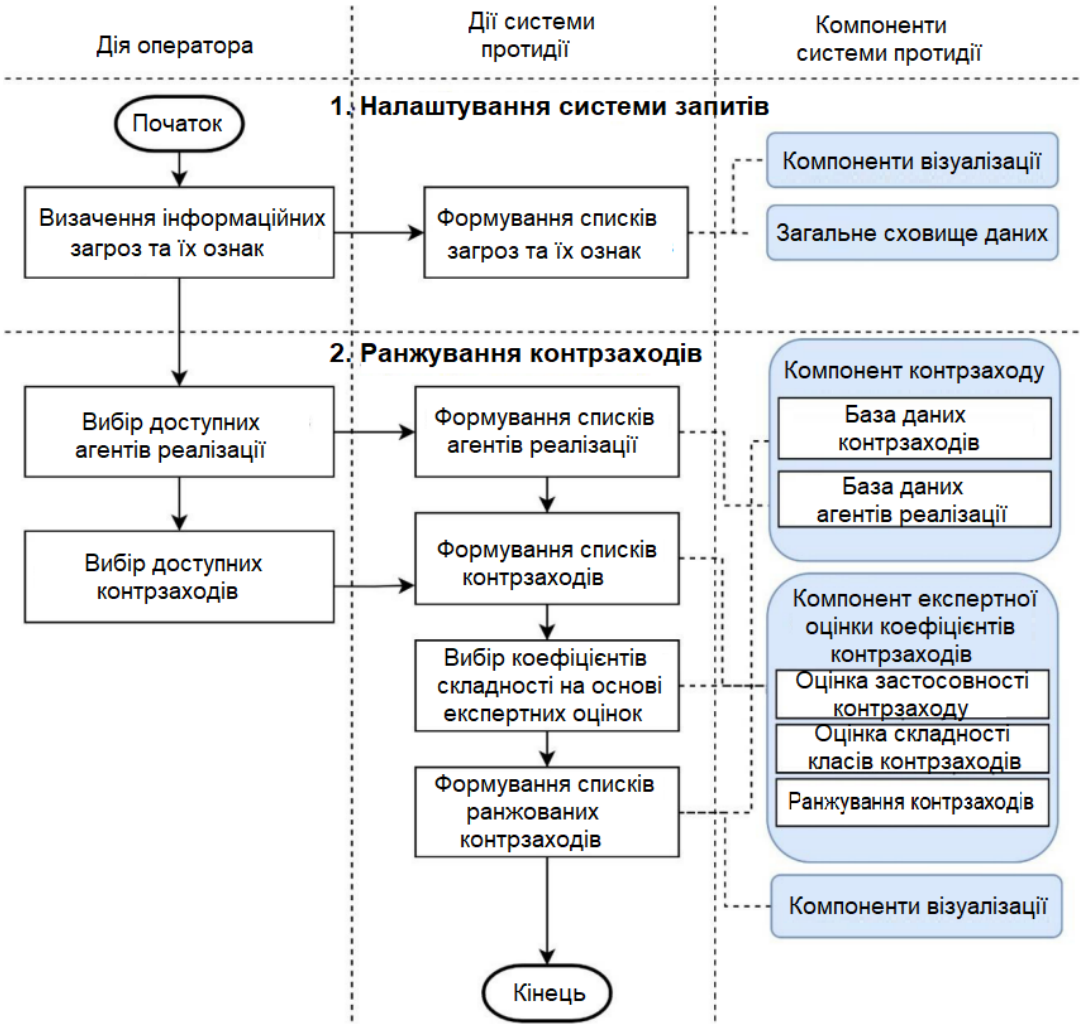



Рисунок 3 – Метод протидії в соціальних мережах поширенню та виявлення шкідливої інформації

2. Ранжування контрзаходів. Оператор вибирає доступні агенти реалізації: браузер; оператор зв'язку; black_list; антивірус; система батьківського контролю; операційна система. Формується та зберігається список доступних агентів реалізації. Оператор вибирає доступні контрзаходи: блокування через соцмережу; блокування через оператора зв'язку; блокування через спеціальне програмне забезпечення; блокування через black_list; фільтрація через систему батьківського контролю; фільтрація через антивірус. Формується список контрзаходів протидії, на основі експертних оцінок формуються коефіцієнти складності, згідно алгоритму вибору коефіцієнтів складності. Алгоритм вибору коефіцієнтів складності використовує наступні величини: вага $w_i$, визначає внесок у складність контрзаходу класу $KC_i$; рівень складності $lc_{i,j}$, визначає внесок у складність контрзаходу екземпляра класу $kc_{i,j}$; початкова складність $cw_x$ заходу протидії. Величини залежать від кваліфікації співробітників, доступних ресурсів та задаються експертним шляхом. Для вибору значень пропонується використовувати Дельфі-метод експертних оцінок, в результаті серії дій експертів формується узагальнений результат, який дозволяє уникнути суб'єктивних оцінок [4,11].

Алгоритм вибору коефіцієнтів складності включає наступні кроки:

1. Вибір експертів. Групі експертів надаються відомості про можливі заходи протидії.

2. Голосування. Визначаються властивості які застосовуються до заходів протидії. Для кожної величини $cp_{x,i,j}$ експерти виставляють оцінки застосовності від одиниці до десяти.

3. Опрацювання результатів. Виконується усереднення отриманих значень (4):

$$cp_{x,i,j} = \frac{\sum_{l=1}^{N} cp_{x,i,j,l}}{10 \cdot N} \tag{4}$$

Отримане значення округляється до 0 чи 1, і визначається, чи застосовний даний екземпляр $kc_{i,j}$ класу властивостей заходів протидії для даного контрзаходу.

4. Голосування. Для уточнючих величин $\left(w_i, lc_{i,j}\right)$ експерти виставляють оцінки складності від 1 до 10.

5. Опрацювання результатів. Виконується усереднення отриманих значень (5):

$$\begin{aligned} w_i &= \frac{\sum_{l=1}^{N} w_{i,l}}{N} \\ lc_{i,j} &= \frac{\sum_{l=1}^{N} lc_{i,l}}{N} \end{aligned} \tag{5}$$

6. Голосування. Експерти для заходів протидії виставляють оцінки початкової складності $cw_x$ від 1 до 10.

7. Опрацювання результатів. Виконується усереднення для початкової складності отриманих значень (6).

$$coefficient\left(cw_i\right) = \frac{\sum_{l=1}^{N} cw_{x,l}}{N} \tag{6}$$

Результатом роботи алгоритму є отримані показники визначення складності застосування заходів протидії.

Розглянемо метод протидії в соціальних мережах поширенню та виявлення шкідливої інформації на стадії експлуатації. Етап експлуатації аналізу об'єктів впливу та запиту інформації містить наступні кроки:

1. Запит на збирання інформації (даних). Оператор із збереженого списку вибирає інформаційні загрози, задає нові інформаційні ознаки, у випадку необхідності. Оператор запускає процес збирання інформації, система протидії поширенню та виявлення шкідливої інформації надсилає запит до моніторингу зовнішніх систем та отримує, як результат, набір даних із повідомленнями, джерелами та параметрами, що містять шкідливу інформацію, необхідними для подальшого аналізу.

2. Сортування та ранжування об'єктів впливу: джерела ранжуються за потенціалом та оцінюються, формуються кортежі $< messageURL, sourceID, potentialIndex, activityIndex, viewIndex, impactIndex >$. Далі сортуються інформаційні об'єкти впливу за пріоритетом, формуються списки, які в результаті передаються оператору.

3. Протидія поширенню шкідливої інформації в соцмережах. Оператор системи отримує інформацію про потенціал джерела мережі, на яке, опублікованих на його сторінці у соціальній мережі, впливає кількість повідомлень, інформацію про пріоритет впливу, на який впливає кількість переглядів, рівень активності користувачів джерела. Оператор коригує списки об'єктів впливу, формуються пари ціль-контрзахід, перевірка відповідних пар оператором та запуск системи протидії поширенню шкідливої інформації в соціальних мережах. Оператор передає команду на запуск системи протидії поширенню шкідливої інформації в соціальних мережах, запускається через агентів реалізації, демонструє проміжні результати процесу проведення протидії оператору системи. Формується звіт про результати роботи системи протидії, інформаційній загрозі та визначеними у ході експлуатації системи об'єктів впливу протидію.

Вхідними даними методу протидії поширенню шкідливої інформації в соціальних мережах є: параметри об'єктів впливу, відповідно до яких оператор розподіляє черговість прийняття рішення про протидію; сформовані пари ціль-контрзахід для протидії поширенню шкідливої інформації у соціальних мережах через доступні агенти реалізації; контрзаходи та їх коефіцієнти, інформаційні загрози, доступні агенти реалізації заходів протидії, ознаки.

Запропонований метод протидії поширенню та виявленню шкідливої інформації в соціальних мережах, з урахуванням вимог до обґрунтованості, на різних етапах життєвого циклу дозволяє: визначити потенціал джерела повідомлень, значення якого залежить від кількості повідомлень на сторінці; оцінити індекс активності джерела повідомлень мережі, на значення впливає рівень активності користувачів повідомлень із вмістом шкідливої інформації; оцінити індекси перегляду повідомлень мережі, також джерела; визначити індекс впливу джерела повідомлень, значення залежить від активності та перегляду інформації в цілому.

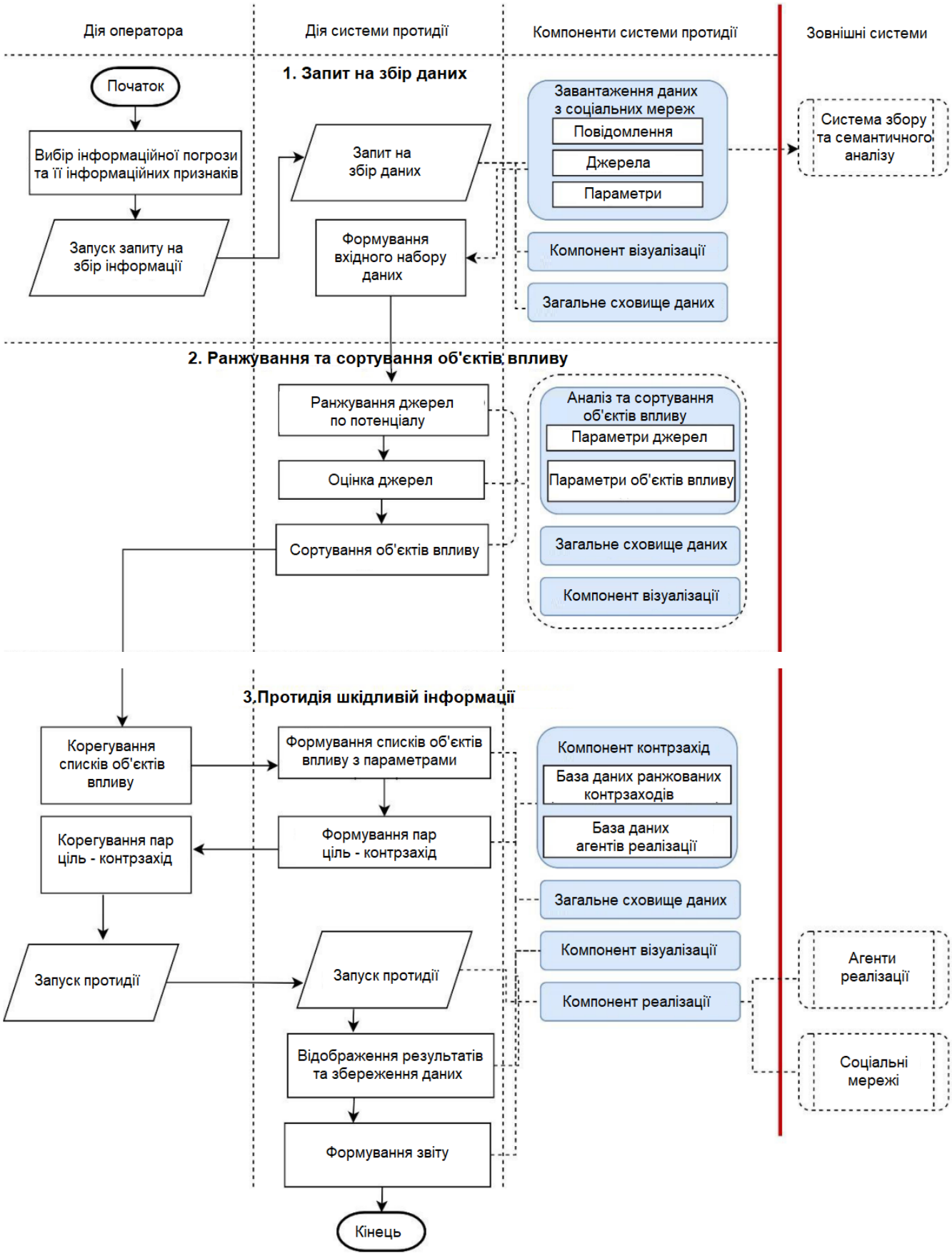



Рисунок 4 – Метод протидії в соціальних мережах
поширенню та виявлення шкідливої інформації на стадії експлуатації

Метод протидії дозволяє: визначити пріоритет об'єкта впливу протидії, на об'єкт впливу впливають індекс впливу та потенціал джерела; для підтримки прийняття рішення оператором, сортувати об'єкти впливу протидії за пріоритетом; сформувати відповідні пари ціль-контрзахід, для підтримки прийняття відповідного рішення про протидію поширення шкідливої інформації в соціальній мережі.

**Висновки**. З метою підвищення ефективності системи протидії в Інтернет - мережах вирішена задача розробки відповідного підходу підвищення обґрунтованості прийнятого рішення на протидію поширення та виявлення шкідливої інформації за рахунок збільшення числа параметрів, що враховуються при виборі інформаційного об'єкта впливу та дійових контрзаходів. Вирішення поставленої задачі досягається за рахунок проведення ранжування контрзаходів та аналізу джерел мережі шкідливої інформації. Запропонований метод протидії та виявлення в соціальних мережах поширення шкідливої інформації, ґрунтується на використанні запропонованих алгоритмів, моделей, забезпечує, на відміну від аналогів, аналіз інформації соцільних мереж; формування списків інформаційних об'єктів впливу для проведення протидії об'єктам впливу, сортування інформаційних об'єктів; надання оператору системи протидії пропонованого та альтернативних варіантів з обґрунтуванням вибору. Розроблений метод протидії виявлення та поширення шкідливої інформації в соціальних мережах відрізняється від існуючих, використанням запропонованих алгоритмів оцінки джерел повідомлень, ранжуванням та аналізом контрзаходів, в результаті підвищується обґрунтованість прийняття рішення про протидію поширенню шкідливої інформації та вибору контрзаходу, відповідним чином скорочується час роботи оператора системи у процесі протидії поширенню шкідливої інформації у соціальних мережах. Система протидії загрозам соціальних мереж забезпечує ранжування контрзаходів доступних у системі для протидії поширенню та виявлення шкідливої інформації в Інтернет - мережі.

ЛІТЕРАТУРА:

1. Ленков, С.В. Модель безпеки поширення забороненої інформації в інформаційно-телекомунікаційних мережах / С.В. Ленков, В.М. Джулій, В.С. Орленко, О.В. Сєлюков, А.В. Атаманюк // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2020. – Вип. №68. – С. 53-64.

2. Соціальні мережі – реальні загрози віртуального світу. [Електронний ресурс]. – Режим доступу : http://ogo.ua/ articles/view/011–02–23/26490.htm.

3. Ленков, С.В. Методы и средства защиты информации. В 2-х томах /С.В. Ленков, Д.А. Перегудов, В.А. Хорошко –К: Арий, 2008.–464с

4. Остапов С. Е. Технології захисту інформації: навчальний посібник / С.Е. Остапов, С.П. Євсеєв, О.Г. Король – Харків : Вид-во ХНЕУ, 2016. – 476 с.

5. Лєнков, С.В. Аналіз існуючих методів та алгоритмів виявлення атак в бездротових мережах передачі даних / С.В. Лєнков, В.М. Джулій, Н.М. Берназ, С.О. Божук // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2017. – Вип. № 56. – С.124-132

6. Довгий, С.О. Сучасні телекомунікації: мережі, технології, економіка, управління, регулювання / С.О. Довгий, О.Я. Савченко, П.П. Воробієнко – К.: Український Видатничій Центр, 2012. – 520 с.

7. Джулій, В.М. Інформаційно-ознакова модель шкідливої інформації в соціальних мережах/ І.В. Муляр, В.М. Джулій, В. М. Пічура, О.О Зацепіна – Вимірювальна та обчислювальна техніка в технологічних процесах № 3 (2022)-73–78с.

8. Джулій, В.М. Модель потоку текстових повідомлень тематичних інтернет-ресурсів системи прогнозування інформаційної безпеки/ В.М. Джулій, Ю.В. Хмельницький, Н.С. Петляк, О.В. Пахар– Вісник Хмельницького національного університету. Технічні науки. 2022. № 5. С. 294-300с.

9. Джулій, В.М., Кльоц Ю.П., Муляр І.В., Жилевич М.Л., Джулій А.В. Контроль додатків інтернет-трафіка комп'ютерних мереж методами машинного навчання. Вісник Хмельницького національного університету. Технічні науки. 2021. № 5. С. 22-26.

10. Джулій, В.М. Метод класифікації додатків трафіка комп'ютерних мереж на основі машинного навчання в умовах невизначеності / В.М. Джулій, О.В. Мірошніченко, Л.В. Солодєєва // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – К.: ВІКНУ, 2022. – Вип. №74. – С. 73-82.

11. Лавров, Є. А. Математичні методи дослідження операцій : підручник / Є. А. Лавров, Л. П. Перхун, В. В. Шендрик – Суми : Сумський державний університет, 2017. – 212 с.

REFERENCES:

1. Lenkov, S.V. (2020), Model bezpeky poshyrennia zaboronenoi informatsii v informatsiino-telekomunikatsiinykh merezhakh / S.V. Lenkov, V.M. Dzhulii, V.S. ORLENKO, O.V. Sieliukov, A.V. Atamaniuk // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – №68. – pp. 53-64.

2. Cotsialni merezhi – realni zahrozy virtualnoho svitu. [Elektronnyi resurs]. – Rezhym dostupu : http://ogo.ua/ articles/view/011– 02–23/26490.htm

3. Lenkov, S.V. (2008), Metodyy sredstva zashchyty ynformatsyy. V 2-kh tomakh / S.V. Lenkov, D.A. Perehudov, V.A. Khoroshko –K: Aryi–464s.

4. Ostapov, S. E. (2016) Tekhnolohii zakhystu informatsii: navchalnyi posibnyk / S.E. Ostapov, S.P. Yevseiev, O.H. Korol–Kharkiv : Vyd-vo KhNEU. – 476 s.

5. Lenkov, S.V. (2017), AnalIz Isnuyuchih metodiv ta algoritmiv viyavlennya atak v bezdrotovih merezhah peredachI danih / S.V. Lenkov, V.M. Dzhuliy, N.M. Bernaz, S.O. Bozhuk // Zbirnik naukovih prats Viyskovogo Institutu Kiyivskogo natsionalnogo universitetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vip. No 56. – p.124-132

6. Dovhyi, S.O. (2012), Suchasni telekomunikatsii: merezhi, tekhnolohii, ekonomika, upravlinnia, rehuliuvannia /S.O. Dovhyi, O.I. Savchenko, P.P. Vorobiienko – K.: Ukrainskyi Vydatnychii Tsentr. – 520p.

7. Dzhulii, V.M. Informatsiino-oznakova model shkidlyvoi informatsii v sotsialnykh merezhakh/ I.V. Muliar, V.M. Dzhulii, V. M. Pichura, O.O Zatsepina – Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh № 3 (2022)-73–78s.

8. Dzhulii, V.M. Model potoku tekstovykh povidomlen tematychnykh internet-resursiv systemy prohnozuvannia informatsiinoi bezpeky/ V.M. Dzhulii, Yu.V. Khmelnytskyi, N.S. Petliak, O.V. Pakhar– Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. 2022. № 5. 294-300s.

9. Dzhulii V.M., Klots Yu.P., Muliar I.V., Zhylevych M.L., Dzhulii A.V. (2021), Kontrol dodatkiv internet-trafika kompiuternykh merezh metodamy mashynnoho navchannia. Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. – Khmelnytskyi. – №5. – pp. 22–26.

10. Dzhulii, V.M. (2022), Metod klasyfikatsii dodatkiv trafika kompiuternykh merezh na osnovi mashynnoho navchannia v umovakh nevyznachenosti / V.M. Dzhulii, O.V. Miroshnichenko, L.V. Solodieieva // Zbirnyk naukovykh prats Viiskovoho instytutu Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. – K.: VIKNU. – Vyp. №74. – pp. 73-82.

11. Lavrov, Ye. A. (2017.), Matematychni metody doslidzhennia operatsii : pidruchnyk / Ye. A. Lavrov, L. P. Perkhun, V. V. Shendryk – Sumy : Sumskyi derzhavnyi universytet, – 212 p.

**Doctor of Technical Science, Lienkov S.V.,**
**Ph.D. Dzhuliy V.M.,**
**Solodeeva L.V.**

## METHOD OF COUNTERACTION AND DETECTION OF HARMFUL INFORMATION IN SOCIAL NETWORKS

***The paper studies the task of detecting and counteracting the spread of malicious information in social networks, including "fake news". There is a particularly urgent need to counter the spread of news on social media that generates panic waves during a pandemic. Currently, there is a war in Ukraine. Fake news travels six times faster on social media than the truth. Russian propaganda has become one of the main elements of the war in Ukraine, it is qualitatively camouflaged under the guise of Western media materials - DW, CNN or BBC.***

***The main difficulty in detecting and counteracting the spread of malicious information in social networks follows directly from the use of information technology development trends at the present stage, namely: an increase in the speed of dissemination of malicious information in social networks; the rate of emergence of new sources of dissemination of malicious information; increase in the volume of information containing malicious information; speed of replication of messages in the network; the number of scenarios for attracting the attention of the audience; level of data heterogeneity. By their architecture, social networks are multicomponent solutions; the network architecture contains: components that process content; components that provide the functions of marketing, administration, data storage. Social networks do not contain a separate component for detecting and counteracting the spread of malicious information on the network.***

***The analysis and study of evaluating the effectiveness of information-analytical systems and informatization of processes showed that the problem of detecting and counteracting the spread of malicious information in social networks cannot be considered solved and requires new research at this stage and allows us to determine the general requirements for the countermeasure system, as the basis for implementation which is based on the model-methodical apparatus.***

***In order to increase the effectiveness of the countermeasure system in Internet networks, the problem of developing an appropriate approach to improve the validity of the decision to counter the spread and detection of harmful information by increasing the number of parameters taken into account when choosing an information object of influence and effective countermeasures has been solved. The solution of the task is achieved by ranking countermeasures and analyzing the sources of the network of malicious information. A method of counteracting and detecting the spread of malicious information in social networks is proposed, based on the use of the proposed models, algorithms, provides, unlike analogues, the analysis of information from social networks; formation of lists of information objects of influence on the conduct of counteraction to objects, sorting of information objects; providing the system operator with a countermeasure to the proposed and alternative options with a justification for the choice. The developed method of detecting and counteracting the spread of malicious information in social networks differs from the existing ones by using algorithms for evaluating message sources, analyzing and ranking countermeasures, as a result, the validity of decision-making on countering the spread of harmful information and choosing a countermeasure increases, correspondingly, the time of the system operator in the process is reduced countermeasures against the spread of malicious information in social networks.***

***Keywords: malicious information, social networks, countermeasures, sources of messages, method of countermeasures, information system.***

УДК 355/358

к.т.н., доц. **Маміч В.В**. (ВА м. Одеса)
к.т.н. **Берназ А. М.,** (ШСВ ЗСУ)
к.т.н., **Максименко Ю.А.** (ВА м. Одеса)
д.н. з держ.упр., проф. **Попов С.А.** (ВА м. Одеса)
**Шаршаткін Д.Ю.** (ВА м. Одеса)

DOI: https://doi.org/10.17721/2519-481X/2022/77-10

# ДОСЛІДЖЕННЯ АНАЛІТИЧНОЇ РОБОТИ З ОБРОБЛЕННЯ ДАННИХ В ОРГАНАХ РОЗВІДКИ

***Актуальним питанням сьогодення стало широке впровадження сучасних інформаційних технологій, на думку вчених, воно є безумовною вимогою часу та стало невід'ємною відзнакою роботи сучасних органів управління. В сучасних умовах у галузі інформаційних технологій завжди існували два взаємодоповнюючих один одного напрямки розвитку: системи, орієнтовані на операційну обробку даних – системи обробки даних та системи,орієнтовані на аналіз даних – системи підтримки прийняття рішень. На сучасному етапі інформатизації аналітичної роботи новий підхід знайшов своє вираження в концепціях банків даних (БнД). Банк даних – це інформаційна система, що включає комплекс спеціальних методів і засобів для підтримки динамічної інформаційної моделі галузі свого застосування з метою інформаційного обслуговування користувачів. При цьому вхідна інформація (підготовлена до введення в інформаційну модель і така, що є результатом роботи підсистем збору і реєстрації інформації в АСУ), а також вихідна інформація (отримана в результаті обробки інформації, укладеної в моделі, і, що надходить на вхід підсистем розподілу і відображення інформації в АСУ) не розглядаються як частина інформаційної моделі. Задача підтримки інформаційної моделі в необхідному стані полягає в тому, щоб у БнД виконувалися операції збереження і модифікації інформаційної моделі відповідно до виникаючих змін в складі об'єктів предметної галузі, зв'язках між ними і їхнім станом. Задача забезпечення інформаційних запитів користувачів має два аспекти, які необхідно враховувати при проектуванні БнД. Перший аспект – це визначення меж конкретної предметної галузі і розробка відповідної інформаційної моделі. Другий аспект – розробка банку даних, орієнтованого на ефективне обслуговування запитів користувачів. На сьогоднішній день впровадження банку даних і нових технологій обробки інформації дозволить отримати значне підвищення швидкості та ефективності в аналітичної роботі розвідувально-інформаційних підрозділів.***

***Ключові слова: структурована інформація, інформаційно-аналітична робота, алгоритм дій, інформаційні технології, інструмент боротьби, автоматизовані інформаційні системи,інформація як особливий вид ресурсу.***

**Постановка проблеми.** На думку провідних вчених з аналітичної роботи вся інформація характеризується як не достатньо структурована, непогоджена, розрізнена, не завжди достовірна. Таким чином, виникла проблема між великими обсягами накопиченої в органах державного воєнного управління інформації та неспроможністю традиційних засобів обробки даних реалізувати аналітичний потенціал цієї інформації. Наукова робота присвячена вирішенню цієї проблеми та завдяки використанню засобів інформаційно-аналітичної підтримки забезпечується суттєве підвищення ефективності роботи системи управління на всіх етапах життєдіяльності Збройних Сил України. Сучасні локальні війни показують, що боротьба ведеться не тільки матеріальними ресурсами, а й, перед усім, та переважно інтелектуальними в різноманітних сферах: економічній, політичній, ідеологічній, фінансовій, соціальній і, в майже останню чергу, у військовій. З досвіду ведення бойових дій на сході України відомо, що основою боротьби, її інструментом та ціллю є інформація [1].

**Аналіз останніх досліджень і публікацій.** Інформаційно – аналітична діяльність та вибуховий розвиток інформаційних технологій в останні десятиріччя призвів до того, що сучасне управління в складних системах організаційного типу майже неможливо уявити без застосування комп'ютерної техніки. Питання інформаційно-аналітичної діяльності розглядається у таких публікаціях як: Варенко В. М. Інформаційно-аналітична діяльність :

навчальний посібник. – К. : Університет "Україна", 2014. – 417 с.; Захарова І. В. Основи інформаційно-аналітичної діяльності : навчальний посібник. – К. : "Видавництво "Центр учбової літератури", 2013. – 336 с.; Процеси розвідувальної діяльності. Стандарт НАТО. Союзницька об'єднана настанова AJP–2.1 (видання B, варіант 1)/ Управління стандартизації НАТО, 2016. – 80 с. Але, на думку вчених сучасна техніка без спеціального програмного забезпечення не здатна задовольнити постійно зростаючи потреби по ефективному управлінню. На думку військових вчених шлях вирішення даної проблеми є утворення спеціальних автоматизованих інформаційних систем (АІС) [2]. В залежності від предметної галузі, вони можуть дуже відрізнятися між собою за функціями, архітектурою, реалізацією. Однак можна виділити ряд властивостей, що є загальними для всіх подібних систем: АІС призначені для збору, збереження і обробки інформації. Тому основою будь-якої з них є середовище збереження і доступу до даних. АІС орієнтовані на кінцевого користувача, який не є кваліфікованим фахівцем в галузі застосування інформаційних технологій. Тому клієнтські додатки АІС повинні мати простий, зручний інтерфейс, що легко засвоюється, який надає користувачеві усі необхідні для роботи функції, але в той же час не дає змоги виконувати зайві дії. Таким чином, при розробці інформаційних систем необхідно вирішувати принаймні дві основних задачі: - задачу розробки бази даних, призначеної для збереження інформації; - задачу розробки графічного інтерфейсу користувача клієнтських додатків. Поняття інформація є одним з фундаментальних у сучасній науці взагалі і базовим для досліджуваної, нами дисципліни. Інформацію разом з речовиною й енергією розглядають у якості найважливіший сутності світу, у якому ми живемо. Однак якщо задатися метою формально визначити поняття "інформація", то зробити це буде надзвичайно складно. Сам термін інформація походить від латинського informatio – роз'яснення, викладення [3]. У найпростішому розумінні з терміном "інформація" зазвичай асоціюються деякі відомості, дані, знання тощо. До середини минулого сторіччя інформація трактувалася як відомості, що передаються людьми усно, письмово чи в інший (знаками, технічними засобами) спосіб. Розвиток обчислювальної техніки і наукових дисциплін, що з нею пов'язані, призвів до появи нових, розширених трактувань поняття інформації. При імовірно-статистичному (або ентропійному) підході і поняття інформації стали трактувати як зменшення ступеня невизначеності знання про якийсь об'єкт, систему, процес або явище, або зміна невизначеності стану самого об'єкта, системи, явища, процесу. Існує нормативно-правове трактування інформації. Так в законі" Про інформацію" інформація трактується як будь-які відомості та/або дані, які можуть бути збережені на матеріальному носії або відображені в електронному вигляді[4].

Цей закон надає і правове визначення інформації. В подальшому ми будемо користуватися таким трактуванням. Інформація – зміна обсягу і структури знання про деяку предметну галузь (осіб, предмети, факти, події, явища, процеси) системою, що сприймає (людина, організаційна структура, автоматизована інформаційна система) незалежно від форми і способу подання знання. Людині властиво суб'єктивне сприйняття інформації через деякий набір її властивостей: важливість, вірогідність, своєчасність, приступність і т.д. Інформацію варто вважати особливим видом ресурсу, при цьому мається трактування "ресурсу" як запасу деяких знань, матеріальних предметів або енергетичних, структурних чи будь-яких інших характеристик предмета. На відміну від ресурсів, зв'язаних з матеріальними предметами, інформаційні ресурси є невичерпаємими і припускають істотно інші методи виробництва і відновлення, чим матеріальні ресурси. До основних властивостей інформації відносять: запам'ятованість; передаваємість; перетворюваність; відтворюваність; зтираємість. Іншим ключовим для теорії і практики створення АІС є поняття даних, які відрізняються від інформації конкретною формою подання і являє деяку її підмножиною, що визначається цілями і задачами збору і обробки інформації. Розвиток обчислювальної техніки і програмування супроводжувався еволюцією представлень про роль даних і їхню організацію. Однією із властивостей комп'ютерів є здатність зберігати величезні обсяги інформації і забезпечувати легкий доступ до неї. Ці питання розглянуті у нижче переліченої наукової

літературі: Курносов Ю. Аналітика як інтелектуальна зброя. – М.: Ритм, 2015, - 613 с.; Оленович І.Ф., Сбітнев А.І. та ін. Методологія дослідження складних систем військового призначення, Київ, вид. НАОУ, 2003, 400 с.; Великі технічні системи, проектування та керування // Артюшин Л.М., Зиатдинов Ю.К., Харченко А.В. Під ред. И.А. Попова,. – Харків: Факт, 1997. – 400 с.; Гущин В.М. Управління розробками авіа та ракетно – космічних комплексів. – М.: МАІ, 1999. – 76 с.

**Мета статті** полягає у дослідженні аналітичної роботи зі збору та оброблення даних спеціальної інформації, застосування інформаційних технологій у процесах військового управління що є важливою задачею сьогодення у органах розвідки.

**Виклад основного матеріалу.** Загальна проблема дослідження аналітичної роботи з оброблення Даниних в органах розвідки розглянута достатньо глибоко, але є і невирішені раніше частини цієї проблеми. Особливо це відноситься до зберігання, оброблення та аналізу Даниних розвідувальної інформації. Інформація, що підлягає обробці, у деякому змісті являє абстракцію фрагмента реального світу. [5] Ми говоримо про дані як про абстрактне подання реальності, оскільки деякі властивості і характеристики реальних об'єктів при цьому ігноруються (як несуттєві для даної задачі). Тому визначимо дані як інформацію, що відображує визначений стан в деякій предметній галузі в конкретній формі подання і містить лише найбільш суттєві з погляду цілей і задач збору і обробки інформації елементи образу фрагмента дійсності, що відображується. Таким чином, інформація на стадії даних характеризується визначеною формою подання і додатковою характеристикою, яка виражається терміном "структура". Структура даних пов'язана з поняттям "подання інформації" і визначається функціональною, логічною, технічною тощо структурою предметної галузі, інформацію про яку містять дані. Вирішуючи конкретну задачу, необхідно вибрати множину даних, відображаючи реальну ситуацію. Потім слід обрати спосіб подання цієї інформації. У науковому середовищі доведено, що сучасне представлення даних визначається виходячи з засобів і можливостей обчислювальної системи (комп'ютерів і їх програмним забезпеченням). Однак дуже важливу роль грають і властивості самих даних операції, що повинні виконуватися над ними. З розвитком обчислювальної техніки і програмних засобів, можливості представлення даних одержали великий розвиток і тепер дозволяють використовувати як найпростіші неструктуровані дані, так і дані більш складних типів, отримані за допомогою комбінації найпростіших даних. Такі дані називають структурованими, оскільки вони мають деяку організацію [6].

Різкий ріст обсягів інформації, що переробляється, з одного боку, і накопичений досвід використання електронно-обчислювальної техніки, іншого боку, дозволили з принципово нових позицій підійти до питання організації обробки інформації в АСУ. Отже, БнД повинний мати спеціальні засоби для забезпечення санкціонованого доступу користувачів доданих. Користувачі банку даних відрізняються один від одного за формою подання запитів, з якими вони звертаються до БнД, а також за формою подання викликаної інформації. За цими ознаками усіх користувачів поділяють на дві групи: користувачі – задачі і користувачі – люди. Користувачі – задачі звертаються до банку даних з регламентованими за формою і за змістом запитами. Видана ним інформація відповідним чином обробляється і компонується на підставі прийнятих у системі формальних правил і угод. Користувачі – люди звертаються до банку даних з довільними або зарегламентованими за змістом запитами. Видавана ним інформація повинна мати зручну для людини форму подання: у вигляді тексту природною мовою, таблиць з поясненнями, графіків і т.п. [7] Основні користувачі цієї групи: прикладні програмісти і не програмісти. Прикладні програмісти – особлива категорія користувачів. Вони виконують роботи з програмування функціональних задач. Користувачі цієї категорії звичайно вміють працювати на декількох мовах програмування, знайомі з засобами обробки,що маються в складі використовуваного банку даних. Для забезпечення нормальної роботи цієї категорії користувачів необхідна наявність у системі словника даних і добре поставленої служби спостереження за його станом. Зі словника даних дізнаються про наявні типи даних, їхню структуру і зв'язки між ними, про всі зміни, що відбуваються в структурі інформаційної

моделі. Непрограмісти – найбільш численна група користувачів, для задоволення інформаційних потреб яких і створюється банк даних. Тому їх ще називають кінцевими користувачами. Це фахівці у своїй галузі діяльності,що звичайно не мають необхідної підготовки по програмуванню. Вони охоче звертаються до системи, якщо не потрібно багато витрат на формування запиту. Для цієї групи користувачів ідеальної може бути система, спілкування з якою відбувається природною мовою. Тому доцільно забезпечувати кінцевих користувачів спеціальною формалізованою мовою запитів, що нагадують природну мову, і працювати на цій мові в режимі діалогу "користувач – система", метою якого є уточнення запиту користувача, надання йому допомоги в ознайомленні з можливостями системи. У зв'язку з тим, що послугами банку даних користуються різні користувачі, у БнД передбачається словник даних – спеціальний засіб приведення всіх запитів до єдиної термінології. Крім того, використовуються спеціальні методи еквівалентних граматичних перетворень запитів для побудови оптимальних процедур їх обробки, спеціальні методи організації доступу до тим самим даних різних користувачів при збігу в часі запитів, що надійшли. Розглянуті групи користувачів називають зовнішніми користувачами БнД. З огляду на вищевикладене, БнД повинний виконувати наступні вимоги з боку зовнішніх користувачів: задовольняти актуальним інформаційним потребам, забезпечувати можливість збереження і модифікації великих обсягів багатоаспектної інформації, задовольняти виявленим і знову виникаючим потребам зовнішніх користувачів; забезпечувати заданий рівень вірогідності збереженої інформації і несуперечність; забезпечувати доступ до даних тільки тих користувачів, що мають відповідні повноваження; забезпечувати можливість пошуку інформації з довільної групи ознак; задовольняти заданим вимогам продуктивності при обробці запитів; мати можливість реорганізації і розширення при зміні меж предметної галузі;забезпечувати видачу інформації користувачам у різній формі; забезпечувати простоту і зручність звертання за інформацією; забезпечувати можливість одночасного обслуговування великої кількості користувачів тощо [8]. Максимальне задоволення перерахованих вимог обумовлює необхідність централізованого управління даними. На думку провідних вчених у порівнянні з традиційним забезпеченням монопольними файлами кожного додатка централізоване управління даними має наступні переваги: скорочує надмірність збережених даних; усуває суперечливість збережених даних; дозволяє організувати багатоаспектне використання даних; забезпечує можливість стандартизації в представленні даних; забезпечує можливість санкціонованого доступу до даних; дозволяє здійснити комплексну оптимізацію при проектуванні БнД. Централізоване керування даними висуває на перший план проблему забезпечення незалежності прикладних програм від даних [9]. Ця проблема існувала і до появи БнД у зв'язку з великими витратами ручної праці на написання і коректування програм. З появою банків даних проблема зажадала кардинального рішення, оскільки при інтеграції даних і оптимізації структур збереження з метою поліпшення характеристик процесів обслуговування запитів користувачів потрібно змінювати збережене подання даних і методи доступу до них. Розглядаючи дані як один з ресурсів АСУ, можна сказати, що БнД централізовано керує цим ресурсом в інтересах усієї системи. Таким чином, банк даних – це інформаційна система, що реалізує централізоване управління даними в інтересах усіх користувачів АСУ, до складу якої вона входить. Сучасне наукове трактування моделі даних належать К. Дейту. Згідно Дейта, реляційна модель складається з трьох частин: структурної частини; цілісної частини; маніпуляційної частини. Структурна частина описує, які об'єкти розглядаються реляційною моделлю. Постулірується, що єдиною структурою даних, використовуваної в реляційної моделі, є нормалізовані n-парні відносини. Цілісна частина описує обмеження спеціального виду, що повинні виконуватися для будь-яких відносин у будь-яких інформаційних базах даних. Це цілісність сутностей і цілісність зовнішніх ключів. Маніпуляційна частина описує два еквівалентних способи маніпулювання реляційними даними – реляційну алгебру і реляційні числення. Будь-які дані, використовувані в програмуванні, мають свої типи даних. Реляційна модель вимагає, щоб типи використовуваних даних були простими. Для уточнення цього твердження розглянемо, які

взагалі типи даних звичайно розглядаються в програмуванні. Як правило, типи даних поділяються на три групи: прості типи даних; структуровані типи даних; посилальні типи даних [10]. Прості, чи атомарні, типи даних не мають внутрішню структуру. Дані такого типу називають скалярами. До простих типів даних відносяться наступні типи: логічний; строковий; чисельний. Різні мови програмування можуть розширювати й уточнювати цей список, додаючи такі типи як: цілий; речовинний; дата; час; грошовий; інтервальний і т.д. Звичайно, поняття атомарності досить відносно. Так, строковий тип даних можна розглядати як одномірний масив символів, а цілий тип даних – як набір бітів. Важливо лише те, що при переході на такий низький рівень губиться семантика (зміст) даних. Якщо рядок, що виражає, наприклад, прізвище співробітника, розкласти в масив символів, то при цьому губиться зміст такого рядка як єдиного цілого. Структуровані типи даних призначені для завдання складних структур даних. Структуровані типи даних конструюються зі складових елементів,називаних компонентами, що, у свою чергу, можуть мати структуру. Як структуровані типи даних можна привести наступні типи даних: масиви; опису (структури). З математичної точки зору масив являє собою функцію з кінцевою областю визначення. Значення цієї функції для деякого значення індексу називається елементом масиву. Аналогічно можна задавати багатомірні масиви. Запис (чи структура) являє собою кортеж з деякого декартового добутку безлічей. Дійсно, запис являє собою іменований упорядкований набір елементів, кожний з який належить типу. Таким чином, запис є елемент безлічі. Повідомляючи нові типи записів на основі вже наявних типів, користувач може конструювати як завгодно складні типи даних. Загальним для структурованих типів даних є те, що вони мають внутрішню структуру, використовувану на тім же рівні абстракції, що і самі типи даних. Пояснимо це в такий спосіб. При роботі з чи масивами записами можна маніпулювати чи масивом записом і як з єдиним цілим (створювати, видаляти, копіювати цілі чи масиви записи), так і поэлементно [11]. Для структурованих типів даних є спеціальні функції – конструктори типів, що дозволяють створювати чи масиви записи з елементів більш простих типів. Працюючи ж із простими типами даних, наприклад з числовими, ми маніпулюємо ними як неподільними цілими об’єктами. Щоб “побачити”, що числовий тип даних насправді складний (є набором битов), потрібно перейти на більш низький рівень абстракції. На рівні програмного коду це буде виглядати як ассемблерні вставки в код мовою високого чи рівня використання спеціальних подібних операцій. Посилальний тип даних (покажчики) призначений для забезпечення можливості вказівки на інші дані. Покажчики характерні для мов процедурного типу, у яких є поняття області пам’яті для збереження даних. Посилальний тип даних призначений для обробки складних структур, що змінюються, наприклад дерев, графів, рекурсивних структур. Власне, для реляційній моделі даних тип використовуваних даних неважливий. Вимога, щоб тип даних був простим, потрібно розуміти так, що в реляційних операціях не повинна враховуватися внутрішня структура даних. Звичайно, повинні бути описані дії, які можна робити з даними як з єдиним цілим, наприклад, дані числового типу можна складати, для рядків можлива операція конкатенації і т.д. З цього погляду, якщо розглядати масив, наприклад, як єдине ціле і не використовувати заелементних операцій, то масив можна вважати простим типом даних. Більш того, можна створити свій, як завгодно складних тип даних, описати можливі дії з цим типом даних, і, якщо в операціях непотрібно знання внутрішньої структури даних, те такий тип даних також буде простим з погляду реляційної теорії. Можна описати функції додавання, множення, вирахування і розподіли, і всі дії з компонентами і виконувати тільки у середині цих операцій. Тоді, якщо в діях з цим типом використовувати тільки описані операції, то внутрішня структура не грає ролі, і тип даних ззовні виглядає як атомарний. Саме так у деяких постреляційних СКБД реалізована робота з як завгодно складними типами даних, створюваних користувачами. У реляційній моделі даних з поняттям тип даних тісно зв'язаний поняття доменна, яких можна вважати уточненням типу даних [12]. Домен – це семантичне поняття. Домен можна розглядати як підмножина значень деякого типу даних що мають визначений зміст. Домен характеризується наступними властивостями: домен має унікальне ім’я (у межах бази даних);домен визначений на деякому

простому типі чи даних на іншому домені; домен може мати деяку логічну умову, що дозволяє описати підмножина даних, припустимих для даного домена; домен несе визначене значеннєве навантаження. Наприклад, домен, зміст, що має, "вік співробітника" можна описати як підмножина безлічі натуральних чисел. Якщо тип даних можна вважати безліччю всіх можливих значень даного типу, то домен нагадує підмножина в цій безлічі. Відмінність домена від поняття підмножини складається саме в тому,що домен відбиває семантику, визначену предметною областю. Може бути декілька доменів, що збігаються як підмножини, але мають різний зміст. Наприклад, домени "Вага деталі" і "Наявна кількість" можна однаково описати як безліч не негативних цілих чисел, але зміст цих доменів буде різним, і це будуть різні домени. Основне значення доменів полягає в тому, що домени обмежують порівняння. Некоректно, з логічної точки зору, порівнювати значення зрізних доменів, навіть якщо вони мають однаковий тип. У цьому виявляється значеннєве обмеження доменів. Синтаксично правильний запит "видати список усіх деталей, у яких вага деталі більше наявної кількості" не відповідає змісту понять "кількість" і "вага". Поняття домена допомагає правильно моделювати предметну область. При роботі з реальною системою в принципі можлива ситуація коли потрібно відповісти на запит, приведений вище. Система дасть відповідь, але, імовірно, він буде безглуздим. Не всі домени мають логічну умову, що обмежує можливі значення домена. У такому випадку безліч можливих значень домена збігається з безліччю можливих значень типу даних. Не завжди очевидно, як задати логічну умову, що обмежує можливі значення домена [13].

**Висновки.** Таким чином, у роботі доведено, що при розробці інформаційних систем необхідно вирішувати принаймні дві основних задачі: - задачу розробки бази даних, призначеної для збереження інформації; - задачу розробки графічного інтерфейсу користувача клієнтських додатків. Поняття інформація є одним з фундаментальних у сучасній науці взагалі і базовим для дослідження аналітичної роботи з оброблення Даниних в органах розвідки. Інформацію разом з речовиною й енергією розглядають у якості найважливіший сутності світу, у якому ми живемо. Однак якщо задатися метою формально визначити поняття "інформація", то зробити це буде надзвичайно складно.

**Напрямки подальших досліджень.** Відмічено, що з розвитком обчислювальної техніки і програмних засобів, можливості представлення даних одержали великий розвиток і тепер дозволяють використовувати як найпростіші неструктуровані дані, так і дані більш складних типів, отримані за допомогою комбінації найпростіших даних. Будь-які дані, використовувані в програмуванні, мають свої типи даних. Органи розвідки вимагають, щоб типи використовуваних даних були простими. Для уточнення цього твердження необхідно розглянути, які взагалі типи даних звичайно розглядаються в програмуванні. Як правило, типи даних поділяються на три групи: прості типи даних; структуровані типи даних; посилальні типи даних. Рекомендовано використання вбудованих конструкторів складених типів. Ієрархія структурних комплексних даних пропонує додаткову властивість, спадкування типу. Тобто структурний тип може мати підтипи,що використовують усі його атрибути і містять додаткові атрибути, специфіковані в підтипі. Питання аналітичної роботи зберігання, оброблення та аналізу Даниних розвідувальної інформації повинні постійно удосконалюватися та аналізуватися у подальших дослідженнях. Інформація, що підлягає обробці, у деякому змісті являє абстракцію фрагмента реального світу. Ми говоримо про дані як про абстрактне подання реальності, оскільки деякі властивості і характеристики реальних об'єктів при цьому зберіганні, обробленні та аналізу Даниних розвідувальної інформації максимально відповідають дійсності.

ЛІТЕРАТУРА:

1. Курносов Ю. Аналітика як інтелектуальна зброя. – М.: Ритм, 2015, - 613 с.

2. Оленович І.Ф., Сбітнев А.І. та ін. Методологія дослідження складних систем військового призначення, Київ, вид. НАОУ, 2003, 400 с.

3. Артюшин Л.М., Зиатдинов Ю.К., Харченко А.В. Під ред. И.А. Попова – Великі технічні системи, проектування та керування. – Харків: Факт, 1997. – 400 с.

4. Гущин В.М. Управління розробками ракетно – космічних комплексів. – М. МАІ, 1999. 76 с.

5. Волков Л.І. Управління експлуатуванням літальних комплексів.: Вища школа, 1981 – 368 с.

6. Пермяков О.Ю.,Сбітнев А.І. Інформаційні технології і сучасна збройна боротьба - Луганск: Знання, 2008. – 204 с.

7. Казачинський В.З. Математичні методи рішення воєнно-спеціальних задач. – К.: ВА ВПВО, 1980.- 292 с.

8. Вернер І.Є., Козаков Ю.І., Рябцев В.В. Застосування сучасних інформаційних технологій в роботі органів управління. – К.: НАОУ, 2006. – 368 с.

9. Методичні рекомендації з розробки розвідувальних оцінок (за стандартами провідних країн-членів НАТО). – К. : ГУР МО України, 2018. – 118 с.

10. Варенко В. М. Інформаційно-аналітична діяльність: навчальний посібник. – К. : Університет "Україна", 2014. – 417 с.

11. Захарова І. В. Основи інформаційно-аналітичної діяльності: навчальний посібник. – К. : "Видавництво "Центр учбової літератури", 2013. – 336 с.

12. Процеси розвідувальної діяльності. Стандарт НАТО. Союзницька об'єднана настанова AJP–2.1 (видання B, варіант 1)/ Управління стандартизації НАТО, 2016. – 80 с.

13. Основи розвідувально-інформаційної діяльності: настанова Штабу розвідки Міністерства оборони Великобританії. – К. : ГУР МО України, 2015. – 51 с.

REFERENCES:

1. Kurnosov Yu. Analytics as an intellectual weapon. - M.: Rytm, 2015, - 613 p.

2. Olenovich I.F., Sbitnev A.I. etc. Methodology of research of complex systems of military purpose, Kyiv, ed. NAOU, 2003, 400 p.

3. Artyushin L.M., Ziatdinov Yu.K., Kharchenko A.V. Under the editorship I.A. Popova - Large technical systems, design and management. - Kharkiv: Fakt, 1997. - 400 p.

4. Gushchin V.M. Management of the development of rocket and space complexes. - M.: MAI, 1999. 76 p.

5. Volkov L.I. Management of operation of flying complexes.: Higher school, 1981 - 368 p.

6. Permyakov O.Yu., Sbitnev A.I. Information technologies and modern armed struggle - Luhansk: Znannia, 2008. – 204 p.

7. Kazachynskyi V.Z. Mathematical methods of solving military special problems. - K.: VA VPVO, 1980. - 292 p.

8. Werner I.E., Kozakov Yu.I., Ryabtsev V.V. Application of modern information technologies in the work of management bodies. - K.: NAOU, 2006. - 368 p.

9. Methodological recommendations for the development of intelligence assessments (according to the standards of leading NATO member countries). - K.: GUR Ministry of Defense of Ukraine, 2018. - 118 p.

10. Varenko V. M. Information and analytical activity: study guide. - K.: "Ukraine" University, 2014. - 417 p.

11. Zakharova I. V. Fundamentals of information and analytical activity: a study guide. - K.: "Centre of Educational Literature" Publishing House, 2013. - 336 p.

12. Intelligence activity processes. NATO standard. Allied Joint Instruction AJP–2.1 (edition B, version 1)/ NATO Standardization Office, 2016. – 80 p.

13. Basics of intelligence and information activities: instruction of the Intelligence Staff of the Ministry of Defense of Great Britain. - K.: GUR Ministry of Defense of Ukraine, 2015. - 51 p.

**Ph.D. Mamych V.V.,**
**Ph.D., Maksimenko Yu.A.,**
**Doctor of Science from public administration, Popov S.A.,**
**Sharshatkin D.Yu.**

# STUDY OF ANALYTICAL WORK ON DATA PROCESSING IN INTELLIGENCE BODIES

***Abstract:*** ***Wide implementation of modern information technologies has become an urgent issue today, according to scientists, it is an absolute requirement of the time and has become an integral feature of the work of modern management bodies. In modern conditions in the field of information technologies, there have always been two mutually complementary directions of development: systems focused on operational data processing - data processing systems and systems focused on data analysis - decision support systems. At the current stage of informatization of analytical work, a new approach found its expression in the concepts of data banks (DB). The data bank is an information system that includes a set of special methods and tools to support the dynamic information model of the field of its application for the purpose of providing information to users. At the same time, the input information (prepared for input into the information model and that is the result of the operation of the information collection and registration subsystems in the ACS), as well as the output information (obtained as a result of the processing of the information included in the model and which is received at the input of the distribution subsystems and display of information in ACS) are not considered as part of the information model. The task of maintaining the information model in the required state is that the operations of preservation and modification of the information model are carried out in the BND in accordance with the emerging changes in the composition of the objects of the subject field, the connections between them and their state. The task of providing information requests of users has two aspects that must be taken into account when designing BnD. The first aspect is the definition of the boundaries of a specific subject area and the development of an appropriate information model. The second aspect is the development of a data bank focused on efficient service of user requests. To date, the introduction of a data bank and new information processing technologies will allow for a significant increase in speed and efficiency in the analytical work of intelligence and information units.***

***Keywords: structured information, information-analytical work, algorithm of actions, information technologies, tool of struggle, automated information systems, information as a special kind of resource.***

УДК 621.391 к.т.н., с.н.с. **Міночкін Д.А.** (НТУУ «КПІ ім. Ігоря Сікорського»)
**Нсер А.М.** (НТУУ «КПІ ім. Ігоря Сікорського»)

DOI: https://doi.org/10.17721/2519-481X/2022/77-11

# ПРОГРАМНІ МЕТОДИ МОНІТОРИНГУ МЕРЕЖЕВОЇ БЕЗПЕКИ

***В роботі розглянуто програмні методи моніторингу мережевої безпеки (NSM - Network Security Monitoring). Із зростанням і швидким розвитком мобільного зв'язку, великих даних і технологій штучного інтелекту ми вступаємо в еру мобільного Інтернету. З безперервною інтелектуалізацією мережевої безпеки та інфраструктури інформаційних технологій, вони широко використовуються в галузі промислового контролю, що робить мережеву безпеку все більш відкритою. В даний час спостерігається зростання кількості інформаційних загроз та факторів, що призводять до нестабільного функціонування мереж передачі даних. Передумовами цього зростання є масовість застосування, ускладнення ієрархії обчислювальних мереж та збільшення їх структурної складності, збільшення гетерогенності програмних та апаратних засобів, ускладнення функціональності мережевих сервісів, що призводить до появи різноманітних вразливостей. У таких умовах розробка та вдосконалення способів виявлення інформаційних загроз набувають великої важливості. Одним із компонентів забезпечення інформаційного захисту мереж є програмні комплекси, призначені для виявлення шкідливої чи підозрілої активності – методи моніторингу мережевої безпеки (NSM). Методи моніторингу мережевої безпеки (NSM) використовуються для моніторингу та обміну даними по мережі щодо подій, пов'язаних з інформаційною безпекою.***

***У статті наведено визначення методів моніторингу мережевої безпеки, їх класифікація, цикл NSM та їх опис. Розглянуто деякі з найвідоміших і широко використовуваних багатомодульних рішень NSM. Найвідомішими прикладами таких комбінацій є IDS/IPS, SEM/SIEM і UTM. Моніторинг мережевої безпеки перевіряє, чи працюють перші лінії захисту, надає можливість усунути загрози, перш ніж вони завдадуть реальної шкоди. Якщо в системі є вразливість, NSM дозволяє зрозуміти, де ці вразливості та як запобігти атакам.***

***Ключові слова: NSM, Network Security Monitoring, програмні методи моніторингу мережевої безпеки.***

**Вступ.** На сьогодні більшість зусиль у сфері мережевої безпеки зосереджені на запобіганні атакам, однак рішення та методи, засновані на виявленні та реагуванні, набувають все більшої актуальності [1, 2]. У спільноті безпеки інформаційних технологій (IT) існує загальне переконання, що зловмисники рано чи пізно перевершують заходи профілактики. У цей момент необхідно застосувати механізми виявлення та реагування [3]. Моніторинг безпеки мережі (NSM) є одним із найкращих підходів до безпеки мережі [4].

Метою NSM є моніторинг стану даної мережі для виявлення аномальних подій і, якщо вони виявлені, для своєчасної реакції на них. Це серйозний виклик, оскільки комунікаційні мережі виробляють величезний обсяг даних з високою швидкістю, відповідно до визначення проблеми Big data [5]. Це ще складніше завдання, якщо взяти до уваги поширеність нових сценаріїв використання мережі, таких як 5G та IoT, або адаптацію до нових мережевих технологій (наприклад, SDN) [6, 7].

**Аналіз останніх досліджень та публікацій.** В літературі та дослідженнях розглядаються різні інструменти безпеки мережі, які реалізують декілька модулів NSM. А саме системи виявлення вторгнень (IDS) / системи запобігання вторгненням (IPS), системи керування подіями безпеки (SEM) / системи керування інформацією та подіями безпеки (SIEM), універсальний контроль загроз (UTM) і колекції інструментів; включаючи приклади як відкритих, так і комерційних рішень [8]. Однак, більшість досліджень присвячені лише певним типам загроз, заснованим на рішенні вузького спектру задачах безпеки мережі. Актуальним лишається створення методу, який зможе протистояти декільком загрозам одночасно та буде більш універсальним до більшості методів атак. Пропонується

використовувати існуючі методи та інструменти у взаємодії один з одним, таким чином створюючи потужну та масштабовану архітектуру для виявлення інцидентів.

**Мета статті.** Метою статті є наведення програмних методів моніторингу мережевої безпеки (NSM).

**Виклад основного матеріалу.** NSM - це збір, виявлення та аналіз даних безпеки мережі. Інформаційна безпека традиційно поділяється на багато різних типів, але відповідно до DoD 8500.2.1 [9] їх можна класифікувати наступним чином:

1. Захист. Даний тип зосереджується на захисті систем, щоб запобігти несанкціонованому використанню та вторгненню. Деякі з функцій, які зазвичай виконуються в цьому типі, включають оцінку вразливості, оцінку ризиків, керування захистом від шкідливих програм, навчання користувачів та інші загальні завдання забезпечення інформаційної безпеки.

2. Виявлення. Цей тип зосереджений на виявленні вторгнень, які активно відбуваються або мали місце раніше. Воно включає в себе моніторинг безпеки мережі та виявлення і попередження атак.

3. Відповідь. Третій тип зосереджений на відповіді після виявлення. Це включає стримування інцидентів, криміналістику мережі та хостів, аналіз зловмисного програмного забезпечення та звітування про інциденти.

4. Підтримка. Останній тип відповідає за керування людьми, процесами та технологіями, пов'язаними з інформаційною безпекою. Це включає укладання контрактів, підбір персоналу та навчання, розробку та впровадження технологій, а також управління системами підтримки.

Цикл NSM складається з трьох окремих фаз: збір даних, виявлення та аналіз (Рис.1.) [10].


Рисунок 1 – Фази NSM

Цикл NSM починається з найважливішого етапу – збору даних. Збір даних відбувається за допомогою апаратного та програмного забезпечення, яке використовується для генерування, упорядкування та зберігання даних для подальшого виявлення та аналізу. Збір даних є найважливішою частиною циклу, оскільки вжиті кроки формують здатність організації виконувати ефективне виявлення та аналіз. Є кілька типів даних NSM і кілька способів їх збору. Найпоширеніші категорії даних NSM включають повні дані вмісту, дані сеансу, статистичні дані, дані пакетів і дані оповіщення. Залежно від потреб організації, архітектури мережі та доступних ресурсів ці типи даних можуть використовуватися переважно для виявлення. Спочатку збір даних може бути однією з найбільш трудомістких частин циклу NSM через кількість необхідних людських ресурсів. Ефективний збір даних вимагає узгоджених зусиль керівництва організації, команди з інформаційної безпеки та груп адміністрування мережі та систем. Збір даних включає такі завдання, як:

1. Визначення того, де в організації існує найбільший ризик
2. Виявлення загроз
3. Виявлення відповідних джерел даних
4. Уточнення частин збору джерел даних
5. Налаштування портів SPAN для збору пакетних даних
6. Створення сховища SAN для зберігання даних

7. Налаштування апаратного та програмного забезпечення збору даних.

Виявлення – це процес, за допомогою якого перевіряються зібрані дані та генеруються сповіщення на основі спостережених подій і аномальних даних. Зазвичай це робиться за допомогою певної форми сигнатури, аномалії або на основі статистики. Це призводить до створення даних сповіщення. Незважаючи на те, що основна частина виявлення виконується програмним забезпеченням, деяке виявлення відбувається шляхом ручного аналізу джерел даних. Особливо це стосується ретроспективного аналізу.

Аналіз є завершальним етапом циклу NSM, і він відбувається, коли людина інтерпретує та досліджує дані. Це часто включатиме збір додаткових дослідницьких даних з інших джерел, дослідження розвідувальних даних із відкритим кодом (OSINT), пов'язаних із типом сповіщення, створеного механізмом виявлення, та проведення OSINT-досліджень[11], пов'язаних із будь-якими потенційно ворожими хостами. Існує безліч способів проведення аналізу, але це може включати такі завдання, як:

1. Аналіз пакетів
2. Криміналістична експертиза мережі
3. Криміналістична експертиза хосту
4. Аналіз шкідливого програмного забезпечення

Системи виявлення вторгнень (IDS – Intrusion Detection Systems) є одними з найбільш використовуваних засобів безпеки. Вони в основному складаються з датчика, аналізатора та механізму виявлення. Якщо ці системи також дозволяють розгортати захисну відповідь на атаки вони називаються системами запобігання вторгненням (IPS – Intrusion Prevention Systems). Деякі з IDS еволюціонували до систем керування подіями безпеки (SEM – Security Event Management), які включають модуль інтегратора для покращення можливостей виявлення шляхом збору даних із різних джерел [12].

IDS – це системи, які реалізують набір методів для виявлення підозрілих дій (потенційних вторгнень) шляхом моніторингу та аналізу подій у мережі чи пристрої [12, 13]. Вони класифікуються як Host IDS (HIDS) і Network IDS (NIDS) відповідно до походження зібраних даних [13, 14]. HIDS розгортаються в кінцевих системах (хостах) і відстежують активність користувачів і поведінку внутрішніх процесів. NIDS спочатку збирають дані з мережі за допомогою датчиків мережевого трафіку; потім вони аналізують дані, щоб виявити порушення безпеки. Незалежно від типу IDS, коли дані отримані та ідентифіковані як (потенційно) шкідливі, система сповіщає операторів безпеки. Оскільки найвідоміші IDS є відкритими, ми розглядаємо лише цю категорію.

Snort це найпопулярніший IDS, його також можна використовувати як сніфер [13]. Snort - це NIDS на основі сигнатур, який дозволяє сканувати порти, а також реєструвати та сповіщати про будь-яку визначену аномалію. В останніх випусках цей IDS також дозволяє визначати базові відповіді у формі правил, які дозволяють блокувати мережевий трафік, пов'язаний із даним сповіщенням. Unified2 - це вихідний формат журналу, створений Snort. Реєстрація може генеруватися в трьох режимах: реєстрація пакетів, реєстрація попереджень і справжня уніфікована реєстрація. Журналювання пакетів використовується для захоплення пакетів, тоді як журнал попереджень реєструє лише події IT-безпеки. Справжнє уніфіковане журналювання дозволяє записувати як події, так і пакети.

Suricata - це мережева IDS у реальному часі та мережева IPS. Він відстежує мережевий трафік і виконує офлайн-обробку файлів pcap. Suricata базується на підписах і надає вивід у стандартних форматах, таких як YAML або JSON, але його також можна налаштувати для створення журналів у Unified2 [15].

OSSEC - це HIDS з відкритим кодом, який виконує аналіз журналів, перевірку цілісності, моніторинг записів Windows і виявлення руткітів. Крім того, OSSEC надає сповіщення та зберігає копії змінених файлів. Це також дозволяє налаштувати правила брандмауера для блокування зловмисного мережевого трафіку, включаючи певні IP-адреси. OSSEC є мультиплатформенним, оскільки його можна використовувати в більшості операційних систем. Незважаючи на те, що цей механізм має деякі функції SIEM, такі як можливість

кореляції журналів з кількох пристроїв і форматів, а також механізми для відповідності політикам безпеки, він традиційно вважається IDS [16].

Система управління подіями безпеки (SEM – Security Event Management) відповідає за збір, аналіз і посилення індикацій і попереджень для виявлення та реагування на вторгнення. Його метою є візуалізація та розуміння мережевих даних за допомогою єдиного уніфікованого інструменту, який поєднує різні джерела даних. З цією метою SEM дозволяє перемикатися між різними джерелами даних для проведення аналізу даних, що значно скорочує час, необхідний для розслідування інциденту безпеки (особливо якщо звітування здійснюється за допомогою графічних засобів). Однією з особливостей, яка робить систему SEM таким потужним інструментом, є те, що вона дозволяє візуалізувати та пріоритезувати події, таким чином допомагаючи операторам служби безпеки інтерпретувати та розуміти сигнали тривоги [13].

Систему безпеки та управління подіями (SIEM – Security Information and Event Management) можна описати відповідно до визначення Gartner [17] як систему, яка «аналізує дані про події в режимі реального часу для раннього виявлення цілеспрямованих атак і витоку даних, а також збирає, зберігає, розслідує та звітує про дані в журнал для реагування на інциденти». Системи SIEM - це комбінація двох різних систем: SEM і систем керування інформацією про безпеку (SIM). Основна відмінність від SEM полягає в тому, що SIEM також створює звіти та включає функції для відповідності нормативним вимогам, тоді як SEM не обов'язково цього робити (насправді, це функція, яка зазвичай надається модулем SIM). SIEM є найпопулярнішим (і дорогим) типом систем інтеграції в галузі.

Zeek був розроблений Верном Паксоном і Робіном Соммером як дослідницька робота. Зараз він еволюціонував і широко використовується компаніями, а також дослідницькими та освітніми організаціями [18]. Це повний інструмент з відкритим кодом для NSM, який дозволяє як виявляти аномалії, так і виявляти інциденти на основі сигнатур [12, 18]. Zeek збирає мережевий трафік за допомогою libpcap. Потім механізм подій обробляє дані, виконуючи пасивний аналіз таких даних. Це також дозволяє збирати й аналізувати сеанси певних служб. Крім того, Zeek можна запрограмувати на виконання дій при оцінці подій (наприклад, на виконання програми для забезпечення активної реакції на виявлену подію).

Prelude це SIEM для Linux, який збирає, поєднує та контролює події безпеки. Prelude реалізує стандартний формат IDMEF (RFC 4765) як частину компонента синтаксичного аналізу, щоб він міг читати широкий спектр форматів журналів [19]. Крім того, він створює звіти про події. Його інтерфейс забезпечує криміналістичний режим, який дозволяє досліджувати дані за великі періоди. Цей SIEM можна використовувати в комерційній версії, ціни на яку налаштовуються для кожної організації та залежать від обсягу заходів.

Wazuh - це SIEM для виявлення вторгнень на основі сигнатур, який був розроблений одноіменною компанією [20]. Wazuh базується в OSSEC і використовується в поєднанні з Elastic Stack. Це дозволяє контролювати систему для аналізу безпеки, виявлення вторгнень і вразливостей. Крім того, Wazuh забезпечує реагування на інциденти безпеки, включаючи цілісність і відповідність [20]. Завдяки функціям Elastic Stack реалізовано компонент парсингу.

OSSIM (Open Source Security Information Management) - це SIEM, розроблений компанією Alien Vault (AT&T Cybersecurity з лютого 2019 року) [21], і він використовує модуль аналізу загроз Open Threat Exchange (OTX), який дозволяє користувачам вносити та отримувати оновлену інформацію про безпеку в режимі реального часу. Можливості OSSIM включають виявлення активів, оцінку вразливостей, виявлення вторгнень, моніторинг поведінки та кореляцію подій. Він інтегрує різні програмні модулі, щоб забезпечити повне рішення NSM. Серед інших інструментів це рішення включає як хост, так і мережевий IDS. Частина NIDS забезпечує виявлення вторгнень і сканування мережевого трафіку. Він також шукає сигнатури останніх атак, а також зловмисне програмне забезпечення або інші можливі способи спроб скомпрометувати систему. HIDS аналізує поведінку та стан системи, сповіщаючи, коли підозрює, що щось не так. Подібно до інших SIEM, OSSIM дозволяє виявляти та пріоритезувати найважливіші загрози та аномалії.

UTM – це тип багатофункціонального продукту мережевої безпеки, який використовується малим і середнім бізнесом [22]. Ці пристрої мають функціональні можливості високого рівня (багатофункціональний шлюз), якими можуть бути, наприклад, брандмауер на прикладному рівні моделей TCP/IP та OSI, запобігання та виявлення вторгнень (IPS та IDS), антивірус, захист від спаму та антифішинг. Основними перевагами UTM є їх низька вартість і складність, а недоліками є те, що UTM зазвичай мають обмежену потужність обробки, і вони не можуть корелювати події. Оскільки це апаратне рішення, неможливо знайти реалізації з відкритим кодом. Таким чином, ми включаємо лише комерційні інструменти в цій частині огляду.

Barracuda CloudGen Firewall - комерційний UTM, який забезпечує виявлення вторгнень і захист. CloudGen Firewall також захищає від відомих атак, таких як відмова в обслуговуванні (DoS) або ботнет-атаки. Крім того, це рішення забезпечує автентифікацію та підключення до VPN. Його брандмауер дозволяє перевіряти та фільтрувати пакети [23].

WatchGuard - комерційний UTM, який забезпечує виявлення вторгнень і захист. WatchGuard корелює дані з різних джерел, що покращує його здатність виявляти загрози та реагувати на них, а також генерувати звіти. Крім того, він забезпечує антивірусні функції та контроль програм, який пов’язаний з поведінкою користувача. WatchGuard пропонує розширений блокувальник постійних загроз, який дозволяє виявляти складні атаки, такі як програми-вимагачі, і діяти проти них; а також має функцію запобігання спаму [25].

Sophos - комерційний UTM, який забезпечує виявлення вторгнень і захист. Sophos дозволяє виявляти загрози та діяти проти них. Коли Sophos виявляє заражену систему, вона ізолює цю систему. Крім того, він надає механізми віддаленого доступу, такі як VPN. Це рішення також включає розширений брандмауер для моніторингу даних трафіку та функції захисту від спаму [26]. Sophos класифікується як лідер у Gartner’s Magic Quadrant у 2018 році [24].

Колекції інструментів - це інструменти мережевої безпеки, які складаються з низки різнорідних програмних рішень. Крім того, оскільки вони є з відкритим кодом, вони постійно розвиваються.

Sguil — це набір інструментів з відкритим кодом для моніторингу безпеки мережі, який дозволяє збирати, аналізувати, сповіщати та реагувати на вторгнення. Sguil надає інтерфейс реального часу та включає два IDS. Деякі інструменти з набору Sguil: [27]:

1.MySQL, як служба бази даних.

2. Snort і Suricata для виявлення та сканування вторгнень у мережу, а також для реєстрації пакетів і вирішення інцидентів.

3. Tcpdump, для збору мережевого трафіку з журналів пакетів.

4. Wireshark для аналізу зібраних пакетів.

Security Onion - це набір інструментів з відкритим кодом, який надається як дистрибутив Linux. Security Onion дозволяє відстежувати, записувати та керувати журналами, а також виконувати виявлення вторгнень і реагувати на інциденти безпеки IT. Він реалізує всі модулі NSM. Деякі інструменти з набору Security Onion [28]:

5. Elastic Stack і Logstash, як механізм пошуку та аналізу, який також перетворює та централізує дані, забезпечуючи функціональні можливості візуалізаці.

6. Snort, Suricata та Zeek для виявлення мережевих вторгнень, сканування та видачі сповіщень, а також для реєстрації пакетів.

7. Wazuh, для виявлення вторгнень на хост.

8. Sguil для моніторингу безпеки мережі та аналізу приводу подій.

9. Squert для перегляду та візуалізації даних Sguil.

10. Cyberchef для шифрування, стиснення та аналізу даних.

11. NetworkMiner, для криміналістичного аналізу.

Журнали брандмауера є одним із найкорисніших джерел даних безпеки, оскільки вони надають інформацію про кожен доступ (невдалий чи успішний, авторизований чи ні) до

мережі. Однією з головних переваг брандмауерів є те, що їх можна знайти в будь-якій мережі. Наприклад, Windows Defender в операційних системах Windows 10, але є також вдосконалені брандмауери, такі як Sophos, які фактично включені в рішення UTM.

Інструменти оцінки вразливостей запускаються в мережі та кінцевих системах. Ці інструменти виявляють слабкі місця та діри в безпеці, які можуть уможливити несанкціонований доступ до системи. Двома добре відомими інструментами для цієї мети є Nmap і Nessus. Nmap (Network Mapper) - це програма з відкритим кодом для сканування портів для оцінки безпеки операційних систем, що дозволяє виявляти вразливості та надавати корисну інформацію про відкриті порти та служби. Хоча спочатку Nmap розроблявся для Linux, тепер він є мультиплатформенним. Nessus також є багатоплатформною програмою для сканування вразливостей в операційних системах. Спочатку Nessus був з відкритим вихідним кодом, але тепер це приватне програмне забезпечення (хоча існують альтернативи з відкритим кодом, такі як OpenVAS (Open Vulnerability Assessment Scanner)). Аналіз оцінки вразливості зазвичай починається зі сканування портів, яке можна зробити, наприклад, за допомогою Nmap. Після виявлення відкритих портів Nessus надсилає кілька запитів проти таких портів, щоб виявити наявні вразливості. Результати можна експортувати в різні формати, такі як простий текст або XML. Іншими корисними ресурсами, які дозволяють отримати дані про вразливості, є національна база даних вразливостей (NVD – National Vulnerability Database) і бази даних загальних вразливостей (CVE – Common Vulnerabilities and Exposures). NVD - це державна служба, яка надається Національним інститутом стандартів і технологій США (NIST) для перерахування та класифікації існуючих уразливостей у поточному програмному та апаратному забезпеченні [29]. CVE - ще одна подібна послуга, що надається MITRE6, яка також включає NVD. Ці бази даних пропонують найновішу інформацію про відомі вразливості в операційних системах і програмах/службах, а також про їх вирішення (якщо відомо). Уразливості зазвичай виявляють за допомогою будь-якого з вищезгаданих або подібних інструментів.

Системи FIM дозволяють виявляти зміни у файлах, що зберігаються на пристроях, відносно базової копії таких файлів. Деякі з параметрів, які перевіряє FIM, це: дата модифікації/створення, дозволи на доступ і модифікацію, і контрольна сума (хеш) вмісту. Однією з проблем цього типу джерела даних є величезний обсяг даних і кількість помилкових спрацьовувань, які вони, як правило, генерують. Одним із інструментів, який реалізує можливості FIM, є OSSEC.

Threat Intelligence – це механізм, схожий на соціальну мережу або канали RSS, який дозволяє користувачам отримувати оновлену інформацію про загрози безпеці та/або проблеми. Це дозволяє обмінюватися корисною інформацією про безпеку між організаціями, що також може бути корисним для вдосконалення механізмів виявлення. Наприклад, якщо організація виявляє нову атаку, решта організацій, які використовують аналіз загроз, отримують інформацію, що дозволяє їм запобігти атаці або боротися з нею більш ефективним способом. Крім того, Threat Intelligence використовує знання, пов’язані з організацією, включаючи контекст або індикатори ризику, а також наявні звіти про попередні атаки, серед інших даних [30]. Мета використання інформації від організації полягає в тому, щоб передбачити загрози на основі попереднього досвіду, беручи до уваги загрози як внутрішніх, так і зовнішніх організацій. Інструменти Threat Intelligence відповідають за збір цієї інформації та створення звітів, які можна інтегрувати з іншими механізмами безпеки, такими як системи SIEM. Threat connect і Cyber Threat Alliance є двома комерційними інструментами для аналізу загроз, тоді як Open Threat Intelligence і Collective Intelligent Framework є прикладами рішень з відкритим кодом.

**Висновки.** У цій статті було розглянуто сучасний стан моніторингу безпеки мережі (NSM), надано загальне розуміння та уніфіковану класифікацію його основних компонентів. Розглянуто програмні багатомодульні рішення, проаналізовано деякі інструменти безпеки мережі, які реалізують декілька модулів NSM. А саме системи виявлення вторгнень (IDS) / системам запобігання вторгненням (IPS), системам керування подіями безпеки (SEM) / системам керування інформацією та подіями безпеки (SIEM), універсальний контроль загроз (UTM) і колекції інструментів; включаючи приклади як відкритих, так і комерційних рішень. Ці модулі можна комбінувати різними способами, створюючи потужну та масштабовану архітектуру для виявлення інцидентів. Висвітлено сильні та слабкі сторони визначених модулів. Було розглянуто деякі з найвідоміших і широко використовуваних багатомодульних рішень NSM. Найвідомішими прикладами таких комбінацій є IDS/IPS, SEM/SIEM і UTM. Серед SIEM систем у плані функціоналу немає рішень, що явно виділяються. Однак системи Prelude та OSSIM добре підходять лише для невеликих мереж, у той час як OSSEC не має проблем із продуктивністю при використанні у великих проектах. Узагальнено відкриті питання та майбутні дослідницькі інтереси для кожного з модулів NSM. Таким чином, ландшафт безпеки як для традиційних, так і для сучасних мереж виграє від проектування систем, які включають усі визначені компоненти та комбінація різних систем багатомодульних рішень. Ба більше, все ще необхідно надавати ефективні рішення, які враховують обмежені ресурси, а також покращують стійкість у критичних інфраструктурах.

REFERENCES:


1. Samson R., (2020) “Prevention vs DetectionBased Security Approach,” Clearnetwork, www.clearnetwork.com/prevention-vsdetection-cybersecurity-approach/, *Tech. Rep*.,
2. Rapid7, (2015) “Prevention vs Detection, Rebalancing Your Security Program,” www.rapid7.com/resources/prevention-vsdetection/
3. Comodo, (2020) “Advanced Threat Protection: Security Incident Response Tools,”, *Tech. Rep.*
4. Bejtlich, R. (2005) The TAO of the Network Security Monitoring. Beyond Intrusion Detection.
5. Camacho, J. Maciá-Fernández, G. Verdejo, J. E. D. and García-Teodoro, P. (2014) “Tackling the Big Data 4 Vs for Anomaly Detection,” *INFOCOM’2014 Workshop on Security and Privacy in Big Data*, pp. 500–505
6. X. Ji, K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You, X. Xu, H. Zhao, J. Wu, and M. Yi, (2018) “Overview of 5G security technology,” Science China Information Sciences, vol. 61, no. 8, pp. 1869–1919,.
7. Thudumu, S. Branch, P. Jin, J. and Singh, J. J. “A comprehensive survey of anomaly detection techniques for high dimensional big data,” vol. 7, no. 1.
8. Fuentes-García, M. Camacho, J. and Maciá-Fernández, G. “Present and Future of Network Security Monitoring” 10.1109/access.2017.doi
9. US Department of Defense Instruction 8500.2, (2003) “Information Assurance (IA) Implementation” http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf.
10. Sanders, C. (2014). “The Practice of Applied Network Security Monitoring. Applied Network Security Monitoring”, 1–24. doi:10.1016/b978-0-12-417208-1.00001-5
11. Dokman, T. Ivanjko, T. (2020). “Open Source Intelligence (OSINT): issues and trends”. doi:10.17234/infuture.2019.23
12. Collins, M. “Network Security Through Data Analysis. Building situational awareness”, *O. Media, Ed. O’Reilly*, 2014.

13. INCIBE, (2017) “Diseño y Configuración de IPS, IDSy SIEM en Sistemas de Control Industrial,” https://www.incibe-cert.es/blog/diseno-yconfiguracion-ips-ids-y-siem-sistemas-controlindustrial

14. Alpcan, T. and Basar, T. (2011) “Network Security. A Decision and Game-Theoretic Approach”. *Cambridge University Press*

15. ATT Cybersecurity, (2020) “Suricata IDS: an overview of threading capabilities,” https://cutt.ly/jyZbAeI, *Tech. Rep*.

16. OSSEC Project Team,(2008) “Open Source HIDS SECurity,” https://www.ossec.net/

17. Gartner, (2019) “What is Security Information and Event Management (SIEM)?” https://www.gartner.com/reviews/market/securityinformation-event-management

18. Paxson, V. and Sommer, R. “The Zeek Network Security Monitor (Bro),” https://www.zeek.org/

19. Prelude, (2020) “PRELUDE SIEM. Smart Security,” https://cutt.ly/bfTTiuN

20. Wazuh Inc., (2019) “The Open Source Security Platform,” https://wazuh.com/

21. AT&T-cybersecurity,(2019) “AlienVault(R) Unified Security Management(R) (USM),” https://www.alienvault.com/products

22. Gartner, (2019) “Unified Threat Management (utm)” https://www.gartner.com/en/informationtechnology/glossary/unified-threat-management-utm

23. Barracuda, (2020) “Barracuda CloudGen Firewall,” https://cutt.ly/FgefB

24. BAKOTECH, (2018) “WatchGuard UTM is Recognized the Only Visionary in the Gartner Magic Quadrant for the 4th Time,” https://bit.ly/3aNkYO8

25. WatchGuard, (2020) “WatchGuard Security Services,” https://www.watchguard.com/wgrdproducts/security-services

26. Sophos, (2020) “The world’s best visibility, protection, and response,” https://www.sophos.com/enus/products/next-gen-firewall.aspx

27. Visscher, B. (2014) “Sguil,” https://sourceforge.net/projects/sguil/

28. Security Onion Solutions, (2008) “Security Onion,”https://securityonion.net/

29. National Institute of Standards and Technology (NIST), (2019) “National Vulnerability Database (NVD),” https://nvd.nist.gov/

30. Molina, J. (2016) “Threat Intelligence: el porqué de las cosas,” https://www.welivesecurity.com/laes/2016/12/01/threat-intelligence/.

**Ph. D. Minochkin D.A.,**
**Nser A.M.**

## SOFTWARE METHODS OF NETWORK SECURITY MONITORING

***The software methods for monitoring network security (NSM - Network Security Monitoring) are discussed. With the growth and rapid development of mobile communications, rich data and artificial intelligence technologies, we are entering the era of the mobile Internet. With the continuous intellectualization of network security and infrastructure, information technology is widely used in the field of industrial control, making network security more and more open, bringing a new network security control system to the traditional relatively closed industrial control system. Currently, there is an increase in the number of information threats and factors leading to the unstable operation of data transmission networks. The prerequisites for this growth are the mass application, the complication of the hierarchy of computer networks and the increase in their structural complexity, the increase in the heterogeneity of software and hardware, the complication of the functionality of network services, which leads to the emergence of various vulnerabilities. Under such conditions, the development and improvement of methods for identifying information threats are of great importance. One of the components of ensuring information protection of networks is software systems designed to detect harmful or suspicious activity - network security monitoring methods (NSM). Network security monitoring techniques (NSM) are used to monitor network***

***communications for information security events. For maximum effect, a combination of capturing the entire packet in addition to logging network activity is recommended.***

***This article provides definitions of network security monitoring methods, their classification, phases of the method cycle and their description. Some of the best known and widely used multi-module NSM solutions have been reviewed. The best known examples of such combinations are IDS/IPS, SEM/SIEM and UTM.***

***Network security monitoring is important because it checks if the first lines of defense are working, gives us the opportunity to eliminate threats before they cause real damage if there is a vulnerability somewhere in your system, and allows us to understand where these vulnerabilities are and how to fix them before something will happen.***

***Keywords: NSM, Network Security Monitoring, network security monitoring software methods.***

**УДК 351.74**

**Черноусов Д. О. (НАДПСУ)**
к. військ. н. **Поліщук В. В. (НАДПСУ)**
д. т. н. **Бабій Ю. О. (НАДПСУ)**
**Мартинюк В. П. (НАДПСУ)**
**Мартинюк О. В. (НАДПСУ)**

DOI: https://doi.org/10.17721/2519-481X/2022/77-12

# ДЖЕРЕЛА, ХАРАКТЕР ЗАГРОЗ ТА ВИКЛИКІВ НА ДЕРЖАВНОМУ КОРДОНІ УКРАЇНИ

***Зважаючи на основні тенденції та наслідки глибинних трансформацій геополітичного та геоекономічного простору, виникла потреба в проведенні ґрунтовних досліджень у сфері забезпечення прикордонної безпеки нашої держави, як складової національної безпеки, а також визначення чіткого місця і ролі суб'єктів її гарантування в ході реалізації зазначеної функції, особливо з появою нових видів загроз, зокрема військової агресії російської федерації, яка 24 лютого 2022 року перейшла у фазу відкритого протистояння проти України, тимчасової окупації нею території Автономної Республіки Крим і м. Севастополя, Херсонської області та ряду інших територій нашої держави. Своєю чергою виникла нагальна потреба в обґрунтуванні структури та змісту сучасної моделі прикордонної безпеки, як основи подальшого розвитку Державної прикордонної служби України, окрім того, для України питання прикордонної безпеки, з огляду на курс євроатлантичної інтеграції та останнє розширення Європейського Союзу, геополітичне положення України обумовлюють той факт, що кордони нашої держави відіграють важливу і загальновизнану роль у формуванні системи загальноєвропейської безпеки. Слід зауважити, що інтереси України і європейського співтовариства стосовно управління спільними кордонами, безумовно, збігаються. Це забезпечення надійної охорони протяжних ділянок державного кордону України; безперешкодне законне перетинання кордону громадянами і транспортними засобами у пунктах пропуску поряд із високим рівнем контрольних процедур; належне управління міграційними потоками; ефективна протидія проявам організованої транскордонної злочинності тощо. Наша держава підтримує створення принципово нової системи європейської безпеки, яка базується на несилових (політичних, економічних, соціальних, енергетичних, екологічних, інформаційних тощо) аспектах. Таким чином, необхідним є обґрунтування структури та змісту моделі прикордонної безпеки, що є основою формування та реалізації сучасної прикордонної політики європейського зразка, зокрема, приведення прикордонного законодавства України до норм європейського права; забезпечення готовності людських ресурсів; технічного переоснащення; досягнення сучасного стану інфраструктури державного кордону; інформаційної інтеграції; якісно нового рівня прикордонного співробітництва. З огляду на вище зазначене, у статті розроблені концептуальні засади прикордонної безпеки України, її прикордонної політики, а також механізму їх реалізації. Виконання вищезазначених завдань сприятиме реалізації стратегічного курсу України на інтеграцію до Європейського Союзу та забезпечить підвищення ефективності діяльності Державної прикордонної служби України у сфері забезпечення національних інтересів держави взагалі та на державному кордоні зокрема.***

***Ключові слова: ризик; загроза; національна безпека; прикордонна безпека; модель прикордонної безпеки.***

**Вступ.** Радикальні зміни міжнародної обстановки, які відбуваються, значно впливають на погляди щодо характеру загроз безпеці у прикордонному просторі, шляхів їх своєчасного виявлення, запобігання та нейтралізації. Тому є актуальними виявлення, формулювання та систематизація проблем, що виникають, загострилися та мають перспективу розвитку у сфері

прикордонної безпеки. Їх розгляд доцільно проводити через призму аналізу воєнно-політичних викликів, ризиків та загроз на державному кордоні з точки зору їх практичного забезпечення в умовах швидкоплинних змін в міжнародному та загальносвітовому безпекових середовищах.

**Постановка проблеми.** Роль, місце та функції Державної прикордонної служби України (далі – ДПСУ) у забезпеченні безпеки державного кордону були закладені ще у 1991 році та з прийняттям низки законодавчих документів [1–5]. Зокрема кожен новий збройний (воєнний) конфлікт примушує корегувати моделі застосування органів (підрозділів) військових та правоохоронних формувань, зокрема ДПСУ.

Спектр основних можливих загроз національній безпеці України у воєнно-політичній сфері розкрито в Законі України «Про основи національної безпеки України» [6], Воєнній доктрині [7] та Стратегії національної безпеки України [4]. Проте на сьогодні вони потребують уточнення та конкретизації місця та ролі ДПСУ з урахуванням їх забезпечення у прикордонному просторі.

**Аналіз останніх досліджень і публікацій.** Забезпечення національної безпеки у прикордонному просторі буде можливим при відповіді на питання, що необхідно зробити ДПСУ для її забезпечення. Результат залежатиме від розуміння змісту поняття «національна безпека України у прикордонному просторі» (далі – нацбезпека) як складової національної безпеки України, де необхідно виділити процеси забезпечення захищеності інтересів людини і громадянина, суспільства і держави [1]. Такий підхід дозволить зрозуміти: де, як та коли виникають у цих процесах перешкоди і передбачити ризики, виклики та загрози їх виникнення та джерела. Без методологічного встановлення змісту зазначених понять для умов забезпечення національної безпеки України у прикордонному просторі не можливе їх визначення та градація.

**Мета статті** – розкрити структуру та зміст моделі прикордонної безпеки, як основи подальшого розвитку Державної прикордонної служби України, що є основою формування та реалізації сучасної прикордонної політики європейського зразка.

**Основна частина.** Нацбезпека є складною системою, де тільки люди здатні вибирати способи, прийоми та методи діяльності, які захищають від загроз або націлені на їх знешкодження, ґрунтуючись на аналізі можливості зміни характеру та змісту умов зниження безпеки [8,9]. У прикордонному просторі, як і взагалі, безпека і небезпека існують в умовах взаємодії суб'єктів і об'єктів та середовища їх існування. До них можемо віднести ДПСУ, державні органи, громадські організації та інші установи, до компетенції яких відноситься забезпечення нацбезпеки людині, громадянину, суспільству, державні інтереси яких захищаються, суміжна країна та її компетентні органи та організації, представники злочинного середовища, об'єкти промислової та іншої діяльності, природне, історичне, економічне та інші середовища. Своєю чергою, приходимо до висновку, що нацбезпеку у прикордонному просторі можемо уявити як трьох компонентну складову:

відсутність небезпеки для «людини – громадянина – суспільства – держави»;

захищеність «людини – громадянина – суспільства – держави» у випадку виникнення небезпеки;

наявність засобів і сил та їх здатність попереджувати та долати небезпеку.

Зміст нацбезпеки у прикордонному просторі необхідно уявляти як багатофакторну, багатофункційну та багаторівневу складну систему, яка повинна забезпечити найбільший баланс між життєво важливими інтересами «людини - громадянина – суспільства – держави» та створення необхідних умов щодо функціонування системи їх відношень. Крім того, нацбезпека повинна забезпечувати необхідний рівень непохитності розвитку «людини - громадянина – суспільства – держави», вона також залежить від: національної ідеї як вкладу у розвиток міжнародного співтовариства, де українська держава своїм розвитком підтверджує цей тезис; виживання в кризових міжнародних умовах; реалізації національних інтересів як в середині, так і за межами країни, включаючи силове протистояння у глобальних та регіональних конфліктах.

Нацбезпека у прикордонному просторі є сегментом національної безпеки України, де у прикордонному просторі забезпечується життєво важливі потреби існування та розвитку людини, громадянина, суспільства, держави та середовища їх існування, а також здійснюється їх захист від негативного впливу внутрішніх і зовнішніх факторів. Вивчення Конституції України дозволило згрупувати життєво важливі потреби:

*Людини – громадянин*

Забезпечення прав та свобод;

Духовний та інтелектуальний розвиток;

Гідність людини;

Збереження його життя, здоров'я;

Особиста безпека;

Відповідний рівень матеріальних умов існування за умов сталої тенденції його росту.

*Суспільства*

Формування зрілого суспільства;

Зміцнення сім'ї;

Контроль суспільства над державою;

Подолання демографічного та екологічного кризисів;

Поступовий економічний розвиток;

Духовне відродження нації та її інтелектуальний розвиток.

*Держави*

Захист суверенітету та територіальної цілісності;

Створення основ правової демократичної держави;

Соціально-політична і економічна стабільність;

Захист конституційного устрою та правопорядку, шляхом боротьби з корупцією і організованою злочинністю;

Ефективна зовнішня / внутрішня політика;

Забезпечення обороноздатності країни.

Висновком міркувань над змістом нацбезпеки у прикордонному просторі буде те, що перераховані вище життєво важливі потреби постійно знаходяться під впливом певних умов. Серед них негативні створюють небезпеку існуванню і розвитку «людини – громадянина – суспільства – держави».

Важливе значення для розуміння небезпеки є їх трактування. Тому небезпека - це об'єктивне існування можливого впливу на об'єкт безпеки, який може нанести збиток, принести шкоду, погіршити його стан, надати розвитку не бажану динаміку або параметри. Таке визначення дозволяє ранжувати небезпеки в залежності від масштабів шкоди, яка може бути заподіяна життєво важливим потребам, а також національним інтересам України.

Воєнна доктрина України визначає три види небезпек: військово-політичні ризики, військово-політичні виклики, загроза застосування воєнної сили. Аналіз зарубіжних та вітчизняних джерел [10–13] свідчить про різні погляди на трактування понять «ризики», «виклики», «загрози» та їх ранжування. Пропонується розглядати їх як різні ступені впливу на забезпечення національної безпеки у прикордонному просторі. У понятійному ряду ризик є найнижчим рівнем небезпеки, а загроза її найвищим рівнем.

Наш підхід буде спиратись на прийняті в нашій країні загальнодержавні поняття відповідно до Стратегії національної безпеки України [3]. Зміст поняття «воєнно-політичний ризик» викладено як наміри або дії однієї зі сторін зовнішніх або внутрішніх відносин, які спрямовані на досягнення власних інтересів і можуть за певних умов опосередковано заподіяти шкоду національним інтересам іншої сторони [7]. Приведене поняття ризику забезпечення захищеності «людини – суспільства – держави» не повністю відображає зміст та особливості діяльності ДПСУ як суб'єкта складової державних гарантій цього процесу та є загальним. Воно потребує уточнення, базуючись на зовнішньому і внутрішньому середовищах прикордонного простору та воєнного конфлікту, в якому перебуває зараз наша країна.

Враховуючи різні тлумачення поняття «воєнно-політичний ризик» та особливості службово-бойової діяльності ДПСУ, поняття «воєнно-політичний ризик» можемо сформулювати наступним чином: воєнно-політичний ризик у прикордонному просторі – це сукупність обставин, факторів, намірів або дій учасників соціальних, воєнно-політичних відносин, які існують у прикордонному просторі та які за певних умов можуть призвести до зниження рівня забезпечення національної безпеки ДПСУ.

У нашому випадку, воєнно-політичний ризик - це прогнозована поява явищ у прикордонному просторі, які разом або поодинці здатні принести збиток захищеності «людини – громадянина – суспільства - держави». Його поява з негативними ознаками знижує забезпечення національної безпеки та ускладнює існування позитивного результату. Необхідно розуміти, що за певних обставин воєнно-політичний ризик може трансформуватись у більш вищу ступінь небезпеки. Різні вчені по різному вбачають таке перетікання станів, але більшість з них визнають, що наступний стан є «виклик».

Поняття «воєнно-політичний виклик» згідно [7] – це наміри або дії однієї зі сторін воєнно-політичних відносин, що спрямовані на досягнення власних цілей без урахування інтересів іншої сторони, з усвідомленням можливості заподіяння шкоди таким інтересам.

Так О. В. Левченко, В. В. Троцький, І. С. Василенко [14] вважають, що приведене вище визначення поняття «воєнно-політичний виклик» не дозволяє на практиці провести межу або відокремити його від поняття «воєнно-політичний ризик», тому вони пропонують під викликом розуміти сукупність обставин, факторів та дій протилежної воєнно-політичної сили, які призвели (призводять) до формування передумов до виникнення воєнної загрози Україні. Продовжує їх думку А. А. Сергунін [15], де він розглядає виклик як сукупність обставин, на які необхідно реагувати і у тому випадку, коли вони не несуть загрози, тому що вони негативно впливають на стан безпеки. Деякі вчені вбачають у виклику початок формування загрози.

Проаналізувавши погляди різних вчених щодо змісту поняття «виклик» в умовах забезпечення нацбезпеки у прикордонному просторі, це тлумачення потребує уточнення з урахуванням вище приведених думок. Так, поняття «воєнно-політичний виклик» – це виявлена дія або сукупність дій однієї зі сторін воєнно-політичних відносин, які спонукають іншу сторону до заходів щодо нейтралізації їх негативного впливу на стан національної безпеки у прикордонному просторі та запобігання перетікання їх у воєнну загрозу.

Забезпечення захисту України від загроз є одним із пріоритетних напрямів діяльності держави, що законодавчо визначено та закріплено у відповідних актах. Зміст воєнної загрози як виду небезпеки сформульовано у Воєнній доктрині України [7]. Її найвищім станом є загроза застосування воєнної сили. Саме поняття «загроза застосування воєнної сили» містить наміри або дії однієї зі сторін воєнно-політичних відносин, які свідчать про готовність до застосування воєнної сили проти іншої сторони з метою досягнення власних цілей.

Різні групи вчених по різному тлумачать зміст воєнної загрози [16; 17], де значення слова «загроза» визначається як можливість або неминучість виникнення чогось небезпечного, прикрого, тяжкого для кого, чого-небудь; те, що може заподіяти яке-небудь зло, якусь неприємність, або як сукупність умов і факторів, які створюють небезпеку життєво важливим інтересам особистості, суспільства й держави. Також загрозу трактують як можливість виникнення якогось чинника, здатного заподіяти яке-небудь зло певному об’єкту. Спираючись на наведене та положення Воєнної доктрини України, під поняттям «загроза застосування воєнної сили» пропонується розуміти дії протилежної воєнно-політичної сили, які свідчать про безпосередню підготовку або готовність до застосування воєнної сили проти України [14].

Тлумачення понять «ризик», «виклик», «загроза» приводить до необхідності їх ранжування у відповідності до небезпеки, яку вони можуть заподіяти захищеності інтересів людини і громадянина, суспільства і держави у прикордонному просторі. Їх розставлення за важливістю необхідно здійснити в залежності від рівня міждержавних відношень. Так, першим рівнем вважати міждержавні відносини, де відсутній прямий конфлікт інтересів, а другим –міждержавні відносини, де є ознаки підготовки суміжної держави або групи держав

до вирішення суперечностей воєнним шляхом. Принципова відмінність між такими рівнями небезпеки лежить у площині врегулювання суперечностей, що виникають. Так на першому рівні їх розв'язання може здійснюватись шляхом укладання міждержавних угод, проведення робочих зустрічей найвищих посадових осіб держав, створення міждержавних комісій тощо, своєю чергою, другий рівень потребує заходів військового характеру.

Деякі вітчизняні та іноземні військові науковці не розглядають взагалі міждержавні відносини як фактор ранжування небезпек. Їх погляди спрямовуються до зв'язування ступенів небезпек з підготовкою до застосування воєнної сили. В залежності від наростання останніх формуються заходи та ступені готовності збройних сил до військових дій [14].

Запропонований підхід не відображає змісту забезпечення захисту нацбезпеки у прикордонному просторі, він не враховує змісту понять «ризик» та «виклик» та відводить для них місце, де зароджується загроза. Така класифікація більш стосується процесу перетікання виклику в загрозу та безпосередньо загроз. По відношенню небезпеки у прикордонному просторі їх градація є іншою.

Також не менш важливим для нацбезпеки є існування небезпеки у часовому просторі. «Воєнно-політичний ризик» існує завжди, його вплив залежить від багатьох умов. Більшість вчених притримуються думки, що ризик як результат впливу на нацбезпеку у прикордонному просторі може бути протилежно полярним. Обставини, коли виник ризик як небезпека, з часом та під впливом нових обставин може існувати як не небезпека і навпаки він може посилювати свій негативний вплив.

На відміну від ризику, «воєнно-політичний виклик» відображає зростання небезпеки і потребує втручання у процеси щодо зменшення негативного впливу його на нацбезпеку в прикордонному просторі. В часі він існує з моменту виявлення та до заниження його впливу на нацбезпеку або переростання у «загрозу застосування воєнної сили».

«Загроза застосування воєнної сили» різними групами вчених трактується по різному. Більшість з них розглядають «загрозу застосування воєнної сили» як «воєнну загрозу». Так, згідно [17], загроза застосування воєнної сили - це стан військово-політичних відносин, що характеризується існуванням потенційної можливості застосування воєнної сили проти держави для досягнення політичних і інших цілей одним або групою суб'єктів цих відносин.

Такий стан військово-політичних відносин, як правило, розтягнутий у часі і необов'язково пов'язаний з військовими приготуваннями одного з суб'єктів процесу, але він вказує на потенційну можливість рішення суперечностей військовим шляхом. Його найвищим ступенем напруженості є відкрите протистояння сторін, які намагаються вирішити протиріччя воєнними діями.

Формулюючи ознаки ризиків, викликів та загроз для нацбезпеки України у прикордонному просторі необхідно зважати на вплив світових тенденцій, які несуть небезпеку. Це глобалізація як вільний ринок, де процвітають найбільш конкурентоспроможні і ефективні держави, що призводить до загострення протиріч як в середині країни, так і між державами. Загрози розповсюдження зброї масового ураження, ядерної війни; проблеми збереження навколишнього середовища, вичерпаності багатьох природних ресурсів, наростання соціальних нерівностей і злочинності тощо.

Вивчення змісту приведених вище понять приводить до висновку, що їх виникнення та існування у прикордонному просторі на сучасному етапі розвитку людства в певній мірі не залежить від суб'єктів військово-політичних відносин.

До таких чинників впливу можемо віднести:

фактори небезпек у прикордонному просторі формуються далеко від нього,

швидке скорочення часу пересування загроз у просторі;

збільшення ризиків інтернаціонального рівня;

поява ризиків з характеристикою неочікуваємості, непередбачувальності та які несуть руйнівну дію;

загальна мобільність активно сприяє виникненню небезпек та змінює значення національних кордонів.

Перераховані чинники разом з територіальними умовами створюють систему загроз для різних рівнів безпек, що вимагає структурного підходу до забезпечення протидії їх впливу, де певному рівню загроз протидіє відповідний рівень безпеки та разом з ними нижній рівень безпеки теж готовий до протидії загрози вищого порядку.

Таким чином, сьогоднішня національна безпека України в цілому, так і нацбезпека у прикордонному просторі повинна опиратись не лише на себе, а й на міжнародну співпрацю.

Досвід України сьогодні свідчить про те, що дестабілізація одного регіону призводить до проблем забезпечення безпеки в Європі в цілому.

Додатковим підтвердженням є те, що у світі з'явились трансграничні та транснаціональні загрози. Це: міжнародний тероризм; сепаратизм; організована міжнародна трансгранична злочинність; розповсюдження наркотиків; різновид міграції; порушення прав людини; розповсюдження зброї масового ураження; бідність; хвороби; занепад оточуючого середовища; воєнні конфлікти тощо.

Їх виявлення та розпізнавання ускладняються тим, що їх більшість тісно переплетені між собою. Так, тероризм тісно зв'язаний з незаконним обігом наркотиків та зброї, організована злочинність – з наркобізнесом і нелегальною міграцією, конфлікти і бідність – з міграцією тощо. За таких умов складно класифікувати небезпеки притаманні окремо прикордонному простору. Вивчення [16, 17] дозволило об'єднати небезпеки для прикордонного простору в шість груп:

соціально-економічні загрози;

міждержавні конфлікти, зокрема воєнні;

внутрішньодержавні конфлікти;

засоби масового знищення людей;

тероризм;

транснаціональна організована злочинність.

Серед причин існування визначених груп небезпек є економічні і соціальні труднощі, міжнародні та внутрішні суперечності між державами і в державі.

Для України, як і для більшості країн світу, загрозою нацбезпеки у прикордонному просторі є міждержавні та внутрішньодержавні конфлікти. На відмінність від загрози протиправної діяльності трансграничної злочинності, яка усувається правоохоронними методами, в умовах конфліктів не виключене застосування військової сили.

Щодо класифікації конфліктів, думки експертного середовища різняться. Більшість вважають що міждержавні конфлікти втрачають лідерство та їх замінюють внутрішньодержавні. Вони характеризуються сепаратизмом, крайніми формами націоналізму та релігійного фундаменталізму, тероризмом, активізацією злочинності, міграцією, вони стають початком громадянської війни [18].

Підґрунтям таких конфліктів стають проблеми економіки, соціального життя населення, боротьба за владу і інше, де держава втрачає лідерство щодо їх вирішення. Окремо необхідно зазначити роль та місце в розпалювані внутрішньодержавних конфліктів іноземних держав. Такі держави вирішують міждержавні суперечності підривом устрою країни з середини, розпалюючи внутрішні конфлікти, для утворення світових конфліктних ліній [19].

В умовах можливого застосування воєнної сили у прикордонному просторі для зниження їх негативного впливу на нацбезпеку необхідно охарактеризувати ознаки таких загроз та виділити серед них такі, яким зобов'язана протидіяти ДПСУ.

Аналізуючи вторгнення російської федерації на територію України, розпалення сепаратизму та тероризму дозволили сформулювати основні групи ознак загроз нацбезпеці у прикордонному просторі. До них відносяться:

формування антиукраїнських настроїв населення прикордоння під тиском військових;

розпалювання сепаратистських настроїв серед населення прикордоння опираючись на етнічні меншини;

різке зниження соціальних стандартів жителів прикордоння і загалом;

наростаюча міграція у пошуку кращих умов життя у найближчому прикордонні сусідньої держави;

зниження впливу та авторитету конституційних інститутів влади;

різке збільшення не конструктивних контактів на рівні прикордонних представників;

різке збільшення перетину кордону поза пунктами пропуску;

штучне обмеження пропускних операцій через кордон;

активне залучення прикордонників зі складу місцевого населення у політичні процеси, які проходять у прикордонні;

ведення розвідки у відношенні військових частин та військових формувань;

активізація транскордонної злочинності та використання її, як дестабілізуючої складової у прикордонні.

У відповідності до закону України «Про Державну прикордонну службу України» розділ 4 [1], вона повинна забезпечити протидію загрозам нацбезпеці у прикордонному просторі через виконання низки завдань. Їх згрупування може бути таким:

припинення самостійно, або у взаємодії зі Збройними Силами України і військовими формуваннями України посягань на територіальну цілісність держави;

припинення самостійно, або у взаємодії зі Збройними Силами України і військовими формуваннями України провокацій на державному кордоні України;

участь у взаємодії із Збройними Силами України та іншими військовими формуваннями у відбитті вторгнення або нападу на територію України збройних сил іншої держави або групи держав;

участь у виконанні заходів територіальної оборони, а також заходів, спрямованих на додержання правового режиму воєнного і надзвичайного стану;

боротьба з транскордонною організованою злочинністю у прикордонному просторі;

забезпечення контролю за перетином державного кордону в установленому порядку осіб, транспортних засобів, вантажів та іншого майна;

боротьба з незаконною міграцією;

виконання відповідно до законодавства системи особливих заходів щодо захисту військовослужбовців та працівників ДПСУ від зазіхань на життя, здоров'я, честь, майно у зв'язку з їх службово-бойовою діяльністю, а також їхніх близьких родичів;

протидія і запобігання корупційним діянням та злочинам у сфері службової діяльності особового складу ДПСУ;

участь у межах своєї компетенції у взаємодії з органами Служби безпеки України, органами внутрішніх справ та іншими правоохоронними органами;

участь прикордонних представників у роботі спільних міжнародних комісій з розгляду прикордонних спорів, інцидентів, конфліктів;

здійснення самостійно або разом зі спеціально уповноваженими на те органами виконавчої влади і посадовими особами контролю у районах несення служби за збереженням природних ресурсів, додержанням правил промислової та іншої діяльності, охороною довкілля;

інформаційна діяльність серед місцевого населення про обстановку на державному кордоні України, у прикордонній смузі та в контрольованих прикордонних районах.

**Висновки.** З урахуванням цих та інших факторів в безпековій, міграційній, економічній, екологічній та іншій сферах залежно від конкретних умов повинні бути диференційовані пріоритети прикордонної політики України, уточнено їхню ієрархію, коло суб’єктів і об’єктів та їх функції, роль суміжних територій в рамках позитивної транскордонної взаємодії.

Це надважливі державні завдання, які потребують теоретичного опрацювання, системних досліджень, пошуку шляхів розв’язання проблем і суперечностей, які існують у цій сфері та які будуть розглянуті нами у подальшому.

ЛІТЕРАТУРА:

1. Про Державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV. Відомості Верховної Ради України. 2003. № 27. Ст. 208.

2. Про оборону України : Закон України від 06.12.1991 № 1932-XII. Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернен

3. Про рішення Ради національної безпеки і оборони України від 25.03.2021 "Про Стратегію воєнної безпеки України" : Указ Президента України від 25.03.2021 № 121/2021. Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/121/2021#n2 (дата звернення: 13.08.2021).

4. Про стратегію національної безпеки України : Указ Президента України "Про рішення Ради національної безпеки і оборони України" від 14.09.2020 № 392/2020 "Про Стратегію національної безпеки України". Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/121/2021#n2 (дата звернення: 13.08.2021).

5. Про правовий режим воєнного стану України : Закон України від 12.05.2015 № 389-VIII. Відомості Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/389-19 (дата звернення: 14.08.2021).

6. Про основи національної безпеки України : Закон України від 19.06.2003 р. Відомості Верховної ради України. 2003. № 39.

7. Указ Президента України "Про рішення Ради національної безпеки і оборони України" від 25 вересня 2015 року № 555/2015 "Про нову редакцію Воєнної доктрини України". Відомості Верховної Ради України. URL: http://zakon.rada.gov.ua/laws/show/555/2015 (дата звернення: 14.08.2021).

8. Бабій Ю. О. Удосконалення декомпозиції загроз і небезпек національній безпеці держави у прикордонній сфері. Збірник наукових праць Національної академії Державної прикордонної служби України. Серія : військові та технічні науки. Хмельницький : Вид-во НАДПСУ, 2016. № 4(70). С. 185–196.

9. Бабій Ю. О., Лисий М. І., Балицький І. І. Декомпозиція загроз і небезпек у сфері прикордонної безпеки. Збірник наукових праць Військової академії. Одеса : Вид-во ВА, 2016. 2(6). С. 127–132.

10. Богданович В. Ю., Маначинский А. Я. Методологические основы системных исследований проблем военной безопасности государств. Киев, 2001. 172 с.

11. Косевцов В. О. Національна безпека України : теорія, реальність і прогноз : монографія. Київ : НІСД, 1999. 101 с.

12. Torichnyi V., Biletska T., Rybshchun O., Kupriyenko D., Ivashkov Yu., Bratko A. Information and propaganda component of the Russian Federation hybrid aggression: conclusions for developed democratic countries on the experience of Ukraine. Trames: A Journal of the Humanities and Social Sciences, 2022, no. 25 (3), pp. 355–368.

13. Shynkaruk, O. N., Babii, Y. A., Kyrylenko, V. A., Kupriyenko, D. A., Farion, O. B., Babaryka, A. O. Conceptual and scientifically-methodical principles of realization of policy in the field of the State border security in Ukraine : collective monograph. Lviv-Toruń : Liha-Pres, 2019. ISBN 978-966-397-184-1.

14. Левченко О. В., Троцько В. В., Василенко І. С. Уточнення понятійного апарату з питань оцінювання рівня воєнної загрози національній безпеці України. Наука і оборона. №2 URL: http://www.nio.mil.gov.ua/index.php?id=autor&lang=ua (дата звернення: 11.11.2020).

15. Сергунин А. А. Международная безопасность: новые подходы и концепты. Политические исследования. 2005. № 6. С. 126–137.

16. Ліпкан В. А. Національна безпека України URL: http://westudents.com.ua/knigi/368-natsonalna-bezpeka-ukrani-lpkan-va.html (дата звернення: 11.11.2020).

17. Bratko A., Zaharchuk D., Zolk V. Hybrid warfare – a threat to the national security of the statea. Revista de Estudios en Seguridad Internacional, 2022, no. 7 (1), pp. 147–160.

18. Радецький В. Г. Основи стратегії національної безпеки та оборони держави. Київ, 2009. С. 225.

19. Ліпкан В. А. Сутність гібридної війни проти України. Глобальна організація союзницького лідерства. URL: http://goal-int.org/sutnist-gibridnoi-vijni-proti-ukraini/ (дата звернення: 11.11.2020).

REFERENCES**:**

1. Zakon Ukrainy “Pro Derzhavnu prykordonnu sluzhbu Ukrainy” № 661-IV [Law of Ukraine about the State Border Guard Service of Ukraine activity no. 661-IV]. (2003, 3 April). Vidomosti Verkhovnoyi Rady Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/661-15 (accessed 13 August 2021).

2. Zakon Ukrainy “Pro oboronu Ukrainy” № 1932-XII [Law of Ukraine “On the Defense of Ukraine” activity no. 1932-XII]. (1991, December 6). Vidomosti Verkhovnoyi Rady Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/1932-12#Text (accessed 14 August 2021).

3. Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy “Pro Stratehiiu voiennoi bezpeky Ukrainy” № 121/2021 [Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine "On the Strategy of Military Security of Ukraine" activity no. 121/2021]. (2021, March 25). Vidomosti Verkhovnoyi Rady Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/121/2021#n2 (accessed 13 August 2021).

4. Ukaz Prezydenta Ukrainy Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy “Pro Stratehiiu voiennoi bezpeky Ukrainy” № 392/2020 [Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine "On the Strategy of Military Security of Ukraine" activity no. 392/2020]. (2020, September 14). Vidomosti Verkhovnoyi Rady Ukrayiny.

5. Zakon Ukrainy “Pro pravovyi rezhym voiennogo stany Ukrainy” № 389-VIII [Law of Ukraine “On the legal regime of martial law of Ukraine” activity no. 389-VIII]. (2015, May 12). Vidomosti Verkhovnoyi Rady Ukrayiny. Retrieved from: https://zakon.rada.gov.ua/laws/show/389-19 (accessed 14 August 2021).

6. Pro osnovy natsionalnoi bezpeky Ukrainy : Zakon Ukrainy vid 19.06.2003 r. [Law of Ukraine “On the basics of national security of Ukraine”]. (2003, March 19). Vidomosti Verkhovnoi rady Ukrainy. (accessed 14 August 2021).

7. Ukaz Prezydenta Ukrainy “Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy” vid 25 veresnia 2015 roku № 555/2015 "Pro novu redaktsiiu Voiennoi doktryny Ukrainy" [Decree of the President of Ukraine on the decision of the National Security and Defense Council of Ukraine" on the new edition of the Military Doctrine of Ukraine activity no. 555/2015]. (2015, September 25). Vidomosti Verkhovnoyi Rady Ukrayiny. Retrieved from: http://zakon.rada.gov.ua/laws/show/555/2015 (accessed 14 August 2021).

8. Babii Yu. O. (2016). Udoskonalennia dekompozytsii zahroz i nebezpek natsionalnii bezpetsi derzhavy u prykordonnii sferi [Improving the decomposition of threats and dangers to the state's national security in the border area] .Zbirnyk naukovykh prats Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy. Seriia : viiskovi ta tekhnichni nauky. Khmelnytskyi : NADPSU, no. 4(70), pp. 185–196.

9. Babii Yu. O., Lysyi M. I., Balytskyi I. I. (2016). Dekompozytsiia zahroz i nebezpek u sferi prykordonnoi bezpeky [Decomposition of threats and dangers in the field of border security]. Zbirnyk naukovykh prats Viiskovoi akademii. Odesa : VA, no. 2(6), pp. 127–132.

10. Bohdanovych V. Yu., Manachynskyi A. Ya. (2001). Metodolohycheskye osnovu systemnukh yssledovanyi problem voennoi bezopasnosty hosudarstv. Kyev, 172 s.

11. Kosevtsov V. O. (1999). Natsionalna bezpeka Ukrainy : teoriia, realnist i prohnoz. Kyiv: NISD, 101 p.

12. Torichnyi V., Biletska T., Rybshchun O., Kupriyenko D., Ivashkov Yu., Bratko A. Information and propaganda component of the Russian Federation hybrid aggression: conclusions for developed democratic countries on the experience of Ukraine. Trames: A Journal of the Humanities and Social Sciences, 2022, no. 25 (3), pp. 355–368.

13. Shynkaruk, O. N., Babii, Y. A., Kyrylenko, V. A., Kupriyenko, D. A., Farion, O. B., Babaryka, A. O. (2019). Conceptual and scientifically-methodical principles of realization of policy in the field of the State border security in Ukraine. Lviv-Toruń : Liha-Pres. ISBN 978-966-397-184-1.

14. Levchenko O. V., Trotsko V. V., Vasylenko I. S. Utochnennia poniatiinoho aparatu z pytan otsiniuvannia rivnia voiennoi zahrozy natsionalnii bezpetsi Ukrainy. Nauka i oborona. №2 Retrieved from: http://www.nio.mil.gov.ua/index.php?id=autor&lang=ua (accessed 11 November 2020).

15. Serhunyn A. A. (2005). Mezhdunarodnaia bezopasnost: novue podkhodu y kontseptu [International security: new approaches and concepts]. Polytycheskye yssledovanyia, no 6, pp. 126–137.

16. Lipkan V. A. Natsionalna bezpeka Ukrainy [National security of Ukraine]. Retrieved from: http://westudents.com.ua/knigi/368-natsonalna-bezpeka-ukrani-lpkan-va.html (accessed 11 November 2020).

17. Bratko A., Zaharchuk D., Zolk V. (2022). Hybrid warfare – a threat to the national security of the statea. Revista de Estudios en Seguridad Internacional, no. 7 (1), pp. 147–160.

18. .Radetskyi V. H. (2009). Osnovy stratehii natsionalnoi bezpeky ta oborony derzhavy. Kyiv, p. 225.

19. Lipkan V. A. Sutnist hibrydnoi viiny proty Ukrainy [The essence of the hybrid war against Ukraine]. Hlobalna orhanizatsiia soiuznytskoho liderstva. Retrieved from: http://goal-int.org/sutnist-gibridnoi-vijni-proti-ukraini/ (accessed 11 November 2020).

**Chernousov D. O.,**
**PhD in Military Sciences Polishchuk V. V.,**
**Doctor of Technical Sciences, Babiy Yu. A.,**
**Martynyuk V. P.,**
**Martynyuk O. V.**

**SOURCES NATURE OF THREATS AND CHALLENGES AT THE STATE BORDER OF**

***Taking into account the main trends and consequences of deep transformations of the geopolitical and geoeconomic space, there was a need to conduct thorough research in the field of ensuring the border security of our state, as a component of national security, as well as defining a clear place and role of the subjects of its guarantee in the course of the implementation of the specified function, especially with the emergence of new types of threats, in particular, the military aggression of the Russian Federation, which on February 24, 2022 entered the phase of open confrontation against Ukraine, its temporary occupation of the territory of the Autonomous Republic of Crimea and the city of Sevastopol, the Kherson region and a number of other territories of our state. In turn, there was an urgent need to justify the structure and content of the modern model of border security as the basis for the further development of the State Border Service of Ukraine, in addition, for Ukraine, the issue of border security, given the course of Euro-Atlantic integration and the latest expansion of the European Union, the geopolitical position of Ukraine determines the the fact that the borders of our state play an important and universally recognized role in the formation of the pan-European security system. It should be noted that the interests of Ukraine and the European community regarding the management of common borders certainly coincide. This is the provision of reliable protection of long stretches of the state border of Ukraine; unhindered legal crossing of the border by citizens and vehicles at checkpoints along with a high level of control procedures; proper management of migration flows; effective counteraction to manifestations of organized cross-border crime, etc. Our state supports the creation of a fundamentally new European security system based on non-power (political, economic, social,***

***energy, environmental, informational, etc.) aspects. Thus, it is necessary to justify the structure and content of the border security model, which is the basis for the formation and implementation of modern border policy of the European model, in particular, bringing the border legislation of Ukraine to the norms of European law; ensuring the readiness of human resources; technical re-equipment; achievement of the state-of-the-art infrastructure of the state border; information integration; a qualitatively new level of cross-border cooperation. In view of the above, the article develops the conceptual principles of border security of Ukraine, its border policy, as well as the mechanism of their implementation. Completion of the above-mentioned tasks will contribute to the implementation of Ukraine's strategic course for integration into the European Union and will ensure an increase in the effectiveness of the State Border Service of Ukraine in the field of ensuring the national interests of the state in general and at the state border in particular.***

***Key words: risk; threat; National security; border security; model of border security.***

УДК 519.65
**Шевченко А.М.** (ВІКНУ)

DOI: https://doi.org/10.17721/2519-481X/2022/77-13

# КОМПЛЕКСНА МОДЕЛЬ СИСТЕМНИХ ДОСЛІДЖЕНЬ ПРОБЛЕМ БЕЗПЕКИ ОБ`ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

***Дана стаття присвячена розробці методологічних підходів до розв`язання недостатньо вивченої проблеми, а саме системному дослідженню аспектів забезпечення безпеки важливих об`єктів критичної інфраструктури. Згідно з Законом «Про основи національної безпеки України» об`єктами критичної інфраструктури є: транспорт та зв'язок; енергетика та енергозабезпечення; забезпечення житлово-комунальних господарств; промисловість та наукова-технічна діяльність в військово-промисловому комплексі; технології подвійного призначення; інформаційні технології та захист інформації; використання надр; земельних на водних ресурсів; корисних копалин; захист екології тощо. Розроблено систему класифікацій методів прогностичного моделювання у вигляді трьохрівневої структури: за прийомами прогнозування та інформаційними підставами; за матеріальною основою інструменту здобуття кінцевого результату; за схемою класифікації призначених конкретних методів.***

***Розроблена комплексна модель системних досліджень проблем безпеки держави з позиції Збройних Сил України. Наведено математичний апарат аналізу та оцінки рівня національної (воєнної) безпеки у тому числі, воєнно-політичної, воєнно-економічної, воєнно-політичної моделей держави. Визначені особливості класів задач за напрямком, а саме добре та слабко структурованих задач. Запропоновано використання теорії ігор для скомпенсування статистичного вибору. Наведено основні методи прийняття рішень: методи теорії корисності (узагальненого критерію); сукупна очікувана корисність як обґрунтований метод дерев рішень; методи теорії проспектів; методи порогів незрівнянності; методи аналізу ієрархій, які спираються на багатокритеріальний опис проблеми; евристичні методи. Показано, що найбільш розвинутою теоретичною основою, що знаходить застосування при визначенні станів безпеки об`єктів критичної інфраструктури та безпеки в цілому, є експертні методи чи методи багатомірного аналізу з елементами таксономії. Проте ці підходи передбачають існування еталонних об'єктів чи уявленого експертами сценарію прояву впливу факторів на кінцевий результат. Зроблено важливий висновок, що в основі наукового протиріччя лежить необхідність створення достатньо досконалого механізму рішення задач об'єктивного обґрунтування рішень у воєнній сфері за умов суттєвої обмеженості в набутті упереджених даних для превентивного попередження конфліктів у воєнній сфері та відсутності закінченої наукової теорії визначення результату комплексного впливу різноманітних факторів.***

***Ключові слова: забезпечення безпеки; об`єкти критичної інфраструктури; національна та воєнна безпека; методи прийняття рішень.***

**Вступ, аналіз останніх досліджень та постановка задачі.** Понятійний апарат теорії національної та воєнної безпеки держави в достатній мірі визначено в Законі "Про основи національної безпеки України" [1]. Крім того, в наукових дослідженнях [2-5] додатково представлено пояснення значення деяких термінів і визначень, зроблені пропозиції по окремим напрямкам національної безпеки, вивчені основи їх стратегії, надані теоретичні і практичні приклади по їх реалізації та по попередженню, прийняттю наукових, методичних та інструментальних заходів.

Дана стаття присвячена недостатньо вивченій проблемі - системному дослідженню проблем безпеки об`єктів критичної інфраструктури. При цьому, насамперед хотілося б розкрити сутність деяких, найбільш важливих визначень, а саме:

***національна безпека*** - це захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у сферах правоохоронної діяльності, боротьби з корупцією,

прикордонної діяльності та оборони, міграційної політики, охорони здоров'я, освіти та науки, ***науково-технічної*** та інноваційної політики *(тут і далі в тексті Закону курсивом виділені найбільш вагомі напрямки безпеки об`єктів критичної інфраструктури),* культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки, соціальної політики та пенсійного забезпечення, ***житлово-комунального господарства***, ринку фінансових послуг, захисту прав власності, фондових ринків і обігу цінних паперів, податково-бюджетної та митної політики, торгівлі та ***підприємницької діяльності***, ринку банківських послуг, інвестиційної політики, ревізійної діяльності, монетарної та валютної політики, захисту інформації, ліцензування, ***промисловості*** та сільського господарства, ***транспорту та зв'язку, інформаційних технологій, енергетики та енергозбереження,*** функціонування природних монополій, використання надр, земельних та водних ресурсів, ***корисних копалин, захисту екології*** і навколишнього природного середовища та інших сферах державного управління при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам;

***національні інтереси*** - життєво важливі матеріальні, інтелектуальні і духовні цінності Українського народу як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток;

***загрози національній безпеці*** - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України;

***Система забезпечення національної безпеки*** – це комплекс організаційних структур, засобів, скоординованих дій і заходів, що здійснюються з метою розроблення та реалізації стратегії національної безпеки, цілеспрямованих рішень щодо захисту життєво важливих інтересів людини, суспільства і держави від внутрішніх і зовнішніх загроз [2-7].

Система забезпечення національної безпеки це організована державою сукупність об’єктів: державних органів, громадських організацій, посадових осіб та окремих громадян, об’єднаних цілями та задачами щодо захисту національних інтересів, яка створюється з метою реалізації національних інтересів, інтересів особистості та суспільства з урахуванням та на основі взаємозалежності соціальних, економічних, політичних, воєнних, техногенних, інформаційних та інших факторів. На систему покладається проведення комплексу погоджених заходів щодо захисту національних інтересів у політичній, економічній, воєнній, інформаційній та інших сферах.

***Система забезпечення воєнної безпеки*** держави є підсистемою більш загальної складної системи забезпечення національної безпеки держави, найважливішою її складовою частиною, головним інструментом реалізації державної політики забезпечення національних інтересів України в оборонній сфері, знаходиться на одному рівні ієрархії з іншими підсистемами і має з ними інформаційні і функціональні зв’язки [8, 9]. Сьогодні проблема забезпечення воєнної безпеки держави – це не тільки і не стільки питання удосконалення військової компоненти держави. Забезпечення воєнної безпеки України необхідно розглядати, насамперед, як похідну від рівня розвитку економічної, інформаційної, власне військової і науково-технологічної бази держави, системи політичних стосунків у суспільстві, ступеня демократичного розвитку держави, системи міжнародних відносин і сформованої структури "світового порядку", інтеграційних об’єднань різних держав та ін.

Система забезпечення воєнної безпеки стосується практично всіх галузей функціонування суспільства і держави, головними з яких є [4, 7, 9]:

✓ воєнна сфера (питання військової організації держави, системи оборонного планування, у т.ч. питання оперативної і бойової підготовки військ (сил));

✓ військово-політична сфера (питання регіональної і глобальної безпеки, миротворчої діяльності);

✓ військово-економічна сфера (питання економічного і ресурсного забезпечення військового будівництва, підтримки життєдіяльності військ (сил) нарівні, що забезпечує необхідний ступінь бойової готовності і боєздатності, питання формування оборонного

бюджету і розподіл та оптимізація бюджетних ресурсів);

✓ військово-соціальна сфера (питання морально-психологічної підготовки населення до вирішення оборонних завдань, морально-психологічні проблеми військових колективів, соціальні проблеми військових);

✓ військово-технічна сфера (питання розвитку фундаментальної науки в інтересах забезпечення оборони країни, пошукових і прикладних досліджень, базових військових технологій, питання створення, модернізації та утилізації зразків озброєння і військової техніки, підготовка спеціальних і науково-технічних кадрів);

✓ військово-технологічна сфера (питання розвитку базових військових технологій для вирішення оперативно-стратегічних і оперативно-тактичних завдань – систем розвідки та управління військами і зброєю, розвідувально-ударні комплекси тощо), створення принципово нових зразків озброєння і військової техніки і таке інше.

**Виклад основних результатів.** У сучасних умовах важливими аспектами забезпечення інтегрованого управління захистом важливих об`єктів критичної інфраструктури є випереджувальне виявлення загроз і ризиків на протязі життєвого циклу їх експлуатації в умовах мирного та воєнного часу. Це потребує здійснення переходу до прогностичних форм діяльності з використанням багатоваріантних моделей розвитку обстановки в державі та її регіонів, не просто констатації фактів (ознайомлення з первинною інформацією), а системного підходу до вирішення проблеми загалом на основі поєднання інтелектуальних здібностей персоналу інформаційно-аналітичних підрозділів (керівного складу) з функціональними можливостями сучасних інформаційно-телекомунікаційних систем та з використанням сучасних технічних засобів космічної, повітряної, наземної та інших видів розвідок.

***Методи прогностичного моделювання.*** Орієнтація на передбачення (прогнозування), завчасне виявлення тенденцій розвитку ситуації обумовлює потребу застосування різних аналітичних методів опрацювання інформації: порівняльного, ситуаційного, SWOT-аналіз (метод стратегічного планування, заснований на аналізі сильних і слабих сторін, можливостей і загроз) і PEST – інструмент (політичні, економічні, соціальні та технологічні аспекти) та інших методів аналізу загроз і ризиків.

На рис. 1 наведено методи прогностичного моделювання схеми. При цьому, на *першому* (найвищому) *рівні* класифікації методи прогнозування поділяються за прийомами прогнозування на інформаційній підставі, тобто за способом одержання вхідних даних для прогнозування, які засновані або на використанні експертних оцінок, або на моделюванні, або на сполученні цих методів.

*Другий рівень* класифікації базується на матеріальній основі інструменту здобуття кінцевого результату.

*Третій рівень* наведеної схеми класифікації призначений для конкретизації методу.

У загальному випадку послідовність прогнозування включає такі основні операції:

1. Визначення об’єкта прогнозування за його фізичним змістом, призначенням, зв’язком з іншими об’єктами, призначенням і складом інформації, яка повинна бути отримана при прогнозуванні.

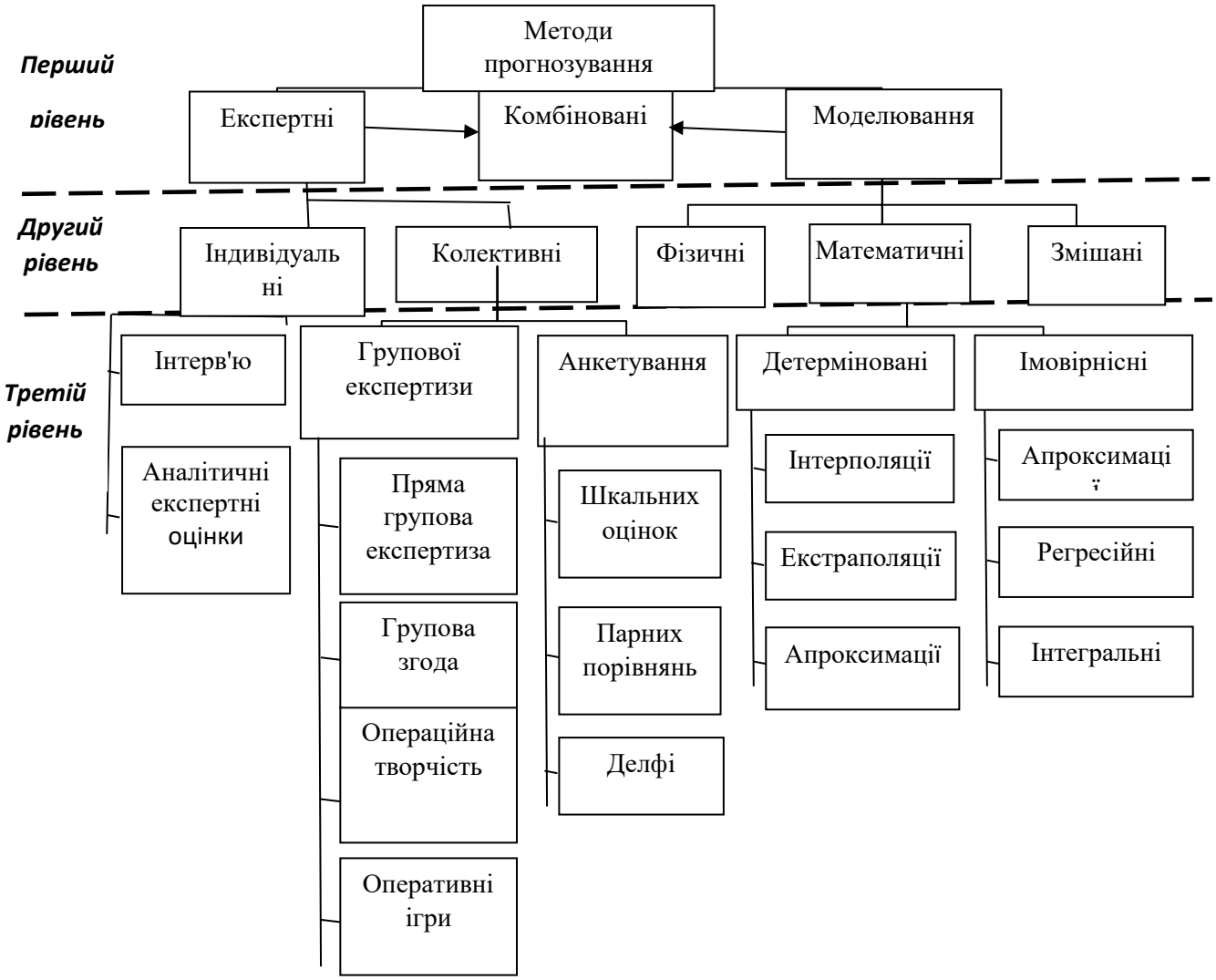



Рисунок 1. Методи прогностичного моделювання

2. Збирання й аналіз інформації, що належить до об’єкта прогнозування. Ця інформація може містити дані про подібні об’єкти у минулому і теперішньому. До необхідної інформації належать також закономірності поведінки подібних об’єктів в аналогічних умовах.

3. Побудова моделі об’єкта, що досліджується, на основі закономірностей, що виявлені. На вибір моделі прогнозування впливають мета і задачі прогнозування, а також інтервал прогнозування. На даному етапі визначальним фактором є обрана матеріальна основа інструменту отримання кінцевого результату, що виливається в застосування суб’єктивних експертних методів, заснованих на досвіді експертів, чи об’єктивних методів фізичного чи знакового (математичного) моделювання.

4. Визначення невідомих параметрів моделі процесу, що прогнозується. Безпосередньо прогнозування, тобто розроблення прогнозу щодо майбутнього стану об’єкта.

Отримані результати прогнозування, що отримані, піддаються логічному аналізу, за результатами якого можуть бути зроблені уточнення до процесу прогнозування. В основі прогнозування лежать три джерела інформації про майбутнє: 1. Оцінка перспектив розвитку, прогнозування стану об’єкта (процесу або явища) на основі досвіду, найчастіше за допомогою аналогії з достатньо добре відомими об’єктами (процесами або явищами) – застосовується в основному для забезпечення експертних методів;

2. Умовне прогнозування у майбутнє (екстраполяція тенденцій, закономірності розвитку яких у минулому і теперішньому достатньо добре відомі) – здебільшого застосовується в методах імітаційного моделювання;

3. Модель прогнозування стану того чи іншого об’єкта (процесу або явища), що побудована відповідно до очікуваних або бажаних змін ряду умов, перспективи розвитку яких достатньо добре відомі – здебільшого застосовується різними методами математичного моделювання.

***Науково-методичний апарат оцінювання і прогнозування рівня воєнної безпеки.*** Наукове обґрунтування стратегічних рішень у сфері воєнної безпеки і визначення пріоритетних напрямків формування воєнної політики здійснені з позиції системного підходу щодо їх внеску в загальну ефективність системи забезпечення національної безпеки, раніше застосували відомий апарат [9 - 11], а також викладені в [4, 5, 7].

Для моделювання і дослідження проблем воєнної безпеки держави використовується воєнно-політична модель держави у вигляді окремого модуля, комплексна модель системних досліджень (КМСД) [11]. Традиційні методи, що використовуються для вирішення таких завдань, базуються, як правило, на методах експертного оцінювання, проб і помилок, що вносить елементи суб’єктивізму і супроводжується досить великими похибками. Науково-методичний апарат оцінювання і прогнозування рівня воєнної безпеки базується на використанні методів дослідження операцій, аналізу ієрархій, векторної алгебри, експертного оцінювання і математичного моделювання. Приклад КМСД проблем воєнної безпеки держави представлено на рис. 2. Складовими даного науково-методичного апарату оцінювання і прогнозування рівня воєнної небезпеки для держави є:

1. Методика аналізу воєнно-політичної обстановки в регіоні.
2. Метод прогнозування динаміки воєнно-політичної обстановки з використанням експертно-значимих проміжних станів.
3. Методика визначення множини держав, що можуть складати воєнну небезпеку для України.
4. Методика оцінювання рівня воєнної небезпеки для держави.
5. Методика оцінювання впливу дестабілізуючих чинників воєнно-політичної обстановки на рівень воєнної безпеки держави.

Основними проблемами практичного застосування даного науково-методичного апарату є визначення:

- ✓ періодичності проведення оцінок комплексного показника рівня воєнної небезпеки;
- ✓ числових значень порогів виникнення воєнної загрози;
- ✓ оптимальної структури експертів;
- ✓ припустимої величини неузгодженості думок експертів;
- ✓ кількість генерованих можливих сценаріїв розвитку воєнно-політичної обстановки.

***Аналіз та оцінка рівня національної безпеки та її складових.*** Одним із перспективних методичних підходів щодо аналізу та оцінки рівня національної безпеки є методика багатовимірного порівняльного аналізу, яка ґрунтується на методах таксономії з елементами факторного аналізу і складається з наступних кроків (етапів):

1. Визначаються до розгляду об’єкти, які визначають стан національної безпеки;
2. Визначаються показники, які описують властивості цих об’єктів;
3. Формується матриця вхідних даних:

$$\left[X_{ij}\right],\ \left(i=\overline{1,\omega},\ j=\overline{1,n}\right),$$

де $i$ – номер об’єкта,

$j$ – номер його властивості;

4. Матриця вхідних даних зводиться до стандартизованого вигляду:

$$\overline{X}_j = \frac{1}{\omega}\sum_i X_{ij},$$

$$S_j = \sqrt{\frac{1}{\omega - 1}\sum_i \left(X_{ij} - \overline{X}_j\right)^2},$$

$$Z_{ij} = \frac{X_{ij} - \overline{X}_j}{S_j}.$$

5. Розраховується матриця відстаней (абсолютна середня різниця значень показників):

$$C_{rs} = \frac{1}{\omega}\sum_l \left|Z_{rl} - Z_{sl}\right|,$$

$$l = \overline{1, \omega},\ r, s = \overline{1, n};$$

Властивості матриці: $C_{rr} = 0$, $C_{rs} = C_{sr}$, $C_{rs} \le C_{rv} + C_{vs}$.

6. Визначається критична відстань - найбільша відстань між показниками, що розташовані поблизу один до одного: $C = \max_i \min_j \left(\alpha_i, \alpha_j\right)$.

7. Визначається для кожного показника відстань, яка не перевищує критичну:

$$Q_j = (r, h)\left|\rho(\alpha_r, \alpha_h) \le C,\ r, h = \overline{1, n}\right.$$.

8. Знаходиться сума відстаней для кожного показника:

$$: \omega = \sum \rho(\alpha_r, \alpha_h),\ (r, h) \in Q_j.$$

9. Знаходиться максимальна сума відстаней:

$$\omega_m = \max\ \omega_j;$$

10. Визначаються коефіцієнти ієрархії показників:

$$\lambda_j = \frac{\omega_j}{\omega_m}.$$

11. Здійснюється розподіл показників стимулятори (конструктори), збільшення яких призводить до зростання узагальненого показника - $S$; стимулятори (деструктори), зростання яких призводить до зменшення узагальненого показника - $D$.

12. Здійснюється побудова еталонного об’єкта – точки з координатами

$$Z_{01}, Z_{02}, \ldots, Z_{0n},\ Z_{0F} = \begin{cases} \max\ Z_{RF}, & \textit{якщо} \quad F \in S; \\ \min\ Z_{RF}, & \textit{якщо} \quad F \in D. \end{cases}$$

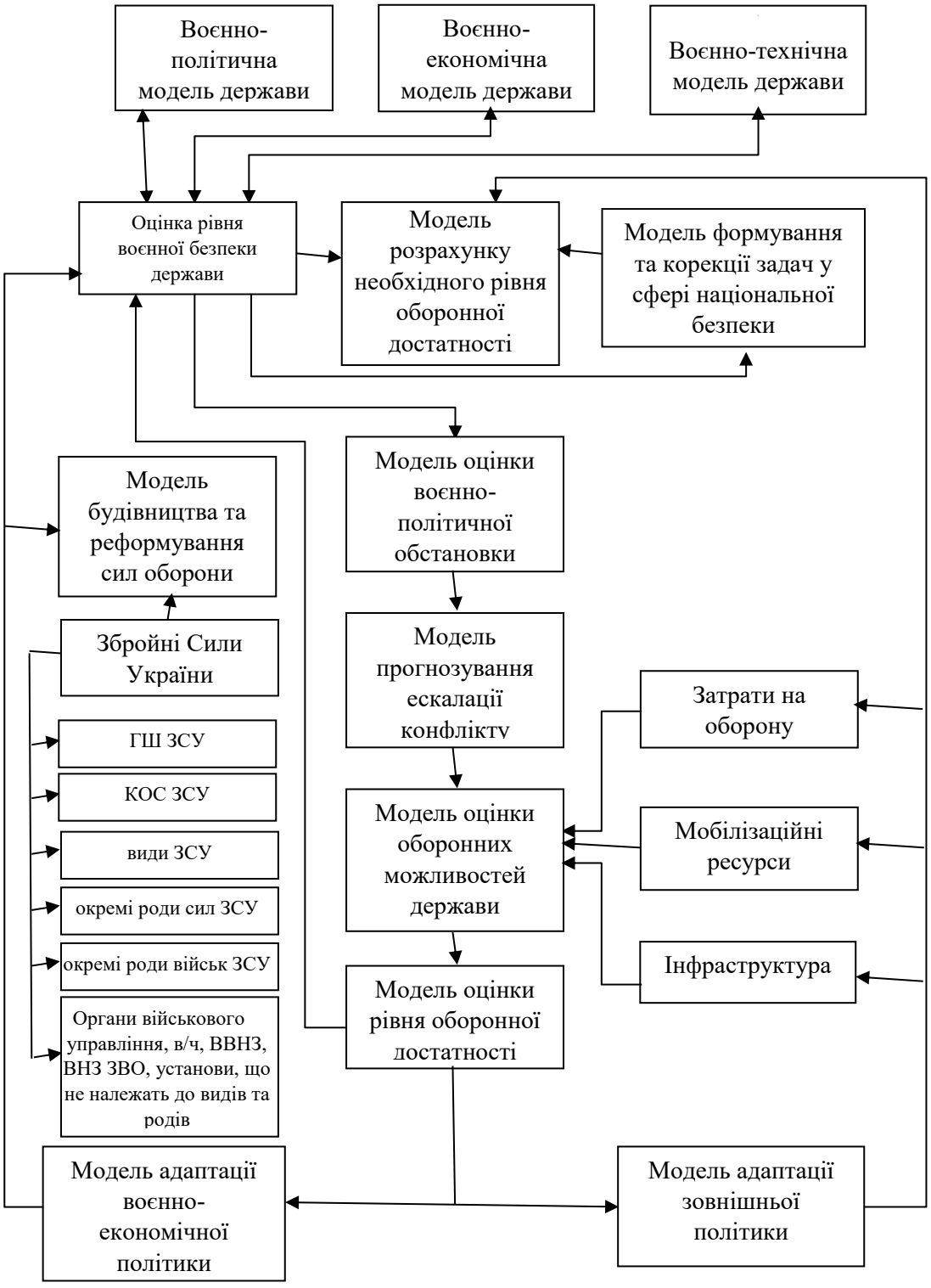



Рисунок 2 – Комплексна модель системних досліджень проблем воєнної безпеки держави

13. Розраховується відстань між еталонною точкою та точками-об’єктами:

$$C_{i0} = \sqrt{\sum \left(Z_{if} - Z_{of}\right)^2}\ ,\ f = \overline{1, n}\ ,\ i = \overline{1, \omega}\ ;$$

14. Розраховується середньоквадратичне відхилення відстані:

$$S_0 = \sqrt{\frac{1}{\omega}\sum \left(C_{i0} - \overline{C_0}\right)^2}\ ,$$ при цьому $C_0 = \bar{C}_0 \mp S_0$

15. Розраховуються відносні узагальнені показники об’єкту:

$$d_i^* = \frac{C_{i0}}{C_0}\quad .$$

16. Розраховуються модифіковані узагальнені показники:

$$d_i = 1 - d_i^*\quad .$$

Розгляд атрибутів інтегрованої задачі аналізу ризиків [13, 14] дозволяє визначити наступне:

вхідні дані, такі як показники рівня безпеки об`єктів інфраструктури, апріорі окреслені нечітко, їх зміст є скоріше лінгвістичним, ніж таким, що вкладається в чисельну оцінку;

характеристики об’єктів системи забезпечення безпеки держави, які є визначальними для формалізації процесу, не завжди можуть бути визначені точно та часто залежать від неконтрольованих параметрів;

механізми впливу ризиків в кінцевому рахунку на стан безпеки не завжди можуть бути визначені точно, часто невідомими є не тільки параметри функції впливу, а й структура такої функції; множинність часткових цілей, покликаних забезпечити інтегрований контроль стану об`єкта, ускладнює (чи навіть унеможливлює) повну їх чітку формалізацію, більшість цілей рідко можуть бути оцінені чисельно, а надаються лише вербально; ускладнена формалізація координаційних зв’язків системи інтегрованого контролю.

При цьому, класи поставлених задач можливо поділити на:

1. ***Добре структуровані задачі*** характеризуються тим, що в них суттєві залежності виявлені настільки явно, що можуть бути описані кількісними залежностями [16]. Але це не означає відсутність труднощів в опису проблем та їх вирішенню. Однією з значних труднощів на даному рівні може бути, наприклад, масштабність та рівень деталізації проблем (процесів).

2. ***Слабко структуровані задачі*** містять в собі елементи якісного та кількісного характеру, перші мають тенденцію домінування. У зв’язку з цим їх формалізований опис може бути здійснений, як правило, тільки за допомогою "м’яких" формалізмів [10,14].

До даного класу проблем (ситуації) відносяться проблеми змішаного характеру. Наприклад, при ліквідації стихійних лих, техногенних катастрофах тощо. Аналітичні моделі можуть бути використані для визначення ступеня і характеру втрат. "М’які" (збалансовані) моделі використовуються при здійсненні вибору способів ліквідації наслідків цих подій. До цього класу проблем відносяться також проблеми екологічного, економічного, національного, політичного, медичного характеру.

Для розв’язання слабко структурованих задач зазвичай використовується методологія системного аналізу [10]. Оскільки будь-який аналіз складної системи неможливий без використання можливостей обчислювальної техніки, то говорячи про методи системного аналізу, мають на увазі види процедур, які засновані на використанні комп`ютерної техніки.

Потреба не просто вивчати явище чи факт, а встановлювати його зв'язок з іншими

чинниками, як у часі так і у просторі, вивчення причинно-наслідкових зв`язків, привела до появи спеціального терміну "системний підхід". Системний підхід – це деякий загальнометодологічний принцип. Його гносеологічний аспект – це теорія систем, апаратна реалізація – це системний аналіз [17]. Процедура прийняття рішень (ПР) включає наступні основні етапи та типові методи їх реалізації [18-20]:

1. Формулювання проблемної ситуації методами системного аналізу апріорної інформації, експертних оцінок та прогнозування ситуацій.
2. Визначення цілей методами побудови дерева цілей, експертних оцінок та соціологічного аналізу.
3. Визначення критеріїв досягнення цілей методами теорії корисності, статистичними та експертних оцінок.
4. Побудова моделі для обґрунтування рішень методами імітаційного моделювання, економетричних та оптимізаційних моделей, моделей масового обслуговування та задовольняння обмеженням, інших концептуальних та графічних моделей.
5. Пошук оптимального (припустимого) варіанта рішення методами оптимізації, імітаційного експерименту, задовольняння обмеженням тощо.
6. Узгодження рішення методами раціонального компромісу, теорії ігор, ділових ігор, правових норм.
7. Підготовка рішення до реалізації методами мережевого планування в часі та планування в просторі.
8. Затвердження рішення (урахування правових та моральних норм тощо, ділових якостей виконавців, наслідків від подібних рішень).
9. Управління ходом реалізації рішення методами мережевого управління, контролю виконання доручень.
10. Перевірка ефективності рішення методами соціологічного, виробничого та фінансового аналізу.

При цьому одним з важливих напрямів подальших наукових досліджень є розроблення державних механізмів моніторингу обстановки на об`єктах критичної інфраструктури, оцінювання загроз і ризиків у сфері безпеки та ефективності інтегрованого управління ними [13, 20].

При визначенні впливу загроз на стан безпеки об’єктів критичної інфраструктури постає проблема прийняття рішень. Найбільш розвинутою теоретичною основою прийняття рішень в умовах невизначеності та протидії є теорія ігор [21, 22].

Теорія ігор має досить значні досягнення, а саме, вона дозволяє:

✓ структурувати задачу, подати її в оглядовому вигляді, знайти області кількісних оцінок, упорядкувань, переваг та невизначеностей, виявити домінуючі стратегії, якщо вони існують;

✓ до кінця вирішити задачі, які описуються стохастичними моделями;

✓ виявити можливість досягнення згоди та дослідити поведінку систем, здатних до згоди (кооперації), тобто області взаємодії поблизу сідлової точки, точки рівноваги чи згоди Парето [21].

Та все ж попри зазначені досягнення для реальних ситуацій цього зовсім недостатньо. В цьому випадку запропоновано використовувати методи теорії ігр, а саме наступна структура:

1. Теорія ігор здійснює пошук рішень, оптимальне чи раціональне в середньому, в той час як конфлікти (навіть типові) ситуаційні та унікальні. Коли мова йде про загальні рекомендації, статистична постановка питання досить доречна [24]. У конкретних обставинах необхідне більш глибоке проникнення в суть конкретної задачі.

2. Теорія ігор виходить з принципу мінімуму середнього ризику, що зовсім неприйнятно для конфлікту.

В конфлікті кожна сторона готова ризикувати, виходячи з припущення „більший ризик – більший імовірний успіх”, тому у конфлікті діє принцип припустимого ризику [20].

3. Прогностичний аспект пізнання, що пов’язаний з передбаченням тих стратегій, які фактично будуть обиратися учасниками гри теорія ігор в сучасному стані не займається.

4. Питання, що пов’язані з передбаченням однією стороною тієї чи іншої стратегії, яку буде обирати інша сторона на основі яких-небудь міркувань (принципів оптимальності) не розглядаються, хоча це не виключає використання теорії ігор при формуванні прогнозів як складової більш загального апарату [21,25].

5. Апріорне встановлення змісту можливих стратегій сторін практично недосяжне. Стратегії, що лежать на поверхні, в конфлікті представляють найменшу цінність – головна задача сторін виявити скриті можливості.

6. В реальних конфліктах найчастіше ніхто не грає за правилами, які приписуються теорією ігор [26].

В цілому теорія ігор орієнтована на скомпенсований статистичний вибір, взагалі ж у конфлікті поведінка далеко не найкраща і не універсальна, в екстремальних ситуаціях може бути навіть програшна.

Принципова відмінність векторних задач прийняття рішення полягає в тому, що для них існує багато різних принципів оптимальності, що приводять до вибору різних оптимальних рішень. Це висуває жорсткі вимоги до вибору принципу оптимальності. При розв’язанні задач багатокритеріальної оптимізації виникає ряд проблем, головними з яких є наступні:

- ✓ визначення області поступки;
- ✓ вибір схеми поступки й принципу оптимальності;
- ✓ нормалізація критеріїв;
- ✓ засоби урахування пріоритетів критеріїв.

Слід зазначити, що всі, крім першої, проблеми мають концептуальний характер, при вирішенні яких необхідно використовувати різні евристичні процедури, в яких важлива роль належить експертам.

Як уже відзначалося, у багатокритеріальних задачах ПР у складних системах між деякими критеріями існують протиріччя. Ці протиріччя є нестрогими, оскільки в противному випадку задача була б конфліктною, антагоністичною. Тому область припустимих рішень $D_x$ ділиться на дві області: область згоди $D_x$ та область поступки $D_x^k$. Очевидно, що оптимальне рішення належить тільки області поступки, тобто, $x_{opt} \in D_x^k$, тому що в області згоди рішення може (і повинне) бути поліпшене за всіма критеріями. В області поступки якість рішення не може бути поліпшене за одним критерієм без погіршення за іншим.

Одним із засобів визначення області поступки є виділення множини рішень, оптимальних по Парето [24]. Рішення $x^*$ є оптимальним за Парето (парето-оптимальним), якщо не знайдеться жодного іншого рішення $x^0$ такого, щоб виконувалися співвідношення: $e_g(x^0) \le e_g(x^*)$, для всіх $g = 1,\dots,k$ (якщо критерії потрібно мінімізувати) або $e_g(x^0) \ge e_g(x^*)$, для всіх $g = 1,\dots,k$ (якщо критерії потрібно максимізувати), причому хоча б одна нерівність сувора.

Вибір або побудова схеми поступки й принципу оптимальності розкриває зміст оптимізації, формалізує систему переваг особи, що приймає оптимальне рішення.

Аналіз літератури з проблеми багатокритеріального вибору [наприклад 23,27,28] показує, що найпоширенішими схемами поступки й принципами оптимальності є наступні.

1. Принцип виділення головного критерію: виділяється один критерій як головний, а інші перекладаються в систему обмежень. Тоді проводиться оптимізація головного критерію

з умовою, що інші критерії не перевищують заданих значень (тут і надалі вважаємо, що критерій необхідно мінімізувати).

2. Метод лексикографічного упорядкування критеріїв: оптимізація $g$-го критерію проводиться тільки після того, як отримані мінімальні значення всіх попередніх $(g-1)$ критеріїв.

Модифікацією цього методу є метод послідовних поступок, суть якого полягає в тому, що на кожному $g$-му кроці послідовній оптимізації задається поступка $\Delta e_{g-1}$, що характеризує припустиме відхилення критерію $e_{g-1}$ від його заданого значення.

Ці методи припускають наявність домінуючої переваги одного критерію над іншим.

3. Принцип рівномірності:

*Принцип рівності:* $optE = \{e_1 = e_2 = \ldots = e_k\}$.

*Принцип квазірівності* (критерії різняться не більше, ніж на розмір:

$$optE = \{E : [e_g - e_v] \le a, g, v = 1, 2, \ldots, k\}.$$

*Принцип мінімаксу* (гарантованого результату): $optE = \max \min e_g, \quad g = 1, \ldots, k.$

*Принцип домінуючого результату*: $optE = \max \max e_g, \quad g = 1, \ldots, k.$

Принцип гарантованого результату (для обережного ПР) і принцип домінуючого результату (для ПР, що веде до ризику) широко застосовуються, наприклад, при вирішенні економічних задач.

4. Принцип справедливої поступки базується на оцінці і порівнянні збільшення (зменшення) рівня локальних критеріїв.

В усіх відомих методах визначення числових значень вагових коефіцієнтів від оптимального ПР потрібно або задати точні числові оцінки, або порівняти важливість усіх локальних критеріїв між собою. Проте, здебільшого людині не під силу задати точну числову інформацію. Їй легше уявити інформацію в неформальному вигляді, на неформальному рівні. Таку інформацію можна одержати за допомогою лінгвістичних змінних на основі порядкових шкал. Всі відомі нині у теорії ПР методи розв'язання задач багатокритеріального вибору можуть бути згрупованими наступним чином, а саме:

1. Методи теорії корисності (узагальненого критерію). Теорія корисності, носить аксіоматичний характер. Автори роботи [29] показали, що, якщо переваги людей стосовно визначених ігор (лотерей) задовольняють ряду аксіом, то їх поведінка може розглядатися як максимізація очікуваної корисності.

2. Сукупна очікувана корисність як обґрунтований метод дерев рішень, суть якого полягає у поділі задачі на ряд підзадач, які, у свою чергу, розподіляються на інші підзадачі, і так далі. У результаті основна задача зображається у вигляді дерева рішень [30].

3. Методи теорії проспектів (ТП). Проспект це гра з імовірнісними виходами. У методах ТП враховуються 3 поведінкових ефекти:

- ✓ ефект визначеності – тенденція додавати більшу вагу детермінованим виходам;
- ✓ ефект відображення – до виміру переваг при переході від виграшів до втрат;
- ✓ ефект ізоляції – тенденція до спрощення вибору шляхом виключення загальних компонентів варіантів рішення.

4. Методи *ELECTRE* (методи порогів незрівнянності). Французькою школою теорії ПР, очолюваною Б. Руа, був запропонований конструктивний підхід до вироблення рішень, у рамках якого методи, моделі й концепції розглядаються як допоміжні засоби практичного аналізу ситуації.

5. Метод аналізу ієрархій, який спирається на багатокритеріальний опис проблеми. У методі використовується дерево критеріїв, у якому загальні критерії поділяються на критерії окремого характеру. Для кожної групи критеріїв визначаються коефіцієнти важливості.

Альтернативи також порівнюються між собою за окремими критеріями з метою визначення кожної з них.

6. Евристичні методи. До евристичних методів належать такі методи.

*Метод зваженої суми оцінок критеріїв*. Кожній альтернативі дається числова (бальна) оцінка за кожним з критеріїв. Критеріям приписуються кількісні ваги, що характеризують їх порівняльну важливість. Ваги збільшуються на критеріальні оцінки, отримані числа підсумовуються – так визначається цінність альтернативи. Далі вибирається альтернатива з найбільшим показником цінності.

*Метод компенсації*. Даний метод використовується при попарному порівнянні альтернатив.

Перевагою всіх евристичних методів є простота й зручність, а основний недолік − відсутність наукового обґрунтування.

Таким чином, проведений аналіз показав, що розглянуті методи, носять аксіоматичний і евристичний характер, тобто не мають суворого наукового доказу.

**Висновки та напрямки подальших досліджень**

1. Комплексний вплив викликів та загроз на стан безпеки об`єктів критичної інфраструктури не належить до тих явищ, які підлягають простому уявленню та якими можна керувати на підставі життєвого досвіду.

Для визначення результуючого стану безпеки та передбачити для нього хоч який ефективний вплив, необхідно визначити істинні витоки та причини формування саме такого стану внаслідок дії різноманітних чинників, виявити закономірності їх впливу та можливі моделі оцінки всього комплексного впливу.

2. Об’єктом комплексного наукового аналізу у сформульованій задачі постають механізми впливу загроз в цілому з усіма їх базовими ознаками, елементами та принципами прояву і розвитку, предметом можна вважати загальні закономірності виникнення та впливу загроз.

3. Найбільш розвинутою теоретичною основою, що знаходить застосування при визначенні станів безпеки об`єктів критичної інфраструктури та безпеки в цілому, є експертні методи чи методи багатомірного аналізу з елементами таксономії. Проте ці підходи передбачають існування еталонних об’єктів чи уявленого експертами сценарію прояву впливу факторів на кінцевий результат.

3. Інформація про механізм комплексного впливу окремих загроз не може бути отримана суто експериментальним шляхом, будь-який експеримент з реальною системою небезпечний, може навіть привести до руйнування дорогої системи, можливо унікальної.

4. Системна модель служить не стільки для отримання точних кількісних характеристик, скільки для находження оцінок, які дозволяють спостерігати припустимі межі дій, можливості процесів, тенденції їх розвитку. Від моделей не слід очікувати конкретних вказівок, але завжди можна виявити області, де можливе отримання таких оцінок, які з високою імовірністю вказуватимуть на конкретні процеси та їх наслідки.

5. Зміст дослідження полягає в об’єктивному встановленні механізму впливу різноманітних чинників на стан безпеки об`єктів. Передбачається, що апріорі фізичний зміст даного механізму невідомий і не підлягає логічному трактуванню. Завданням дослідження є об’єктивне встановлення зазначеного механізму впливу на етапі становлення системи інтегрованого управління безпеки.

6. В основі наукового протиріччя лежить необхідність створення достатньо досконалого механізму рішення задач об’єктивного обґрунтування рішень у воєнній сфері за умов суттєвої обмеженості в набутті упереджених даних для превентивного попередження конфліктів у воєнній сфері та відсутності закінченої наукової теорії визначення результату комплексного впливу різноманітних факторів. Це і є основним напрямком подальших досліджень.

ЛІТЕРАТУРА:

1. Закон України «Про національну безпеку України». Відомості Верховної Ради, 2018, №31, ст.241.

2. Косевцов В. О. Національна безпека України: теорія, реальність, прогноз / - К.: ЦМБСС, Сатсанга, 2000. – 80 с.

3. Богданович В. Ю. Воєнна безпека України: методологія дослідження та шляхи забезпечення / – К. : "Тираж", 2003. – 322 с.

4. Дузь-Крятченко О.П., Грицай П.М., Грищенко В.П., Кліменко В.С.. Козинець І.П., Косевцов В.О., Нечхаєв С.М., Пунда Ю.В. Основи стратегії національної безпеки та оборони держави: підручник – 3-е вид. – К.: НУОУ ім. Івана Черняховського, 2015. – 620 с.

5. Горбулін В.П. Світова гібридна війна: український фронт:монографія / за заг.ред. В.П. Горбуліна. – К.: НІСД, 2017. – 496 с.

6. Національна безпека України у викликах новітньої історії / автор укладач В.І. Шпак, кер.авт.кол. С.І. Табачніков. – К.: ДП «Експрес-об`ява», 2019. – 468 с.

7. Ліпкан В.А. Національна безпека України : [навч. посіб.] / — [2-е вид.]. - К. : КНТ, 2009. — 576 с.

8. Богданович В. Ю., Маначинский А.Я. Методологические основы системных исследований проблем военной безопасности государства / – К. :, 2001. – 172 с.

9. Методи моделювання процесів діяльності міністерства оборони України : [звіт про науково-дослідну роботу (проміжний, шифр “Афіна-2”) / наук. кер. В. Л. Шевченко]. – К. : НУОУ, 2010. – 90 с.

10. Лєнков С.В., Дергильова О.В., Винярський Я.Я. Системотехнічні прийоми формалізації слабко структурованих задач для рішення практичних задач сфери забезпечення національної безпеки держави // Вісник інженерної академії України. – 2011. – № 3-4. – С.89 – 93.

11. Саати Т. Принятие решений: Метод анализа иерархий / Т. Саати; пер. с англ. В. Г. Вогнадзе. – М. : Радио и связь, 1993. – 184 с.

12. Косевцов В. О., Бінько І. Ф., Матвієвський О. М. Методичний підхід до аналізу й оцінки рівня національної безпеки та її складових // Наука і оборона. – 1995. - № 1. – С. 74–77.

13 Горбулін В.П., Качинський О.Б. Системно-концептуальні засади стратегії національної безпеки України: монографія. – К.: ДП «НВЦ Євроатлантікіформ», 2007. – 592 с.

14. Клир Д. Системология: Автоматизация решения системных задач / Д. Клир ; пер. с англ. – М.: Радио и связь, 1990. – 544 с.

15. Щедріна О.І. Системний аналіз як інструмент прийняття управлінських рішень в бізнесі. Вісник КНЕУ – К: КНЕУ, 2020. №99. С170-184, DOI 10/3311| 99.15.

16. Рабочая книга по прогнозированию / Редкол. И. В. Бестужев-Лада (отв. ред.). – М.: Мысль, 1982. – 430 с.

17. Моисеев Н. Н. Математические задачи системного анализа / Н. Н. Моисеев. – М. : Наука, 1981. – 488 с.

18. Порнев А.Г., Румянцева З.П., Соломатин Н.А. Управление организацией. Учебник – 2-е изд. перераб.и доп. – М.: - 2000 – 669 с.

19. США: современные методы управления / под общ. ред. Б. З. Мильнера. – М. : Наука, 1971. – 334 с.

20. Колпаков В.М., Пономаренко С.О., Сєлюков О.В. Основи стратегії: монографія. – К.: Видавництво Людмила, 2021. – 474 с.

21. Авинаш Диссит, Барри Нейлтафф. Теория игр. Искусство математической экономики. – М.: Макс-пресс. 2011 – 464 с.

22. Хог Э. Прикладное оптимальное проектирование / Хог Э., Арора Я. – М. : Мир, 1983. – 478 с.

23. Кох Ричарз. Принцип 80/2. Монография. Перевод с анг. – М. Эксмо, 2012, - 444 с.

24. Huntington S. P. The Lonely Superpower / Huntington S. P. // Foreign Affairs? March/April 1999? Vol. 78, # 2, pp. 35-49.

25. Воробьёв В. В. Основы теории игр. Бескоалиционные игры / В. В. Воробьёв. – М. : Наука, 1984. – 496 с.

26. Васин А.А., Морозов В.В. Теория игр и модели математической экономики. – М.: Макс-пресс. 2005 – 272 с.

27. Steuen R.T. Multyple Criterial optimization: Theory, Computations and Application. – New York, John Wilay & Sons, Iпс, 1986. – 420 p.

28. Собол И.М. Выбор оптимальных параметров в задачах со многими критериями. – М.: Дрофа, 2006. – 176 с.

29. О. Моргенштерн, Дж. Фон Нейман. Теория игр и экономическое поведение. – М.: Книга по требованию, 2013. – 708 с.

30. Р.Кінні, Х. Райф. Прийняття рішень при багатьох критеріях: переваги й заміщення. Х.: Знання, 2010. – 248 с.

REFERENCES:

1. Zakon Ukraine (2018), «Pro natsIonalnu bezpeku Ukraine» [About the national security of Ukraine]. VIdomostI VerhovnoYi Radi, No.31, pp.241.

2. Kosevtsov, V. O. (2000), NatsIonalna bezpeka UkraYini: teorIya, realnIst, prognoz [National security of Ukraine: theory, reality, forecast] - K.: TsMBSS, Satsanga,. – 80 p.

3. Bogdanovich, V. Yu. (2003), VoEnna bezpeka UkraYini: metodologIya doslIdzhennya ta shlyahi zabezpechennya [Military security of Ukraine: research methodology and ways of ensuring] – K. : "Tirazh", – 322 p.

4. Duz-Kryatchenko, O.P., Gritsay, P.M., Grischenko, V.P., KlImenko, V.S., Kozinets, I.P., Kosevtsov, V.O., NechhaEv, S.M., Punda, Yu.V. (2015), "Osnovi strategiyi natsionalnoyi bezpeki ta oboroni derzhavi: pIdruchnik" [Basics of the strategy of national security and defense of the state] – K.: NUOU Im. Ivana Chernyahovskogo, – 620 p.

5. GorbulIn, V.P. (2017), SvItova gIbridna vIyna: ukraYinskiy front:monografIya [World hybrid war: Ukrainian front: monograph], za zag.red. V.P. GorbulIna. – K.: NISD, – 496 p.

6. Shpak, V.I., TabachnIkov, S.I. (2019), "NatsIonalna bezpeka Ukraine u viklikah novitno v istorivi" [National security of Ukraine in the challenges of recent history] – K.: DP «Ekspres-ob`yava», – 468 p.

7. Lipkan, V.A. (2009), "NatsIonalna bezpeka Ukraine" [National security of Ukraine] - K. : KNT, — 576 p.

8. Bogdanovich, V. Yu., Manachinskiy, A.Ya. (2001), "Metodologicheskie osnovyi sistemnyih issledovaniy problem voennoy bezopasnosti gosudarstva" [Methodological basis of system studies of problems of military security of the state] – K.; – 172 p.

9. Shevchenko, V. L. (2010), "Metodi modelyuvannya protsesIv dIyalnostI mInIsterstva oboroni Ukraine" [Methods of modeling the activity processes of the Ministry of Defense of Ukraine] – K. : NUOU, – 90 p.

10. Lenkov, S.V., Dergilova, O.V., Vinyarskiy, Ya.Ya. (2011), "Sistemotehnichni priyomi formalizatsiyi slabko strukturovanih zadach dlya rishennya praktichnih zadach sferi zabezpechennya natsionalnoyi bezpeki derzhavi" [System-technical methods of formalization of weakly structured problems for solving practical problems in the sphere of ensuring the national security of the state]. Visnik Inzhenernoyi akademiyi Ukraine, No. 3-4. – pp. 89 – 93.

11. Saati, T., Vognadze, V. G., (1993), "Prinyatie resheniy: Metod analiza ierarhiy" [Decision-making: Hierarchical analysis method] , M. : Radio i svyaz, 1993. – p.184.

12. Kosevtsov, V.O., Binko, I. F., Matvievskiy, O. M. (1995), "Metodichniy pidhid do analizu y otsinki rivnya natsionalnoyi bezpeki ta yiyi skladovih" [A methodical approach to the analysis and assessment of the level of national security and its components] Nauka i oborona. – No. 1. – pp. 74–77.

13. GorbulIn, V.P., Kachinskiy, O.B. (2007), "Sistemno-kontseptualnI zasadi strategIYi natsIonalnoYi bezpeki UkraYini: monografIya" [Systemic and conceptual principles of the national security strategy of Ukraine: monograph] – K.: DP «NVTs EvroatlantIkIform», – 592 p.

14. Klir, D. (1990), "Sistemologiya: Avtomatizatsiya resheniya sistemnyih zadach" [Systemology: Automation of solving system problems], – M.: Radio i svyaz, – 544 p.

15. SchedrIna, O.I. (2020), "Sistemniy analIz yak Instrument priynyattya upravlInskih rIshen v bIznesI" [System analysis as a tool for making management decisions in business] Visnik KNEU – K: KNEU, No. 99. Pp.170-184, DOI 10/3311| 99.15.

16. Bestuzhev-Lada, I.V. (1982), "Rabochaya kniga po prognozirovaniyu" [Workbook on forecasting] – M.: Myisl, – 430 p.

17. Pornev, A.G., Rumyantseva, Z.P., Solomatin, N.A. (2000), "Upravlenie organizatsiey" [Management of organizations]. Uchebnik – 2-e izd. pererab.i dop. – M.: – 669 p.

18. Pornev, A.G., Rumyantseva, Z.P., Solomatin, N.A. (2000), "Upravlenie organizatsiey" [Management of organizations]. Uchebnik – 2-e izd. pererab.i dop. – M.: – 669 p.

19. Milnera, B. 3. (1971), "SShA: sovremennyie metodyi upravleniya" [USA: modern management methods]. – M. : Nauka, – 334 p.

20. Kolpakov, V.M., Ponomarenko, S.O., Selyukov, O.V. (2021), "Osnovi strategyii": monografIya [Basics of strategy] – K.: Vidavnitstvo Lyudmila, – 474 p.

21. Avinash Dissit, Barri Neyltaff. (2011), "Teoriya igr. Iskusstvo matematicheskoy ekonomiki" [Game theory. The art of mathematical economics]. – M.: Maks-press. – 464 p.

22. Hog, E. (1983), "Prikladnoe optimalnoe proektirovanie" [Applied optimal design], Arora Ya. – M. : Mir, – 478 p.

23. Koh, Richarz. (2012), "Printsip 80/2". [Principle 80/2.]. Monografiya. Perevod s ang. – M. Eksmo, - 444 p.

24. Huntington, S. P. (1999), "The Lonely Superpower" [The Lonely Superpower] March/April, Vol. 78, No. 2, pp. 35-49.

25. Vorobyov, V. V. (1984), "Osnovyi teorii igr. Beskoalitsionnyie igryi" [Basics of game theory. Non-coalition games]. – M. : Nauka, – 496 p.

26. Vasin, A.A., Morozov, V.V. (2005), "Teoriya igr i modeli matematicheskoy ekonomiki" [Game theory and models of mathematical economics]. – M.: Maks-press. – 272 p.

27. Steuen, R.T. (1986), "Multyple Criterial optimization: Theory, Computations and Application" [Multiple Criterion Optimization: Theory, Computations and Applications]. – New York, John Wilay & Sons, Ips, 420 p.

28. Sobol, I.M. (2006), "Vyibor optimalnyih parametrov v zadachah so mnogimi kriteriyami" [Selection of optimal parameters in problems with many criteria]. – M.: Drofa, 176 s.

29. Morgenshtern, O., Fon Neyman, Dzh. (2013), "Teoriya igr i ekonomicheskoe povedenie" [Game theory and economic behavior]. – M.: Kniga po trebovaniyu, – 708 p.

30. KInnI, R., Rayf, H. (2010), "Priynyattya rIshen pri bagatoh kriterIyah: perevagi y zamIschennya" [Decision-making with multiple criteria: advantages and substitutions]. H.: Znannya, – 248 p.

**Shevchenko A.M.**

## A COMPLEX MODEL OF SYSTEM RESEARCH OF CRITICAL INFRASTRUCTURE FACILITIES SECURITY PROBLEMS

***The development of methodological approaches to the solution of an understudied problem, namely to the systematic study of aspects of ensuring the safety of important critical infrastructure facilities is shown in the paper. According to the Law "On the Basics of National Security of Ukraine", the objects of critical infrastructure are: transport and communication; energy and energy supply; provision of housing and communal services; industry and scientific and technical activity in the military-industrial complex; dual purpose technologies; information technologies and information protection; use of subsoil; land on water resources; mineral resources; environmental protection, etc. A system of classifications of prognostic modeling methods has been developed in the form of a three-level structure: by forecasting methods and information bases; according to the material basis of the instrument for obtaining the final result; according to the classification scheme of the specified specific methods.***

***The complex model of system research of critical infrastructure facilities security problems from the position of the Armed Forces of Ukraine has been developed. The mathematical apparatus of analysis and assessment of the level of national (military) security, including military-political, military-economic, military-political models of the state, is presented. The specific features of problem classes by direction, namely well and weakly structured problems, are determined. The use of game theory to compensate for statistical selection is proposed. The main methods of decision-making are given: the methods of utility theory (generalized criterion); the cumulative expected utility as a valid method of decision trees; the methods of prospect theory; the methods of inequality thresholds; the methods of analyzing hierarchies, that are based on a multi-criteria description of the problem; the heuristic methods. It's shown that the most developed theoretical basis, that finds application in determining the security status of critical infrastructure objects and security in general, are expert methods or methods of multidimensional analysis with elements of taxonomy. However, these approaches assume the existence of reference objects or the scenario of the influence of factors on the final result imagined by experts. An important conclusion was made that the basis of the scientific contradiction is the need to create a sufficiently perfect mechanism for solving the problems of objectively justifying decisions in the military sphere under the conditions of significant limitations in the acquisition of biased data for the prevention of conflicts in the military sphere and the absence of finished scientific theory for determining the result of the complex impact of various factors***

***Keywords: ensuring security; objects of critical infrastructure; national and military security; decision-making methods.***

## ЗАГАЛЬНІ ПИТАННЯ

УДК 355.5

к.військ.н., доц. **Георгадзе О.А. (**НУОУ)
**Салаш О.А. (**НУОУ)

DOI: https://doi.org/10.17721/2519-481X/2022/77-14

# ЧАСТКОВА МЕТОДИКА ОЦІНЮВАННЯ СТАНУ КОЛЕКТИВНОЇ ПІДГОТОВКИ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ

***Необхідність впровадження нових підходів щодо організації та проведення колективної підготовки в органах військового управління Збройних Сил України, яка проводиться з метою набуття (підтримання) органами військового управління (їх структурними підрозділами) оперативних спроможностей, зумовлено збройною агресією Російської Федерації проти України. Зазначене неможливо без використання відповідного науково-методичного апарату з оцінювання її стану.***

***На основі науково-методичних підходів з оцінювання ефективності складових (видів) підготовки у Збройних Силах України та досвіду проведення колективної підготовки в органах військового управління, в статті викладено часткову методику оцінювання стану колективної підготовки органів військового управління, як складової комплексної методики оцінювання ефективності оперативної підготовки. До показників, які характеризують стан колективної підготовки органів військового управління віднесено сукупний рівень злагодженості його структурних підрозділів та рівень організації колективної підготовки. Оцінка рівня злагодженості структурного підрозділу визначається за залежністю, яка враховує результати відпрацювання стандартів колективної підготовки та досвід посадових осіб на займаних посадах під час проведення заходів колективної підготовки. До показників, які характеризують рівень організації колективної підготовки віднесено якість Плану підготовки, рівень всебічного забезпечення та керівництва колективною підготовкою. Якість Плану підготовки залежить від діяльності суб'єктів підготовки, щодо визначення обсягу навчально-оперативних завдань які необхідно виконати структурним підрозділам. Рівень всебічного забезпечення заходів колективної підготовки залежить від достатності забезпечення заходів колективної підготовки навчальною матеріально-технічною базою та фінансовим забезпеченням. Рівень керівництва колективною підготовкою залежить від своєчасного здійснення обліку й підбиття підсумків суб'єктами підготовки та узагальнення передового досвіду і впровадження його в практику діяльності органів військового управління.***

***Дана часткова методика дозволяє провести кількісну оцінку стану колективної підготовки органів військового управління, а також виявити проблемні питання під час її організації та проведення, що зумовлює необхідність розроблення рекомендацій з її удосконалення. Результати проведеного дослідження можуть бути використані суб'єктами підготовки під час оцінювання стану колективної підготовки в органах військового управління та у подальших дослідженнях з даного напряму у наукових установах.***

***Ключові слова: колективна підготовка; органи військового управління; методика оцінювання; злагодженість; організація підготовки.***

**Вступ та постановка проблеми.** Досвід застосування угруповань військ (сил) Збройних Сил (ЗС) України у ході відсічі збройної агресії Російської Федерації свідчить, що успішне виконання ними бойових завдань залежить від рівня їх підготовленості. Саме на досягнення високого рівня підготовленості військових організаційних структур спрямована підготовка ЗС України, яка включає в себе: оперативну підготовку, бойову підготовку та підготовку персоналу [1].

Планування застосування та управління угруповань військ (сил) у ході ведення операцій (бойових дій) здійснюють органи військового управління (далі – ОВУ). Саме під час оперативної підготовки здійснюється їх підготовка. Однією із складових оперативної підготовки являється колективна підготовка ОВУ [2], яка спрямована на формування у них

відповідних оперативних спроможностей. Усе це спонукає до пошуку та реалізації нових підходів щодо організації та проведення колективної підготовки в органах військового управління.

Обмежені можливості існуючих методичних підходів з оцінювання ефективності складових (видів) підготовки у ЗС України для повноцінного застосування під час оцінювання стану колективної підготовки органів військового управління спонукає до удосконалення науково-методичного апарату та обґрунтування запропонованих змін. Таким чином існує потреба у науковому обґрунтуванні часткової методики оцінювання стану колективної підготовки органів військового управління, як складової комплексної методики оцінювання ефективності їх оперативної підготовки. Зазначене свідчить про актуальність теми, яка розглядається.

**Аналіз останніх досліджень.** Аналіз попередніх досліджень та публікацій з даного напряму [3-14] свідчить про те, що єдиного підходу до оцінювання стану колективної підготовки ОВУ не існує. Підходи, які використовувались, стосуються переважно питань оцінювання бойової підготовки і деяких складових організації підготовки та не враховують особливостей її проведення з органами військового управління. Так, у попередніх роботах автора [3-6] викладені методичні підходи щодо оцінювання рівня навченості бригади тактичної авіації, підготовленості танкової бригади у ході відновлення боєздатності, злагодженості військових частин сухопутних військ за стандартами колективної підготовки та навченості органів управління військових частин. У статтях [7-8] висвітлено математичну модель набуття бойових спроможностей частинами і підрозділами інженерних військ у ході проведення заходів бойової підготовки та методику оцінювання рівня підготовки об'єднаних тактичних груп кораблів. Запропоновані в статтях [9-11] аналітичні залежності дозволяють оцінити рівень організації об'єднаної підготовки сил оборони, організації підготовки окремої бригади територіальної оборони та організації навчально-виховного процесу в навчальному центрі, у роботі [12] – стан навчальної матеріально-технічної бази окремої механізованої бригади, яка укомплектована військовослужбовцями військової служби за контрактом. У попередній статті автора [13] був визначений підхід до оцінювання рівня ресурсного забезпечення заходів бойової підготовки військових частин. У роботі [14] розглядався методичний підхід щодо оцінювання рівня готовності навчального закладу до військової підготовки громадян за програмою офіцерів запасу.

У той же час, розроблений попередниками науково-методичний апарат є базовою основою для подальшого удосконалення та може бути використаний частково під час оцінювання стану колективної підготовки ОВУ.

**Виклад основного матеріалу.** Колективна підготовка органів військового управління являється складовою оперативної підготовки та проводиться з метою набуття (підтримання) ними оперативних спроможностей.

Для розрахунку кількісної оцінки стану колективної підготовки оберемо показник $B_{КП}(t)$, за величиною якого визначається спроможність ОВУ виконувати завдання за призначенням на час $t$. Стан колективної підготовки ОВУ залежить від сукупного рівня злагодженості структурних підрозділів та організації колективної підготовки суб'єктами підготовки.

Зважаючи на те, що зазначені показники не залежні один від одного, то для розрахунку стану колективної підготовки $B_{КП}(t)$ пропонується використовувати адитивну агрегацію:

$$B_{КП}(t) = C_З(t) \cdot q_З + C_О(t) \cdot q_О , \qquad (1)$$

де $C_З(t)$ – сукупний рівень злагодженості структурних підрозділів ОВУ на час $t$;

$C_О(t)$ – рівень організації колективної підготовки на час $t$;

$q_з$, $q_о$ – "вагові" коефіцієнти важливості показників сукупного рівня злагодженості структурних підрозділів та рівня організації колективної підготовки ОВУ.

Оцінку сукупного рівня злагодженості структурних підрозділів ОВУ $C_З(t)$ пропонується визначати за показником, який враховує рівень злагодженості кожного структурного підрозділу ОВУ з урахуванням його важливості.

Так, як рівень злагодженості кожного окремого структурного підрозділу не залежить від рівня злагодженості іншого, а отже і їх показники не залежні один від одного, то для оцінювання рівня злагодженості $k$-го структурного підрозділу ОВУ $T_{Зk}(t)$ на час $t$ пропонується використовувати адитивну агрегацію:

$$C_З(t) = \sum_{k=1}^{K} T_{Зk}(t) \cdot q_k, \tag{2}$$

де $T_{Зk}(t)$ – рівень злагодженості $k$-го структурного підрозділу ОВУ на час $t$;

$q_k$ – "ваговий" коефіцієнт важливості $k$-го структурного підрозділу ОВУ;

$K$ – кількість структурних підрозділів в ОВУ.

"Вагові" коефіцієнти важливості $k$-го структурного підрозділу ОВУ $q_k$ розраховуються методом експертного оцінювання.

Оцінку рівня злагодженості $k$-го структурного підрозділу ОВУ $T_{Зk}(t)$ пропонується визначати за показниками, які характеризують як результатами відпрацювання підрозділом стандартів колективної підготовки так і враховують досвід посадових осіб на займаних посадах під час проведення заходів колективної підготовки. Зважаючи на те, що зазначені показники не залежні один від одного, то для розрахунку рівня злагодженості $k$-го структурного підрозділу ОВУ $T_{Зk}(t)$ пропонується використовувати адитивну агрегацію:

$$T_{Зk}(t) = K_{Cmk}(t) \cdot q_{Cmk} + K_{Дk}(t) \cdot q_{Дk}, \tag{3}$$

де $K_{Cmk}(t), K_{Дk}(t)$ – показники, які характеризують результати відпрацювання $k$-им структурним підрозділом ОВУ стандартів колективної підготовки та досвід посадових осіб на займаних посадах під час проведення заходів колективної підготовки на час $t$;

$q_{Cmk}$, $q_{Дk}$ – вагові коефіцієнти показників, які характеризують результати відпрацювання $k$-им структурним підрозділом ОВУ стандартів колективної підготовки та досвід посадових осіб на займаних посадах під час проведення заходів колективної підготовки.

Розрахунок вагових коефіцієнтів показників здійснюється методом експертного оцінювання.

Оцінювання стандартів колективної підготовки $K_{Cmk}(t)$ пропонується здійснювати за оцінками розділів стандарту, які характеризують спроможність підрозділу виконувати певні завдання, за залежністю:

$$K_{Cmk}(t) = \frac{\sum_{s=1}^{S} R_{Cmks}(t)}{S}; \qquad R_{Cmks} = \overline{2,5}, \tag{4}$$

де $R_{Cmks}(t)$ – показник, який характеризує оцінку за результатами виконання $k$-им структурним підрозділом ОВУ $s$-го розділу стандарту колективної підготовки на час $t$;

$S$ – кількість розділів стандарту колективної підготовки ОВУ.

Стандарт колективної підготовки оцінюється:

$$K_{Cmk} = \begin{cases} \text{відмінно, якщо } \dfrac{\sum_{s=1}^{S} R_{Cmks}(t)}{S} \geq 4{,}5; \; R_{Cmks} \geq 4; \\ \text{добре, якщо } \dfrac{\sum_{s=1}^{S} R_{Cmks}(t)}{S} \geq 3{,}5; \quad R_{Cmks} \geq 3; \\ \text{задовільно, якщо } \dfrac{\sum_{s=1}^{S} R_{Cmks}(t)}{S} < 3{,}5; \; R_{Cmks} \geq 3; \\ \text{незадовільно, якщо } R_{Cmks}(t) = 2. \end{cases} \quad (5)$$

У свою чергу, розділи стандарту колективної підготовки складаються із елементів, які необхідно виконати $k$ -му структурному підрозділу ОВУ. Розрахунок оцінки за результатами виконання $s$ -го розділу стандарту колективної підготовки пропонується здійснювати наступним чином:

$$R_{Cmks}(t) = \left( \frac{x + y}{x^* + y^*} \right) \cdot z_x; \qquad z_x = \begin{cases} 1, & x = x^*; \\ 0, & x < x^*, \end{cases} \quad (6)$$

де $x$ – кількість виконаних критично важливих елементів;

$x^*$ – загальна кількість критично важливих елементів;

$y$ – кількість виконаних інших елементів;

$y^*$ – загальна кількість інших елементів;

$z_x$ – індекс валідності кінцевого результату за критично важливими елементами (умова обов'язкового повного виконання).

Розділ стандарту колективної підготовки оцінюється:

$$R_{Cmks}(t) = \begin{cases} \text{відмінно, якщо } R_{Cmks}(t) \geq 0{,}8; \\ \text{добре, якщо } 0{,}7 \geq R_{Cmks}(t) < 0{,}8; \\ \text{задовільно, якщо } 0{,}6 \geq R_{Cmks}(t) < 0{,}7; \\ \text{незадовільно, якщо } R_{Cmks}(t) < 0{,}6. \end{cases} \quad (7)$$

Показник "досвід посадових осіб на займаних посадах" $K_{Дk}(t)$ характеризує вплив набутого досвіду посадових осіб ОВУ під час проведення заходів колективної підготовки. Проведенні дослідження засвідчили, що для досягнення стійких навичок посадовим особам ОВУ необхідно, щоб середня тривалість служби на займаній посаді становила три роки.

Чисельне значення показника $K_{Дkj}(t)$ обчислюється, виходячи з кількості заходів колективної підготовки, у яких $j$ -ий військовослужбовець $k$ -го структурного підрозділу ОВУ приймав участь на посаді, яку обіймає, за останні три роки:

$$K_{Дkj}(t) = \frac{H_{kj}}{H_n \cdot e^{\left(\frac{Hk_j - H_n}{H_n}\right)}}, \quad (8)$$

де $H_{kj}$ – кількість заходів колективної підготовки у яких приймав участь $j$-ий військовослужбовець $k$-го структурного підрозділу ОВУ на займаній посаді за останні три роки;

$H_n$ – загальна кількість заходів колективної підготовки, яка визначена Планом підготовки ОВУ протягом останніх трьох років.

Оцінку рівня організації колективної підготовки $C_O(t)$ пропонується визначати показником, який враховує діяльність суб'єктів підготовки спрямовану на продумане, планове навчання об'єктів колективної підготовки.

Отже, до показників, які характеризують рівень організації колективної підготовки ОВУ $C_O(t)$ пропонується віднести: якість Плану підготовки ОВУ $K_{Пл}(t)$, всебічне забезпечення колективної підготовки $K_{Вз}(t)$ та керівництво колективної підготовки $K_K(t)$.

Зважаючи на те, що зазначені показники не залежать один від одного, то для розрахунку рівня організації колективної підготовки ОВУ $C_O(t)$ пропонується використовувати адитивну агрегацію:

$$C_O(t) = K_{Пл}(t) \cdot q_{пл} + K_{Вз}(t) \cdot q_{вз} + K_K(t) \cdot q_к, \quad (9)$$

де $K_{Пл}(t); K_{Вз}(t); K_K(t)$ – показники, які характеризують якість плану підготовки, всебічне забезпечення та керівництво колективною підготовкою ОВУ на час $t$;

$q_{пл}; q_{вз}; q_к$ – "вагові" коефіцієнти показників якості плану підготовки, всебічного забезпечення колективної підготовки та керівництва колективною підготовкою ОВУ.

Показник "якість Плану підготовки ОВУ" $K_{Пл}(t)$ характеризує діяльність суб'єктів підготовки, щодо визначення обсягу навчально-оперативних завдань які необхідно виконати структурним підрозділам згідно Плану підготовки ОВУ. Його пропонується розраховувати за залежністю, яка враховує частку навчально-оперативних завдань спланованих для виконання $k$-им структурним підрозділам ОВУ від їх загальної кількості, яка визначена у "Типовому каталозі завдань (підзавдань) з підготовки Збройних Сил України":

$$K_{Плk}(t) = \frac{\sum_{k=1}^{K} \eta_k \cdot q_k}{\mu}, \quad (10)$$

де $\eta_k$ – показник, який характеризує кількість навчально-оперативних завдань, які сплановані для виконання $k$-им структурним підрозділом на час $t$;

$\mu$ – показник, який характеризує загальну кількість навчально-оперативних завдань визначених у "Типовому каталозі завдань (підзавдань) з підготовки Збройних Сил України";

$q_k$ – "вагові" коефіцієнти важливості $k$-го структурного підрозділу ОВУ;

$K$ – кількість структурних підрозділів в ОВУ.

Оцінку рівня всебічного забезпечення колективної підготовки ОВУ $K_{Вз}(t)$ пропонується визначати за залежністю, яка враховує достатність забезпеченості заходів

колективної підготовки навчальною матеріально-технічною базою та фінансовим забезпеченням.

Так, як забезпечення навчальною матеріально-технічною базою не залежить від фінансового забезпечення, а отже і їх показники не залежні один від одного, то для оцінювання рівня всебічного забезпечення колективної підготовки ОВУ $K_{Взк}(t)$ пропонується використовувати адитивну агрегацію:

$$K_{Взк}(t) = L_{НМТБ}(t) \cdot q_{нмтб} + L_{Ф}(t) \cdot q_{ф}, \quad (11)$$

де $L_{НМТБ}(t)$ – показник, який характеризує рівень забезпеченості заходів колективної підготовки ОВУ навчальною матеріально-технічною базою на час $t$;

$L_{Ф}(t)$ – показник, який характеризує рівень фінансового забезпечення заходів колективної підготовки ОВУ на час $t$;

$q_{нмтб}$ ,$q_{ф}$ – вагові коефіцієнти показників забезпеченості заходів колективної підготовки навчальною матеріально-технічною базою та фінансовим забезпеченням.

Показник "навчальна матеріально-технічна база" $L_{НМТБ}(t)$ характеризує здатність навчальних об'єктів (районів місцевості, полігонів) і навчального військового майна забезпечити колективну підготовку ОВУ. Його розрахунок пропонується здійснювати за залежністю, яка враховує їх наявну кількість від загальної кількості, визначеної відповідними нормативними документами:

$$L_{НМТБ}(t) = \frac{\sum_{d=1}^{D_н} H_d(t) \cdot q_d}{\sum_{d=1}^{D_з} H_d(t) \cdot q_d}, \quad (12)$$

де $H_d(t)$ – показник, який характеризує $d$ -і навчальні об'єкти і навчальне військове майно навчальної матеріально-технічної бази на час $t$ здатних забезпечити колективну підготовку ОВУ;

$D_н$ – кількість навчальних об'єктів і навчального військового майна навчальної матеріально-технічної бази здатних забезпечити колективну підготовку ОВУ;

$D_з$ – загальна кількість навчальних об'єктів і навчального військового майна навчальної матеріально-технічної бази визначена відповідними нормативними документами;

$q_d$ – ваговий коефіцієнт важливості $d$ -го навчального об'єкта і навчального військового майна навчальної матеріально-технічної бази.

Показник "фінансове забезпечення" $L_{Ф}(t)$ характеризує достатність забезпечення видатками заходів колективної підготовки ОВУ. Його розрахунок пропонується проводити за залежністю, яка враховує фактичне фінансування видатків по статтям на колективну підготовку від необхідної їх потреби:

$$L_{Ф}(t) = \frac{\sum_{g=1}^{G_Ф} T_g(t) \cdot q_g}{\sum_{g=1}^{G_з} T_g(t) \cdot q_g}, \quad (13)$$

де $T_g(t)$ – показник, який характеризує $g$ - і статті видатків для проведення заходів колективної підготовки структурних підрозділів ОВУ на час $t$;

$G_Ф$ – кількість фактично профінансованих статей видатків на колективну підготовку ОВУ;

$G_З$ – загальна кількість статей видатків на колективну підготовку ОВУ;

$q_g$ – ваговий коефіцієнт важливості $g$ - ої статті видатків на колективну підготовку ОВУ.

Оцінку рівня керівництва колективною підготовкою ОВУ $K_K(t)$ пропонується визначати за показниками, які враховують діяльність суб'єктів підготовки щодо виконання основних заходів керівництва над процесом колективної підготовки для набуття (підтримання) ОВУ оперативних спроможностей.

Рівень керівництва колективною підготовкою залежить від своєчасного здійснення обліку і підбиття підсумків колективної підготовки ОВУ $L_{ОП}(t)$ та узагальнення передового досвіду і впровадження його в практичну діяльність $L_Д(t)$.

Так, як своєчасне здійснення обліку і підбиття підсумків колективної підготовки ОВУ не залежить від узагальнення передового досвіду і впровадження його в практичну діяльність, а отже і їх показники не залежні один від одного, то для оцінювання рівня керівництва колективною підготовкою ОВУ $K_K(t)$ пропонується використовувати адитивну агрегацію:

$$K_K(t) = L_{ОП}(t) \cdot q_{оп} + L_Д(t) \cdot q_д, \qquad (14)$$

де $L_{ОП}(t)$ – показник який характеризує своєчасне здійснення обліку і підбиття підсумків колективної підготовки ОВУ на час $t$;

$L_Д(t)$ – показник який характеризує узагальнення передового досвіду і впровадження в практичну діяльність колективної підготовки структурних підрозділів ОВУ на час $t$;

$q_{оп}$, $q_д$ – "вагові" коефіцієнти показників своєчасне здійснення обліку і підбиття підсумків колективної підготовки ОВУ та узагальнення передового досвіду і впровадження його в практичну діяльність.

Показник "своєчасне здійснення обліку і підбиття підсумків" $L_{ОП}(t)$ характеризує діяльність суб'єктів підготовки щодо виконання основних заходів керівництва над процесом колективної підготовки. Його розрахунок пропонується проводити за залежністю, яка враховує своєчасне здійснення обліку і підбиття підсумків до загальної кількості заходів колективної підготовки ОВУ:

$$L_{ОП}(t) = \frac{\sum_{p=1}^{P_C} F_p(t) \cdot q_p}{\sum_{p=1}^{P_З} F_p(t) \cdot q_p}, \qquad (15)$$

де $F_p(t)$ – показник, який характеризує $p$ - е підбиття підсумків зі здійсненням обліку заходів колективної підготовки ОВУ на час $t$;

$P_C$ – кількість своєчасно проведених підбиттів підсумків зі здійсненням обліку заходів колективної підготовки ОВУ;

$P_З$ – загальна кількість заходів колективної підготовки в ОВУ;

$q_p$ – ваговий коефіцієнт важливості $p$ -ого підбиття підсумків зі здійсненням обліку заходів колективної підготовки структурних підрозділів ОВУ.

Показник “узагальнення передового досвіду і впровадження в практичну діяльність” $L_Д(t)$ характеризує діяльність суб’єктів підготовки щодо узагальнення передового досвіду колективної підготовки та впровадження його у практику діяльності структурних підрозділів ОВУ. Його розрахунок пропонується здійснювати за залежністю, яка враховує кількість структурних підрозділів ОВУ у яких було впроваджено передовий досвід від їх загальної кількості:

$$L_Д(t) = \frac{M_В}{M_З}, \tag{16}$$

де $M_В$ – кількість структурних підрозділів ОВУ у яких суб’єктами підготовки було впроваджено передовий досвід у практику їх діяльності;

$M_З$ – загальна кількість структурних підрозділів ОВУ визначених для набуття оперативних спроможностей.

Визначення вагових коефіцієнтів усіх рівнів здійснюється методом експертного оцінювання.

**Висновки та перспективи подальшого розвитку.** Таким чином, у статті було розроблено часткову методику оцінювання стану колективної підготовки органів військового управління, яка дозволяє провести її кількісну оцінку, а також виявити проблемні питання під час її організації та проведення, що зумовлює необхідність розроблення рекомендацій з її удосконалення. До показників, які характеризують стан колективної підготовки органів військового управління віднесено: сукупний рівень злагодженості структурних підрозділів та організація колективної підготовки суб’єктами підготовки.

Перспективами подальших наукових досліджень у даному напрямі буде обгрунтування рекомендацій щодо організації та проведення колективної підготовки в органах військового управління.

ЛІТЕРАТУРА:

1. Доктрина з організації підготовки у Збройних Сил України: за станом на 03 лип. 2020 р. – К.: Генеральний штаб Збройних Сил України, 2020. – 34 с. (Нормативний документ Генерального штабу Збройних Сил України. Доктрина).

2. Про затвердження Настанови з оперативної підготовки у Збройних Силах України: наказ Генерального штабу Збройних Сил України від 13.02.2021 №14.

3. Piekhota, S., Heorhadze, O., Kharabara, V. (2021). Partial methodology for assessing the level of learning of tactical aviation brigade personnel. Political Science and Security Studies Journal, Vol. 2. № 1. P. 68-73. https://doi.org/10.5281/zenodo. 4818549.

4. Георгадзе О.А., Харабара В.І. (2019). Часткова методика оцінювання рівня підготовленості танкової бригади у ході відновлення боєздатності. Journal of Scientific Papers “Social development and security”. 9(4), 131 – 142. https://doi.org/10.33445/sds.2019.9.4.10.

5. Георгадзе О.А. Методичний підхід до оцінювання рівня злагодженості військових частин Сухопутних військ за стандартами колективної підготовки. Збірник наукових праць Національного університету оборони України імені Івана Черняховського “Труди університету”. 2017. – № 4(143). – С. 62 – 64.

6. Георгадзе О.А., Макаліш О.В. Методичний підхід до оцінювання рівня навченості органів військового управління тактичного рівня. Збірник наукових праць Центру військово-стратегічних досліджень Національного університету оборони України імені Івана

Черняховського – 2016. – № 3(58). – С. 104–108. https://doi.org/10.33099/ 2304- 2745/2016-3-58/104-108.

7. Гром В. А. Математична модель набуття бойових спроможностей частинами та підрозділами інженерних військ в ході проведення заходів бойової підготовки. Сучасні інформаційні технології у сфері безпеки та оборони. 2016. № 1 (25). С. 31-34.

8. Bezuhlyi V. Assessment methodology of the level of training of joint tactical groups of ships. The Bulletin of "Carol I" National Defense University. Vol. 9. № 4. – 2020 – P. 25 – 33.

9. Heorhadze O. Metod's for assessing the level of the organization of joint training of defence forces. Сучасні інформаційні технології у сфері безпеки та оборони. Київ : НУОУ, 2022. № 2 (44). С. 43–47. https://doi.org/10.33099/2311-7249/2022-44-2-43-47.

10. Heorhadze O., Barhylevych A. Separate brigade of territorial defence level of training organization assessment methodology. Political Science and Security Studies Journal. Vol. 1. № 1. – 2020 – P. 71 – 75. https://doi.org/ 10.5281/zenodo.4399732.

11. Vynokurov D., Heorhadze O. Comprehensive methodology for evaluating the effectiveness of training the variable composition of the training center. Political Science and Security Studies Journal.Vol. 2. № 2. – 2021 – P. 77 – 85. https://doi.org/10.5281/zenodo.5071081.

12. Семон Б.Й., Шпанчук Г.В. Особливості методичного підходу до оцінювання рівня підготовки штабів окремої механізованої бригади, що укомплектована військовослужбовцями професійної служби // Збірник наукових праць Національного університету оборони України імені Івана Черняховського "Труди університету". 2010. – №98. – С. 72-76.

13. Георгадзе О.А. Методика оцінювання рівня ресурсного забезпечення заходів бойової підготовки військових частин. Сучасні інформаційні технології у сфері безпеки та оборони. 2016. № 3 (27). С. 144-147.

14. Heorhadze O., Kamalov Y. Methods for assessing the readiness level of an educational institution for military training of citizens according to the program of reserve officers. Political Science and Security Studies Journal. Vol. 1. № 2. – 2020 – P. 90 – 97. https://doi.org/10.5281/zenodo.4521176.

REFERENCES:

1. Doktrina z organizatsiyi pidgotovki u Zbroynih Syl Ukrayiny: za stanom na 03 lip. 2020 r. – K.: Generalniy shtab Zbroynih Sil Ukrayini, 2020. – 34 p. (Normativniy dokument Generalnogo shtabu Zbroynih Syl Ukrayiny. Doktrina).

2. Pro zatverdzhennya Nastanovi z operativnoyi pidgotovki u Zbroynih Silah Ukrayini: nakaz Generalnogo shtabu Zbroynih Sil Ukrayini vid 13.02.2021 #14.

3. Piekhota, S., Heorhadze, O., Kharabara, V. (2021). Partial methodology for assessing the level of learning of tactical aviation brigade personnel. Political Science and Security Studies Journal, Vol. 2. # 1.Pp. 68-73. https://doi.org/10.5281/zenodo. 4818549.

4. Georgadze O.A., Harabara V.I. (2019). Chastkova metodika otsinyuvannya rivnya pidgotovlenosti tankovoyi brigadi u hodi vidnovlennya boezdatnosti. Journal of Scientific Papers "Social development and security". 9(4), Pp. 131 – 142. https://doi.org/10.33445/sds.2019.9.4.10.

5. Georgadze O.A. Metodichniy pidhid do otsInyuvannya rivnya zlagodzhenosti viyskovih chastin Suhoputnih viysk za standartami kolektivnoyi pidgotovki. Zbirnik naukovih prats Natsionalnogo universitetu oboroni Ukrayini imeni Ivana Chernyahovskogo "Trudi universitetu". 2017. – # 4(143). – Pp. 62 – 64.

6. Georgadze O.A., MakalIsh O.V. Metodichniy pidhid do otsinyuvannya rivnya navchenosti organiv viyskovogo upravlinnya taktichnogo rivnya. Zbirnik naukovih prats tsentru viyskovo-strategichnih doslidzhen Natsionalnogo universitetu oboroni Ukrayini imeni Ivana Chernyahovskogo – 2016. – # 3(58). – Pp. 104–108. https://doi.org/10.33099/ 2304- 2745/2016-3-58/104-108.

7. Grom V. A. Matematichna model nabuttya boyovih spromozhnostey chastinami ta pidrozdilami inzhenernih viysk v hodi provedennya zahodiv boyovoyi pidgotovki. Suchasni informatsiyni tehnologiyi u sferi bezpeki ta oboroni. 2016. # 1 (25). Pp. 31-34.

8. Bezuhlyi V. Assessment methodology of the level of training of joint tactical groups of ships. The Bulletin of "Carol I" National Defense University. Vol. 9. # 4. – 2020 – Pp. 25 – 33. https://doi.org/10.12753/2284-9378-20-63.

9. Heorhadze O. Metod's for assessing the level of the organization of joint training of defense forces. Suchasni informatsiyni tehnologiyi u sferi bezpeki ta oboroni. Kiyiv : NUOU, 2022. # 2 (44). Pp. 43–47. https://doi.org/10.33099/2311-7249/2022-44-2-43-47.

10. Heorhadze O., Barhylevych A. Separate brigade of territorial defence level of training organization assessment methodology. Political Science and Security Studies Journal. Vol. 1. # 1. – 2020 – Pp. 71 – 75. https://doi.org/ 10.5281/zenodo.4399732.

11. Vynokurov D., Heorhadze O. Comprehensive methodology for evaluating the effectiveness of training the variable composition of the training center. Political Science and Security Studies Journal. Vol. 2. # 2. – 2021 – Pp. 77 – 85. https://doi.org/10.5281/zenodo.5071081.

12. Semon B.Y., Shpanchuk G.V. Osoblivosti metodichnogo pidhodu do otsinyuvannya rivnya pidgotovki shtabiv okremoyi mehanizovanoyi brigadi, scho ukomplektovana viyskovosluzhbovtsyami profesiynoyi sluzhbi. Zbirnik naukovih prats Natsionalnogo universitetu oboroni Ukrayini imeni Ivana Chernyahovskogo "Trudi universitetu". 2010. – #98. – Pp. 72-76.

13. Georgadze O.A. Metodika otsinyuvannya rivnya resursnogo zabezpechennya zahodiv boyovoyi pidgotovki viyskovih chastin. Suchasni Informatsiyni tehnologiyi u sferi bezpeki ta oboroni. 2016. # 3 (27). Pp. 144-147.

14. Heorhadze O., Kamalov Y. Methods for assessing the readiness level of an educational institution for military training of citizens according to the program of reserve officers. Political Science and Security Studies Journal. Vol. 1. # 2. – 2020 – Pp. 90 – 97. https://doi.org/10.5281/zenodo.4521176.

**PhD. Heorhadze O.A.,**
**Salash O.A.**

## PARTIAL METHODOLOGY OF ASSESSING THE STATE OF COLLECTIVE TRAINING OF MILITARY MANAGEMENT BODIES

***The necessity of introducing new approaches to the organization and conduct of collective training in the military management bodies of the Armed Forces of Ukraine, which is conducted with the purpose of acquiring (supporting of the military management bodies (their structural subdivisions) operational capabilities, is conditioned by the armed aggression of the Russian Federation against Ukraine. It is impossible without the use of the appropriate scientific and methodical apparatus for the assessment of its condition.***

***On the basis of scientific and methodical approaches on assessment of effectiveness of components (types) of training in the Armed Forces of Ukraine and experience of conducting collective training in the military management bodies, the article contains a partial methodology of assessing the state of collective training of the military management bodies, as a component of complex methodology of evaluation of effectiveness of operational training.***

***The indicators that characterize the state of collective training of the military management bodies are the overall level of agreement between its structural units and the level of organization the collective training. The assessment of the level of agreement of the structural unit is determined by the dependence, which takes into account the results of the work of the standards of collective training and the experience of officials at the occupied positions during the collective training activities. The indicators that characterize the level of organization the collective training is characterized by the quality of the preparation plan, the level of comprehensive support and the management of collective preparation. The quality of the preparation plan depends on the activity of the subjects of preparation, as to the definition of the volume of educational and operational tasks which should be carried out by structural subdivisions. The level of comprehensive provision of collective training activities depends on the adequacy of provision of collective training activities by the educational material and technical basis and financial support. The level of management of collective training depends on timely accounting and summing up by subjects of preparation and generalization of best practices and its introduction into practice of the military management bodies.***

***This partial method allows to carry out quantitative assessment of the state of collective training of the military management bodies, as well as to identify problem issues during its organization and carrying out, which makes it necessary to develop recommendations on its improvement. The results of the research can be used by the subjects of preparation during the assessment of the state of collective training in the military management bodies and in further researches on this direction in scientific institutions.***

***Keywords: collective training; military management bodies; assessment methodology; agreement; organization.***

**Дані про авторів**

**Бабій Юлія Олександрівна,** доктор технічних наук, головний редактор редакційного відділення видавництва Національної академії Державної прикордонної служби України імені Богдана Хмельницького, ORCID: 0000-0001-7310-8715.

**Берназ Андрій Михайлович,** Начальник організаційно-планового відділу - заступник начальника управлінні сил підтримки Командування сухопутних військ ЗСУ, ORCID: 0000-0003-3221-2860.

**Гахович Сергій Вікторович,** кандидат технічних наук, старший науковий співробітник, старший науковий співробітник науково-дослідного відділу науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-9135-6568.

**Георгадзе Олександр Аміранович**, кандидат військових наук, доцент, заступник начальника кафедори керівництва військами (силами) в мирний час Національного університету оборони України імені Івана Черняховського, ORCID: 0000-0002-9306-6660.

**Глухов Сергій Іванович,** доктор технічних наук, доцент, завідувач кафедри Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-4918-3739.

**Джулій Володимир Миколайович,** кандидат технічних наук, доцент, доцент кафедри кібербезпеки та комп`ютерних систем і мереж Хмельницького національного університету, ORCID: 0000-0003-1878-4301.

**Довгополий Анатолій Степанович,** доктор технічних наук, професор, головний науковий співробітник Центрального науково-дослідного інституту озброєння і військової техніки Збройних Сил України, Київ, Україна, ORCID: 0000-0001-9227-9771

**Караванов Олександр Анатолійович** – ад'юнкт науково-організаційного відділу Національної академія сухопутних військ імені гетьмана П.Сагайдачного, ORCID: 0000-0002-6189-8032.

**Кацалап Віталій Олександрович,** канд. військових наук, доцент, професор кафедри застосування інформаційних технологій та інформаційної безпеки інституту забезпечення військ (сил) та інформаційних технологій Національного університету оборони України імені Івана Черняховського (0000-0003-4804-8022).

**Кирилюк Владислав Олександрович,** магістр кафедри кібербезпеки та програмного забезпечення; Національний університет «Одеська політехніка» (м.Одеса, Україна); ORCID: 0000-0002-0869-820X.

**Кобозєва Алла Анатоліївна,** доктор технічних наук, професор, завідувач кафедри кібербезпеки та програмного забезпечення; Національний університет «Одеська політехніка» (м.Одеса, Україна); ORCID: 0000-0001-7888-0499.

**Коваль Мирослав Олександрович,** доктор філософських наук з інформаційної технології, науковий співробітник науково-дослідного віддвлу військово-технічних та інформаційних досліджень науково-дослідного центру Військово інституту Київського національного університету імені Тараса Шевченка ORCID: 0000-0002-8374-7390.

**Коцюруба Володимир Іванович,** доктор технічних наук, професор, професор кафедри Національного університету оборони України імені Івана Черняховського, Київ, Україна, ORCID 0000-0001-6565-9576.

**Кравченко Олександр Іванович,** кандидат педагогічних наук, старший науковий співробітник науково-дослідноговідділу науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0002-7865-5870.

**Кривцун Володимир Іванович,** кандидат технічних наук, старший науковий співробітник, начальник кафедри інженерної техніки Національної академії Сухопутних військ імені гетьмана Петра Сагайдачного, ORCID: 0000-0002-3907-5320.

**Кошовий Микола Дмитрович**, доктор технічних наук, професор, Національний аерокосмічний університет ім. М.Є. Жуковського "ХАІ", професор кафедри Інтелектуальних вимірювальних систем та інженерії якості, ORCID: 0000-0001-9465-4467.

**Лєнков Сергій Васильович,** доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, головний науковий співробітник науково-дослідного центру, Військовий інститут Київського національного університету імені Тараса Шевченка, ORCID: 0000-0001-7689-239X.

**Маєвський Дмитро Андрійович**, доктор технічних наук, професор, завідувач кафедри електромеханічної інженерії; Національний університет «Одеська політехніка» (м.Одеса, Україна); ORCID: 0000-0003-0666-6199.

**Максименко Юрій Анатолійович,** кандидат технічних наук, начальник кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки Військової академії (м. Одеса), ORCID: 0000-0002-1227-2009.

**Маміч Віктор Володимирович,** кандидат технічних наук, доцент, доцент кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки Військової академії, ORCID: 0000-0001-5574-0901.

**Мартинюк Віктор Петрович,** старший викладач кафедри прикордонної служби, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький, Україна, 0000-0001-9569-1112.

**Мартинюк Олександр Васильович,** старший викладач кафедри прикордонної служби, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький, Україна 0000-0002-0216-1356.

**Мацьовитий Віктор,** Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, ORCID ID 0000-00002-8122-5492.

**Міночкін Дмитро Анатолійович,** кандидат технічних наук, старший науковий співробітник Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», ORCID – 0000-0003-4988-7098.

**Нсер Анжела Махер,** магістрантка кафедри телекомунікацій Інституту телекомунікаційних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», ORCID – 0000-0001-6792-7925.

**Охрамович Михайло Миколайович,** кандидат технічних наук, старший дослідник, начальник відділу-заступник начальника управління Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-0002-8776-3937.

**Омельянчук Андрій Володимирович,** начальник відділу Головного оперативного управління Генерального штабу Збройних Сил України, ORCID – 0000-0002-1171-3415.

**Пилипенко Олександр Тарасович**, аспірант, Національний аерокосмічний університет ім. М.Є. Жуковського "ХАІ".

**Поліщук Віктор Вікторович,** кандидат військових наук, доцент кафедри прикордонної служби, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький, Україна, 0000-0002-9654-9015.

**Попов Сергій Афанасійович,** доктор наук з державного управління, професор, професор кафедри, організації розвідувально-інформаційної роботи та технічних засобів розвідки Військової академії, ORCID: 0000-0002-0729-9581.

**Салаш Олег Анатолійович,** ад'юнкт кафедри керівництва військами (силами) в мирний час Національний університет оборони України імені Івана Черняховського ORCID: 0000-0003-3116-2857.

**Сивак Олександр Володимирович,** головний спеціаліст відділу Головного оперативного управління Генерального штабу Збройних Сил України, ORCID: 0000-0003-0929-9486.

**Солодєєва Людмила Василівна**, науковий співробітник, науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-0002-7979-8443.

**Черноусов Дмитро Олександрович**, викладач кафедри прикордонної служби, Національна академія Державної прикордонної служби України імені Богдана Хмельницького, м. Хмельницький, Україна, ORCID: 0000-0002-9012-2372.

**Шаршаткін Данило Юрійович**, старший викладач кафедри організації розвідувально-інформаційної роботи та технічних засобів розвідки, Військова академія (м. Одеса), ORCID - 0000-0002-3362-2469.

**Шевченко Анатолій Михайлович,** начальник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID: 0000-0003-2723-0378.

**Алфавітний покажчик**

## РЕДАКЦІЙНА ПОЛІТИКА ТА ЕТИЧНІ НОРМИ

## ПРИНЦИПИ ФОРМУВАННЯ ТА ДОСТУП ДО ЗМІСТУ «ЗБІРНИКА ВІКНУ»

Редакційна політика «Збірника ВІКНУ» заснована на принципах об'єктивності та неупередженості при відборі статей для публікації; високих вимог до якості наукових досліджень; обов'язковості та конфіденційності рецензування статей; додержання колегіальності при відборі до публікації статей; доступності та оперативності у спілкуванні з авторами; суворого дотримання авторських і суміжних прав. Запобігання протизаконним публікаціям є відповідальністю кожного автора, редактора, рецензента, видавця.

До друку приймаються оригінальні рукописи, які не опубліковано раніше, не було відправлено до інших редакцій та які повністю відповідають вимогам щодо оформлення та порядку подання статей.

У «Збірнику ВІКНУ» сформовані наступні рубрики: військова техніка і технології подвійного призначення, інформаційні технології, загальні питання.

Редакція підтримує політику відкритого доступу та принципи вільного поширення наукової інформації. Примірники збірників знаходяться у Національній бібліотеці України ім. В.І. Вернадського, науковій бібліотеці ім. М. Максимовича, у бібліотеці Військового інституту та інших бібліотеках України. Електронна версія розміщена на сайті інституту, на сайтах наведених бібліотек та на сайтах «Збірника ВІКНУ»: http://miljournals.knu.ua/index.php/zbirnuk; http://mil.univ.kiev.ua/page/lib/31

### ЕТИКА ПУБЛІКАЦІЙ

Редакційна колегія журналу вимагає від авторів наслідувати формальним та етичним правилам підготовки і публікації наукових робіт, що вони подають до редакції журналу. Ці норми зумовлено стандартами якості наукових статей, прийнятими у світовому науковому співтоваристві, зокрема публікаційними принципами Publishing Ethics Resource Kit (PERK), рекомендаціями Elsevier, Комітету з етики публікацій (Committee on Publication Ethics, COPE), етичним кодексом вченого України, а також досвідом роботи іноземних та українських професіональних спільнот, наукових організацій, редколегій та редакцій видань.

### ЕТИЧНІ ЗОБОВ'ЯЗАННЯ РЕДАКЦІЙНОЇ КОЛЕГІЇ ЖУРНАЛУ

Редакційна колегія у своїй діяльності:

– керується принципами неупередженості, наукової етики рецензування, захисту – інтелектуальної власності,

– несе відповідальність за рівень наукового наповнення журналу,

– виступає проти фальсифікації, плагіату, направлення автором одного рукопису до кількох журналів, багаторазового копіювання тексту статті в різних місцях, введення громадськості в оману щодо реального внеску кожного автора в опубліковану наукову роботу;

– залишає за собою право направити рукопис на розгляд сторонньому рецензенту, у тому числі ретельний відбір через «сліпе» рецензування, відхилити статтю або повернути її на доопрацювання;

– може відхилити рукопис, якщо вважає, що він не відповідає профілю журналу, чи не відповідає етиці та правилам оформлення,

– має право вилучити вже опубліковану статтю в разі виявлення порушення будь-чиїх прав або загальноприйнятих норм наукової етики, про даний факт вилучення статті редакція повідомляє як автору статті, так і організації, де було виконано дослідження та повідомляє про це у наступному номері.

Співробітники редакції не надають іншим особам інформації, пов'язаної із змістом рукописів, що перебувають на розгляді, крім осіб, які беруть участь у її фаховій оцінці

Згідно з міжнародним законодавством щодо додержання авторського права на електронні інформаційні ресурси, матеріали сайту, електронного журналу або проекту не можуть бути відтворені повністю або частково в будь-якій формі (електронній чи друкованій) без попередньої письмової згоди редакції журналу. При використанні опублікованих матеріалів у контексті інших документів обов'язково необхідними є посилання на першоджерело.

## ЕТИЧНІ ЗОБОВ'ЯЗАННЯ АВТОРА

Автор:

– несе відповідальність за новизну і достовірність наведених у статтях результатів, тактико-технічних та економічних показників, коректність висловлювань а також за те, що в матеріалах не міститься інформація з обмеженим доступом;

– повинен цитувати ті публікації, які мали визначальний вплив на суть викладеного у статті, а також ті, які можуть швидко ознайомити читача з більш ранніми працями, важливими для розуміння цього дослідження, необхідно також належним чином вказувати джерела принципово важливих матеріалів, використаних у даній роботі, якщо вони не були отримані самим автором;

– забезпечує недопустимість плагіату та подання до публікації раніше надрукованих матеріалів, у випадку виявлення зазначених фактів відповідальність несе автор поданих матеріалів.

Співавторами статті мають бути всі особи, що зробили вагомий науковий внесок у подану роботу і поділяють відповідальність за отримані результати. Автор, який подає рукопис до публікації, відповідає за те, щоб до списку співавторів були включені тільки ті особи, які відповідають критерію авторства, і бере на себе відповідальність за згоду інших авторів статті на її публікацію в журналі.

**УВАГА!**

**РЕДАКЦІЙНА КОЛЕГІЯ «ЗБІРНИКА ВІКНУ» ЗДІЙСНЮЄ НЕЗАЛЕЖНЕ («СЛІПЕ») ЕКСПЕРТНЕ РЕЦЕНЗУВАННЯ НАДАНИХ ДО ДРУКУ РУКОПИСІВ ТА ПЕРЕВІРКУ ЇХ НА ПЛАГІАТ. РЕЦЕНЗУВАННЯ ЗДІЙСНЮЄТЬСЯ ЗА АНОНІМНОЮ ФОРМОЮ ЯК ДЛЯ АВТОРІВ, ТАК І ДЛЯ РЕЦЕНЗЕНТІВ.**

## ПОРЯДОК ПОДАННЯ І ОФОРМЛЕННЯ СТАТЕЙ ДО "ЗБІРНИКА НАУКОВИХ ПРАЦЬ ВІЙСЬКОВОГО ІНСТИТУТУ КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА"

До друку приймаються оригінальні рукописи, які не опубліковано раніше, не було відправлено до інших редакцій та які повністю відповідають вимогам щодо оформлення та порядку подання статей.

***Загальні вимоги до технічного оформлення статей:***

*Обсяг рукопису* – **не менше 6 повних аркушів** українською або англійською мовами.

Формат аркуша - **А4 (210 х 297 мм)**.

Розмір полів: верхнє, нижнє, праве, ліве – **2 см.**

Основний шрифт – **Times New Roman №12,** через міжрядковий інтервал **- 1,0.** Абзац має становити **10 мм.**

Стаття повинна мати такі необхідні елементи:

***УДК*;**

***назва статті,*** яка лаконічно відображає зміст та новизну статті;

***анотація;***

***вступ та постановка задачі чи проблеми*** у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

***аналіз останніх досліджень*** і публікацій, в яких започатковано **розв'язання даної проблеми** і на які спирається автор, виділення невирішених раніше частин загальної проблеми, котрим присвячується означена стаття, формулювання цілей статті;

***виклад основного матеріалу*** дослідження з повним обґрунтуванням отриманих наукових результатів, практичних рішень та експериментів;

***висновки*** з даного дослідження і перспективи подальшого розвитку у даному напрямку.

***список літератури,***

***References,***

***дані про авторів*** трьома мовами.

***Анотація*** до статті виконується українською та англійською мовами загальний обсяг кожної не менш ніж **1800** знаків, включаючи ключові слова.

Вона повинна містити коротке повторення структури статті, що включає вступ, цілі і завдання, методи, результати, висновки.

Анотацію друкують курсивом, шрифт Times New Roman, №11. Після анотації розміщуються **ключові слова** (5–7 термінів).

***Список літератури (References***) повинен включати не менш 12 джерел, з яких 50 % видані за останні 10 років. При цьому не менш 25 % джерел повинно відноситися до іноземної періодики. Самоцитування авторів у списку літератури повинно бути, як правило, не більш за 15 %.

Якщо основною мовою статті є українська або російська, то оформлюються два списки літератури:

перший (список літератури мовою оригіналу джерела) – згідно наказу МОН від 12.01.2017 № 40 та відповідно до ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання: загальні положення та правила складання»;

другий (REFERENCES) з урахуванням ДСТУ 8302:2015, наказу МОН від 12.01.2017 № 40 та міжнародного Гарвардського стилю BSI (British Standards Institution).

***На адресу редколегії (03680. м. Київ, вул Ломоносова 81, тел.: +38 (044) 521 - 33 - 82) мають бути надіслані наступні матеріали:***

***експертний висновок,*** про можливість відкритого публікування, завірений печаткою

***У відомостях про авторів*** (українською та англійською мовами) наводиться:

– прізвище, ім'я та по батькові;

– науковий ступінь, вчене звання, почесні звання;

– посада та назва установи, де працює автор, її місце розташування (місто, країна);

– обліковий запис автора ORCID;

– адреса електронної пошти, контактний телефон.

***Вимоги до оформлення References***

References потрібно приводити окремим блоком, повторюючи послідовність попередньо наведеного Списку літератури. Джерела при цьому оформлюються за такими основними правилами (Harvard style оформлення BSI: British Standards Institution):

– запис завжди починається з прізвища автора, потім, через кому, ініціали (між ініціалами пропуски не ставляться), за якими в дужках вказується дата видання; два автори відокремлюються «and» без коми; кілька авторів розділяються комами, але останнє прізвище повинно бути відокремлено «and» без коми;

– витяги з публікацій, тобто назви статей журналів, глав в книгах наводять у "лапках";

– назва журналу або книги завжди виділяється курсивом;

– ім'я видавця вказується перед місцем видання;

– коми використовують для поділу елементів запису;

– для джерел українською або російською мовою, що наводяться у References, назви статей журналів, глав в книгах наводять латиницею (транслітерацією) у "лапках" та перекладом на англійську мову у квадратних дужках. Онлайн-конвертер з української мови для транслітерації: http://translit.kh.ua/?passport.

***Приклади оформлення References за стилем Harvard British Standards Institution***

**Книга (ДСТУ 8302:2015)**

Інформаційно-психологічна боротьба у воєнній сфері : монографія / Г.В. Пєвцов, А.М. Гордієнко, С.В. Залкін, С.О. Сідченко, А.О. Феклістов, К.І. Хударковський. Х. : Вид. Рожко С.Г., 2017. 276 с.

**Книга (Harvard style BSI)**

Pievtsov, H.V., Hordiienko, A.M., Zalkin, S.V., Sidchenko, S.O., Feklistov, A.O. and Khudarkovskyi, K.I. (2017), "Informatsiino-psykholohichna borotba u voiennii sferi: monohrafiia" [The information and psychological struggle in the military sphere], Rozhko S.H., Kharkiv, 276 p.

**Стаття із періодичного видання (ДСТУ 8302:2015)**

Карпенко, Д.В. Стан та перспективи розвитку зенітного ракетного озброєння Повітряних Сил Збройних Сил України / Наука і техніка Повітряних Сил Збройних Сил України. 2017. № 2(27). С. 75–78.

**Стаття із періодичного видання (Harvard style BSI)**

Karpenko, D.V. (2017),"Stan ta perspektyvy rozvytku zenitnoho raketnoho ozbroiennia Povitrianykh Syl Zbroinykh Syl Ukrainy" [The state and perspectives of the development of anti-aircraft missile armaments in the Air Force of Ukraine], Science and Technology of the Air Force of Ukraine, No. 2(27), pp. 75–78.

**Дисертація (ДСТУ 8302:2015)**

Белозеров, И.В. Религиозная политика: дис. … канд. ист. наук: 07.00.02; защищена 22.01.02; утв. 15.07.02 / Белозеров Иван Валентинович. К., 2002. 215 с.

**Дисертація (Harvard style BSI)**

Belozerov, I.V. (2002),"Relyhyoznaia polytyka: dissertation" [The religious policy: dissertation], Kiev, 215 p.

**Джерела електронного ресурсу віддаленого доступу (ДСТУ 8302:2015)**

Романов В. К вопросу о путях достижения национальной безопасности в условиях глобализации: проблемы теории и практики в контексте внешней политики России и Польши [Електронний ресурс] Безопасность и оборона, 2016. № 1(2), С. 7–15. Режим доступу до журн.: http://www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf.

**Джерела електронного ресурсу віддаленого доступу (Harvard style BSI)**

Romanov, V. (2016), "K voprosu o putyakh dostizheniya natsionalnoy bezopasnosti v usloviyakh globalizatsii: problemy teorii i praktiki v kontekste vneshney politiki Rossii i Polshi" [To the question about the ways to achieve national security in the context of globalization: the problems of theory and practice in the context of the foreign policy of Russia and Poland], Security and Defence Journal, No. 1(2), pp. 7–15, www.desecuritate.uph.edu.pl/images/De_Securitate_12_2016.pdf (accessed 12 July 2017). (примітка: при наведенні URL "http: //" має бути виключено).

Більш детальну інформацію щодо оформлення бібліографічних посилань за стилем Harvard British Standards Institution можна знайти на сайті ***Національної бібліотеки України імені В.І. Вернадського*** та онлайн генератора посилань ***Cite This For Me***.

**Редакційна колегія: e-mail: lenkov_s@ukr.net**

Шрифт

**СХЕМА ОФОРМЛЕННЯ СТАТЕЙ**
**У «ЗБІРНИКУ НАУКОВИХ ПРАЦЬ ВІКНУ»**

УДК

науковий ступінь, вчене звання
**ініціали та прізвище автора (співавторів)**
Місце роботи автора (співавторів)

12 пт

УДК 32.973.202:07.681

д.т.н., проф. **Степанов С.В.** (ВІКНУ)
к.т.н., с.н.с. **Українець О.В.** (ВІКНУ)
к.т.н. **Саленко В.Д.** (ВІКНУ)

**12 пт жирний**

**КЕРУВАННЯ ЕЛЕКТРОННИМИ ПРИСТРОЯМИ ЗА ДОПОМОГОЮ ЖЕСТІВ**

***Анотація*** до статті виконується українською та англійською мовами (загальний обсяг кожної не менш ніж **1800** знаків, включаючи ключові слова).

**11 пт *курсив, жирний***

***Для керування електронними пристроями, для сучасного користувача важливими критеріями є такі, як: зручність та простота керування. Для того щоб надати користувачу такі можливості та зручності в використанні, є досить доцільною розробка системи, яка б надавала такі можливості. Керування системою, яка працює на основі жестів, є надзвичайно перспективним, та може суттєво полегшити користувачу роботу з нею, тому що, жести які потрібні для керування системою, можуть бути інтуїтивно зрозумілими користувачу, порівняно з іншими системами які працюють за допомогою комбінацій клавіш.***

***Для вирішення задач керування за допомогою жестів, пропонується програмно-апаратний комплекс, який побудований на основі різних модулів, кожен з яких в свою чергу виконує відповідну роль в системі, наприклад знаходить точку інтересу з множини чи вираховує глибину сцени. Також в системі є ядро, яке відповідає за аналіз модифікаторів та жестів. На основі даних модулів стає можливо створити систему, яка б працювала на основі жестів. Але для створення даної системи, потрібно вирішити певні задачі, такі як: сегментація, скелетизація, спостереження. Кожна з яких містить в собі відповідні математичні моделі та визначення. Запропонований програмно-апаратний комплекс для керування природніми жестами. Суть програмно-апаратного комплексу полягає в тому, щоб забезпечити користувача таким інтерфейсом, щоб він виконував роботу знаходячись частково віддалено від робочого місця, чи маніпулював інструментами на відстані, тобто за допомогою жестів. Використання пропонованого програмно-апаратного комплексу дозволить покращити показники стерильності в операційних, підвищити технічну безпеку під час виконання безпосередньої роботи користувача з приладами.***

***Ключові слова: штучний інтелект, контролери, модулі, жести, глибина сцени, точка інтересу, аналіз модифікаторів, аналіз жестів, сегментація, скелетизація, спостереження.***

**ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ СТАТТІ**

12 пт

**НЕОБХІДНІ ЕЛЕМЕНТИ СТАТТІ:вступ та постановка проблеми (задачі) у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;** аналіз останніх досліджень **і публікацій, в яких започатковано** розв'язання даної проблеми **і на які спирається автор, виділення невирішених раніше частин загальної проблеми, яким присвячується дана стаття, формулювання цілей статті (**постановка завдання**), виклад основного матеріалу дослідження з повним обґрунтуванням отриманих** наукових результатів**;** їх практичного значення та результатів експерименту чи впровадження; висновки **з даного дослідження і**

**перспективи подальших досліджень у даному напрямку. Література. References.**

Таблиці

УВАГА! Таблиці і рисунки друкують після посилань. Якщо у статті кілька таблиць чи рисунків - їх нумерують. Заголовки таблиць і рисунків необхідно розміщувати по центру, а нумерацію таблиць праворуч від таблиці (стиль **normal**, шрифт – **Times New Roman № 12**). Рисунки повинні бути виконані за допомогою редактора **Word,** згруповані і являти собою один графічний об'єкт. Формули та позначення по тексту обов'язково набирати за допомогою **Equation Editor** - редактора формул **Word**, а не у текстовому режимі. У редакторі формул мають бути встановлені такі параметри - розміри: загальний – **12 pt**. великі індекси – **10 pt** , малі індекси – **7 pt**, великі символи – **14 pt**. малі символи – **10 pt**: стиль: текст, функції, змінні, матриці-вектори, числа – шрифт **Times New Roman**, для решти стилів – шрифт **Symbol**, при цьому: строк. грецькі – прямі. Великі за розміром вирази та рівняння необхідно записувати у кілька рядків.

Рисунки

## ЛІТЕРАТУРА

Перший (список літератури на мові оригіналу джерела) – згідно наказу МОН № 40 від 12.01.2017 та відповідно до ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання: загальні положення та правила складання»;

другий (REFERENCES ) з урахуванням ДСТУ 8302:2015, наказу МОН № 40 від 12.01.2017 та міжнародного Гарвардського стилю BSI (British Standards Institution).

ЛІТЕРАТУРА:

11 пт

**ЗРАЗОК**

1. Лєнков С.В., Толок І.В., Цицарєв В.М., Лєнков Є.С. Моделювання процесів витрачання та поповнення ресурсу угрупування технічних об'єктів. *Системи озброєння і військова техніка*. Харків. 2018. Вип. 1(53). С. 155 – 162.

2. Жиров Г.Б., Лєнков Є.С., Цицарєв В.М., Проценко Я.М. Моделювання процесу відмов об'єктів, що відновлюються з ієрархічною конструктивною структурою. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка.* Київ. 2017. Вип. 55. С. 30-39.

REFERENCES:

**ЗРАЗОК**

11 пт

1. Ljenkov, S.V., Tolok, I.V., Tsytsarev, V.N. and Ljenkov, Ye.S. (2018), "Modeliuvannia protsesiv vytrachannia ta popovnennia resursu uhrupuvannia tekhnichnykh obiektiv" [Modeling of processes of expenditure and resource replenishment grouping of technical objects], Systems of Arms and Military Equipment, No. 1(53), pp. 155-162.

2. Zhyrov, G.B., Ljenkov, Je.S., Cycarjev, V.M. and Procenko, Ja.M. (2017), "Modeljuvannja procesu vidmov ob'jektiv, shho vidnovljujut'sja z ijerarhichnoju konstruktyvnoju strukturoju" [Simulation of the process of failure of objects that are restored with a hierarchical constructive structure], Zbirnyk naukovyh prac' Vijs'kovogo instytutu Kyi'vs'kogo nacional'nogo universytetu imeni Tarasa Shevchenka, No. 55, pp. 30-39.

**Prof. Stepanov S.V., Ph.D. Ukrainets O.V., Ph.D. Salenko V.D.**

***11 пт курсив, жирний***

**CONTROL ELECTRONIC DEVICES USING GESTURES**

***For management of electronic devices, for today's user important criteria are: convenience and ease of management. In order to provide the user with such opportunities and usability to use, it is quite reasonable to develop a system that would provide such opportunities. Managing a gesture-based system is extremely promising, but can greatly facilitate the user to work with it, because the gestures that are needed to manage the system can be intuitive to the user, compared to other systems that operate using keyboard shortcuts. To solve the problems of managing using gestures, a software-hardware complex is proposed that is based on different modules, each of which in turn plays an appropriate role in the system, for example, finds a point of interest from a plurality or calculates the depth of a scene.***

***Also, the system has a kernel that is responsible for analyzing modifiers and gestures. Based on the data of the modules it becomes possible to create a system that would work on the basis of gestures. But for the creation of this system, it is necessary to solve certain problems, such as: segmentation, skeletalization, observation. Each of them contains the corresponding mathematical models and definitions. Proposed hardware and software complex for management of natural gestures. The essence of the software and hardware complex is to provide the user with such an interface that he was performing work while being partially remote from the workplace, or manipulating tools at a distance, that is, using gestures. The use of the proposed software-hardware complex will improve the sterility parameters in the operating system, increase the technical safety during the direct work of the user with the devices.***

***Keywords: artificial intelligence, controllers, modules, gestures, depth of the scene, point of interest, analysis of modifiers, gesture analysis, segmentation, skeletonization, observation.***

**Дані про авторів (прізвище, ім'я по батькові, науковий ступінь, вчене звання, місце роботи) наводяться трьома мовами: українською, англійською), ORCID (https://orcid.org)**

**ЗРАЗОК**

11 пт

**Степанов Сергій Вікторович,** доктор технічних наук, професор, Заслужений діяч науки і техніки України, Лауреат Державної премії України в галузі науки і техніки, головний науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-1202-6512-1234, stepanov@ukr.net, 068 652 26 62.

**Українець Олексій Васильович,** кандидат технічних наук, старший науковий співробітник, провідний науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-1204-6512-1235, ykr@ukr.net, 073 556 6776.

**Саленко Володимир Дмитрович,** кандидат технічних наук, науковий співробітник Військового інституту Київського національного університету імені Тараса Шевченка, ORCID – 0000-1201-6512-1236, salenko@ukr.net, 0938763423.

**Stepanov Sergij,** doctor of technical sciences, professor, Chief Researcher of the Military Institute of Kiev National Taras Shevchenko University (Kiev, Ukraine)

**Ukrainets Oleksij,** candidate of Technical Sciences, Senior Researcher, Leading Researcher of the Military Institute of Kyiv National Taras Shevchenko University (Kiev, Ukraine)

**Salenko Volodymyr,** candidate of engineering sciences, Researcher of the Military Institute of Kiev National Taras Shevchenko University (Kiev, Ukraine).

**Наукове видання**

# ЗБІРНИК НАУКОВИХ ПРАЦЬ

## Військового інституту

## Київського національного університету імені Тараса Шевченка

# № 77

Усі матеріали надруковані в авторській редакції

Підписано до друку 22.12.22 р.
Авт. друк. арк. 11. Формат 60х90/8
Безкоштовно. Замовлення № 10-2012

Надруковано у навчальному картографічному комплексі ВІКНУ

03189, Київ, вул. Ломоносова, 81

т. 521-32-89