ISSN 2311-7249 (Print)
ISSN 2410-7336 (Online)

# СУЧАСНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ У СФЕРІ БЕЗПЕКИ ТА ОБОРОНИ

№ 1(46)
2023

## Науковий журнал

**Засновник і видавець**

Національний університет оборони України
імені Івана Черняховського
Журнал заснований у 2008 році

**Адреса редакції**

Національний університет оборони України
імені Івана Черняховського
Інститут інформаційних технологій

Повітрофлотський проспект, 28,
Київ, 03049
sitnuou@ukr.net
http://www.sit.nuou.org.ua

телефон: (044)-271-07-31, (098)-273-48-62
факс: (044)-271-07-31

Журнал зареєстровано в Державній реєстраційній службі України
(свідоцтво КВ №20490-10290ПР)

Журнал видається
українською та англійською мовами

Журнал виходить 3 рази на рік

Наказом Міністерства освіти і науки України
№409 від 17.03.2020 р. та №886 від 02.07.2020 р.
журнал включено до Переліку наукових фахових
видань України категорії "Б" в галузях
"технічні науки" та "військові науки",
спеціальності – 122, 124, 253, 255

*Рекомендовано до друку Вченою радою Національного університету оборони України імені Івана Черняховського*

При використанні матеріалів посилання на журнал
"Сучасні інформаційні технології
у сфері безпеки та оборони" обов'язкове

Редакція може не поділяти точку зору авторів
Відповідальність за зміст поданих матеріалів
несуть автори

Журнал індексується у наукометричних базах:
*Google Academy, Index Copernicus,*
*The Journal Impact Factor.*
*Directory of Research Journals Indexing (DRJI)*

Журнал представлений у базах даних:
*Bielefeld Academic Search Engine (BASE),*
*Directory of Open Access Journals (DOAJ),*
*Research Bible, WorldCat.*

Журнал внесений до каталогів бібліотек:
*Vernadsky National Library of Ukraine.*

***В номері:***

***Слюсар В.І., Громлюк К.А.*** Удосконалений метод Дейкстри для визначення найкоротших маршрутів між вузлами зв'язку у системі військового зв'язку ..... **5**
***Богом'я В.І., Гудзь А.С.*** Штучний інтелект: сучасний стан і перспективи застосування ..... **13**
***Мороз М.В., Яковчук О.В., Гаценко С.С.*** Розроблення моделі ідентифікації стану різнорідних динамічних об'єктів ..... **18**
***Терновий О.В., Шкуренко О.М., Міненко Л.М.*** Проблемні аспекти кібероборони: місце та роль кіберзахисту в Збройних силах України ..... **23**
***Живило Є.О., Докіль В.М.*** Модель методики оцінювання спроможностей військ зв'язку та кібербезпеки Збройних сил України щодо виконання завдань з відбиття воєнної агресії в кіберпросторі ..... **32**
***Мурасов Р.К., Мельник Я.В.*** Оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України ..... **41**
***Мартинюк О.Р., Кошка В.О.*** Підхід до оцінювання ефективності системи вивчення та впровадження досвіду застосування авіації у Збройних силах України ..... **45**
***Стрельбіцький М.А., Мазур В.Ю., Лемешко В.В.*** Протоколи обміну «агрегованої» інформації в інформаціно–телекомунікаційній системі ..... **51**
***Невмержицький І.М., Гризо А.А., Дідковський А.О.*** Проєктування візуально-імітаційного simulink-додатка для моделювання адаптивних алгоритмів захисту радіолокаційних станцій радіотехнічних військ від активних шумових завад ..... **56**
***Королюк Н.О.*** Підхід щодо автоматизації штурманських розрахунків для управління літаками винищувальної авіації ..... **63**
***Кільменінов О.А., Чопа Д.А.*** Використання системи імітаційного моделювання «JCATS» для оцінювання ефективності бойового застосування зразків озброєння ..... **69**
***Крайнов В.О., Лаврінчук О.В., Грозовський Р.І.*** Основні підходи щодо вибору логічної структури бази даних для автоматизованої інформаційної системи органу військового управління ..... **73**
***Павлунько М.Я., Богатов О.І., Марко В.П.*** Оцінювання похибок вимірювання швидкості в сполучених радіотехнічних системах в умовах впливу неузгодженостей за часом ..... **78**
***Зайцев О.В., Попов М.О., Стефанцев С.С.*** Підхід до оцінювання стану об'єктів на основі спільного використання поточних розвідувальних даних і попередньої інформації ..... **83**
***Андрощук О.В., Черевко Р.М., Петрушен М.В., Голобородько М.Ю.*** Актуальні підходи до побудови інформаційної інфраструктури на основі хмарних технологій з використанням референсної архітектури ..... **89**
***Воробйов О.М., Ткаченко В.В., Бамбуляк М.П., Тягай С.В.*** Вибір та обґрунтування показників електромагнітної стійкості радіоелектронної апаратури інформаційних систем до зовнішніх електромагнітних впливів ..... **95**
***Заїка Л.А., Лаврінчук О.В., Лук'яненко С.В.*** Сучасний стан і перспективи розвитку підготовки та проведення командно-штабних навчань із використанням систем імітаційного моделювання ..... **99**
***Шапран О.О., Махно Є.П.*** Аналіз процесів інтелектуалізації системи дистанційного навчання у Збройних силах України ..... **107**
***Чопа Д.А., Дерев'янчук А.Й., Москаленко Д.Р., Максимчук Д.С.*** Віддалені віртуальні ремонтні лабораторії озброєння та військової техніки: вимоги сьогодення та перспективи ..... **115**
***Салкуцан С.М., Кравченко Ю.В., Онищенко А.М., Тищенко М.Г.*** Концептуальна модель єдиного інформаційного простору дистанційного навчання Збройних сил України ..... **124**
***Загорка О.М., Поліщук С.В., Загорка І.О., Фреган Н.М.*** Нечітко-множинний підхід до оцінювання ризику невиконання завдань угрупованням військ (сил) в обороні ..... **133**
***Заболотний С.В., Кацалап В.О.*** Інформаційна технологія забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил) ..... **141**
***Базарний С.В.*** Метод виявлення агентів соціальних мереж, що мають найбільший вплив ..... **145**

ISSN 2311-7249 (Print)
ISSN 2410-7336 (Online)

# MODERN INFORMATION TECHNOLOGIES IN THE SPHERE OF SECURITY AND DEFENCE

№ 1(46)
2023

## Scientific journal

**Founder and Publisher**

National Defence University of Ukraine
named after Ivan Cherniakhovskyi
The journal was founded in 2008

**Address:**

National Defence University of Ukraine
named after Ivan Cherniakhovskyi,
Information Technology Institute

Povitroflotskiy ave. 28, Kyiv, 03049
sitnuou@ukr.net
http://www.sit.nuou.org.ua

Telephone: (044)-271-07-31, (098)-273-48-62
Fax: (044)-271-07-31

The journal is registered
in the State Registration Service of Ukraine
(certificate КВ №20490-10290ПР)

The journal is published
Ukrainian and English

The journal is published thrice a year

According to the orders of the Ministry of Education and Science of Ukraine № from 17.03.2020 and №886 from 02.07.2020 the journal was included in the List of scientific professional publications of Ukraine, "B" category, "technical sciences" and "military sciences" fields, specialties 122, 124, 253, 255

*Recommended to publication by the Scientific Council of the National Defence University of Ukraine named after Ivan Cherniakhovskyi*



The journal is indexed in the scientometric bases:
*Google Academy, Index Copernicus, The Journal Impact Factor. Directory of Research Journals Indexing (DRJI)*

The journal is presented in the databases:
*Bielefeld Academic Search Engine (BASE), Directory of Open Access Journals (DOAJ), Research Bible, WorldCat.*
The journal is added to the libraries:
*Vernadsky National Library of Ukraine.*

### *Contents:*

***Slyusar V., Hromliuk K.*** An improved Dijkstra method for determining the shortest routes between communication nodes in a military communication system ..... **5**
***Bohomia V., Hudz A*** Artificial intelligence: current state and prospective applications. ..... **13**
***Moroz M., Yakovchuk O., Hatsenko S.*** Development of the identification model state of various dynamic objects ..... **18**
***Ternovyy O., Shkurenko O., Minenko L.*** Problematic aspects of cyber defense: place and role of cyber Defense in the armed forces of Ukraine ..... **23**
***Zhyvylo Y., Dokil V.*** Model of assessment of military communication and cyber security capabilities of the Armed forces of Ukraine for performing tasks of reflecting military aggression in cyber space ..... **32**
***Murasov R., Melnyk Y.*** Assessment of cyber space protection of critical infrastructure facilities of Ukraine ..... **41**
***Martyniuk O., Koshka V.*** Way of evaluating the effectiveness of the air force lessons learned system in the Armed forces of Ukraine ..... **45**
***Strelbitskyi M., Mazur V., Lemeshko V.*** Protocols for the exchange of «aggregated» information in the information and telecommunication system ..... **51**
***Nevmerzhitsky I., Hryzo A., Didkovskyi A.*** Designing of a visual simulation simulink application for modeling adaptive algorithms for the protection of radars of radio engineering troops against active noise interference ..... **56**
***Korolyuk N.*** Approach to the automation of navigation calculations for fighter aviation aircraft control ..... **63**
***Kilmeninov O., Chopa D.*** Some aspects of conducting research to evaluate the efficiency of weapons in the JCATS simulation system environment ..... **69**
***Krainov V., Lavrinchuk O., Hrozovskyi R.*** Main approaches to the choice of the logical structure of the database for the automated information system of the military governance authority ..... **73**
***Pavlunko M., Bogatov O., Marco V.*** Errorsestimation of speed measurements in the combined radio engineering systems in theconditions of influence of inconsistencies in time ..... **78**
***Zaitsev O., Popov M., Stefantsev S.*** An approach to the state of the ob'ects assessing based on the using current intelligence data and previous information ..... **83**
***Androshchuk O., Cherevko R., Petrushen M, Holoborodko M.*** Current approaches to building information infrastructure based on cloud technologies using reference architecture ..... **89**
***Vorobiov O., Tkachenko V., Bambulyak M., Tygai S.*** Selection and justification of indicators of electromagnetic resistance of radio electronic equipment of information systems to external electromagnetic influences ..... **95**
***Zaika L., Lavrinchuk O., Lukianenko S.*** Current status and development prospects of planning and conducting command post exercises using simulation systems ..... **99**
***Shapran O., Makhno Y.*** Analysis of the processes of intellectualization of the distance learning system in the Armed forces of Ukraine ..... **107**
***Chopa D., Derevianchuk A., Moskalenko D., Maksymchuk D.*** Remote virtual repair laboratories of weapons and military equipment: current requirements and perspectives ..... **115**
***Salkutsan S., Kravchenko Y., Onyshchenko A., Tyshchenko M.*** Conceptual model of the unified information space for distance learning of the Armed forces of Ukraine ..... **124**
***Zahorka O., Polishchuk S., Zahorka I., Fregan N.*** Fuzzy-multiple approach to assessing the risk of failure to accomplish tasks by groups of troops (forces) in defense ..... **133**
***Zabolotnyi S., Katsalap V.*** Information technology for ensuring functional sustainability of information space monitoring systems in the interests of troops (forces) ..... **141**
***Bazarnyi S.*** Method for identifying social network agents with the greatest influence ..... **145**

DOI:**10.33099/2311-7249/2023-46-1-5-12**

УДК: 004.72

***Вадим Іванович Слюсар*** *(доктор технічних наук, професор)* [1]
***Катерина Андріївна Громлюк*** [2]

[1]***Центральний науково-дослідний інститут ОВТ Збройних Сил України, Київ, Україна***
[2]***Військовий інститут телекомунікацій та інформатизації, Київ, Україна***

# УДОСКОНАЛЕНИЙ МЕТОД ДЕЙКСТРИ ДЛЯ ВИЗНАЧЕННЯ НАЙКОРОТШИХ МАРШРУТІВ МІЖ ВУЗЛАМИ ЗВ'ЯЗКУ У СИСТЕМІ ВІЙСЬКОВОГО ЗВ'ЯЗКУ

*У статті удосконалено метод Дейкстри для системи військового зв'язку завдяки використанню матриці інцидентності вузлів і ліній зв'язку замість матриці інцидентності вузлів. Удосконалений метод адаптовано до моделі системи військового зв'язку, що формалізується блоковою матрицею інцидентності вузлів і ліній зв'язку з поділом блоків матриці за родами і складовими системи військового зв'язку. Суть удосконалення полягає у введені додаткових блоків до стандартного алгоритму Дейкстри з метою попереднього, точнішого обчислення вагових коефіцієнтів ліній зв'язку. Водночас, на основі використання блокової матриці вторинної інцидентності, а також квадратичної форми матриці інцидентності, запропоновано низку нових аналітичних виразів. Математичне моделювання, на основі спрощеної моделі системи військового зв'язку, підтвердило ефективність удосконаленого методу. Синтезований удосконалений метод точніше відповідає реальним умовам управління системою військового зв'язку і може бути використаний для потреб автоматизації процесу управління системою як основи для розробки інформаційно-аналітичних завдань.*

***Ключові слова:*** *метод Дейкстри; багатошаровий граф; блокова матриця; блоковий торцевий добуток матриць; матриця інцидентності.*

## Вступ

**Постановка проблеми.** В умовах ведення бойових дій важливого значення набувають пошук оптимальних маршрутів проходження інформації, логістичних (транспортних) напрямків, побудови оборонних рубежів, виконання інших завдань, що пов'язані з питаннями оптимізації і можуть бути формалізовані на основі теорії графів і складних мереж [1 – 4].

Для виконання завдання пошуку оптимального шляху в графах існує значна кількість методів: неінформативні методи; інформативні; пошуку найменшого шляху; мінімального остовного дерева та інші. Пропонується розглянути один із методів пошуку найкоротшого шляху – широко відомий алгоритм Дейкстри. Алгоритм був розроблений у 1959 році нідерландським вченим Едсгером Дейкстрою для вирішення завдання пошуку всіх найкоротших шляхів з однієї, наперед заданої, вершини графа до всіх інших [5; 6].

Алгоритм Дейкстри відноситься до родини жадібних алгоритмів [7]. Жадібні алгоритми – прості та прямолінійні евристичні алгоритми, що приймають оптимальні рішення, виходячи з наявних на кожному етапі даних [8], не зважаючи на можливі наслідки, сподіваючись, зрештою, отримати оптимальний розв'язок. Вони необтяжливі у процесі реалізації та є ефективнішими за часом виконання. Водночас чимало задач не можуть бути розв'язані за їх допомогою.

Недоліками даного методу є неможливість обробки графів, в яких є ребра з негативною вагою. Також під час застосування алгоритму Дейкстри необхідно дотримуватися припущення про відсутність петель на маршруті (замкнутих колових маршрутів). У такому випадку доцільно користуватися відмінним від алгоритму Дейкстри методом. Наприклад, алгоритмом Беллмана-Форда, який також знаходить найкоротші шляхи, але передбачає існування у графі ребер з негативною вагою [9; 10]. Проте, обмежимося у статті розглядом лише алгоритму Дейкстри на прикладі системи військового зв'язку..

**Аналіз останніх досліджень і публікацій.** Для удосконалення методу Дейкстри скористаємося аналітичними виразами, що запропоновані професором В. І. Слюсарем у роботах [11; 12], для аналізу топології мереж зв'язку між операціями з матрицями інцидентності вузлів та ліній зв'язку на основі торцевого і транспонованого торцевого

добутку матриць [13–15]. На основі заявленого підходу окреслимо систему військового зв'язку у вигляді багатошарового графа, де кожен шар графу відповідає повному роду військового зв'язку. Для цього в роботі [16] запропонувала аналітичну модель системи військового зв'язку на основі її подання у вигляді блокової матриці інцидентності вузлів і ліній військового зв'язку, де кожен блок відповідає певному роду військового зв'язку. Також було отримано блокові матриці вторинної інцидентності і квадратичні форми блокових матриць інцидентності

**Мета статті.** Метою статті є удосконалення методу Дейкстри завдяки впровадженню блокових матриць інцидентності, блокових матриць вторинної інцидентності, квадратичних форм матриць інцидентності вузлів і ліній зв'язку, що синтезовані у [16] для формалізації опису системи військового зв'язку

## Виклад основного матеріалу дослідження

Вважатимемо, що негативні ваги ребер (ліній зв'язку) і петлі на маршрутах у графі (системі військового зв'язку) відсутні. Наведемо перелік кроків алгоритму Дейкстри: встановлюємо відстань до однієї, наперед заданої вершини графа, рівною нулю; встановлюємо відстань до решти вершин на нескінченне значення; вибираємо не відмічену вершину графа, що знаходиться на найменшій відстані від початкової вершини і відмічаємо її; обчислюємо відстань до інцидентних вершин, обираючи найменшу відстань при кожному оцінюванні; відмічаємо наступний вузол; проводимо ітерацію за наведеними кроками, поки всі вершини не будуть відмічені.

У програмі, що знаходить найближчі шляхи між вершинами за допомогою методу Дейкстри, граф наводитиметься у вигляді не бінарної матриці інцидентності вершин графа [5; 6]. Замість одиниць в ній встановлюються ваги ребер, нулі свідчать про відсутність ребер між вершинами. На рисунку 1 наведено приклад графа із шести вершин і семи ребер зі встановленими вагами.

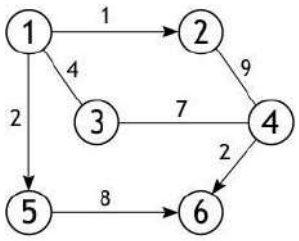



Рис. 1. Приклад графа із шести вершин і семи ребер зі встановленими вагами ребер

Складемо матрицю інцидентності, що необхідна для реалізації програмного методу Дейкстри (рис. 1). Вона описує інцидентність вершин графа між собою і матиме такий вигляд:

$$Q = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}. \qquad (1)$$

За умови встановлення для ребер між $i$ -ми і $j$ -ми вершинами графа вагових коефіцієнтів $\omega_{ij}$, що наведені на рисунку 1, матриця інцидентності вершин трансформується до іншого вигляду (2):

$$Q_{VK} = \begin{bmatrix} 0 & 1 & 4 & 0 & 2 & 0 \\ 1 & 0 & 0 & 9 & 0 & 0 \\ 4 & 0 & 0 & 7 & 0 & 0 \\ 0 & 9 & 7 & 0 & 0 & 2 \\ 2 & 0 & 0 & 0 & 0 & 8 \\ 0 & 0 & 0 & 2 & 8 & 0 \end{bmatrix}. \qquad (2)$$

Наведений масив використовується у методі Дейкстри, як основа для проведення подальших обчислень. При цьому вагові коефіцієнти $\omega_{ij}$ відповідають експлуатаційним витратам для кожної із ліній зв'язку.

Відповідно до [17], лінія зв'язку (лінія передачі інформації) – сукупність технічних пристроїв і фізичного середовища, що забезпечують передавання електричних сигналів одного, двох або багатьох каналів зв'язку на відстань. Аналіз структури ліній зв'язку свідчить, що вони складаються із засобів зв'язку вузлів зв'язку з навченим персоналом, який їх експлуатує, і за необхідності, фізичного середовища розповсюдження сигналу (кабелі зв'язку, оптичне волокно, тощо), що також розгортається і утримується структурними підрозділами одного із вузлів зв'язку. Звідси можливо перейти до розгляду вагового коефіцієнту $\omega_{ij}$ лінії зв'язку між *i*-тим та *j*-тим вузлами зв'язку як суми експлуатаційних витрат *i*-го вузла зв'язку $\omega_i$, *j*-го вузла зв'язку $\omega_j$ і витрат на утримання фізичної лінії зв'язку одним із вузлів зв'язку $\omega_{Fi(j)}$.

Можливий також варіант організації лінії передачі у вигляді мереж зв'язку, коли одна головна станція працюватиме з декількома абонентами мережі й збільшення кількості абонентів такої мережі не буде здійснювати спричинятиме збільшення вартості функціонування засобів зв'язку головного вузла зв'язку означеної мережі.

Проведений аналіз свідчить, що під час фактичного застосування методу Дейкстри для формування матриці інцидентності вузлів зв'язку з ваговими коефіцієнтами необхідно провести попередні значні і доволі складні обчислення вагових коефіцієнтів ліній зв'язку. Водночас зрозуміло, що в реальних умовах виконання завдань за призначенням частинами і підрозділами зв'язку, проведення обчислень вагових коефіцієнтів для ліній і мереж військового зв'язку є не можливим. Реальнішим може бути варіант проведення завчасних обчислень для окремих вузлів зв'язку, що експлуатують штатні зразки техніки зв'язку і мають типові штати. Такий підхід є більш реалістичним і дозволяє відмовитися від застосування матриці інцидентності вузлів зв'язку і перейти до матриці інцидентності вершини та ліній зв'язку [11; 12], а також до методу, що запропонований у роботі [16].

Для наочнішого подання розглянемо запропонований підхід на прикладі системи військового зв'язку, що складається з двох шарів, трьох вузлів зв'язку, двох ліній зв'язку у кожному шарі (рис. 2).

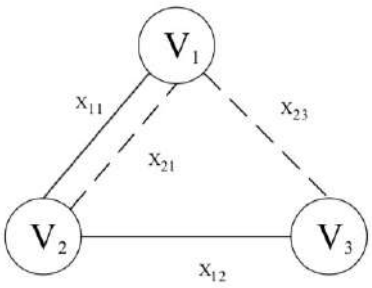



Рис. 2. Багатошарова система військового зв'язку з розподілом шарів за родами військового зв'язку

Матриця інцидентності вузлів та ліній системи військового зв'язку матиме такий вигляд (3):

$$G = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right]. \qquad (3)$$

За такої умови значення одиниці для кожного з вузлів і ліній зв'язку означатиме, що вони поєднані між собою. Для доступнішого сприйняття виразу (3) наведемо його у вигляді таблиці 1.

Таблиця 1

Таблиця інцидентності вершин та ребер багатошарового графу

| Порядковий номер вершини | Порядковий номер ребер у шарах багатошарового графу | | | | | |
|---|---|---|---|---|---|---|
| | $X_{11}$ | $X_{12}$ | $X_{13}$ | $X_{21}$ | $X_{22}$ | $X_{23}$ |
| $V_1$ | 1 | 0 | 0 | 1 | 0 | 1 |
| $V_2$ | 1 | 1 | 0 | 1 | 0 | 0 |
| $V_3$ | 0 | 1 | 0 | 0 | 0 | 1 |

За переходу до вагових коефіцієнтів їх значення будуть відповідати експлуатаційним витратам для підтримання функціонування лінії зв'язку окремо для кожного вузла зв'язку. За реальних умов функціонування об'єднаної системи військового зв'язку, модель, що наведена на рисунку 2, є доволі спрощеною. За умови формування блоків у матриці інцидентності за родами військового зв'язку і подальшим формуванням субблоків, у блоках за типами апаратури зв'язку, доволі просто перейти до формування матриці інцидентності вершин і ліній зв'язку з ваговими коефіцієнтами. Як приклад розглянемо об'єднану систему військового зв'язку, що описується блоковою матрицею інцидентності вузлів і ліній зв'язку такого вигляду (4) [16]:

$$G = \left[\begin{array}{c|c|c|c} G_{11} & G_{12} & \cdots & G_{1n} \\ \hline G_{21} & G_{22} & \cdots & G_{2n} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline G_{m1} & G_{m2} & \cdots & G_{mn} \end{array}\right], \qquad (4)$$

де

$$G_{11} = \begin{bmatrix} g_{1_i 1_1} & \cdots & g_{1_i j_1} \\ \vdots & \ddots & \vdots \\ g_{i_1 1_1} & \cdots & g_{i_1 j_1} \end{bmatrix}, \ldots, G_{mn} = \begin{bmatrix} g_{1_m 1_n} & \cdots & g_{1_m j_n} \\ \vdots & \ddots & \vdots \\ g_{i_m 1_n} & \cdots & g_{i_m j_n} \end{bmatrix}$$

є елементами блокової матриці, що відповідають матрицям інцидентності ребер і вершин у кожному із шарів багатошарового графу;

*j* – номер стовпця, що відповідає відповідній лінії зв'язку в блоках блокової матриці;

*i* – номер рядка, що відповідає відповідному номеру вузла зв'язку у кожній зі складових об'єднаної системи військового зв'язку;

*n* – індекс номера блоку, що відповідає розподілу за родами військового зв'язку;

*m* – індекс номера блоку, що відповідає розподілу за складовими об'єднаної системи військового зв'язку.

За такої умови блоки $G_{11} - G_{1n}$, … , $G_{m1} - G_{mn}$ будуть відповідати кожній зі складових об'єднаної системи військового зв'язку з їх поділом за родами військового зв'язку.

Для того щоб обчислити матрицю інцидентності вузлів і ліній військового зв'язку з урахуванням вагових коефіцієнтів потрібно сформувати, узгоджено зі структурою блокової матриці інцидентності *G*, матрицю вагових коефіцієнтів за родами військового зв'язку *F* і знайти її добуток із матрицею інцидентності вершин і ребер графа відповідно до виразу (5):

$$G_{VK} = F[\otimes]G, \qquad (5)$$

де $F = \left[\begin{array}{c|c|c|c} f_{11} & f_{12} & \cdots & f_{1n} \\ \hline f_{21} & f_{22} & \cdots & f_{2n} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline f_{m1} & f_{m2} & \cdots & f_{mn} \end{array}\right]$ – блокова матриця вагових коефіцієнтів, що формується за родами військового зв'язку;

$\left[\otimes\right]$ – символ блокового добутку Кронекера.

У розглянутому випадку кожен ваговий коефіцієнт $f_{mn}$ зі складу матриці $F$ матиме скалярне значення. Тому, під час виконання операції добутку матриць, вираз (5), буде знайдено добуток кожного блоку матриці $G$ зі встановленим для кожного роду військового зв'язку числовим значенням вагового коефіцієнту. На випадок подальшого ускладнення матриці $G$, з розподілом не лише за родами військового зв'язку, а й за типами апаратури зв'язку, що використовується, або неоднаковими ваговими коефіцієнтами для різних вузлів і ліній зв'язку, структура матриці $F$ також ускладниться. Заразом від блокового добутку Кронекера у виразі (5) потрібно перейти до блокового добутку Адамара. Вираз (5) трансформується і набуде такого вигляду (6):

$$G_{VK} = F\left[\circ\right]G, \qquad (6)$$

де $\left[\circ\right]$ – блоковий добуток Адамара.

За такого застосування наведеного підходу, у процесі прийняття управлінських рішень щодо топології структури системи військового зв'язку, представнику органу управління військовим зв'язком не потрібно проводити обчислення вагових коефіцієнтів для кожної лінії зв'язку. Визначення вагових коефіцієнтів можна покласти на чергову зміну пунктів управління вузлами зв'язку із заповненням відповіднго рядка, що відповідає вузлу зв'язку у загальній таблиці. В умовах швидкоплинних бойових дій це сприятиме оперативності у прийнятті відповідних управлінських рішень. З метою обчислення вагових коефіцієнтів ребер для кожного шару системи військового зв'язку необхідно провести операцію підсумовування за стовбцями, що відповідають лініям зв'язку.

Для спрощення сприйняття матеріалу повернемося до системи військового зв'язку, що наведений на рисунку 2. Встановимо припущення, що вагові коефіцієнти складають: для першого шару 20; для другого 30. За таких умов матриця вагових коефіцієнтів набуде такого вигляду $F = \left[f_1 \mid f_2\right] = \left[20 \mid 30\right]$. Після проведення обчислень за виразом (5) блокова матриця інцидентності з ваговими коефіцієнтами буде такою: $G_{VK} = \left[\begin{array}{ccc|ccc} 20 & 0 & 0 & 30 & 0 & 30 \\ 20 & 20 & 0 & 30 & 0 & 0 \\ 0 & 20 & 0 & 0 & 0 & 30 \end{array}\right]$.

Для подальшого обчислення вагових коефіцієнтів ліній зв'язку $VK_{ЛЗ}$ необхідно підсумувати значення у стовбцях матриці. Скористаємося виразом (6):

$$VK_{ЛЗ} = 1G_{VK}, \qquad (6)$$

де 1 – узгоджений з блоковою матрицею інцидентності блоковий одиничний вектор-рядок.

Проведемо обчислення для варіанту системи військового зв'язку, що розглядається на рис. 2.

$$VK_{ЛЗ} = 1G^{T}_{VK} = \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right] \left[\begin{array}{ccc|ccc} 20 & 20 & 0 & 30 & 30 & 0 \\ 0 & 20 & 20 & 0 & 0 & 0 \\ 0 & 0 & 0 & 30 & 0 & 30 \end{array}\right] =$$
$$= \left[\begin{array}{ccc|ccc} 40 & 40 & 0 & 60 & 0 & 60 \end{array}\right].$$

Для пояснення фізичного змісту сформуємо отримані значення у вигляді таблиці 2.

Таблиця 2

Таблиця вагових коефіцієнтів ліній зв'язку у системі військового зв'язку

| Номер лінії зв'язку | $X_{11}$ | $X_{12}$ | $X_{13}$ | $X_{21}$ | $X_{22}$ | $X_{23}$ |
|---|---|---|---|---|---|---|
| Ваговий коефіцієнт | 40 | 40 | 0 | 60 | 0 | 60 |

Наступним кроком, в узагальнені наведеного підходу, є використання для визначення вагових коефіцієнтів ліній зв'язку матриці вторинної інцидентності вершин графа, що описана у [16], таким виразом (7):

$$M_{ВІВ} = G^{T}\left[\square\right]G^{T} = \left[\begin{array}{c} G_1^T \\ \hline G_2^T \end{array}\right]\left[\square\right]\left[\begin{array}{c|c} G_1^T & G_1^T \\ \hline G_2^T & G_2^T \end{array}\right] = \left[\begin{array}{c|c} G_1^T \square G_1^T & G_1^T \square G_1^T \\ \hline G_2^T \square G_2^T & G_2^T \square G_2^T \end{array}\right], \qquad (7)$$

або його транспонованого варіанта (8):

$$M_{ВІВ} = G\left[\blacksquare\right]G = \left[G_1 \mid G_2\right]\left[\blacksquare\right]\left[G_1 \mid G_2\right] = \left[G_1 \blacksquare G_1 \mid G_2 \blacksquare G_2\right] \qquad (8)$$

Фізичний зміст обчислення матриці вторинної інцидентності можна навести у таблиці 3.

Таблиця 3

Таблиця вторинної інцидентності вершин графа за допомогою його ребер

| Номер ребра графа | Комбінація вершин | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | $V_1$ | | | $V_2$ | | | $V_3$ | | |
| | $V_1$ | $V_2$ | $V_3$ | $V_1$ | $V_2$ | $V_3$ | $V_1$ | $V_2$ | $V_3$ |
| $X_{11}$ | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| $X_{12}$ | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| $X_{13}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $X_{21}$ | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| $X_{22}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $X_{23}$ | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |

Трансформуємо таблицю 3 шляхом поділу її значень на блоки, кожен з яких відповідає інцидентності кожної із вершин з іншими (табл. 4).

Таблиця 4

Таблиця вторинної інцидентності вершин графа за допомогою його ребер

| Номер ребра графа | Комбінація вершин | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | $V_1$ | | | $V_2$ | | | $V_3$ | | |
| | $V_1$ | $V_2$ | $V_3$ | $V_1$ | $V_2$ | $V_3$ | $V_1$ | $V_2$ | $V_3$ |
| $X_{11}$ | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| $X_{12}$ | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| $X_{13}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $X_{21}$ | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 |
| $X_{22}$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| $X_{23}$ | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 |

Враховуючи такий розподіл на блоки, скориставшись виразами (5) і (6), можна отримати блокову матрицю значень вагових коефіцієнтів ліній зв'язку інцидентних із вузлами зв'язку, окремо для кожного вузла зв'язку. За таких умов, під час формування блоків, як показано у таблиці 4, для вершини $V_1$, отримаємо варіант придатний для пошуку найкоротшого шляху у межах всієї системи військового зв'язку. За умови формування блоків, як наведено для вузла зв'язку $V_3$, отримаємо варіант придатний для пошуку найкоротшого шляху в межах кожного окремого шару системи військового зв'язку.

Обидва варіанти є необхідними у процесі планування розгортання та експлуатації системи військового зв'язку. Через високу інтенсивність ведення сучасних бойових дій, застосування противником засобів вогневого ураження, радіоелектронної боротьби, високоточної зброї система військового зв'язку повинна мати високу стійкість ще на етапі її планування. Одним із способів досягнення стійкості є комплексне застосування засобів різних родів зв'язку, що забезпечує резервування зв'язків на випадок виходу з ладу або ураження деяких комунікаційних засобів. Тому зв'язок планується як за окремими родами військового зв'язку, так і узагальнений.

Наведемо приклад застосування запропонованого авторами підходу на основі матриці вторинної інцидентності вершин із виразу (3). Сформуємо блокову матрицю за варіантом, що наведений виразом (7):

$$M_{BIB} = \left[\begin{array}{ccc|ccc|ccc} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right].$$

З урахуванням вагових коефіцієнтів отримаємо такий варіант матриці вторинної інцидентності:

$$M_{BIB,VK} = \left[\begin{array}{ccc|ccc|ccc} 20 & 20 & 0 & 20 & 20 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 20 & 20 & 0 & 20 & 20 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 30 & 30 & 0 & 30 & 30 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 30 & 0 & 30 & 0 & 0 & 0 & 30 & 0 & 30 \end{array}\right].$$

Для отримання вектор-рядка вагових коефіцієнтів ліній зв'язку знайдемо добуток блокового одиничного вектор-рядка, структура якого узгоджена зі структурою матриці вагових коефіцієнтів, з самою наведеною матрицею вагових коефіцієнтів:

$$VK_{ЛЗ} = \left[1 \ \cdots \ 1 \,\middle|\, 1 \ \cdots \ 1 \,\middle|\, 1 \ \cdots \ 1\right] \left[\begin{array}{ccc|ccc|ccc} 20 & 20 & 0 & 20 & 20 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 20 & 20 & 0 & 20 & 20 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 30 & 30 & 0 & 30 & 30 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 30 & 0 & 30 & 0 & 0 & 0 & 30 & 0 & 30 \end{array}\right] =$$

$$= \left[40 \ \ 0 \ \ 0 \ \ 60 \ \ 0 \ \ 60 \,\middle|\, 40 \ \ 40 \ \ 0 \ \ 60 \ \ 0 \ \ 0 \,\middle|\, 0 \ \ 40 \ \ 0 \ \ 0 \ \ 0 \ \ 60\right]$$

З метою пояснення фізичного змісту отриманого результату наведемо його у вигляді таблиці 5.

У блоках таблиці сформовано інцидентність кожного окремого вузла зв'язку (вершини графа) з іншими вузлами зв'язку системи військового зв'язку за допомогою ліній зв'язку. Наявність значення вагового коефіцієнту відмінного від нуля свідчить, що лінія існує. Наявність нуля свідчить про відсутність лінії зв'язку між вузлами зв'язку.

Використання наведеного авторами підходу дозволить удосконалити алгоритм пошуку найкоротшого шляху, тобто алгоритм Дейкстри, завдяки впровадженню запропонованої процедури обчислення вагових коефіцієнтів ліній зв'язку та більш спрощеного формування масиву даних в алгоритмі. Кожен крок алгоритму потребуватиме

роботи з одним із блоків з подальшим переходом до наступного блоку, що позначені у таблиці 5 (не відвіданої вершини), доки не будуть встановлені всі найкоротші шляхи з визначеного вузла зв'язку до всіх інших вузлів зв'язку в системі військового зв'язку.

Таблиця 5

Таблиця інцидентності вузлів зв'язку з лініями зв'язку з урахуванням їхніх вагових коефіцієнтів

| Вузли зв'язку | Лінії вузлів зв'язку | | Вагові коефіцієнти |
|---|---|---|---|
| $V_1$ | $X_{11}$ | $V_2$ | 40 |
| | $X_{12}$ | - | 0 |
| | $X_{13}$ | - | 0 |
| | $X_{21}$ | $V_2$ | 60 |
| | $X_{22}$ | - | 0 |
| | $X_{23}$ | $V_3$ | 60 |
| $V_2$ | $X_{11}$ | $V_1$ | 40 |
| | $X_{12}$ | $V_3$ | 40 |
| | $X_{13}$ | - | 0 |
| | $X_{21}$ | $V_1$ | 60 |
| | $X_{22}$ | - | 0 |
| | $X_{23}$ | - | 0 |
| $V_3$ | $X_{11}$ | - | 0 |
| | $X_{12}$ | $V_2$ | 40 |
| | $X_{13}$ | - | 0 |
| | $X_{21}$ | - | 0 |
| | $X_{22}$ | - | 0 |
| | $X_{23}$ | $V_1$ | 60 |

Запропоноване у статті удосконалення методу Дейкстри полягає у введені до наукового обігу п'яти кроків із визначення вагових коефіцієнтів ліній зв'язку до початку його реалізації, зокрема:

1. Складання матриці інцидентності вузлів зв'язку (вершин графа) та ліній зв'язку (ребер графа) *G*.

2. Знаходження матриці вторинної інцидентності вузлів зв'язку (вершин графа) $M_{BIB}$, вираз (7) або (8).

3. Формування блоків у матриці вторинної інцидентності за одним із принципів, що наведені у таблиці 4.

4. Введення до матриці вторинної інцидентності вузлів зв'язку вагових коефіцієнтів кінців ліній зв'язку $M_{BIB,VK}$.

5. Знаходження вектор-рядка вагових коефіцієнтів ліній зв'язку, вираз (6).

За допомогою застосування удосконаленого алгоритму Дейкстри можна встановити також інші параметри вузлів зв'язку. Наприклад, ексцентричність (eccentricity) – найбільшу відстань із мінімальних відстаней від обумовленого вузла зв'язку до інших; посередництво (betwetnness) – значення кількості найкоротших шляхів, що проходять через обумовлений вузол зв'язку тощо.

За допомогою використання запропонованого у статті удосконаленого алгоритму Дейкстри можна отримати значення найкоротших шляхів від обумовленого вузла зв'язку до всіх інших вузлів зв'язку у системі військового зв'язку. У теорії складних мереж важливим є визначення середньої відстані від обумовленого вузла зв'язку до інших вузлів зв'язку. Позначимо обумовлений вузол зв'язку номером один, тоді номери решти вузлів зв'язку будуть мати значення $i=1...,I$. За такої умови середня відстань від обумовленого вузла зв'язку до інших вузлів зв'язку, відповідно до [18; 19], обчислюватиметься за наступною формулою (9):

$$\widetilde{l}_1 = \frac{2}{I(I+1)} \sum_{i=1}^{I} d_{1I}, \qquad (9)$$

де $d_{1I}$ – найкоротші відстані між першим та іншими вузлами зв'язку у системі військового зв'язку;

$I$ – кількість вузлів зв'язку в системі військового зв'язку.

Під час переходу від розгляду параметрів вузлів зв'язку до параметрів мережі зв'язку мовитимемо про середню відстань між всіма можливим парами вузлів зв'язку в мережі. Для цього необхідно просумувати середні відстані всіх вузлів зв'язку і розділити суму на їх кількість (10):

$$\widetilde{l} = \frac{\sum_{i=1}^{I} \widetilde{l}_i}{I}, \qquad (10)$$

або, відповідно до [18, 19], скористатися таким виразом (11):

$$\widetilde{l} = \frac{2}{n(n+1)} \sum_{i \geq j} d_{ij}, \qquad (11)$$

де $n$ – кількість вузлів зв'язку в системі військового зв'язку;

$d_{ij}$ – найкоротша відстань між $i$-тим та $j$-тим вузлами зв'язку в системі військового зв'язку.

## Висновки й перспективи подальших досліджень

У статті вдосконалено метод Дейкстри для пошуку найкоротших маршрутів між вузлами зв'язку в системі військового зв'язку завдяки його використанню замість матриці інцидентності вузлів зв'язку у стандартному алгоритмі матриці інцидентності вузлів і ліній зв'язку. Такий підхід більш за все відповідає потребам управління системою військового зв'язку. Він дозволяє найоптимальніше сформувати значення вагових коефіцієнтів ліній зв'язку завдяки визначенню уточнених експлуатаційних витрат для функціонування ліній зв'язку кожним окремим вузлом зв'язку. Визначення вагових коефіцієнтів ліній зв'язку можна реалізувати у вигляді окремої інформаційно-аналітичної задачі або удосконалити

алгоритм Дейкстри шляхом введення до нього додаткових блоків. Використання матриці вторинної інцидентності вузлів зв'язку в алгоритмі Дейкстри також дозволить спростити обчислювальну складність алгоритму.

Математичне моделювання на основі спрощеної моделі системи військового зв'язку, що наведена на рисунку 2, підтвердило ефективність удосконаленого методу.

Такий підхід може бути поширений на інші випадки інтерпретації вагових коефіцієнтів в алгоритмі, окрім експлуатаційних витрат. Наприклад, це можуть бути характеристики, що мають ймовірнісний характер. Такі, як імовірність доставки інформаційних повідомлень, імовірність бітової помилки, імовірності стійкості ліній і вузлів зв'язку в умовах ведення сучасних інтенсивних бойових дій, та інші.

## *Література*


**1. Снарський А. О., Ланде Д. В.** Моделювання складних мереж : навчальний посібник. Київ : НТУУ «КПІ», 2015. 212 с. **2. Harary F.** Graph theory. 3rd ed Reading, Massachusetts: Addison-Wesley, 1972. 274 p. **3. Агеев Д. В.** Методика описания структуры современных телекоммуникационных систем с использованием многослойных графов. *Восточно-Европейский журнал передовых технологий.* 2010. № 6. С. 56–59. URL: http://journals.uran.ua/eejet/article/view/3295/3096 (дата звернення: 03.03.2023). **4. Агеєв Д. В.** Моделирование современных телекоммуникационных систем многослойными графами *Проблеми телекомунікацій*. 2010. №1. С.23-34. URL: http://openarchive.nure.ua/handle/document/2722 (дата звернення: 03.03.2023). **5. Dijkstra E. W.** A note on two problems in connexion with graphs. *Numerische Mathematik*. 1959. Vol.1. № 1. P. 269–271. URL: https://doi.org/10.1007/bf01386390 (date of access: 03.03.2023). **6. Cormen T., Leiserson Ch., Rivest R. and Stein C.** Introduction to algorithms, fourth edition. [S. l.] : MIT Press, 2022 – 1332 p. 1312 p. **7. Levitin A.** Introduction to the design & analysis of algorithms. 3rd ed. [S. l.]: Pearson 2011. 565 p. **8. Black P. E.** Greedy algorithm. Dictionary of Algorithms and Data Structures. 2005. URL: https://www.nist.gov/dads/HTML/greedyalgo.html (date of access: 03.03.2023). **9. Bellman R.** On a routing problem. Quarterly of applied mathematics. 1958. Vol. 16. № 1. P. 87–90. URL: https://doi.org/10.1090/qam/102435 (date of access: 03.03.2023). **10. Ford L. R., Fulkerson D. R.** Flows in networks (rand corporation research studies series) [S.l.] : Princeton Univ Pr, 1962. 198 p. **11. Слюсар В. І., Перепеліцин С. О.** Аналіз топології багаторангових мереж на основі торцевого добутку матриць. *Радіотехнічні поля, сигнали, апарати та системи* : зб. наук. пр. IX Міжнар. наук.-техн. конф. 16–22 листопада 2020. Київ : НТУУ КПІ. С. 114–116. DOI:10.13140/RG.2.2.26965.04329. **12. Слюсар В. И., Перепелицын С. А.** Применение торцевого произведения матриц в задачах анализа топологий маршрутизации многоранговых сетей. *Озброєння та військова техніка.* 2021. №1(29). С. 56–63. **13. Слюсар В. И.** Торцевые произведения матриц в радиолокационных приложениях. *Изв. ВУЗов. Радиоэлектроника.* 1998. Т.41. № 3. С. 71–75. **14. Slyusar V. I.** A family of face products of matrices and its properties. *Cybernetics and systems analysis*. 1999. Vol. 35. № 3. P. 379–384. URL: https://doi.org/10.1007/bf02733426 (date of access: 03.03. 2023). **15. Міночкін А. І., Рудаков В. І., Слюсар В. І.** Основи воєнно-технічних досліджень. теорія та приклади : монографія / ред. А. П. Ковтуненко. Київ : Гранмна, 2011. Т.2 «Синтез засобів інформаційного забезпечення озброєння і військової техніки». С. 7–98, 354–521. **16. Зінченко К. А.** Метод формалізації аналітичного опису системи військового зв'язку на основі тензорно-матричної теорії у поєднанні з теорією графів. *Труди університету* : збірник наукових праць Національного університету оборони України імені Івана Черняховського. 2022. №6(175). С. 232–248. **17. Військовий стандарт** «Словник НАТО зі зв'язку. Частина 1 (AComP 01 (Edition 3) NATO COMMUNICATIONS GLOSSARY (Chapter 716–722), MOD)». Вид. офіц. Київ : ВІТІ, 2019. 212 с. **18 Ланде Д. В., Снарський А. О., Безсуднов І. В.** Интернетика: навигация в сложных сетях: модели и алгоритмы. Ліброком, 2006. 264 с. **19. Головач Ю., Олемский О., Фербер К. фон та ін.** Складні мережі. *Журнал фізичних досліджень*. 2006. Т. 10. №4. С. 247-289.


## AN IMPROVED DIJKSTRA METHOD FOR DETERMINING THE SHORTEST ROUTES BETWEEN COMMUNICATION NODES IN A MILITARY COMMUNICATION SYSTEM


***Vadim Slyusar** (Doctor of Technical Sciences, professor)[1]*
***Kateryna Hromliuk**[2]*

*[1]Central Scientific Research Institute of Armament and Military Equipment of the Armed Forces of Ukraine, Kiyv, Ukraine*
*[2] Military Institute of Telecommunications and Information Technologies, Kiyv, Ukraine*



*In the article the authors present improved Dijkstra's method for the military communication system by using the incidence matrix of nodes and communication lines instead of the incidence matrix of nodes. The improved method was adapted to the model of the military communication system, which is formalized by a block matrix of the incidence of nodes and communication lines with the division of matrix blocks by types and components of the military communication system. The improvement implies in the introduction of additional blocks to the standard Dijkstra algorithm for preliminary, more accurate calculation of the weighting factors of*

*communication lines. At the same time, the authors propose a number of new analytical expressions based on the use of the block matrix of secondary incidence, as well as the quadratic form of the incidence matrix. Mathematical modeling based on a simplified model of the military communication system confirmed the efficiency of the improved method. The improved method synthesized by the authors is more relevant to the real conditions of managing the military communication system and can be used for the needs of the system management process automation as a basis for the development of information and analytical tasks.*

***Keywords:*** *Dijkstra's method, multilayer graph, block matrix, block edge product of matrices, incidence matrix.*

## *References*

**1. Snarsky, A. O.. Lande D. V.** (2015) Modeling complex networks: a textbook. Kyiv: NTUU «KPI», 212. **2. Harary, F.** (1972) Graph theory. 3rd ed Reading, Massachusetts: Addison-Wesley. 274. **3. Ageev, D. V**. (2011) Methodology for describing the structure of modern telecommunication systems using multilayer graphs. Vostochno-Evropeyskyi zhurnal peredovih technologiy, 6/4(48), 56–59. URL: http://journals. uran.ua/eejet/article/view/3295/3096 (access date: 03.03.2023). **4. Ageev, D. V.** (2010) Modeling of modern telecommunications systems with multi-layer graphs Problemy telekomunikatsii, 1, 23–34. URL: http://openarchive.nure.ua/handle/document/2722 (date of application: 03.03.2023). **5. Dijkstra, E. W.** (1959) A note on two problems in connexion with graphs. Numerische Mathematik, 1, 1, 269–271. URL: https://doi.org/10.1007/bf01386390 (date of access: 03.03.2023). **6. Cormen, T., Leiserson, Ch., Rivest, R. and Stein, C. (**2022) Introduction to algorithms, fourth edition. [S. l.]:MIT Press,. 1312. **7. Levitin, A.** (2011) Introduction to the design & analysis of algorithms. 3rd ed. [S. l.]: Pearson, 565. **8. Black, P. E.** (2005) Greedy algorithm Dictionary of Algorithms and Data Structures. URL: https://www.nist.gov/dads/HTML/greedyalgo.html (date of access: 03.03.2023). **9. Bellman, R.** (1958) On a routing problem. Quarterly of applied mathematics, 16, 1, 87–90 URL: https://doi.org/10.1090/qam/102435 (date of access: 03.03.2023). **10. Fulkerson, D. R., Ford, L. R.** (1962) Flows in networks (rand corporation research studies series) [S.l.] : Princeton Univ Pr, 198. **11. Slyusar V. I., Perepelitsyn S. O.** (2020) Analysis of the topology of multi-rank networks based on the end product of matrices. Radio Technical Fields, Signals, Devices and Systems : IX International Scientific and Technical Conference. November 16–22, Kyiv : NTUU KPI, 114–116. DOI: 10.13140/RG.2.2.26965.04329. **12. Slyusar, V. I., Perepelitsyn, S. A.** (2021) Application of the end product of matrices in problems of analysis of routing topologies of multi-rank networks, 56–63 p. **13. Slyusar, V. I.** (1998) End products of matrices in radar applications. Izv. universities. Radioelectronics, 41, 3, 71–75. **14. Slyusar, V. I.** (1999) A family of face products of matrices and its properties. Cybernetics and systems analysis, 35, 3, 379–384. URL: https://doi.org/10.1007/bf02733426 (date of access:03.03. 2023). **15. Minochkin, A. I., Rudakov, V. I., Slyusar, V. I.** (2011) Fundamentals of military-technical research. theory and examples: Monograph / ed. A. P. Kovtunenko. Kyiv: Granmna, 2 «Synthesis of means of information support of weapons and military equipment», 7–98, 354–521. **16. Zinchenko, K. A.** (2022) The method of formalization of the analytical description of the military communication system based on the tensor-matrix theory in combination with the graph theory. University Works: Collection of scientific works of the National Defense University of Ukraine named after Ivan Chernyakhovsky, 6 (175), 232-248. **17. Military standard** «NATO communication dictionary. Part 1 (AComP 01 (Edition 3) NATO COMMUNICATIONS GLOSSARY (Chapter 716–722), MOD)». Official. (2019) Kyiv: VITI, 212. **18. Lande, D. V., Snarskyi, A. O., Bezsudnov, I. V.** (2006) Internet: navigation in complex networks: models and algorithms, Librokom, 264. **19. Golovach, Yu**., **Olemskyi, O., Ferber, K. fon et al.** (2006) Complex networks. Journal of physical research, 10, 4, 247–289.

DOI:**10.33099/2311-7249/2023-46-1-13-17**

УДК: 681.324

***Володимир Іванович Богом'я*** *(доктор технічних наук, професор)*
***Андрій Сергійович Гудзь***

***Київський університет інтелектуальної власності та права Національного університету «Одеська юридична академія»***

# ШТУЧНИЙ ІНТЕЛЕКТ: СУЧАСНИЙ СТАН І ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ

*У статті наведено огляд сучасного стану та майбутніх перспектив застосування штучного інтелекту. Він починається з простеження історичного розвитку штучного інтелекту від його зародження в середині XX століття до наших днів. Висвітлено поточний стан штучного інтелекту, оглянуто типи штучного інтелекту, їх застосування у різних сферах і галузях, а також – етичні та соціальні наслідки штучного інтелекту. Розглянуто майбутні перспективи штучного інтелекту та його потенційний вплив на суспільство. Штучний інтелект стає дедалі важливішою технологією в сучасному суспільстві. Він може бути корисним у багатьох сферах і галузях діяльності людини, включаючи охорону здоров'я, транспорт, фінанси та багато інших. Штучний інтелект може забезпечити більш швидке і точне прийняття рішень, підвищити ефективність та знизити витрати. Водночас, він порушує етичні, юридичні та соціальні питання, у тому числі сумніви щодо конфіденційності, упередженості та впливу на зайнятість. Найголовніше у роботі зі штучним інтелектом – розуміти можливості та обмеження технології. Штучний інтелект – це не логічне рішення, здатне вирішити всі проблеми, а скоріше інструмент, який можна використовувати для поліпшення процесу прийняття рішень людиною та покращення результатів у певних сферах і галузях.*

***Ключові слова:*** *штучний інтелект; інформаційна безпека; проблема штучного інтелекту; розробка алгоритмів глибокого навчання.*

## Вступ

**Постановка проблеми.** Сьогодні, в багатьох сферах сучасного буття суспільства стала очевидною супровідна, подекуди провідна, роль штучного інтелекту. Крім того, паралельно стали помітними також проблеми і можливості, що виникають у результаті його використання. Штучний інтелект набуває все більшого значення в сучасному світі через його потенціал для перетворення багатьох сфер і галузей нашого повсякденного життя. Доцільно навести деякі аспекти важливості штучного інтелекту.

Так, підвищення ефективності та продуктивності штучного інтелекту може автоматизувати завдання і процеси, дозволяючи господарюючим суб'єктам працювати ефективніше та продуктивніше. Наприклад, чат-боти зі штучним інтелектом, можуть обробляти запити клієнтів, а алгоритми машинного навчання можуть аналізувати великі обсяги даних [1]. Це дозволить якісніше виявляти закономірності та тенденції, які люди не в змозі встановити, й ухвалювати вірні управлінські рішення у таких сферах, як фінанси, охорона здоров'я, транспорт тощо. Водночас, штучний інтелект можна використовувати для підвищення безпеки і захисту під час виявлення шахрайства і кібератак, прогнозування та запобігання нещасним випадкам, а також – моніторингу громадських місць стосовно підозрілої активності. Досягнення штучного інтелекту в сфері охорони здоров'я можуть сприяти покращенню діагностики, розробці персоналізованих методів лікування і поліпшити догляд за пацієнтами. Наприклад, алгоритми штучного інтелекту можуть аналізувати медичні зображення виявлення ранніх ознак раку чи інших захворювань [2].

Продовжуючи наведення аспектів застосування штучного інтелекту, можна назвати також його використання у сферах інновацій та економічного зростання всіх суб'єктів господарювання. Можуть розроблятися нові продукти, послуги та галузі. Технології на базі штучного інтелекту, такі як безпілотні автомобілі та розумні будинки, – це лише кілька прикладів інновацій, яким може сприяти штучний інтелект.

Проте, незважаючи на потенційні переваги штучного інтелекту, існують також етичні, юридичні та соціальні проблеми, пов'язані з його використанням. До них відносяться сумніви стосовно дотримання конфіденційності, упередженості та впливу на зайнятість. Тому важливими стали питання ґрунтовного розгляду наслідків використання штучного інтелекту і розроблення пропозицій щодо забезпечення максимальних його переваг і мінімізацію ризиків від його застосування.

**Аналіз останніх досліджень і публікацій.** У [1] автори розглянули проблему упередженості в штучному інтелекті. Науковці С. Рассел і П. Норвіг для підтвердження власного аргументу, спираються на кілька останніх досліджень і публікацій. Водночас, дослідження [1; 2] засвідчили, що в алгоритмах машинного навчання може бути багато типів зміщення, включно з історичним, статистичним і репрезентативним. Вчені опираються на цей висновок, обговорюючи конкретні методи, що були запропоновані для усунення різних типів упередженості, але такі методи як збільшення даних і тренування змагальності ними не розглядалися.

У [2] проаналізовано етичні наслідки дослідження етики штучного інтелекту і підкреслено важливість розгляду етичних наслідків досліджень штучного інтелекту, особливо щодо питань упередженості та дискримінації. Автори збагачують цю ідею, обговорюючи етичні міркування, що виникають під час спроби усунути упередженість у штучного інтелекту, проте, наприклад, компроміс між справедливістю і точністю не аналізується.

Незважаючи на те, що дослідження [5; 6] і публікації [1–4] сприяють розумінню упередженості в штучного інтелекту, все ще залишаються не розкритими частини загальної проблеми. Наприклад, хоча існує багато запропонованих методів усунення упередженості, незрозуміло, які методи є найбільш ефективними в різних контекстах. Крім того, існує обмежене дослідження того, як усунути упередженість у нових сферах штучного інтелекту, таких як глибоке навчання з підкріпленням.

Отже, актуальність нашої статті обумовлена наявними невирішеними частинами загальної проблеми, які вимагають подальших досліджень, зокрема щодо визначення найбільш ефективних методів усунення упередженості та усунення упереджень у нових сферах штучного інтелекту.

**Мета статті.** У результаті аналізу джерел [1–7] виокремлюються раніше невирішені частини загальної проблеми сучасного стану і перспективам застосування штучного інтелекту. Враховуючи зазначене, метою статті є висвітлення підходів стосовно збільшення переваг штучного інтелекту та мінімізації ризиків від його застосування.

## Виклад основного матеріалу дослідження

Наразі, штучний інтелект застосовується у таких сферах для [3; 4]:

*Свідомість* – розробки віртуальних помічників і чат-ботів, що природним або діалоговим способом можуть взаємодіяти з людьми. Наприклад, Siri від Apple та Alexa від Amazon – це віртуальні помічники на базі штучного інтелекту, які можуть розуміти природну мову та виконувати завдання для своїх користувачів.

*Безпека* – підвищення безпеки у різних контекстах. Наприклад, технологія розпізнавання осіб на базі штучного інтелекту може використовуватися для ідентифікації людей у громадських місцях, допомагаючи правоохоронним органам виявляти та запобігати злочинам. Крім того, алгоритми штучного інтелекту можна використовувати для аналізу відео з камер спостереження, щоб виявляти підозрілу поведінку та попереджати співробітників служби безпеки:

*Транспорт* – покращення транспортних систем різними способами. Наприклад, безпілотні автомобілі зі штучним інтелектом потенційно можуть знизити кількість дорожньо-транспортних пригод та підвищити ефективність транспортних систем. Крім того, алгоритми штучного інтелекту можна використовувати для оптимізації транспортного потоку та зменшення заторів у міських районах.

*Фінанси* – автоматизації завдань, прогнозування і виявлення шахрайства. Наприклад, чат-боти на базі штучного інтелекту можуть допомагати клієнтам із банківськими транзакціями, а алгоритми машинного навчання можуть аналізувати фінансові дані для прийняття більш ефективних інвестиційних рішень.

*Охорона здоров'я* – розробки персоналізованих методів лікування, покращення діагностики та покращення догляду за пацієнтами. Наприклад, алгоритми штучного інтелекту можуть аналізувати медичні зображення для виявлення ранніх ознак раку або інших захворювань, а чат-боти на основі штучного інтелекту можуть надавати пацієнтам медичні поради та допомогу.

*Освіта* – розробки персоналізованих програм навчання та покращення освітніх результатів. Наприклад, алгоритми штучного інтелекту можуть аналізувати дані учнів, щоб визначати області, у яких учні можуть мати труднощі, і надавати їм адресну підтримку.

Це лише кілька прикладів численних застосувань штучного інтелекту в різних сферах. Як бачимо, він може докорінно змінити сучасні сфери нашого буття, тому надзвичайно важливим є питання ретельного врахування етичних, юридичних і соціальних наслідків його використання.

*2. Проблеми та ризики штучного інтелекту.* Незважаючи на безліч переваг, вчені наголошують на різнопланових етичних, юридичних та соціальних проблемах і ризиках [5; 6]. Ось деякі з основних проблем:

*Конфіденційність*: системи штучного інтелекту можуть збирати і зберігати величезні обсяги даних, що викликає побоювання стосовно конфіденційності та захисту даних. Існує ризик того, що зібрані дані можуть бути використані не за призначенням або потрапити до чужих рук, що може поставити під загрозу конфіденційність окремих осіб.

*Упередженість*: системи штучного інтелекту можуть увічнювати чи, навіть, посилювати упередження в суспільстві. Це може статися, якщо алгоритми штучного інтелекту навчаються на упереджених даних або коли людські упередження відображаються у розробці та реалізації систем штучного інтелекту. Наприклад, було показано, що технологія розпізнавання обличь має більш високий рівень помилок для людей із темнішим відтінком шкіри.

*Зайнятість*: використання систем штучного інтелекту може призвести до скорочення робочих місць та безробіття, оскільки машини все частіше беруть на себе завдання, які раніше виконували люди. Це може мати серйозні соціальні та економічні наслідки, особливо, для працівників у високоавтоматизованих галузях.

*Підзвітність та відповідальність*: системи штучного інтелекту можуть приймати рішення, які істотно впливають на окремих людей і суспільство, що порушує питання про підзвітність та відповідальність. Наприклад, якщо система штучного інтелекту приймає рішення, яке завдає шкоди людині, хто буде нести відповідальність за таке рішення і кого можна притягнути до відповідальності?

*Прозорість*: системи штучного інтелекту можуть бути непрозорими та важкими для розуміння, що ускладнює оцінку їх рішень та результатів. Відсутність прозорості може підірвати довіру до систем штучного інтелекту та завадити їх впровадженню серед суспільства.

Для вирішення означених проблем і ризиків важливо розробити етичні та правові межі для розробки та використання систем штучного інтелекту. Це включає забезпечення того, щоб системи штучного інтелекту розроблялися та впроваджувалися з урахуванням конфіденційності та захисту даних, усунення упередженості в алгоритмах штучного інтелекту, надання підтримки працівникам, звільненим через автоматизацію, а також забезпечення підзвітності та прозорості під час прийняття рішень у галузі штучного інтелекту. Вирішуючи ці проблеми, ми можемо максимізувати переваги штучного інтелекту, зводячи до мінімуму пов'язані з ним ризики та забезпечуючи його використання таким чином, щоб приносити користь суспільству загалом [5–7].

*3. Перспективи штучного інтелекту.* Потенційне майбутнє штучного інтелекту водночас є вражаючим і досить проблематичним, з численними можливостями та потенційними досягненнями, а також з ризиками та проблемами. Розглянемо кілька можливих сценаріїв та тенденцій майбутнього штучного інтелекту:

*Досягнення в галузі штучного інтелекту*: немає сумнівів у тому, що технологія штучного інтелекту продовжуватиме вдосконалюватися завдяки вищій обчислювальній потужності, покращеним алгоритмам та більшій кількості даних, доступних для машинного навчання. Це може призвести до проривів у таких сферах, як охорона здоров'я, енергетика та екологічна стійкість.

*Автоматизація робочих місць*: може призвести до втрати робочих місць в одних галузях, а також створити нові робочі місця в інших.

*Надмір*: деякі експерти передбачають, що штучний інтелект зможе перевершити людський інтелект, що призведе до так званої «сингулярності». Це може мати як позитивні, так і негативні наслідки, залежно від розробки і впровадження штучного інтелекту до певних сфер діяльності.

*Етичні та правові межі*: потреба в етичних і правових засадах для штучного інтелекту зростає у міру того, як технологія стає все більш поширеною та впливовою. Органи державної влади й суб’єкти господарювання повинні розробити політику і правила, що забезпечать розробку та використання штучного інтелекту етичним та відповідальним чином.

*Конфіденційність і безпека*: у міру того, як системи штучного інтелекту стають все інтегрованішими до всіх сфер буття суспільства, зростатиме потреба у забезпеченні конфіденційності та безпеки даних. Ризики кібербезпеки і витоку даних стануть більш поширеними, тому органи державної влади та суб’єкти господарювання мають розробити заходи для зниження цих ризиків.

*Глобальне співробітництво*: у міру того, як технологія штучного інтелекту стає все успішнішою і популярнішою, прослідковується її глобальна важливість. Це включає обмін даними і знаннями, розробку міжнародних стандартів і вирішення проблем, пов'язаних з нерівним доступом до технологій штучного інтелекту.

*Нові можливості*: штучний інтелект зумовлює виникнення нових можливостей у бізнесовій та науковій сферах. Наприклад, він може сприяти новим відкриттям у таких галузях, як геноміка, квантові обчислення та матеріалознавство [7] .

Як показав здійснений нами огляд перспектив штучного інтелекту, водночас існує як значна кількість можливостей, так і викликів [8; 9]. Незважаючи на означені ризики й етичні проблеми, дана технологія має величезний потенціал для трансформації суспільства і вирішення деяких найнагальніших світових проблем. Щоб реалізувати весь потенціал штучного інтелекту, науковці всього світу в співпраці мають розробити етичні та правові межі, а урядові органи країн світу, за допомогою розробки і впровадження нормативно-правового поля, що унормує його використання, мають забезпечити відповідально-безпечне й корисне застосування штучного інтелекту.

*4. Шляхи вирішення деяких проблем.* Дослідження штучного інтелекту – це галузь, що швидко розвивається і спрямована на створення інтелектуальних систем, здатних виконувати завдання, для виконання яких, зазвичай, потрібен

інтелект людського рівня. Останніми роками, дослідження штучного інтелекту досягли значного прогресу в таких сферах, як обробка природної мови, комп'ютерний зір і робототехніка. Одним із найзначніших останніх досягнень науковців з удосконалення штучного інтелекту є розробка алгоритмів глибокого навчання. Ці алгоритми використовують нейронні мережі для вивчення великих наборів даних і зробили прорив у таких сферах, як розпізнавання зображень, розпізнавання мови та обробка природної мови. Наприклад, глибоке навчання дозволило розробити системи, які можуть точно розпізнавати та класифікувати об'єкти на зображеннях або транскрибувати мову з високою точністю. Іншою сферою значного прогресу в дослідженнях штучного інтелекту є розробка алгоритмів навчання з підкріпленням. Ці алгоритми дозволяють машинам навчатися методом проб і помилок, подібно до того, як люди навчаються на досвіді. Навчання з підкріпленням уможливило прорив у таких сферах, як ігри, робототехніка та автономні транспортні засоби.

Окрім зазначених досягнень, дослідження штучного інтелекту також сягнули значного прогресу в таких сферах, як генерація природної мови, що дозволяє машинам генерувати текст, схожий на людину, і неконтрольоване навчання, що дозволяє машинам навчатися на основі даних без явного позначення.

Однак, незважаючи на такі значні досягнення, дослідники штучного інтелекту все ще намагаються подолати кілька проблем. Однією з основних проблем є проблема упередженості в системах штучного інтелекту, яка може призвести до дискримінації та несправедливого ставлення. Вирішення цієї проблеми вимагає ретельного розгляду етичних міркувань, а також розробки методів виявлення та усунення упередженості в системах штучного інтелекту.

Отже, як показує практика останніх років, дослідження штучного інтелекту здійснили прорив у таких сферах глибокого навчання, навчання з підкріпленням, обробки природної мови, комп'ютерного зору, робототехніки тощо. Водночас існують і певні проблеми, зокрема – упередженість в системах штучного інтелекту. Завдяки постійній наполегливій науковій роботі вчених всього світу, штучний інтелект має потенціал докорінно змінити численні аспекти життя сучасного суспільства та створити інтелектуальні системи, здатні виконувати завдання, які раніше вважалися неможливими.

## Висновки й перспективи подальших досліджень

Узагальнюючи зазначимо, що найголовніше у роботі зі штучним інтелектом це розуміти можливості та обмеження технології. Штучний інтелект не є логічним рішенням, що може вирішити всі проблеми, скоріше, він став інструментом, що можна використовувати для покращення процесу прийняття рішень людиною та покращення результатів у певних сферах чи галузях діяльності. Для ефективної роботи з штучного інтелекту важливо добре розуміти алгоритми і дані, що лежать в основі технології. Це включає розуміння того, як попередньо обробляти і очищати дані, як вибрати правильний алгоритм для даної проблеми і як інтерпретувати результати системи штучного інтелекту.

Крім того, важливо усвідомлювати етичні та юридичні наслідки роботи штучного інтелекту, включно із забезпеченням відповідально-безпечного і прозорого проєктування та впровадженням систем штучного інтелекту, вирішенням проблем упередженості й дискримінації, а також захистом конфіденційності та безпеки даних. Важливим фактором також є співпраця з експертами з різних областей знань, наприклад, з фахівцями з обробки даних, інженерами-програмістами та експертами предметної галузі для гарантування того, що системи штучного інтелекту спроєктовані та реалізовані таким чином, щоб відповідати потребам і цінностям усіх зацікавлених сторін. Тобто, щоб переваги були максимізовані, а ризики – мінімізовані.

Вважаємо, що штучний інтелект неймовірно важливий у суспільстві. Він здатний змінити те, як ми живемо, працюємо та взаємодіємо з навколишнім світом. Від покращення охорони здоров'я та транспорту до просування наукових досліджень та покращення наших розваг – штучний інтелект, наразі, вже досить глибок впливає на наше повсякденне життя. Крім практичного застосування, штучний інтелект також стимулює інновації та створює нові можливості в науковій і бізнесовій сферах. Це дозволяє робити нові відкриття в таких галузях, як геноміка, квантові обчислення, матеріалознавство, а також допомагає вирішувати деякі з найнагальніших світових проблем, таких як зміна клімату, бідність та хвороби.

Водночас, як і у випадку з будь-якою потужною технологією, з штучним інтелектом також пов'язані ризики та етичні проблеми, у тому числі сумніви щодо упередженості та дискримінації, конфіденційності даних та впливу штучного інтелекту на зайнятість. Важливо, щоб наукова спільнота розробила етичні та правові межі для штучного інтелекту, що забезпечать відповідально-безпечне та корисне використання технології.

Маємо наголосити, що загалом штучний інтелект може стати однією з найбільш трансформаційних технологій нашого часу, що продовжуватиме власний розвиток і відіграватиме все важливішу роль у забезпеченні різнопланових потреб суспільства.

Перспективними напрямами подальших наукових розвідок мають стати дослідження особливостей штучного інтелекту з питань коректування, перевірки чи налагодження коду програми.

## *Література*

**1. Рассел С., Норвіг П.** Штучний інтелект. Сучасний підхід. Том 1. Рішення проблем: знання і міркування. Вільямс, 2021. 706 с. **2. Курвилль А., Бенджио И., Гудфеллоу Я.** Глубокое обучение. 2020. 652 с. URL: https://akonit.net/328471-glubokoe-obuchenie (дата звернення:23.12.2022). **3. Бостром Н.** Надрозум: шляхи, небезпеки, стратегії. Київ : Наш формат, 2020 452 с. **4. Домінгос П.** Верховний алгоритм: як машинне навчання змінить світ. М., 2016. 336 с. **5. О'Ніл К.** Зброя математичної руйнації: як більші дані збільшують нерівність і загрожують демократії. Київ : Наш формат, 2019. 620 с. **6. Тегмарк М.** Життя 3.0: бути людиною в епоху штучного інтелекту. Київ : Наш формат, 2019. 432 с. **7. Агравала А., Ганс Дж. та Голдфарб А.** Прогнозують машини: проста економіка штучного інтелекту. Harvard Business Review Press, 2018. 550 с. **8. Дранишников Л. В.** Інтелектуальні методи в управлінні: навчальний посібник. Кам'янське : ДДТУ, 2018. 416 с. **9. Brown Carol Ann, Smith Brad** IT as a weapon: what dangers are fraught with the development of high technologies. Alpina, 2020. 456 p.

## ARTIFICIAL INTELLIGENCE: CURRENT STATE AND PROSPECTIVE APPLICATIONS

***Volodymyr Bohomia* (*Doctor of Technical Sciences, Professor*)**
***Andriy Hudz***

***Kyiv University of Intellectual Property and Law of the National University «Odesa Law Academy», Kyiv, Ukraine***

*This article provides an overview of the current state and future prospects of artificial intelligence (AI). It begins by tracing the historical development of artificial intelligence, from its inception in the middle of the 20th century to the present day. The paper then explores the current state of artificial intelligence, discusses different types of artificial intelligence, their applications in different industries, and the ethical and social implications of artificial intelligence. Finally, the paper concludes with an examination of the future prospects of artificial intelligence and the potential impact of artificial intelligence on society.*

*Artificial intelligence is becoming an increasingly important technology in modern society. It can revolutionize many industries, including healthcare, transportation, finance, and many others. artificial intelligence can provide faster and more accurate decision-making, increase efficiency and reduce costs. However, AI also raises ethical, legal and social issues, including concerns about privacy, bias and the impact on employment.*

*The most important thing in working with artificial intelligence is to understand the capabilities and limitations of the technology. Artificial intelligence is not a logical solution that can solve all problems, but rather a tool that can be used to improve human decision-making and improve outcomes in certain industries.*

***Keywords:*** *artificial intelligence; informational security; the problem of artificial intelligence, the development of deep learning algorithms.*

## *References*

**1. Snarsky, A. O.. Lande D. V.** (2015) Modeling complex networks: a textbook. Kyiv: NTUU «KPI», 212. **2. Harary, F.** (1972) Graph theory. 3rd ed Reading, Massachusetts: Addison-Wesley. 274. **3. Ageev, D. V**. (2011) Methodology for describing the structure of modern telecommunication systems using multilayer graphs. Vostochno-Evropeyskyi zhurnal peredovih technologiy, 6/4(48), 56–59. URL: http://journals. uran.ua/eejet/article/view/3295/3096 (access date: 03.03.2023). **4. Ageev, D. V.** (2010) Modeling of modern telecommunications systems with multi-layer graphs Problemy telekomunikatsii, 1, 23–34. URL: http://openarchive.nure.ua/handle/document/2722 (date of application: 03.03.2023). **5. Dijkstra, E. W.** (1959) A note on two problems in connexion with graphs. Numerische Mathematik, 1, 1, 269–271. URL: https://doi.org/10.1007/bf01386390 (date of access: 03.03.2023). **6. Cormen, T., Leiserson, Ch., Rivest, R. and Stein, C. (**2022) Introduction to algorithms, fourth edition. [S. l.]:MIT Press,. 1312. **7. Levitin, A.** (2011) Introduction to the design & analysis of algorithms. 3rd ed. [S. l.]: Pearson, 565. **8. Black, P. E.** (2005) Greedy algorithm Dictionary of Algorithms and Data Structures. URL: https://www.nist.gov/dads/HTML/greedyalgo.html (date of access: 03.03.2023). **9. Bellman, R.** (1958) On a routing problem. Quarterly of applied mathematics, 16, 1, 87–90 URL: https://doi.org/10.1090/qam/102435 (date of access: 03.03.2023). **10. Fulkerson, D. R., Ford, L. R.** (1962) Flows in networks (rand corporation research studies series) [S.l.] : Princeton Univ Pr, 198. **11. Slyusar V. I., Perepelitsyn S. O.** (2020) Analysis of the topology of multi-rank networks based on the end product of matrices. Radio Technical Fields, Signals, Devices and Systems : IX International Scientific and Technical Conference. November 16–22, Kyiv : NTUU KPI, 114–116. DOI: 10.13140/RG.2.2.26965.04329. **12. Slyusar, V. I., Perepelitsyn, S. A.** (2021) Application of the end product of matrices in problems of analysis of routing topologies of multi-rank networks, 56–63 p. **13. Slyusar, V. I.** (1998) End products of matrices in radar applications. Izv. universities. Radioelectronics, 41, 3, 71–75. **14. Slyusar, V. I.** (1999) A family of face products of matrices and its properties. Cybernetics and systems analysis, 35, 3, 379–384. URL: https://doi.org/10.1007/bf02733426 (date of access:03.03. 2023). **15. Minochkin, A. I., Rudakov, V. I., Slyusar, V. I.** (2011) Fundamentals of military-technical research. theory and examples: Monograph / ed. A. P. Kovtunenko. Kyiv: Granmna, 2 «Synthesis of means of information support of weapons and military equipment», 7–98, 354–521. **16. Zinchenko, K. A.** (2022) The method of formalization of the analytical description of the military communication system based on the tensor-matrix theory in combination with the graph theory. University Works: Collection of scientific works of the National Defense University of Ukraine named after Ivan Chernyakhovsky, 6 (175), 232-248. **17. Military standard** «NATO communication dictionary. Part 1 (AComP 01 (Edition 3) NATO COMMUNICATIONS GLOSSARY (Chapter 716–722), MOD)». Official. (2019) Kyiv: VITI, 212. **18. Lande, D. V., Snarskyi, A. O., Bezsudnov, I. V.** (2006) Internet: navigation in complex networks: models and algorithms, Librokom, 264. **19. Golovach, Yu**., **Olemskyi, O., Ferber, K. fon et al.** (2006) Complex networks. Journal of physical research, 10, 4, 247–289.

DOI: **10.33099/2311-7249/2023-46-1-18-22**

УДК 355.40:004.83

***Микола Вікторович Мороз*** [1]
***Олександр Вікторович Яковчук*** [2]
***Сергій Станіславович Гаценко*** (*кандидат технічних наук*) [3]

[1] ***Науково-дослідний інститут Воєнної розвідки, Київ, Україна***
[2] ***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***
[3] ***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# РОЗРОБЛЕННЯ МОДЕЛІ ІДЕНТИФІКАЦІЇ СТАНУ РІЗНОРІДНИХ ДИНАМІЧНИХ ОБ'ЄКТІВ

*Технології штучного інтелекту активно застосовуються для вирішення загальних і вузькоспеціалізованих завдань. У процесі оцінювання (ідентифікації) стану складних і різнорідних об'єктів є високий ступінь апріорної невизначеності стосовно їх стану та малий обсяг вихідних даних, що їх описують. Тенденції збройних конфліктів останніх десятиліть, а також закономірності розвитку інформаційних систем переконливо свідчать про необхідність зміни підходів до збору інформації від різнотипних джерел та їх аналізу. Відбувається постійна трансформація форм подання інформації і порядку зберігання та доступу до різнотипних даних. Невирішеною повністю також є проблема інтеграції різнорідних джерел збору інформації в єдиний інформаційний простір. Саме тому, питання підвищення оперативності оцінювання стану складних і різнорідних динамічних об'єктів є важливим та актуальним питанням. Об'єктом дослідження є різнорідні динамічні об'єкти, а предметом – ідентифікація стану різнорідних динамічних об'єктів. У статті розроблену модель ідентифікації стану різнорідних динамічних об'єктів. Новизна запропонованої методики полягає у: врахуванні ступеня невизначеності про стан різнорідного динамічного об'єкту; врахуванні ступеня зашумленості даних у результаті викривлення даних, що характеризують стан різнорідного динамічного об'єкту; зменшенні обчислювальних витрат з оцінювання стану різнорідних динамічних об'єктів; можливості проведення розрахунків із вихідними даними, що є різні за природою та одиницями вимірювання. Зазначену методику доцільно реалізувати у спеціалізованому програмному забезпеченні, яке використовується для аналізу стану складних технічних систем та прийнятті рішень.*

***Ключові слова:*** *різнорідні динамічні об'єкти; складні технічні системи; комплексний аналіз; обробка різнотипних даних.*

## Вступ

**Постановка проблеми.** Штучний інтелект (ШІ) набув широкого використання для вирішення різноманітних завдань [1−3]. ШІ використовується для збільшення ефективності обробки даних, обробки великих масивів даних і підтримки прийняття рішень [3−5]. Аналіз зміни форм і способів збройних конфліктів останніх десятиліть [1−5], а також тенденції розвитку інформаційних систем різного функціонального призначення [6−10] переконливо свідчать про необхідність зміни підходів до: збору інформації від різнотипних джерел; аналізу різнотипних даних; форм представлення інформації; порядку зберігання та доступу до різнотипних даних; інтеграції різнорідних джерел інформації в єдиний інформаційний простір.

**Аналіз останніх досліджень і публікацій**. В праці [1] проведено огляд тенденцій розвитку інтегрованих систем зв'язку та передачі даних для потреб Збройних Сил України (ЗС України). Водночас учені акцентували увагу на розвиток єдиного інформаційного простору для потреб ЗС України та інших складових сектору безпеки і оборони. У [2] запропоновано підхід до навчання штучних нейронних мереж, що еволюціонують. Запропоновано використовувати зазначений підхід як універсальний для машинного навчання в інформаційних та автоматизованих системах спеціального призначення. У [3] запропоновано метод знаходження рішень щодо стану радіоелектронної обстановки в регіоні відповідальності за допомогою нейро-нечітких експертних систем. В [4] запропоновано підхід до комплексного оцінювання та прогнозування радіоелектронної обстановки за допомогою нечітких когнітивних моделей. В [5, 6] запропоновано комплексний підхід до обробки різнотипних даних в інформаційних системах спеціального призначення, що є різними за походженням та одиницями виміру. В роботі [7] запропонований підхід до збору, обробки та формування баз даних польоту роботизованих систем. В [8] наведено основні підходи з інтелектуальної обробки даних, їх галузі використання і наявні переваги та недоліки, пов'язані з їх використанням. В [9] запропоновано структурно-аналітичну модель для вирішення

завдань прийняття рішень у системах підтримки прийняття рішень з вирішення завдань будівництва, а в [10] – платформу для вирішення завдань прийняття рішень у системах підтримки прийняття рішень з ліквідації надзвичайних ситуацій та безпеки.

**Мета статті.** Враховуючи зазначене, метою дослідження є розроблення моделі ідентифікації стану різнорідних динамічних об'єктів. Об'єктом дослідження є різнорідні динамічні об'єкти, а предметом – ідентифікація стану різнорідних динамічних об'єктів.

## Виклад основного матеріалу дослідження

Вихід динамічного об'єкта представлений вимірами, що формують вибірку об'єму *s*, тобто $\{y_i, t_i\}, i = \bar{1}, \bar{s}$, де $y_i \in R$ – вимірювання виходу динамічної системи в момент часу $t_i \in [0, +\infty), u = u(t)$ – відомі дані керування входом динамічної системи. Відомо також, що система є лінійною та описується лінійним диференціальним рівнянням виду та вважаємо відомим початкова умова рівняння:

$$a_k \cdot x^{(k)} + a_{k-1} \cdot x^{(k-1)} + \ldots + a_0 \cdot x = b \cdot u(t), \quad x(0) = x_0. \tag{1}$$

Необхідно за даними вибірки визначити параметри системи та порядок *n* диференціального рівняння, який ми вважатимемо обмеженим, тобто $n - 1 \le M, M \in N$. Передбачається, що у каналі виміру виходу системи діє симетрично розподілена адитивна завада $\xi: M(\xi) = 0, D(\xi) \langle \infty$, тобто $y_i = x(t_i) + \xi_i$.

Для невідомого порядку системи розв'язується задача структурно-параметричної ідентифікації, водночас ця задача буде частково параметризованою, оскільки максимальний ступінь похідної, що входить до рівняння (1), визначається заздалегідь, обмежуючи нею розмірність пошукового простору. Для системи будь-якого порядку її коефіцієнт, за умов старшого ступеня, дорівнює одиниці, таким чином:

$$x^{(k)} + \frac{a_{k-1}}{a_k} \cdot x^{(k-1)} + \ldots + \frac{a_0}{a_k} \cdot x = \frac{b}{a_k} \cdot u(t), \tag{2}$$

або

$$x^{(k)} + \tilde{a}_k \cdot x^{(k-1)} + \ldots + \tilde{a}_1 \cdot x = \tilde{b} \cdot u(t). \tag{3}$$

Розв'язання задачі ідентифікації визначається як диференціальне рівняння порядку $m \le M, M \in N$, за заданих початкових умов:

$$x^{(k)} + \hat{a}_k \cdot x^{(k-1)} + \ldots + \hat{a}_1 \cdot x = \hat{b} \cdot u(t), \quad \hat{x}(0) = x_0. \tag{4}$$

з параметрами $\hat{a} = (0 \ldots 0 \quad \hat{a}_m \ldots \hat{a}_1 \quad \hat{a}_0)^T \in R^n$, тобто $n = M + 1$, доставляють екстремум обраної функції,

$$I_1(a) = \sum_{i=1}^{N\Sigma} |y_i - \hat{x}(t_i)| \left| \hat{a} = a \to \underset{a \in R^n}{\overset{min}{\overset{max}{}}} \right|$$
$$I_2(a) = {}_i |y_i - \hat{x}(t_i)| \left| \hat{a} = a \to \underset{a \in R^n}{min} \right| \tag{5}$$

Для динамічної моделі процесу за виразом (2) як рішення однієї із задач на пошук екстремуму: (4) або (5), необхідно володіти інформацією про початкове положення системи так, щоб могла бути вирішена задача Коші.

Вектор початкового положення системи, якщо він є не відомим спочатку, може бути чисельно оцінений, що, звичайно, не завжди можливо і залежить від властивостей вибірки. Іншим варіантом визначення початкового положення системи є включення вектору завдання оптимізації.

Припустимо, що потрібно формалізувати математичну модель динамічного процесу, яку зручно представити у матричному вигляді:

$$\tilde{x}' = \hat{A} \cdot \tilde{x}(t) + \hat{B} \cdot u(t), x(0) = x_0, \tag{6}$$

де $\hat{A} = \left(\hat{a}_{ij}\right)_{i=1,j=1}^{n,n}$ – матриця системи лінійних диференціальних рівнянь;

$\hat{B} = \left(\hat{b}_{ij}\right)_{i=1,j=1}^{n,m}$ – матриця правих частин, коефіцієнти керування;

$\tilde{x}(t) \in R^n$ – модель стану системи;

$u(t) \in R^m$ – керуючі дії, наведені у вигляді векторної функції.

Зважаючи на те, що спостерігається кілька різних виходів системи, які можуть відрізнятися за амплітудою відгуку, необхідно нормувати кожен окремо взятий критерій. Для цього визначимо діаметр множини вимірювань для кожного спостережуваного виходу за включення до цього безлічі початкового положення виходу. Тоді екстремум функції набуває такого вигляду:

$$I(a) = \sum_{j=1}^{N_0\Sigma} \frac{\sum_{i=1}^{s_j} \left| y_i^j - \hat{x}^j\left(t_i^j\right) \right|}{sup\left(|a-b| : a, b \in Y^j \cup x_0^j\right)} \left| \hat{A} = A, \hat{B} = B \to \underset{A,B}{min} \right| \tag{7}$$

де $N_0$ – кількість виходів динамічної системи;

$s_j, j = \bar{1}, \bar{N}_0$ – обсяг вибірки кожного виходу динамічної системи;

$y_i^j, i = \bar{1}, \bar{s}_j, j = \bar{1}, \bar{N}_0$ – вимірювання виходів, що утворюють вибірки;

$t_i^j, i = \bar{1}, \bar{s}_j, j = \bar{1}, \bar{N}_0$ – часи вимірів для кожного *j*-ого виходу;

$sup\left(|a-b| : a, b \in Y^j \cup x_0^j\right)$ – діаметр множини даних вимірювань для кожного виходу;

$\hat{x}^j(t) \left| \hat{A} = A, \hat{B} = B \right.$ – *j*-ий вихід моделі при матрицях *A, B*.

Екстремум функції (7), є аналогічним критерію завдання з одним входом і одним виходом (5). Таким чином, завдання ідентифікації динамічного об'єкта було приведене до пошуку екстремуму на просторі векторів з дійсними координатами. За таких умов особливість представлення структури об'єкта призводить до складної поведінки цільової функції в околиці деяких точок простору, для яких перші координати вектору наближаються до нуля.

Методика ідентифікації стану різнорідних динамічних об'єктів має у своєму складі такі взаємопов'язані процедури:

1. Введення початкових даних про стан різнорідного динамічного об'єкту.

2. Ініціалізація початкової моделі на основі виразів (1)−(7).

3. Введення корегувальних коефіцієнтів на зашумленість і апріорну невизначеність про стан об'єкту з використанням виразів [2]. Зважаючи на відсутність апріорної інформації про коефіцієнти та порядок диференціального рівняння використання бінарного подання змінних оптимізації стає скрутним і неефективним у сенсі знаходження рішення. Відповідно до прийнятого переходу від вектору, тобто індивіда, до диференціального рівняння, вектор, зважаючи на особливості обраного подання рішення, містить у собі інформацію про порядок, структуру та коефіцієнти диференціального рівняння, що необхідно враховувати для удосконалення роботи алгоритму.

4. Визначення порядку диференціального рівняння. Припустимо, що $\hat{a}$ − вектор, що містить вирішення задачі, тоді, $i_{order} \in N, i_{order} \leq M, i_{order}: \hat{a}_{i_{order}} \neq 0, \hat{a}_i = 0, i\rangle i_{order}$ Якщо $\hat{a}_M \neq 0 \rightarrow i_{order} = M$. Тоді порядок рівняння буде визначатися індексом $i_{order}$. Враховуючи запропонований підхід до визначення порядку диференціального рівняння, зауважимо на важливості того, щоб алгоритм вирішення задачі мав можливість зберігати деякі координати дорівнює нулю.

*5. Округлення координат векторів*. Однією зі спеціальних модифікацій алгоритму було введення операції округлення координат векторів:

$$op_j^i = round\left(op_j^i\right), j = \bar{1}, \bar{n}, i = \bar{1}, \bar{N}_1 \quad (8)$$

де $round(\cdot): R \rightarrow Z$ – функція, що округлює число до його найближчого цілого.

Такий оператор, що впливає на об'єктивні параметри алгоритму, вирішує завдання приведення координат вектору до цілих чисел. Оскільки для подання структури системи важливо, щоб у деяких випадках певна кількість координат рішення поспіль звертаються в нуль, а стохастичний пошуковий алгоритм обурює змінні через природу операції мутації, потрібен оператор, який зберігав би знайдений порядок. Оператор округлення застосовується безпосередньо після оператора мутації і після округлення відбувається локальне поліпшення отриманої популяції.

6. Мутація особин у популяції. Для підвищення ефективності пошуку рішень щодо стану різнорідного динамічного об'єкту був модифікований оператор мутації, таким чином, ймовірність мутації для кожної пари типу об'єктивний – стратегічний параметр, $p_m = \frac{1}{q}$. Тоді, випадкові збурення не призводять до сильного розкиду індивідів наступної популяції навколо деякого знайденого рішення, який не усувається за подальшого локального поліпшення альтернативи після округлення.

7. Генерація початкової популяції. Оскільки випадкове розігрування коефіцієнтів для стартової популяції не призведе до появи в популяції різних рішень, що відповідали б рівнянням різного порядку. Враховуючи подібне подання рішень, генеруватимемо популяцію таким чином:

1. До кожного індивіда з ймовірністю $\frac{1}{M}$ обирається порядок диференціального рівняння.

2. Для обраного порядку $i_{order}$ кожна ненульова координата розв'язується рівномірно на інтервалі [-5, 5].

3. Усі стратегічні параметри індивіда розігруються рівномірно в інтервалі [0, 1].

Запропонована схема була обрана як найкраща шляхом перебору різних варіантів початкового генерування рішень. Необхідно враховувати деякі особливості локального покращення альтернатив запропонованим алгоритмом випадкового покоординатного спуску. Оператор округлення (8) кожної координати призводить до того, що втрачається точність рішення через відсічення мантиси. Для того щоб компенсувати втрати точності й підвищити ефективність алгоритму в цілому, необхідно, щоб покоординатний спуск здійснював таку кількість кроків, що за обраної довжини кроку, округлений коефіцієнт міг бути уточнений так, що поверталося значення, яке передувало цілому.

Для оцінювання ефективності розробленої методики ідентифікації стану різнорідних динамічних об'єктів було випадково згенеровано 100 систем: по 10 систем за кожний порядок диференціального рівняння, з першого по десятий. Параметри кожної системи розігрувалися так: $\hat{a}_k^i \sim U(-5{,}5), \hat{b}_k \sim U(-5{,}5), i = \bar{1}, \bar{10}, k = \bar{1}, \bar{\imath}$ Час функціонування системи було обрано рівним 5.

Функція управління всіх завдань, що були проаналізовані, була обрано одиничною функцією, тобто $u(t) = 1$. Вибіркові дані відбираються з чисельного рішення диференціального рівняння. Припустимо, що $\{x_i, t_i\}, i = \bar{1}, \bar{T}/\bar{h}_{ode}$ – чисельне рішення системи. Тоді для заданого обсягу вибірки $s\langle T/h_{ode}, s = 100$ виберемо $s$ різних точок випадково з чисельного рішення диференціального рівняння.

Для того щоб оцінити ефективність параметрів оптимізаційного алгоритму була розглянута ідентифікація без збурень у каналах вимірювань, щоб цей фактор не вносив додаткової складності до завдання і можна було оцінити знайдені рішення. З цієї причини обсяг вибірки було обрано досить великим, щоб з'явилася можливість оцінити її репрезентативність, тобто, щоб вибірковими даними були всі особливості перехідного процесу. Для кожної окремої системи здійснювалося по 20 запусків алгоритму із певними налаштуваннями. Усі початкові умови даних завдань були прийняті рівними нулю. Обсяг популяції було обрано рівним 50, число популяцій – 50, параметри локального спуску $N_1 = 50, \quad N_2 = 50$ та $N_3 = 1$ за умови, що $h_l = 0.05$ .

Визначення ефективності запропонованої методики свідчить, що середня придатність зростає з наближенням порядку реального об'єкта до встановленого параметра-обмеження максимального порядку динамічної моделі. Отже, алгоритми мають працювати так, щоб зберігати можливість знижувати порядок системи, зберігаючи рівність перших координат нуль. Тому модифікація мутації або підключення оператора округлення призводять до істотного поліпшення.

Водночас важливо відзначити, що зростання придатності пов'язане з тим, що, за час спостережень, система вищого порядку поводиться так, що простіше побудувати її модель, ніж за аналогічних умов – модель нижчого порядку. Перехідні процеси різних систем можуть збігатися в певному інтервалі, тому лише збільшення інтервалу спостереження за виходом системи і збільшення частоти зняття вимірювань здатні підвищити ефективність знаходження рішення. З іншого боку, причиною цього може бути наявність великої кількості локальних оптимумів і досить сильна зона тяжіння.

Запропонована методика на відміну від існуючих [3−8]:

враховує ступінь невизначеності інформації про стан різнорідного динамічного об'єкту та зашумленості вихідних даних про його стан;

підвищує оперативність прийняття рішень під час оцінювання стану різнорідних об'єктів за рахунок пошуку рішення з використанням особин популяції;

вирішує проблему потрапляння до глобального екстремуму.

До переваг зазначеного дослідження слід віднести:

під час розрахунків враховується ступінь невизначеності про стан різнорідного динамічного об'єкту;

врахування ступеня зашумленості даних у результаті викривлення інформації про стан різнорідного динамічного об'єкту;

зменшення обчислювальних витрат за оцінювання стану різнорідних динамічних об'єктів;

можливість проведення розрахунків із вихідними даними, що є різні за природою та одиницями вимірювання.

До недоліків зазначеного дослідження слід віднести наявність відповідних обчислювальних потужностей та часу для проведення розрахунків.

Зазначену модель доцільно реалізувати у спеціалізованому програмному забезпеченні, яке використовується для аналізу стану складних технічних систем і прийнятті управлінських рішень.

## Висновки й перспективи подальших досліджень

У статті наведено модель ідентифікації стану різнорідних динамічних об'єктів. Новизна запропонованої методики полягає у:

врахуванні, при розрахунках корегувального коефіцієнту ступеню невизначеності про стан різнорідного динамічного об'єкту;

додаванні корегувального коефіцієнту на зашумленість даних у результаті викривлення інформації про стан різнорідного динамічного об'єкту;

зменшенні обчислювальних витрат під час оцінювання стану різнорідних динамічних об'єктів;

можливості проведення обчислень за вихідними даними, що є різними за природою та одиницями вимірювання.

Модель пропонується реалізувати у спеціалізованому програмному забезпеченні аналізу стану складних технічних систем і прийнятті управлінських рішень.

Перспективним напрямом подальших досліджень слід вважати удосконалення зазначеної моделі.

## *Література*


1. **Шишацький А. В., Башкиров О. М., Костина О. М.** Розвиток інтегрованих систем зв'язку та передачі даних для потреб Збройних Сил. *Озброєння та військова техніка.* 2015. № 1(5). С. 35–40. **2. Dudnyk V., Sinenko Yu., Matsyk M., Demchenko Ye., Zhyvotovskyi R., Repilo Iu., Zabolotnyi O., Simonenko A., Pozdniakov P., Shyshatskyi A.** Development of a method for training artificial neural networks for intelligent decision support systems. *Eastern-European Journal of Enterprise Technologies*. 2020. Vol. 3. № 2(105). P. 37–47. DOI: https://doi.org/10.15587/1729-4061.2020.203301. **3. Sova O., Shyshatskyi A., Salnikova O., Zhuk O., Trotsko O., Hrokholskyi Y.** Development of a method for assessment and forecasting of the radio electronic environment. EUREKA: *Physics and Engineering.* 2021. № 4. P. 30–40. DOI: https://doi.org/10.21303/2461-4262.2021.001940.

**4. Pievtsov H., Turinskyi O., Zhyvotovskyi R., Sova O., Zvieriev O., Lanetskii B., Shyshatskyi A.** Development of an advanced method of finding solutions for neuro-fuzzy expert systems of analysis of the radioelectronic situation. *EUREKA: Physics and Engineering*. 2020. № 4. P. 78–89. DOI: https://doi.org/10.21303/2461-4262.2020.001353. **5. Zuiev P., Zhyvotovskyi R., Zvieriev O., Hatsenko S., Kuprii V., Nakonechnyi O., Adamenko M., Shyshatskyi A., Neroznak Y., Velychko V.** Development of complex methodology of processing heterogeneous data in intelligent decision support systems. Eastern-*European Journal of Enterprise Technologies*. 2020. Vol. 4. № 9(106). P. 14–23. DOI: https://doi.org/10.15587/1729-4061.2020.208554. **6. Shyshatskyi A., Zvieriev O., Salnikova O., Demchenko Ye., Trotsko O., Neroznak Ye.** Complex Methods of Processing Different Data in Intellectual Systems for Decision Support System. International Journal of Advanced Trends in Computer Science and Engineering. 2020. Vol. 9. № 4. P. 5583–5590. DOI: https://doi.org/10.30534/ijatcse/2020/206942020. **7. Yeromina N., Kurban V., Mykus S., Peredrii O., Voloshchenko O., Kosenko V., Kuzavkov V., Babeliuk O., Derevianko M., Kovalov H.** The Creation of the Database for Mobile Robots Navigation under the Conditions of Flexible Change of Flight Assignment. *International Journal of Emerging Technology and Advanced Engineering.* 2021. Vol. 11. Iss. 05. P. 37–41. DOI: https://doi.org/10.46338/ijetae0521_05.

**8. Ротштейн А. П.** Интеллектуальные технологии идентификации: нечёткие множества, генетические алгоритмы, нейронные сети. Винница : «УНИВЕРСУМ», 1999. 320 с. **9. Ramaji I. J., Memari A. M.** Interpretation of structural analytical models from the coordination view in building information models. Automation in Construction. 2018. Vol. 90. P. 117–133. DOI: https://doi.org/10.1016/j.autcon.2018.02.025. **10. Pérez-González C. J., Colebrook M., Roda-García J. L., Rosa-Remedios C. B.** Developing a data analytics platform to support decision making in emergency and security management. *Expert Systems with Applications*. 2019. Vol. 120. P. 167–184. DOI: https://doi.org/10.1016/j.eswa.2018.11.023.

# DEVELOPMENT OF THE IDENTIFICATION MODEL STATE OF VARIOUS DYNAMIC OBJECTS

*Mykolay Moroz* [1]
*Olexandr Yakovchuk* [2]
*Serhii Hatsenko (Candidate of technical sciences)* [3]

[1] *Research Institute of Military Intelligence, Kyiv, Ukraine*
[2] *Military Institute of Telecommunications and Informatization named after Geroev Krut, Kyiv, Ukraine*
[3] *National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine*

*Artificial intelligence technologies are actively used to solve general and highly specialized tasks. In the process of assessing (identifying) the condition of complex and heterogeneous objects, there is a high degree of a priori uncertainty regarding their condition and a small amount of initial data describing them. The trends of armed conflicts of the last decades, as well as the patterns of development of information systems, convincingly indicate the need to change approaches to the collection of information from various sources and their analysis. There is a constant transformation of information presentation forms and the order of storage and access to various types of data. The problem of integrating disparate sources of information collection into a single information space is also not fully resolved. That is why the issue of improving the efficiency of assessing the state of complex and heterogeneous dynamic objects is an important and urgent issue. The object of research is heterogeneous dynamic objects, and the subject is identification of the state of heterogeneous dynamic objects. The article develops a model for identifying the state of heterogeneous dynamic objects. The novelty of the proposed method consists in: taking into account the degree of uncertainty about the state of a heterogeneous dynamic object; taking into account the degree of data noise as a result of distortion of data characterizing the state of a heterogeneous dynamic object; reduction of computing costs for assessing the state of heterogeneous dynamic objects; the possibility of performing calculations with raw data that are different in nature and units of measurement. It is advisable to implement the mentioned technique in specialized software, which is used to analyze the state of complex technical systems and make decisions.*

***Keywords:*** *heterogeneous dynamic objects; complex technical systems; comprehensive analysis; processing of various types of data.*

## *References*

**1. Shyshatskyi, A. V., Bashkyrov, O. M. and Kostyna, O. M.** (2015). Development of integrated communication and data transmission systems for the needs of the Armed Forces. Ozbroyennya ta viys'kova tekhnika, 1(5). **2. Dudnyk, V., Sinenko, Yu., Matsyk, M., Demchenko, Ye., Zhyvotovskyi, R., Repilo, Iu., Zabolotnyi, O., Simonenko, A., Pozdniakov, P. & Shyshatskyi, A.** (2020). Development of a method for training artificial neural networks for intelligent decision support systems. Eastern-European Journal of Enterprise Technologies, 3, 2 (105), 37–47. DOI: https://doi.org/10.15587/1729-4061.2020.203301. **3. Sova, O., Shyshatskyi, A., Salnikova, O., Zhuk, O., Trotsko, O., & Hrokholskyi, Y.** (2021). Development of a method for assessment and forecasting of the radio electronic environment. EUREKA: Physics and Engineering, 4, 30–40. DOI: https://doi.org/10.21303/2461-4262.2021.001940. **4. Pievtsov, H., Turinskyi, O., Zhyvotovskyi, R., Sova, O., Zvieriev, O., Lanetskii, B., and Shyshatskyi, A.** (2020). Development of an advanced method of finding solutions for neuro-fuzzy expert systems of analysis of the radioelectronic situation. EUREKA: Physics and Engineering, 4, 78–89. DOI: https://doi.org/10.21303/2461-4262.2020.001353. 5. **Zuiev, P., Zhyvotovskyi, R., Zvieriev, O., Hatsenko, S., Kuprii, V., Nakonechnyi, O., Adamenko, M., Shyshatskyi, A., Neroznak, Y. and Velychko, V.** (2020). Development of complex methodology of processing heterogeneous data in intelligent decision support systems, Eastern-European Journal of Enterprise Technologies 4, 9(106), 14–23. DOI: https://doi.org/10.15587/1729-4061.2020.208554. **6. Shyshatskyi, A., Zvieriev, O., Salnikova, O., Demchenko, Ye., Trotsko, O. and Neroznak, Ye.** (2020). Complex Methods of Processing Different Data in Intellectual Systems for Decision Support System. International Journal of Advanced Trends in Computer Science and Engineering, 9, 4, 5583–5590. DOI: https://doi.org/10.30534/ijatcse/2020/206942020.

**7. Yeromina, N., Kurban, V., Mykus, S., Peredrii, O., Voloshchenko, O., Kosenko, V., Kuzavkov, V., Babeliuk, O., Derevianko, M. and. Kovalov, H**. (2021). The Creation of the Database for Mobile Robots Navigation under the Conditions of Flexible Change of Flight Assignment. International Journal of Emerging Technology and Advanced Engineering, 11, 05, 37–41. DOI: https://doi.org/10.46338/ijetae0521_05. **8. Rotshteyn, A. P.** (1999). Intelligent identification technologies: fuzzy sets, genetic algorithms, neural networks. Vinnitsa: «UNIVERSUM», 320. **9. Ramaji, I. J. and Memari, A. M**. (2018). Interpretation of structural analytical models from the coordination view in building information models. Automation in Construction, 90, 117–133. DOI: https://doi.org/10.1016/j.autcon.2018.02.025. **10.Pérez-González, C. J., Colebrook, M., Roda-García, J. L. and Rosa-Remedios, C. B.** (2019). Developing a data analytics platform to support decision making in emergency and security management. Expert Systems with Applications. 120. 167–184. DOI:https://doi.org/10.1016/j.eswa.2018.11.023.

DOI:**10.33099/2311-7249/2023-46-1-23-31**

УДК: 338.242(477)

***Олександр Васильович Терновий***
***Олексій Миколайович Шкуренко***
***Людмила Миколаївна Міненко*** ***(доктор філософії)***

***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# ПРОБЛЕМНІ АСПЕКТИ КІБЕРОБОРОНИ: МІСЦЕ ТА РОЛЬ КІБЕРЗАХИСТУ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

*У статті розглянуто проблемні аспекти кібероборони нашої держави, а також місце та роль кіберзахисту в Збройних Силах України. Акцентовано зосередженість на тому, що формування інформаційного суспільства зумовило численні кібернетичні загрози. Показано, що кіберпростір не лише надає ресурси і можливості, а несе певні проблеми, що мають руйнівний характер, спричиняють небезпеку існуванню держави, її функціонуванню та розвитку. Звернуто увагу, що Україна не є в числі передових у сфері інформаційно-комунікаційних технологій і кібероборони серед цивілізованих країн світу. Аргументовано, що саме такі напрями наукових досліджень є надзвичайно актуальними тому, що кібернетичний захист є стратегічно важливим як у цивільній царині, так і в сфері військової діяльності. Доведено, що в умовах війни Україна є однією з країн, яка найбільше потерпає від кіберзагроз. Головну небезпеку, в цьому сенсі, становить російська федерація, як військовий агресор. Підкреслено, що саме тому одним із основних завдань сьогодення є забезпечення кібернетичної безпеки. Проаналізовано наукові праці за темою статті, систематизовано та охарактеризовано зміст нормативно-правових актів України в сфері кібербезпеки, висвітлено заходи, що передбачено для підготовки до протистояння інформаційній агресії й кібернетичним атакам. Означено, що вже сьогодні є ряд проблемних питань стосовно кібероборони держави, що потребують нагального вирішення. Згруповано і представлено низку практичних рекомендацій для Міністерства оборони України і Збройних Сил України, щодо доцільності виконання нормативно-правових й адміністративно виважених кроків та використання алгоритму їх реалізації.*

***Ключові слова:*** *кіберпростір; інтерактивне інформаційне середовище; кібероборона; кібербезпека; кіберзагрози; кіберзахист; рекомендації стосовно кібероборони держави.*

## Вступ

**Постановка проблеми.** Швидкий розвиток інформаційних технологій і комп'ютеризації зумовили формування інформаційного суспільства та, водночас, виникнення глобального кібернетичного простору, що відзначається невичерпним потенціалом поєднання можливостей отримання інформації і знань й відіграє провідну роль в економічному та соціальному розвитку передових країн світу. Фактично, кіберпростір виступає середовищем, де виробляється і поширюється різнопланова інформація, що створена та працює на основі принципів і методів кібернетики. По суті, сьогодні він є абсолютно новим двигуном зростання економіки, сучасною основою соціального управління, інноваційним способом міжнародного співробітництва та інтерактивною інформаційною сферою, що прямо впливає на безпеку державного суверенітету країни, спонукає займатися питаннями кібероборони. Реально, тотальна цифровізація та інфокомунікаційний зв'язок збільшили ризики кібербезпеки (комплексу заходів, що допомагають мінімізувати негативні наслідки від кібератак), зробивши суспільство вразливішим до кіберзагроз і розширивши коло специфічних проблем, з якими стикаються люди. Саме тому, протидія загрозам, у першу чергу національній безпеці, що надходять з кіберпростору, набула абсолютно нового сенсу. Варто зазначити, що кіберзагрози дедалі почастішали, стали більш організованими і збитковими для державної економіки в цілому та об'єктів критичної інфраструктури зокрема. Вони здатні досягти небезпечного рівня і негативно вплинути на національний розвиток та євроатлантичні прагнення нашої держави, безпеку і стабільність європейської спільноти. Джерелами таких загроз можуть бути іноземні військові й розвідувальні служби, організовані злочинні угруповання, терористичні та екстремістські групи тощо. За сформованих умов, основним завданням державних органів безпеки та оборони України, є застосування заходів, спроможних зменшити, а іноді, й цілком унеможливити негативні наслідки кіберзагроз. Значну роль у виробленні загальновизнаних підходів стосовно забезпечення кібербезпеки відіграє Організація

Північноатлантичного договору (або Північноатлантичний альянс) (далі – НАТО) як складова національної безпеки країн-членів договору. Сукупність способів потенційного застосування кіберзасобів висуває перед НАТО одне з головних завдань щодо розуміння її власної ролі в створенні умов для функціонування необхідних процесів кібербезпеки країн-членів і країн-партнерів Альянсу. Отже, актуальність нашого дослідження полягає у розгляді практичних питань кібероборони, у першу чергу місця і ролі кібернетичного захисту інформаціїї, зокрема, у Збройних Силах України (далі – ЗС України), в співпраці з НАТО.

**Аналіз останніх досліджень і публікацій.** Вивчення наукових праць вітчизняних вчених та аналіз нормативно-правових актів України і НАТО дозволило сформувати виклад основного матеріалу статті. Зокрема, В. Ліпкан та О. Ліпкан опрацювали понятійний апарат у сфері національної і міжнародної безпеки [7]. Основи кібернетичної безпеки і світові тенденції та виклики для України у цій сфері виклали Р. Грищук, Ю. Даник, В. Бурячок, В. Толубко, В. Хорошко, С. Толюпа , Д. Дубов, М. Ожеван [2; 3; 4]. Проблеми і перспективи подолання кіберінтервенції та кібербезпеки визначив і дослідив Ю. І. Грицюк [1]. Огляд практичних питань організації створення кібервійськ України і рекомендації щодо визначення їхніх завдань визначили і розробили Р. Кирилюк та Є. Шелест [5]. Правове забезпечення системи кібернетичної безпеки України, основні напрями її вдосконалення, а також деякі практичні питання в сфері попередження правопорушень у кіберпросторі роз'яснили О. Климчик, С. Мельник, В. Кащук, В. Шеломенцев [6; 8; 9]. Науковці В. Дідик, А. Гончарук., І. Сімоненкова висвітлили основні проблеми кіберзахисту в ЗС України у ході протидії можливим варіантам кіберзлочинності [11]. Кібербезпеку як напрям євроатлантичної інтеграції України розглянув А. Войціховський [12]. Крім того, питання підготовки фахівців у сфері кібербезпеки, в частині забезпечення дистанційного навчання, авторами статті розглядалося з точки зору дотримання норм Стратегії програми НАТО з удосконалення військової освіти (DEEP) [10]. Головним чином, з'ясуванню теми сприяло вивчення національних нормативно-правових актів, а саме:

Указів Президента України: «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"» від 25.02.2017 р. №47/2017; «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України"» від 14.09.2020 р. №392/2020; «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"» від 15.03.2016 р. №96/2016; «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» 26 серпня 2021 року № 447/2021; «Про Положення про Генеральний штаб Збройних Сил України» від 30.01.2019 р. № 23/2019; «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"» від 26.08.2021 р. № 446/2021; «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» від 17.09.2021 р. № 473/2021, а також:

Законів України: «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII; «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII; «Про оборону України» від 06.12.1991 р. № 1932-XII.

**Мета статті.** Окреслити проблемні аспекти кібероборони нашої держави, кокретизувати місце та роль кіберзахисту в Збройних Силах України, розробити практичні рекомендації.

## Виклад основного матеріалу дослідження

В Указі Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про Доктрину інформаційної безпеки України"» від 25.02.2017 р. №47/2017 вказується, що важливою загрозою національним інтересам та національній безпеці України в інформаційній сфері є здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу ЗС України та інших військових формувань, а також провокування екстремістських проявів, підживлення панічних настроїв, загострення й дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання в Україні міжетнічних і міжконфесійних конфліктів. Так, дійсно, як показує практика, проблематика захисту від кібернетичних загроз є одним із головних пріоритетів для збройних сил будь-якої країни. Україна не стала винятком. Починаючи з 2014 року наша держава була змушена давати відсіч гібридній російській збройній агресії, включаючи кіберпростір. Однак, офіційне визнання необхідності кібероборони відбулось лише у березні 2016 року завдяки Указу Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України"» від 15.03.2016 р. №96/2016. Зміни і доповнення до нього були введені Указом Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26 серпня 2021 року № 447/2021.

Відповідно до цієї Стратегії, національна система кібербезпеки перебуває у віданні Міністерства оборони України (далі – МО України), Державної служби спеціального зв'язку

та захисту інформації України (далі – ДССЗЗІ України), Служби безпеки України (далі – СБ України), Національної поліції України та Національного банку України. Через це, вперше, для МО України і Генерального штабу Збройних Сил України (далі – ГШ ЗС України) було визначено додаткові завдання: здійснення заходів щодо підготовки держави до відбиття воєнної агресії в кіберпросторі (кібероборони); здійснення військової співпраці з НАТО у поєднанні із забезпеченням безпеки кіберпростору та спільного захисту від кіберзагроз; забезпечення за допомогою тісної взаємодії з ДССЗЗІ України України і СБ України кіберзахисту інформаційної інфраструктури. З цією метою утворено Національний координаційний центр кібербезпеки, що став робочим органом Ради національної безпеки і оборони України (далі – РНБО України). Основними завданнями цього органу затверджено розроблення і внесення до РНБО України та подання її Голові пропозицій стосовно: здійснення заходів, спрямованих на державну підтримку стратегічно вагомих для кібероборони держави наукових установ і організацій; зростання рівня дієвості реалізації військово-технічної політики й політики військово-технічної співпраці в сфері кібероборони; гарантування належного стану кібероборонних можливостей країни [9, 311]. Водночас, Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України"» від 14.09.2020 р. №392/2020 провідними загрозами національній безпеці України в інформаційній сфері визначив ведення інформаційної війни проти України й відсутність структурованої комунікативної політики держави та належний рівень медіа-культури суспільства.

Крім того, варто зазначити, що ще у 2015 році науковці В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко , С. В. Толюпа виокремили основні напрями державної політики стосовно забезпечення інформаційної безпеки, що були враховані у процесі розроблення вищезгаданої Стратегії національної безпеки України, а саме: реалізація політики інформаційної безпеки на основі асиметричних дій проти всіх форм та проявів інформаційної агресії; розробка інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям свідомістю населення та поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; впровадження регульованої інформаційної політики органів державної влади та ін. [4]. Зі свого боку, зустріч голів держав і голів урядів країн-членів НАТО, що відбулась у Варшаві у 2016 році, підтвердила важливість кіберзахисту для функціонування органів державної влади України та її Збройних Сил. На зустрічі вперше було підписано Договір між Європейським союзом (далі – ЄС) і НАТО про співробітництво в сфері безпеки, зокрема, це стосувалось питань гібридних війн і кібератак. Тож було окреслено такі пріоритетні сфери діяльності, як: протистояння гібридним загрозам; оперативне реагування й співробітництво у військово-морській сфері; кібербезпека та оборона; потенційні можливості захисту, оборонні промислові й відповідні наукові дослідження; тренування та узгодження дій партнерів. МО України підтримало проєкт НАТО, що спрямовувався на підготовку фахівців у сфері кібербезпеки. Так, фахівці Альянсу розробили Стратегію програми НАТО з удосконалення військової освіти (DEEP), до якої долучились не лише країни-члени НАТО, а й партнери, серед яких – Україна [10].

Саме тому, в Законі України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII (далі – Закон про кібербезпеку) було вперше визначено необхідні терміни цієї проблеми, а саме: *кібербезпека* – належний стан захисту життєво вагомих інтересів людини та громадянина, суспільства і держави під час використання кіберпростору, за якої забезпечений стабільний розвиток інформаційного суспільства та цифрового комунікативного середовища, вчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національній безпеці України у кіберпросторі; *кіберзахист* – сукупність організаційних, нормативно-правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, що спрямовуються на запобігання кібервипадкам, протидії кібератакам, ліквідацію їх наслідків, відновлення стабільності та надійності функціонального існування комунікаційних та технологічних систем; *кібероборона* – комбінація, що включає політичні, економічні, соціальні, військові, наукові, науково-технічні, інформаційні, правові, організаційні та ряд інших заходів, що здійснюються у кіберпросторі та спрямованих на захист суверенітету та обороноздатності держави, запобігання збройним конфліктам і відсіч збройним агресіям. Підсумково, Законом про кібербезпеку для МО України та ГШ ЗС України визначено те, що вони мають: здійснюватися заходи із забезпечення готовності держави до відбиття воєнної агресії у кіберпросторі (кібероборони); організовувати і проводити військову співпрацю з НАТО та різними суб'єктами оборонної сфери стосовно забезпечення безпеки кіберпростору й спільного захисту від кіберзагроз. Окремо передбачається те, що повинні впроваджуватись заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури у випадках надзвичайного і воєнного стану [13].

Разом із тим, для посилення уваги до кібероборони, у жовтні 2017 року до Закону України «Про оборону України» від 06.12.1991 р.

№ 1932-XII було внесено зміни, що передбачають підготовку держави до оборони в мирний час, під час якої мають бути реалізовані заходи стосовно кібероборони (активний кіберзахист) з метою захисту суверенітету держави, забезпечення її обороноздатності, запобігання збройним конфліктам і відсічі збройним агресіям [14]. У подальшому, не менше важливим національним нормативно-правовим актом для гарантування кібербезпеки став Закон України «Про національну безпеку України» від 21.06.2018 р. № 2469-VIII. Його засади частково розкрили особливості Стратегії кібербезпеки України. В Законі викладено винятково загальні положення, що не містять конкретних заходів. Це призвело до недоліків у сфері безпеки та оборони України, наслідком чого продовжилися збої в роботі органів державної влади, приватного бізнесу та ін.

Тому, з метою конкретизації заходів з оборони нашої держави і, зокрема, кібероборони, Указом Президента України «Про Положення про Генеральний штаб Збройних Сил України» від 30.01.2019 р. № 23/2019 (далі – Положення про ГШ ЗС України) було затверджено відповідне Положення. Серед основних його завдань визначено: організовувати розгортання, здійснювати управління та забезпечувати функціональне існування системи захисту інформації та кіберзахисту в інформаційно-телекомунікаційних системах МО України і ЗС України; брати участь у створенні національної системи кібербезпеки та проведенні її огляду на періодичній основі; організовувати планування та виконання у межах компетенції заходів з підготовки держави до відбиття воєнних агресій в кіберпросторі (кібероборони); координувати виконання завдань щодо підготовки до кібероборони органами виконавчої влади, органами місцевого самоврядування та іншими складовими сил оборони; забезпечувати інформаційну безпеку в ЗС України і протидіяти системним та масштабним діям проти інтересів України в кіберпросторі. Фактично, це дії з боку іноземних держав (груп держав) із одночасним залученням кіберпідрозділів збройних сил іноземних держав з одночасним використанням спеціальних засобів (кіберозброєнь) [15].

Згодом, для покращення вирішення стратегічно важливих національних питань оборонного характеру, у тому числі й заходів з кібербезпеки, на початку лютого 2020 року в ЗС України були створені чотири нові командування та призначені їхні командувачі. Одним із вказаних командувань стало Командування Військ зв'язку та кібернетичної безпеки ЗС України. Через це, наприкінці березня 2020 року, внесено зміни до Положення про ГШ ЗС України, відповідно до яких даний орган військово управління додатково: організовує планування операцій ЗС України та інших складових сил оборони у кіберпросторі; у тісній взаємодії з ДССЗЗІ України та СБ України займається організацією кіберзахисту інформаційної інфраструктури МО України та ЗС України [15].

Отже, як зазначалося вище, 26 серпня 2021 року було затверджено нову редакцію Стратегії кібербезпеки України. Чинною вона стала завдяки виданню Указу Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26.08.2021 № 447/2021. Принципово важливим у цьому нормативному документі стало те, що першою стратегічною ціллю у формуванні потенціалу стримування визначено дієву кібероборону для досягнення якої Україна має: створити і забезпечити розвиток підрозділів із повноваженнями ведення збройного протиборства в кіберпросторі; сформувати належну правову, організаційну і технологічну модель їх функціонування та застосування; здійснити забезпечення ефективної взаємодії головних суб'єктів національної системи кібербезпеки і сил оборони під час здійснення заходів з кібероборони, належний рівень навчання та фінансового забезпечення цих структур; організувати систематичне проведення кібернавчань, оцінювання спроможностей та ефективності підрозділів, розробку та імплементацію індикаторів оцінки їх діяльності [16].

Водночас, Указом Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"» від 26.08.2021 р. № 446/2021 Кабінету Міністрів України, з метою створення в системі МО України кібервійськ і набуття ними відповідних спроможностей, доручено здійснити розрахунки потреб щодо: обсягу матеріально-технічних і фінансових ресурсів, необхідних для створення й забезпечення належного функціонування кібервійськ; комплектування особового складу кібервійськ з урахуванням оптимального співвідношення військовослужбовців, працівників МО України, а також зарахованих у запас, резервістів та інших категорій осіб [17].

Крім того, Указом Президента України «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» від 17.09.2021 р. № 473/2021 було затверджено черговий Стратегічний оборонний бюлетень України. У цьому документі значна увага надавалася питанням забезпечення кібероборони держави. Даний документ оборонного планування унормував поняття воєнної агресії в кіберпросторі, дій у кіберпросторі, кіберзагроз воєнного характеру, кіберборотьби, кібердій, кібердорозвідки, кіберзброї та кіберінфраструктури. Також Указом зроблено акцент на тому, що для протидії силам і засобам противника мають бути поєднані дії, спрямовані на радіоелектронну боротьбу і протистояння в кібер- та інформаційному просторах [18].

Отже, здійснивши огляд головних нормативно-правових актів, що регулюють сферу кібербезпеки України та її Збройних Сил, з метою підкреслення актуальності цієї проблеми додатково розглянемо деякі питання захисту інформації під час застосування електронних

систем обміну даними, що використовуються МО України і підпорядкованими йому підрозділами. Так, дійсно, у Законі про кібербезпеку зазначено, що вдосконалення систем інформаційної і кібербезпеки, систем захисту інформації та безпеки інформаційних ресурсів є серед головних завдань МО України та ГШ ЗС України [13]. Цим же законом окреслено інші завдання, зокрема: забезпечення інформаційної та кібербезпеки; посилення спроможностей зміцнення інституціональних і технічних можливостей суб'єктів сектору безпеки та оборони з метою дієвої боротьби з кіберзагрозами воєнного характеру, кіберзлочинністю, кібершпигунством, та кібертероризмом; поглиблення міжнародного співробітництва у цій сфері; формування підрозділів забезпечення кібербезпеки й кіберзахисту ЗС України; здійснення міжвідомчої координації та взаємодії з цих питань в інтересах забезпечення обороноздатності держави; створення необхідних матеріально-технічних ресурсів для забезпечення здатності протидіяти іноземним технічним розвідкам, інформаційним, кібернетичним атакам, спецопераціям противника; створення ефективних сучасних зразків кіберзброї; розвитку Мережі реагування на комп'ютерні надзвичайні події «Команда реагування на комп'ютерні надзвичайні події України» (англ. «Computer Emergency Response Team of Ukraine») (далі – CERT-ua).

Через це, важливе значення має той факт, що з початку 2014 року головний орган військового управління ЗС України під час обміну інформацією в електронних системах для захисту конфіденційності документа використовує криптографічні засоби, а саме електронно-цифровий підпис. Означений підпис може бути застосований завдяки використанню відкритого ключа, підтвердження належності фізичній чи юридичній особі якого здійснюється спеціальною організацією або підрозділом у ЗС України та акредитованим центром сертифікації ключів, який, таким чином, забезпечує надійність і захист криптографічних ключів.

інформаційної системи України. Водночас, задля протидії кіберзагрозам у ЗС України функціонують окремі підрозділи, що стежать за належним станом використання ІТС на організаційному, технічному й правовому рівнях. Проте, незважаючи на заходи, що гарантують захист інформації у кіберпросторі, мусимо констатувати прояви негативних факторів, що впливають на якість кіберзахисту ЗС України, зокрема: дефіцит спеціалістів ІТ напряму відповідної підготовки для роботи у кіберпросторі й протидії кіберзагрозам; відсутність належним чином затвердженої для кожного рівня управління штатної структури, положень про структурні підрозділи, посадові інструкції і відповідно

З огляду на це, науковці В. Дідик., А. Гончарук та І. Сімоненкова акцентували увагу на тому, що для надійного протистояння кіберзлочинам у ЗС України, завдяки використанню надсучасних програмних алгоритмів, має бути створена система протидії, яка здатна протистояти атакам і втручанням в роботу інформаційно-телекомунікаційних систем (далі – ІТС). Тобто, на різних рівнях кіберпростору необхідно застосовувати систему захисту інформації, що гарантуватиме здійснення таких заходів: розмежування доступу користувачів до ІТС із використанням криптографічного захисту інформації під час зберігання та обміну нею; застосування міжмережевого екранування з одночасним використанням маршрутизаторів та фаєрволів; забезпечення створення й практичного застосування віртуальних приватних мереж; системне використання антивірусного захисту; унеможливлення застосування програмних продуктів потенційними опонентами; застосування системи виявлення вторгнень (IDS) за умови використання підсистеми профілактики вторгнень (IPS); встановлення механізму автентифікації й авторизації; забезпечення резервного зберігання даних на носіях інформації, до яких обмежений будь-який несанкціонований доступ [11].

Натомість, маємо констатувати, сьогодні, організування і керівництво забезпеченням кібербезпеки й виконання інших функцій управління зв'язку, у тому числі зазначених вище заходів, здійснюють підрозділи ГШ ЗС України, а саме: Головне управління зв'язку та кібербезпеки (далі – ГУЗК ГШ ЗС України) і Центральне управління охорони державної таємниці та захисту інформації (ЦУ ОДТта ЗІ ГШ ЗС України). З метою захисту інформації та протидії кіберзагрозам підрозділи ГУЗК ГШ ЗС України співпрацюють зі СБ України, ДССЗЗІ України, Національною поліцією України. Крім того, вони взаємодіють із CERT-ua, що входить до структури ДССЗЗІ України, і виконують завдання в сфері кібернетичного захисту національної підібраних фахівців, які спроможні діяти проти будь-яких потенційних кіберзлочинів і працювати в команді; нестача, а в окремих випадках, повна відсутність сучасного технічного забезпечення, інформаційних та інфокомунікаційних технологій, призначених для захисту і протидії кіберзагрозам; нестача ліцензійного програмного забезпечення і невикористання антивірусних захистів; низький рівень обізнаності особового складу, що працює на персональних комп'ютерах, про правила їх використання, недопущення потрапляння і подальшого поширення шкідливого програмного забезпечення [11].

На наше переконання, за умов, що склалися для МО України та ЗС України важливим і вкрай

необхідним є питання розробки та затвердження ІТ-стратегії, якою має передбачатися створення єдиної системи управління з власним центром обробки даних і започаткуванням роботи підрозділів з кібербезпеки. За таких обставин, нова ІТ-стратегія має передбачати практичне формування дієздатних підрозділів оборонного відомства в сфері кіберборотьби не лише на верхніх рівнях управління, а й у військових частинах (підрозділах), що комплексно забезпечуватиме надійну і захищену обробку даних. Також, доцільно внести зміни і доповнення до діючих нормативно-правових актів, що регулюють нагальні проблеми національного кіберпростору, враховуючи вимоги стандартів НАТО і міжнародних стандартів в галузі ІТ (ISO/IEC).

Отже, як показує практика цивілізованих країн світу, організація високого рівня кібероборони вимагає вирішення цілої низки важливих завдань і, насамперед, усунення прогалин у нормативно-правовій базі. Як можна було пересвідчитися, дотепер законодавством України не конкретизовано основи кібероборони, що унеможливлює адекватне формування завдань для кібервійськ, які мають відігравати провідну роль у виконанні практичних заходів кібероборони і повинні бути створені на вимогу Указу Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"» від 26.08.2021 р. № 446/2021.

Саме тому, слід розробити та ухвалити окремий Закон України «Про кібероборону України», в якому, з-поміж решти аспектів, визначити особливості національної кібероборони, її суб'єкти та об'єкти, мету (цілі), принципи і завдання, структуру побудови та управління, вимоги до підготовки кадрів, специфіку організування і реалізації. Крім того, унормувати місце і роль кібервійськ ЗС України в ній, а також – відповідні повноваження, функції та завдання органів військового управління, ряду інших державних інституцій, обов'язки, права і відповідальність посадових осіб, а також права й обов'язки громадян України та ін. Тобто, законодавчо варто передбачити необхідність реформування існуючих Військ зв'язку і кібербезпеки ЗС України в окремі спеціальні війська, зокрема, у Війська зв'язку ЗС України і Кібервійська ЗС України. Для цього доцільно врахувати досвід США та інших країн-членів НАТО. Структура, склад і чисельність новостворених Кібервійськ ЗС України мають, насамперед, окреслюватися на основі визначених для них переліку й обсягів завдань, спрямованих на забезпечення кібероборони України, їхні частини та підрозділи – входити до структури всіх видів та окремих родів військ (сил) ЗС України.

За таких умов варто переформувати сучасне Командування Військ зв'язку та кібербезпеки ЗС України у Командування сил кібероборони ЗС України. Реформоване Командування повинне займатися питаннями ведення кібернетичної, радіоелектронної та інформаційної боротьби, протидії технічним розвідкам противника та управління електромагнітним спектром. Його склад повинен включати наступні компоненти: кібервійська ЗС України; Війська радіоелектронної боротьби ЗС України, які зараз перебувають у підпорядкуванні Командування сил підтримки ЗС України; сили й засоби здійснення інформаційних операцій; структуру з управління електромагнітним спектром. У зв'язку із запропонованим, у проєктах Державних Програм розвитку ЗС України та їхнього озброєння і військової техніки, а також у Стратегічному плані застосування ЗС України та інших документах оборонного планування і планування оборони держави доречно конкретизувати мету (цілі), завдання і заходи з розвитку Кібервійськ ЗС України, вимоги до підготовки їхнього особового складу та практичне застосування.

Для повноцінного аналізу ситуації, доцільно також визнати, що на сьогодні, разом із не вирішеними кадровими, фінансовими, матеріально-технічними і нормативними проблемами, стосовно зміцнення кібероборони держави й створення ефективних Кібервійськ ЗС України, існує ще одна, більш складна. Ця проблема стосується зміни усвідомленого системно-персонального мислення і дій щодо перспектив розвитку цієї сфери. У даному випадку мається на увазі відмова від комплексного розгляду питань кібероборони, здебільшого, через призму виконання заходів кіберзахисту і кібербезпеки ЗС України й набуття ними спроможностей для виконання поставлених завдань всеохоплюючої оборони держави, першочергово її кібероборони, в кіберпросторі та через кіберпростір. Зважаючи на вищевикладені застереження, вважаємо за доцільне висловити власне бачення вирішення проблем кібероборони держави і посилення ролі кіберзахисту в ЗС України, а саме:

розробити і внести в установленому порядку на розгляд РНБО України проєкт Стратегії кібероборони України і, за таких умов, звернути увагу не лише на кіберзахисних (кібероборонних) діях об'єднаних сил/військ кібероборони, а й інших напрямах діяльності;

визначити цілі, завдання і заходи щодо розбудови об'єднаних сил/військ кібероборони, організування їх ефективної підготовки з метою подальшого використання під час відбивання збройних агресій. Пропонується вказані аспекти передбачити у проєктах Стратегії воєнної безпеки України, Стратегічному оборонному бюлетені України, Державних програмах розвитку ЗС України та їх озброєння і військової техніки, а також у проєкті Плану оборони України. Водночас, першочергово врахувати в проєкті Стратегічного плану застосування ЗС України,

інших структурних частинах сил оборони з відсічі збройній агресії;

окреслити в нормативно-правових актах структуру системи кібероборони держави, завдання, функції і склад суб'єктів її забезпечення, а також об'єкти кібероборони;

відобразити в Щорічному плані Кабінету Міністрів України заходи по реалізації Стратегії кібербезпеки України, що застосовуватимуться МО України і ГШ ЗС України з метою посилення кібероборони держави й підвищення кібероборонних спроможностей об'єднаних сил/військ кібероборони, першочергово, для виконання яких, надаватиметься допомога з боку НАТО;

унормувати термін «кібероборонні спроможності» і його поняття у Військовому стандарті 01.004.002-2019(02) «Воєнна безпека. Стратегічне планування. Терміни та визначення» від 01.01.2020 р. й внести його до Єдиного переліку (каталогу) спроможностей МО України, ЗС України та інших складових сил оборони, затвердженого Наказом МО України «Про затвердження Порядку організації та здійснення оборонного планування в МО України, ЗС України та інших складових сил оборони» від 22.12.2020 р. № 484. Використовувати цей термін під час оборонного планування і планування оборони країни;

врахувати те, що Директорат інформаційної політики в сфері оборони і стратегічних комунікацій МО України й Департамент військово-технічної політики, розвитку озброєння та військової техніки МО України, мають під час формування і реалізації воєнної й військово-технічної політики та політики військово-технічного співробітництва з іншими державами визначати пріоритети, напрями і заходи в сфері кібероборони України;

внести необхідні зміни до структури і штату Головного управління зв'язку й кібербезпеки ГШ ЗС України для підвищення його спроможностей у плануванні кібероборони держави та забезпечення належної реалізації інших повноважень ГШ ЗС України, пов'язаних із діями ЗС України у кіберпросторі;

скоригувати назву Командування Військ зв'язку та кібербезпеки ЗС України, замінивши в ній лексичну одиницю «кібербезпеки» на лексичну одиницю «кібероборони»;

окреслити в Положенні про Командування Військ зв'язку та кібероборони ЗС України виконання ним завдань з підготовки об'єднаних сил/військ кібероборони, нарощування їхніх кібероборонних спроможностей та ін.

Крім запропонованих рекомендацій, варто також звернути увагу на результати аналізу тенденцій у безпековій політиці НАТО, що був здійснений вітчизняним вченим А. Войціховським, і, на наше переконання, доцільно використати для гарантування національної кібероборони. Зокрема науковець засвідчив:

Україна потребує такої системи кібернетичної безпеки, що постійно трансформується і відповідає вимогам країн-членів НАТО, де виклики національній безпеці дедалі частіше отримують риси, відмінні від традиційних загроз. Питання захисту у кіберпросторі – невід'ємна складова реалізації державної політики в сфері забезпечення національної безпеки;

поглиблення співробітництва України з НАТО значною мірою посилює спроможності нашої країни в протидії кіберзагрозам. Завдяки використанню ресурсів Трастового фонду НАТО з кібербезпеки, Україна змогла зміцнити власний кіберзахист, а також співпраця вигідна Альянсу, оскільки дає змогу в реальних умовах випробувати технічні та організаційні рішення;

зважаючи на значний прогрес і досвід НАТО у виробленні та удосконаленні механізму забезпечення кібербезпеки країн-членів НАТО, Україна має стати активним учасником безпекових процесів. Беручи до уваги євроатлантичні прагнення України, це сприятиме покращенню її іміджу, а також впливатиме на формування організаційно-правової основи її національної кібербезпеки, залучення до Альянсу і формування моделі надійного захисту кіберпростору України;

в умовах розроблення національної системи кібербезпеки, дієвим фактором є запозичення досвіду країн-членів НАТО та їх певних органів щодо організації протидії кіберзагрозам, запровадження в Україні інформаційно-комунікаційних і технологічних стандартів НАТО, а також розвиток технічних можливостей груп реагування CERT на кібервипадки. В умовах російської агресії та запровадження практик електронного врядування питання кібербезпеки мають постійно перебувати в центрі уваги державної політики України [12].

## Висновки та перспективи подальших досліджень

Підсумовуючи зазначимо, що в статті окреслено стан, проблеми і можливі перспективи щодо покращення кіберзахзисту в Збройних Силах України**.** У цьому контексті встановлено, що кібероборона, кібербезпека і кіберзахист є самостійними й водночас різними за змістом, складовими компонентами (суб'єктами та об'єктами) в діяльності кіберпростору України. Не зважаючи на таке розмежування, мусимо констатувати, що до нині залишаються невизначеними на рівні нормативно-правових актів структура кібероборони держави, склад, функції і завдання суб'єктів її забезпечення, а також об'єкти кібероборони. Наразі виконання провідних завдань із забезпечення кібероборони і кіберзахисту держави, відповідно до чинного законодавства, покладається на Міністерство оборони України та Генеральний штаб Збройних Сил України, що покликані застосовувати заходи з кібероборони (активного кіберзахисту) для забезпечення суверенітету держави, її

обороноздатності, запобігання збройним конфліктам і відсічі збройних агресій. Визнаючи, що кіберзахист як складова кібероборони, є важливою частиною сучасної загальної оборони держави, і з метою посилити кібероборону, запропоновано низку можливих, на думку авторів статті, рекомендацій для Міністерства оборони України і Збройних Сил України. На наше переконання, формування і реалізація державної політики України в сфері оборони мають здійснюватися з урахуванням пріоритетів, напрямів й заходів щодо кібероборони, кібербезпеки, кіберзахисту, а також у співпраці з НАТО.

Перспективи подальших досліджень полягають у вивченні специфіки залучення провідних засобів кіберзахисту в Збройних Силах України.

## *Література*


**1. Грицюк Ю.І.** Кіберінтервенція та кібербезпека України: проблеми та перспективи їх подолання. *Науковий вісник НЛТУ України.* 2016. Вип. 26. С. 8. **2. Грищук Р.В., Даник Ю.Г.** Основи кібернетичної безпеки: монографія. Житомир : ЖНАЕУ, 2016. 636 с. **3. Дубов Д.В., Ожеван М.А.** Кібербезпека: світові тенденції та виклики для України. Київ : Вид-во НІСД, 2011. 30 с. **4. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В.** Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ : ДУТ, 2015. 288 с. **5. Кирилюк Р., Шелест Є.** Кібервійська як складова трансформації системи національної безпеки. *Оборонний вісник :* Центр воєнної політики та політики безпеки. 2021. № 9. С. 4–10. **6. Климчик О.О**. Кримінально-правова кваліфікація використання комп'ютерних технологій для вчинення терористичних актів. *Інформаційна безпека людини, суспільства, держави.* 2010. №1 (3). С. 26–30. **7. Ліпкан В.А., Ліпкан О.С.** Національна і міжнародна безпека у визначеннях та поняттях. Київ : Текст, 2008. 400 с. **8. Мельник С.В., Кащук В.І.** Актуальні напрями попередження правопорушень у кіберпросторі як складова стратегії кібернетичної безпеки держави. *Інформаційна безпека: виклики і загрози сучасності* : зб. матеріалів наук.-практ. конф. 5 квітня 2013 р., м. Київ. Київ : Наук.-вид. центр НА СБ України, 2013. 416 с. **9. Шеломенцев В.П.** Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. Вип. 1. С. 312–320. **10. Стратегія** програми НАТО з удосконалення військової освіти (DEEP) в частині забезпечення дистанційного навчання. 2021. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230208-deep-strategy-for-distance-learni-1.pdf (дата звернення: 05.12.2022). **11. Дідик В. О., Гончарук А. А., Сімоненкова І. В.** Кіберзахист в Збройних Силах України для протидії можливим варіантам кіберзлочинності. *Кібербезпека в Україні: правові та організаційні питання*: матер. Всеукр. наук.-практ. конф. (м. Одеса, 17 листопада 2017 р.). Одеса: Одес. держ. ун-т внутр. спр., 2017. С. 94–95. **12. Войціховський А. В.** Кібербезпека як напрям євроатлантичної інтеграції України. *Право і безпека у контексті європейської та євроатлантичної інтеграції*: збірник статей та тез наукових повідомлень за матеріалами дискусійної панелі II Харківського міжнародного юридичного форуму, м. Харків, 28 вересня 2018 р. / редкол: Ю. Г. Барабаш, Т. М. Анакіна, Д. В. Аббакумова. Харків : Право, 2018. С. 42–48. **13. Закон України** «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 05.12.2022). **14. Закон України** «Про оборону України» від 06.12.1991 р. № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 05.12.2022). **15. Указ Президента України** «Про Положення про Генеральний штаб Збройних Сил України» від 30.01.2019 р. № 23/2019. URL: https://zakon.rada.gov.ua/laws/show/23/2019#Text (дата звернення: 05.12.2022). **16. Указ Президента** України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 05.12.2022). **17. Указ Президента України** «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави"» від 26.08.2021 р. № 446/2021. URL: https://zakon.rada.gov.ua/laws/show/446/2021#Text (дата звернення: 05.12.2022). **18. Указ Президента України** «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» від 17.09.2021 р. № 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121 (дата звернення: 05.12.2022).


## PROBLEMATIC ASPECTS OF CYBER DEFENSE: PLACE AND ROLE OF CYBER DEFENSE IN THE ARMED FORCES OF UKRAINE


***Olexandr Ternovyy*[1]**
***Oleksii Shkurenko*[2]**
***Liudmyla Minenko (Ph.D.)*[3]**

***The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine***



*The article discusses the problematic aspects of our country's cyber defense, as well as the place and role of cyber defense in the Armed Forces of Ukraine. The authors emphasizes that the formation of the information society has led to numerous cyber threats. It is shown that cyberspace not only provides resources and opportunities, but also carries certain problems that are destructive in nature and pose a threat to the existence of the State, its functioning and development. The authors emphasizes that Ukraine is not among the leading*

*countries in the field of information and communication technologies and cyber defense among the civilized countries of the world. It is argued that such areas of scientific research are extremely relevant because cyber defense is strategically important both in the civilian sphere and in the military sphere. It has been proven that in times of war, Ukraine is one of the countries most affected by cyber threats. The main danger in this sense is posed by the Russian Federation as a military aggressor. It is emphasized that this is why one of the main tasks of today is to ensure cybersecurity. The authors analyzes scientific works on the topic of the article, systematizes and characterizes the content of Ukraine's regulatory legal acts in the field of cybersecurity, and highlights the measures envisaged to prepare for countering information aggression and cyber attacks. It is noted that today there are a number of problematic issues related to the cyber defense of the State that need to be urgently addressed. The authors groups and presents a number of practical recommendations for the Ministry of Defense of Ukraine and the Armed Forces of Ukraine regarding the expediency of taking regulatory and administrative steps and using an algorithm for their implementation.*

***Keywords:*** *cyberspace; interactive information environment; cyber defense; cybersecurity; cyber threats; cyber defense; recommendations for state cyber defense.*

## *References*

**1. Hrytsiuk, Yu. I.** (2016). Cyber Intervention and Cybersecurity in Ukraine: Problems and Prospects for Overcoming Them. Naukovyi visnyk, 26, 8. **2. Hryshchuk, R. V., Danyk, Yu. H.** (2016). Basics of cyber security: monohrafiia. Zhytomyr : ZhNAEU, 636. **3. Dubov, D. V., Ozhevan, M. A.** (2011). Cybersecurity: global trends and challenges for Ukraine. Kyiv: Vyd-vo NISD, 30. **4. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., Toliupa, S. V.** (2015). Information and cybersecurity: the socio-technical aspect: pidruchnyk. Kyiv : DUT, 288. **5. Kyryliuk, R., Shelest, Ye.** (2021). Cyber Forces as a Component of the National Security System Transformation. Oboronnyi visnyk : Tsentr voiennoi polityky ta polityky bezpeky, 9, 4–10. **6. Klymchyk, O. O.** (2010). Criminal Legal Qualification of the Use of Computer Technologies for Committing Terrorist Acts. Informatsiina bezpeka liudyny, suspilstva, derzhavy, 1(3), 26–30. **7. Lipkan, V. A., Lipkan, O. S.** (2008). National and international security in definitions and concepts. Kyiv : Tekst, 400. **8. Melnyk, S. V., Kashchuk, V. I.** (2013). Current Areas of Prevention of Offenses in Cyberspace as a Component of the State's Cyber Security Strategy: zb. materialiv nauk.-prakt. konf. 5 kvitnia 2013 r., m. Kyiv. Kyiv : Nauk.-vyd. tsentr NA SB Ukrainy, 416. **9. Shelomentsev, V. P.** (2012). Legal support of the cyber security system of Ukraine and the main directions of its improvement. Fighting organized crime and corruption (theory and practice), 1, 312–320. **10. Strategy of the NATO** Defence Education Enhancement Program (DEEP) in terms of distance learning. (2021). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230208-deep-strategy-for-distance-learni-1.pdf (data zvernennia: 05.12.2022). **11. Didyk, V. O., Honcharuk, A. A., Simonenkova, I. V.** (2017). Cybersecurity in the Armed Forces of Ukraine to counter possible variants of cybercrime. Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia: mater. Vseukr. nauk.-prakt. konf. (m. Odesa, 17 lystopada 2017 r.). Odesa: Odes. derzh. un-t vnutr. spr., 94–95. **12. Voitsikhovskyi, A. V.** (2018). Cybersecurity as a direction of Ukraine's Euro-Atlantic integration. Pravo i bezpeka u konteksti yevropeiskoi ta yevroatlantychnoi intehratsii: zbirnyk statei ta tez naukovykh povidomlen za materialamy dyskusiinoi paneli II Kharkivskoho mizhnarodnoho yurydychnoho forumu, m. Kharkiv, 28 veresnia 2018 r. / redkol: Yu. H., Barabash, T. M., Anakina, D. V., Abbakumova. Kharkiv : Pravo, 42–48. **13. Law of Ukraine** «On the Basic Principles of Ensuring Cybersecurity of Ukraine», 05.10.2017, 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (data zvernennia: 05.12.2022). **14. Law of Ukraine** «On Defense of Ukraine», 06.12.1991, 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (data zvernennia: 05.12.2022). **15. Decree of the President of Ukraine** «On the Regulation on the General Staff of the Armed Forces of Ukraine», 30.01.2019, 23/2019. URL: https://zakon.rada.gov.ua/laws/show/23/2019#Text (data zvernennia: 05.12.2022). **16. Decree of the President of Ukraine** «On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"», 26.08.2021, 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (data zvernennia: 05.12.2022). **17. Decree of the President of Ukraine** «On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On Urgent Measures for the State's Cyber Defense"», 26.08.2021, 446/2021. URL: https://zakon.rada.gov.ua/laws/show/446/2021#Text (data zvernennia: 05.12.2022). **18. Decree of the President of Ukraine** «On the Decision of the National Security and Defense Council of Ukraine of August 20, 2021 "On the Strategic Defense Bulletin of Ukraine"», 17.09.2021, 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121 (data zvernennia: 05.12.2022).

DOI:**10.33099/2311-7249/2023-46-1-32-40**

УДК: 351.865

***Євген Олександрович Живило*** *(кандидат наук з державного управління)*[1]
***Валентин Миколайович Докіль***[2]

[1] ***Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, Київ, Україна***
[2] ***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# МОДЕЛЬ МЕТОДИКИ ОЦІНЮВАННЯ СПРОМОЖНОСТЕЙ ВІЙСЬК ЗВ'ЯЗКУ ТА КІБЕРБЕЗПЕКИ ЗБРОЙНИХ СИЛ УКРАЇНИ ЩОДО ВИКОНАННЯ ЗАВДАНЬ З ВІДБИТТЯ ВОЄННОЇ АГРЕСІЇ В КІБЕРПРОСТОРІ

*Інновації керували військовою стратегією з часу появи людства. Винахід пороху, органної гармати та двигуна внутрішнього згоряння мали величезний вплив не лише на тенденції розвитку військової стратегії, а й на всю хронологію світової історії. Не стало винятком і XX століття. Інтернет, що розвивається, продовжує розширювати можливості інформаційних технологій. Але, як й інші великі винаходи, його можливості часто використовуються задля досягнення негативних цілей та результатів. Сьогодні, в ході повномасштабного російського вторгнення в Україну, наше суспільство і держава зіткнулися з новою загрозою, що має значний військовий і геополітичний потенціал. За короткий проміжок часу, вразливості системи управління технологічними процесами, що мають єдині системи електронних комунікацій, перетворились на ефективний імовірний набір реальних і потенційних загроз національній безпеці України у кіберпросторі. Зазначені загрози здатні порушити штатний режим функціонування комунікаційних систем спеціальних користувачів, у тому числі зрив та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами. За таких умов, ключову роль у підтриманні сталого функціонування таких систем у складі сил безпеки та оборони України відіграють Війська зв'язку та кібербезпеки Збройних Сил України. Так, порядок організації проведення оцінювання спроможностей у Збройних Силах України, як елемент планування на основі спроможностей, здійснюється з урахуванням підходів, прийнятих у держав-членів НАТО. Зазначена сфера застосування охоплює питання методології процесу організації проведення оцінювання спроможностей, визначення учасників цього процесу, процедури і порядку його проведення, взаємозв'язку з іншими процесами, використання результатів цієї діяльності.*

*Наразі Законом України «Про національну безпеку України» внормовано питання оцінювання спроможностей, в рамках якого поставлено завдання до розроблення відповідних методик щодо прогнозування, виявлення та надання оцінки загрозам національної безпеки держави в кіберпросторі та через кіберпростір. Окремо слід підкреслити необхідність визначення порядку організації проведення оцінювання спроможностей, розроблення методики оцінювання спроможностей військ зв'язку та кібербезпеки Збройних Сил України із виконання завдань з відбиття воєнної агресії в кіберпросторі.*

***Ключові слова:*** *цифрове суспільство; інформаційно-комунікаційні системи; оцінювання спроможностей; кіберзагрози; кібербезпека; кіберпростір.*

## Вступ

**Постановка проблеми.** Оцінювання спроможностей – це процес, який є складовою частиною планування на основі спроможностей. Планування на основі спроможностей – процес, який здійснюється періодично під час оборонного огляду та циклів середньострокового планування і зосереджується на визначенні перспективних спроможностей, структури і складу Збройних Сил України (далі – ЗС України) на довгострокову перспективу з урахуванням майбутнього безпекового та оперативного середовища і встановлених ресурсних обмежень.

Доволі часто, в ході здійснення планування на основі спроможностей низка органів військового управління (далі – ОВУ) проводить формальне відпрацювання зазначеного заходу. Мають місце: не узгоджені із завданнями пропозиції, що визначені Указом Президента України «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» від 17.09.2021 р. № 473/2021 і Наказом Міністерства оборони України «Про затвердження Основних напрямів підготовки до відбиття воєнної агресії у кіберпросторі (підготовки та ведення кібероборони) у системі Міністерства оборони України» від 01.04.2019 р. № 10/ДСК; неузгодженість пропозицій відповідно до

положень Єдиного переліку (каталогу) спроможностей Міністерства оборони України та ЗС України. При цьому виконавцями зазначених пропозицій не розкривається, а нерідко і не включається інформація про критерії оцінювання та їх результати, власне, очікувані результати у процесі життєвого циклу, джерела та обсяг фінансування (виділення інших ресурсів) взагалі не обґрунтовується.

Враховуючи зазначене, постає доволі серйозна проблематика щодо визначення складових елементів самих спроможностей Військ зв'язку та кібербезпеки ЗС України, в частині виконання завдань з кібербезпеки і, як похідна, розроблення методик їх оцінювання під час виконання завдань з відбиття воєнної агресії в кіберпросторі (далі – КП).

**Аналіз останніх досліджень і публікацій.** В умовах глобалізації світу окрема держава практично не може протистояти можливим кіберзагрозам (далі – КЗаг) сучасності без інформаційного обміну з іншими. Нормативно-правовою базою (далі – НПБ) України [1; 2; 3; 4] значна увага надається співпраці з ЄС, НАТО та іншими міжнародними суб'єктами із забезпечення безпеки КП та спільного захисту від КЗаг, в тому числі, у військовій та оборонній сферах. Дуже важливим індикатором готовності систем кібербезпеки (далі – КБ) та кібероборони (далі – КО) держав-партнерів є досягнення визначеного рівня їх інтероперабельності. Але, в ході проведення чисельних консультацій, практичних навчань, науково-практичних конференцій, семінарів і тренінгів, що займають значне місце серед різноманітних заходів програм взаємодії між Україною – НАТО та США у сфері КБ, були виявлені суперечності базового термінологічного апарату, що, як мінімум, знижує ефективність заходів та не дозволить в майбутньому ефективно виконувати завдання передбачені [2; 5; 6] та рядом інших домовленостей. Аналіз існуючих законів України та інших нормативно-правових актів України [2; 5; 6], ЄС, НАТО, провідних країн світу, зокрема США, свідчить про дефініційну, термінологічну та нормативно-правову невизначеність або/та розбіжність об'єктно-предметної області декількох десятків понять, що складають базовий термінологічний набір терміносистеми сфери КБ та КО, зокрема таких як «кібербезпека», «кіберзахист», «кіберзброя», «кібероборона», «кібертероризм», «кіберпростір» тощо [7]. Так, США, Міжнародна спілка з телекомунікацій (ITU), Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) розглядають КП як сферу діяльності складних технічних систем, а в Україні – складних соціотехнічних систем [8; 9; 10; 11].

В цілому, розвиток та широке впровадження систем і комплексів зв'язку з використанням інноваційних інформаційних та комунікаційних технологій в системах військового призначення відбувається у відповідності до міжнародних правил ведення кібервійн на зразок Женевської конвенції. Водночас, основні принципи формування систем КБ та КО провідних країн світу науково обґрунтовані законодавчо, врегульовані НПБ та дефініційно-термінологічно визначені на державному рівні. За таких умов трансформування НПБ відбувається під впливом постійної мілітарізації національних сегментів КП з урахуванням критеріїв (індикаторів) загроз у сфері КБ та КО провідних держав, рівня готовності систем та набуття відповідних спроможностей тощо.

Сьогодні, для організації та проведення оцінювання спроможностей, в ЗС України використовуються чинні національні стандарти, методики та керівництва, також – міжнародні практики, описані відповідними стандартами і публікаціями НАТО. Зокрема, для проведення оцінювання спроможностей організаційно-штатними структурами (далі – ОШС) використовуються такі документи:

Рекомендації з оборонного планування на основі спроможностей в Міністерстві оборони України (далі – МО України) та ЗС України, затверджені Міністром оборони України 12.06.2017 р.;

Військовий стандарт ВСТ 01.004.005-2017(01) «Воєнна політика, безпека та стратегічне планування. Стратегічне планування розвитку спроможностей Збройних Сил України. Абревіатури»;

Військовий стандарт ВСТ 01.004.006-2017(01) «Воєнна політика, безпека та стратегічне планування. Стратегічне планування розвитку спроможностей ЗС України. Терміни та визначення»;

Стандарт НАТО (Allied Forces Standard) AFS Vol. I (General force standards) – загальні вимоги до спроможностей військ (сил);

Стандарт НАТО AFS Vol. II (Standards for Land Forces) – вимоги до спроможностей сухопутних військ;

Стандарт НАТО AFS Vol. III (Standards for Air Forces) – вимоги до спроможностей повітряних сил;

Стандарт НАТО AFS Vol. IV (Standards for Maritime Forces) – вимоги до спроможностей військово-морських сил;

Стандарт НАТО AFS Vol. V (Joint Headquarters) – вимоги до спроможностей об'єднаних штабів;

Стандарт НАТО AFS Vol. X (Standards for Special Operations Forces) – вимоги до спроможностей спеціальних операцій.

**Метою статті** є визначення показників оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України із виконання завдань із відбиття воєнної агресії в КП для формування методики оцінювання спроможностей військ

зв'язку та кібербезпеки ЗС України в ході їх підготовки та застосування.

## Виклад основного матеріалу дослідження

Нормативно-правові акти МО України та ЗС України, більшість з яких має обмеження доступу, видаються відповідно до вимог законів України, підзаконних актів державних органів, уповноважених у сферах комунікації (телекомунікації), інформатизації, захисту інформації тощо [12; 13; 14]. Разом із тим, спираючись на [13; 14], є можливим й доцільним цитування в частині КЗ інформаційно-комунікаційних систем (далі – ІКС) військового призначення, окремих положень та завдань з нормативно-правових актів МО України і ЗС України, які не є інформацією з обмеженим доступом. Так, визначено, що функціональна складова КЗ включає системи на:

запобігання (англійською мовою – «Prevention») – заходи щодо завчасного виявлення, уникнення, стримування, запобігання можливих (потенційних) КЗаг чи кібератак, припинення підготовки до них;

захисту (англійською мовою – «Protection») – заходи щодо забезпечення випереджувального захисту від можливих кібератак (кібервпливу) противника, в першу чергу, в інтересах всебічного та сталого забезпечення у КП процесів управління власними військами;

попередження (англійською мовою – «Mitigation») – заходи щодо безпосереднього виявлення, відвернення загрози, зменшення можливих втрат (збитків, пошкоджень) у разі безпосередньої загрози проведення кібератак;

реагування (англійською мовою «Response») – заходи комплексного реагування на вплив противника, у тому числі заходи захисту власної інфраструктури, особового складу, активів та ресурсів, тощо;

відновлення (англійською мовою – «Recovery») – заходи, спрямовані на відновлення інформаційної та іншої інфраструктури, що стала об'єктом кібератак противника, стабілізацію ситуації та ліквідації інших негативних наслідків.

Відповідним ОВУ, що здійснює управління військовими ОШС, які уповноважені на виконання вищезазначених функцій, визначені завдання щодо:

співпраці (реалізації спільних проектів та заходів, підтримання взаємодії) у межах повноважень з суб'єктами забезпечення воєнної безпеки та КБ держави, а також з НАТО, Європейським Союзом, державами-партнерами в частині спільного виконання завдань КО;

реагування (практичного виконання необхідних заходів) на поточні загрози КБ у воєнній сфері шляхом їх попередження, завчасного виявлення, випереджувального реагування на них, усунення (мінімізації, ліквідації наслідків) їх впливу;

здійснення КЗ власної інформаційної інфраструктури (далі – ВІІ) (засобів рухомого зв'язку, як апаратної, так і контентної складових, додатків та сервісів зв'язку, інших ІКС та об'єктів інформаційної діяльності суб'єктів оборони держави) від кібератак та кібервпливу противника, що забезпечує необхідний рівень інформаційного забезпечення управління військами та зброєю, інші дії в КП тощо.

У 2016 р. введена в дію Стратегія кібербезпеки України [1], яка системно базувалася на положеннях Конвенції про кіберзлочинність, законодавство України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої була встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України [15] та стала першим офіційним документом, який визначив дефініцію КБ, як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в КП, що досягається комплексним застосуванням сукупності правових, організаційних та інформаційних заходів. Стратегія [1] визначила МО України та ГШ ЗС України завдання, щодо здійснення заходів з підготовки держави до відбиття воєнної агресії у КП (КО) та КЗ ВІІ. Вона передбачала гармонізацію нормативних документів України у сфері КБ відповідно до міжнародних стандартів і стандартів ЄС та НАТО. За результатами експертних оцінок, стан реалізації Стратегії за визначеними показниками не перевищує 40 %, а саме:

не розроблені індикатори виконання Стратегії кібербезпеки України;

не вирішені питання оперативного обміну інформацією про КЗаг;

недостатніми є організація і проведення наукових досліджень у сфері КБ;

не створена ефективна система підготовки кадрів;

не створено дієву модель державно-приватного партнерства.

При цьому, Національна система КБ включає в тому числі й оборонні заходи, також визначено МО України та ГШ ЗС України завдання щодо підготовки держави до відбиття воєнної агресії у КП (КО); передбачено військову співпрацю з НАТО та іншими суб'єктами оборонної сфери щодо забезпечення безпеки КП та спільного захисту від КЗаг.

Проаналізувавши існуючу НПБ щодо завдань визначених перед МО України та ЗС України з відбиття воєнної агресії в КП є необхідним наголосити, що у 2021 р. було прийнято низку логічно взаємопов'язаних (рис. 1) документів оборонного та довгострокового планування.

Відкритими документами оборонного та довгострокового планування передбачено:

здійснення заходів із підготовки держави до

відбиття воєнної агресії у КП (КО), координація діяльності державних органів та органів місцевого самоврядування щодо підготовки та ведення КО;

отримання та узагальнення від основних суб'єктів забезпечення КБ інформації щодо об'єктів критичної ВІІ воєнної сфери та сфери оборони держави;

проведення інформаційно-аналітичної діяльності та прогнозування розвитку обстановки у воєнній сфері, пов'язаної з КЗаг та КП;

підтримання сил та засобів для дій в КП в готовності до виконання завдань за призначенням, здійснення адекватного нарощування їх готовності залежно від рівня загроз та ступенів реагування на них;

забезпечення несення бойового чергування визначених сил та засобів в інтересах підготовки та ведення КО;

здійснення підготовки та застосування ЗС України в КП щодо виконання ними завдань за призначенням та безпечного використання ними КП;

здійснення розвитку необхідних спроможностей МО України, ЗС України для дій в КП, підготовки та ведення КО, створення та розвиток відповідних ОШС, їх комплектування, підготовку та всебічне забезпечення [16];

здійснення військової співпраці з НАТО, пов'язаної з безпекою КП та спільним захистом від КЗаг, в тому числі й з військовими CERT країн-членів НАТО;

формування дієвої єдиної мережі ситуаційних центрів. Розгортання ситуаційних центрів МО України та ЗС України на одній ІТ – платформі в режимі реального часу у тісній взаємодії із ситуаційними центрами органів державної влади (резервними, на рухомій базі);

використання національного спеціального програмного забезпечення, яке дозволить здійснити інформаційне-аналітичне супроводження, моніторинг, прогнозування, прийняття рішень, проведення аудиту та безпеки. Зазначені процеси повинні відбуватись в одному цифровому середовищі, надійно захищеному від зовнішнього несанкціонованого втручання та кібератак;

реалізацію сталої технічної підтримки функціонування програмно-апаратного комплексу (платформи).

Виходячи із зазначеної НПБ держави, одним із головних безпекових аспектів у воєнній сфері на національному рівні, сфері оборони і військового будівництва визначено підтримання, нарощування (розвиток) та координація із забезпечення КБ, КЗ та КО під час підготовки та ведення всеохоплюючої оборони України [17].

Нинішні спроможності військ зв'язку та кібербезпеки ЗС України щодо виконання завдань з відбиття воєнної агресії в КП складаються з сукупності показників спроможностей, а саме з:

прогнозування, виявлення та оцінки загроз національній безпеці держави в КП та через КП (кіберрозвідки);

активного КЗ (кібервпливу);

кіберзахисту.


Рис. 1. Модель формування нормативно правової бази України, МО України та ЗС України сфери КБ та КО

Зазначені показники спроможностей, в свою чергу, складаються з окремих показників виконання завдань, а саме:

1. Прогнозування, виявлення та оцінки загроз національній безпеці держави в КП та через КП (кіберрозвідка):

прогнозування та оцінка загроз національній безпеці держави в КП та через КП;

моніторинг КП, у тому числі щодо виявлення загроз в ІКС ЗС України;

здійснення розвідувальної діяльності щодо загроз національній безпеці держави у КП, інших подій і обставин, що стосується сфери КБ;

заходів, щодо виявлення уразливостей об'єктів КО, у тому числі шляхом моделювання, тестування на уразливість від КЗаг (кібератак), тощо;

оперативного інформаційного обміну між суб'єктами забезпечення КБ держави, щодо реалізованих та потенційних КЗаг;

інфомаційно-аналітичної діяльності та прогнозування розвитку обстановки у воєнній сфері, пов'язаній з КЗаг та КП.

2. Активного КЗ (кібервплив):

підготовки і проведення скоординованих заходів у КП суб'єктами КО (у тому числі щодо підготовки ВІІ) з метою запобігання виникнення воєнних конфліктів, стримування та відсічі воєнної агресії;

здатності зі створення сприятливих умов у КП для застосування ЗС України, інших військових формувань та правоохоронних органів, їх ефективних дій в КП, сприяння забезпеченню інформаційної безпеки держави у воєнній сфері;

реагування на поточні загрози КБ у воєнній сфері шляхом їх запобігання, завчасного виявлення, стримування та випереджувального реагування на них, усунення (мінімізації,

ліквідації) її наслідків;

порушення функціонування ВІІ противника, систем (процесів) прийняття ним рішень та здійснення управління військами (силами) під час одночасного захисту власного КП;

спроможності щодо проведення розвідувальним органом МО України відповідно до компетенції заходів протидії зовнішнім загрозам національній безпеці України у КП;

випереджувального та/або оперативного реагування на проведення противником заходів у КП та через КП, мінімізація результатів їх впливу;

з отримання доступу (у тому числі фізичного) до ВІІ противника, у тому числі на контрольованій ним території;

проведення заходів фізичного впливу в інтересах та під час ведення КО, у тому числі шляхом виведення з ладу особового складу, озброєння, технічних засобів, комунікацій противника, а також проведення спеціальних дій (диверсій), вогневого ураження, інших форм кінетичного та іншого впливу, що призводить до припинення функціонування, механічного руйнування, пошкодження конструкції, виведення з ладу або знищення фізичного об'єкта ВІІ (його інформаційних ресурсів) та суб'єктів інформаційної діяльності, сил і засобів інформаційних (кібер) операцій;

проведення правових, організаційних, технічних заходів припинення функціонування (блокування) об'єктів ВІІ в інтересах підготовки та ведення КО;

створення електромагнітних перешкод, радіоелектронного придушення роботи телекомунікаційних та інших засобів в інтересах КО;

спроможності щодо спеціальних дій підрозділів спеціального призначення та інформаційно-психологічних операцій в інтересах КО.

3. Кіберзахист:

КЗ ІКС ЗС України (статистичний та мобільний КЗ);

КЗ систем управління озброєнням та військовою технікою;

КЗ (участь у заходах КЗ) об'єктів критичної ІІ держави в умовах правового режиму надзвичайного та воєнного стану;

КЗ об'єктів інфраструктури МО України, ЗС України, Державної спеціальної служби транспорту (арсеналів, баз, складів, позицій чергування засобів ППО, місць базування авіації та ВМС, спеціальних споруд тощо).

Модель методики оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України щодо виконання завдань з відбиття воєнної агресії в КП можна навести такою логіко-структурною схемою (рис. 2).

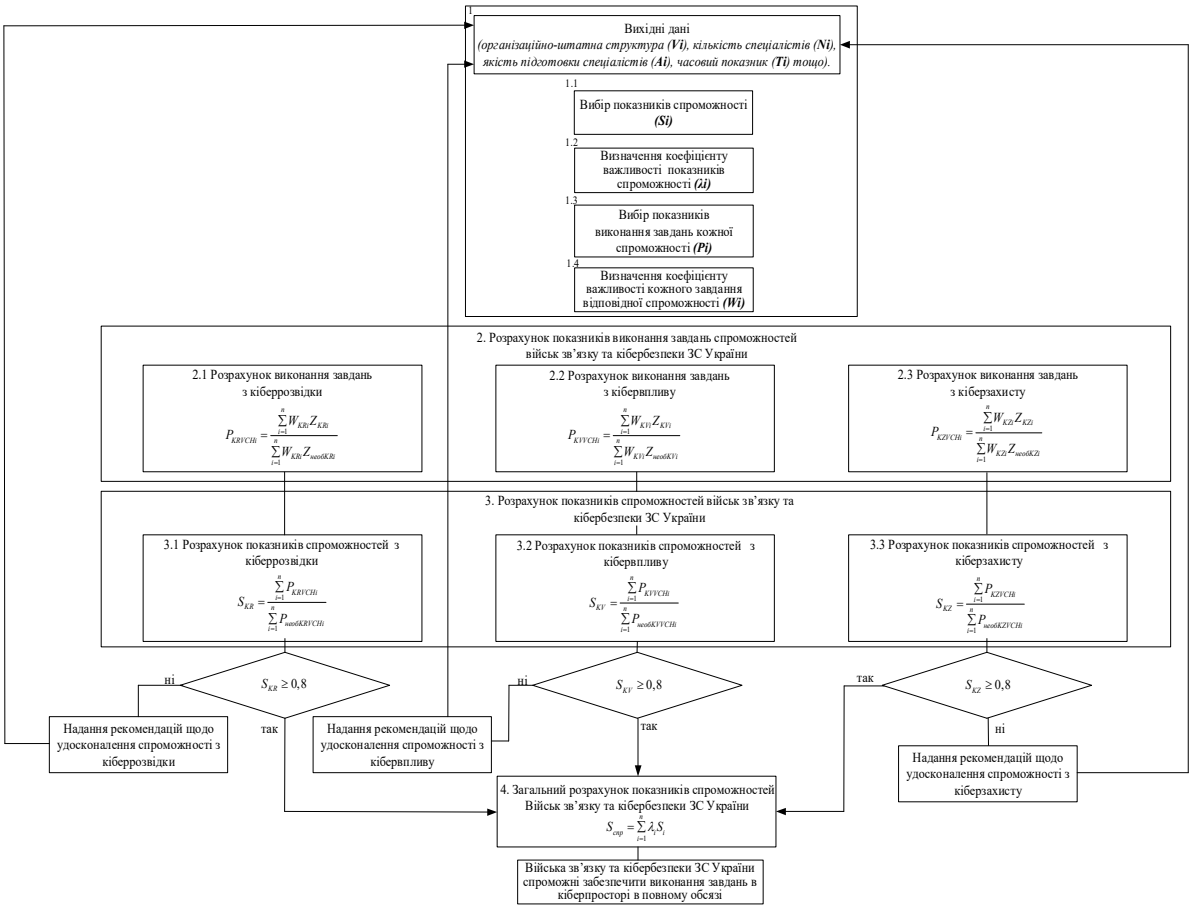



Рис. 2. Логіко-структурна схема моделі методики оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України щодо виконання завдань з відбиття воєнної агресії в кіберпросторі

Запропонована модель методики дає можливість послідовно крок, за кроком проводити розрахунок спроможностей військ зв'язку та кібербезпеки ЗС України із виконання завдань з відбиття воєнної агресії в КП. По даній методиці розрахунок спроможностей військ зв'язку та кібербезпеки ЗС України щодо виконання завдань з відбиття воєнної агресії в КП займає дуже багато часу та сил, але затрачені зусилля на проведення розрахунків спроможностей компенсуються отриманим, об'єктивним результатом. Зазначене, дає змогу найбільш ефективно застосовувати війська зв'язку та кібербезпеки ЗС України для виконання бойових задач із КБ та активних дій, від характеру виконання загальних дій яких залежить якість, ефективність, мобільність, оперативність управління військами (силами) в операціях. При цьому пропорційно збільшуються показники з бойового потенціалу військ зв'язку та кібербезпеки ЗС України в ході планування на їх бойове застосування.

Для оцінки спроможностей військ зв'язку та кібербезпеки ЗС України в частині виконання завдань з відбиття воєнної агресії в КП в цілому необхідно оцінити виконання окремих завдань кожної спроможності, а саме:

1. Прогнозування, виявлення та оцінка загроз національній безпеці держави в КП та через КП (здійснення кіберрозвідки) (табл. 1).

Таблиця 1

Оцінювання спроможностей військ зв'язку та кібербезпеки в частині виконання завдань із кіберрозвідки

| Показник $KRVCHi$ | Розрахунок показника $P_{KRVCHi}$ |
|---|---|
| Головний об'єднаний ЦЗІ та КБ ЗС України, у складі: | $P_{KRVCHi}$ |
| ЦЗІ та КБ | $P_{KRVCHi}$ |
| … | … |
| ЦЗІ та КБ | $P_{KRVCHi}$ |
| … | $P_{KRVCHi} = \frac{\sum_{i=1}^{n} W_{KRi} Z_{KRVCHi}}{\sum_{i=1}^{n} W_{KRi} Z_{max KRVCHi}}$ |
| $S_{KR}$ – показник спроможності військ зв'язку та кібербезпеки ЗС України щодо виконання завдань з кіберрозвідки загалом | $S_{KR} = \frac{\sum_{i=1}^{n} P_{KRVCHi}}{\sum_{i=1}^{n} P_{max KRVCHi}}$ |

де $P_{KRVCHi}$ – загальний показник оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України в частині виконання завдань із кіберрозвідки;

$Z_{KRVCHi}$ – показник оцінювання окремого завдання з кіберрозвідки за кожну визначену військову частину військ зв'язку та кібербезпеки ЗС України;

$W_{KRi}$ – коефіцієнт важливості виконання кожного окремого завдання з кіберрозвідки.

Показник спроможності військ зв'язку та кібербезпеки ЗС України з кіберрозвідки загалом розраховується, як зважена та нормована оцінка показників здатності виконання завдань з кіберрозвідки.

2. Активного КЗ (здійснення кібервпливу). (табл. 2).

Таблиця 2

Оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України в частині виконання завдань з кібервпливу

| Показник $KVVCHi$ | Розрахунок показника $P_{KVVCHi}$ |
|---|---|
| Головний об'єднаний ЦЗІ та КБ ЗС України, у складі: | $P_{KVVCHi}$ |
| ЦЗІ та КБ | $P_{KVVCHi}$ |
| … | … |
| ЦЗІ та КБ | $P_{KVVCHi}$ |
| … | $P_{KVVCHi} = \frac{\sum_{i=1}^{n} W_{KVi} Z_{KVVCHi}}{\sum_{i=1}^{n} W_{KVi} Z_{max KVVCHi}}$ |
| $S_{KV}$ – показник спроможності військ зв'язку та кібербезпеки ЗС України виконання завдань з кібервпливу загалом | $S_{KV} = \frac{\sum_{i=1}^{n} P_{KVVCHi}}{\sum_{i=1}^{n} P_{max KVVCHi}}$ |

де $P_{KVVCHi}$ – загальний показник оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України в частині виконання завдань з кібервпливу;

$Z_{KVVCHi}$ – показник оцінювання окремого завдання з кібервпливу за кожну визначену військову частину військ зв'язку та кібербезпеки ЗС України;

$W_{KVi}$ – коефіцієнт важливості виконання кожного окремого завдання з кібервпливу.

Показник спроможності військ зв'язку та кібербезпеки ЗС України з кібервпливу загалом розраховується, як зважена та нормована оцінка показників здатності виконання завдань з кібервпливу.

3. Кіберзахист (здійснення КЗ) (табл. 3).

Таблиця 3

Оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України в частині виконання завдань з кіберзахисту

| Показник $KZVCHi$ | Розрахунок показника $P_{KZVCHi}$ |
|---|---|
| Головний об'єднаний ЦЗІ та КБ ЗС України, у складі: | $P_{KZVCHi}$ |
| ЦЗІ та КБ | $P_{KZVCHi}$ |
| … | … |
| ЦЗІ та КБ | $P_{KZVCHi}$ |
| … | $P_{KZVCHi} = \frac{\sum_{i=1}^{n} W_{KZi} Z_{KZVCHi}}{\sum_{i=1}^{n} W_{KZi} Z_{max KZVCHi}}$ |
| $S_{KZ}$ – показник спроможності військ зв'язку та кібербезпеки ЗС України виконання завдань з кіберзахисту загалом | $S_{KZ} = \frac{\sum_{i=1}^{n} P_{KZVCHi}}{\sum_{i=1}^{n} P_{max KZVCHi}}$ |

де $P_{KZVCHi}$ – загальний показник оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України в частині виконання завдань з кіберзахисту;

$Z_{KZVCHi}$ – показник оцінювання окремого завдання з кіберзахисту за кожну визначену військову частину військ зв'язку та кібербезпеки

ЗС України;

$W_{KZi}$ – коефіцієнт важливості виконання кожного окремого завдання з кіберзахисту.

Показник спроможності військ зв'язку та кібербезпеки ЗС України з кіберзахисту загалом розраховується, як зважена та нормована оцінка показників здатності виконання завдань з кіберзахисту.

Якщо показники $S_{KR} \geq 0{,}8, S_{KV} \geq 0{,}8, S_{KZ} \geq 0{,}8$, то для оцінки спроможності військ зв'язку та кібербезпеки ЗС України щодо виконання завдань з відбиття воєнної агресії в КП в цілому розраховуємо загальний коефіцієнт виконання спроможностей:

$$S_{спр} = \sum_{i=1}^{n} \lambda_i S_i,$$

де $S_i - S_{KR}, S_{KV}, S_{KZ}$ – спроможність військ зв'язку та кібербезпеки ЗС України до виконання завдань з кіберрозвідки, кібервпливу та кіберзахисту загалом;

$\lambda_i$ – коефіцієнт важливості показника кожної спроможності.

$S_{спр}$ – спроможність військ зв'язку та кібербезпеки ЗС України виконувати завдання з відбиття воєнної агресії в кіберпросторі в повному обсязі.

Водночас, слід пам'ятати, що проведення аналізу відповідності окремих спроможностей, груп спроможностей, функціональних груп спроможностей, чи органів військового управління (військ зв'язку та кібербезпеки ЗС України) та здійснення їх оцінювання проводиться відповідно до сценаріїв оборонного планування. Результатом зазначеного аналізу є вироблення обґрунтованих рекомендацій для формування узгоджених, реалістичних та прийнятних рішень (матеріальних і нематеріальних) з розвитку відповідних спроможностей.

Типовими проблемами під час виконання процесу оцінювання спроможностей можуть бути:

неможливість досягти визначених, в ході оборонного огляду спроможностей, в реальних умовах (потребує матеріальних рішень);

недостатні кількісні та якісні показники спроможності (потребує матеріальних і нематеріальних рішень);

закінчення життєвого циклу носіїв спроможності (потребує матеріальних рішень);

політичні обмеження, які унеможливлюють досягнення окремих спроможностей (необхідні нематеріальні рішення).

Отже, загалом, процедура оцінювання спроможностей передбачає: порівняння наявних спроможностей з тими, які будуть потрібні у майбутньому; виявлення недоліків у вимогах до спроможностей; встановлення нових чи оновлення існуючих вимог. Водночас, у ході оцінювання спроможностей розробляються рекомендації щодо проведення відповідних змін одночасно у всіх споріднених організаційних структурах та носіях відповідних спроможностей.

## Висновки й перспективи подальших досліджень

Отже, в межах розгляду шляхів розбудови національної системи КБ, на основі досвіду провідних країн світу з протистояння в КП, встановлено, що провідні держави світу дедалі більше уваги надають розвитку й захисту власних інформаційних ресурсів, а також можливості впливати на інформаційні ресурси інших країн, що загалом описується як проблема забезпечення КБ держави.

Водночас залишаються невирішеними питання в міжнародному нормативно-правовому полі, які унеможливлюють формалізацію безпекової політики в КП. Відсутній консенсус щодо правил поведінки в КП, не визначені загальноприйняті методології оцінки наслідків кіберзлочинів та їх розгляд як об'єкта міжнародних норм і правил (зокрема, щодо визнання кібератаки як акту війни).

Сьогодні, для організації та проведення оцінювання спроможностей в ЗС України використовуються існуючі національні стандарти, методики та керівництва, також використовуються міжнародні практики, описані відповідними стандартами і публікаціями НАТО.

В цілому, з огляду на зазначене, в статті визначено показники оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України із виконання завдань з відбиття воєнної агресії в КП, сформовано методику оцінювання спроможностей військ зв'язку та кібербезпеки ЗС України в ході їх підготовки та застосування.

## *Література*

**1. Указ Президента України** «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26.08.2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 23.12.2022). **2. Закон України** «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 23.12.2022). **3. Закон України** «Про оборону України» від 06.12.1991 р. № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 23.12.2022). **4. Закон України** «Про Збройні Сили України» від 6 грудня 1991 р. № 1934-XII. URL: https://zakon.rada.gov.ua/laws/show/1934-12#Text (дата звернення: 23.12.2022). **5. Ertan A.** (Eds.) Cyber Threats and NATO 2030: Horizon Scanning and Analysis: URL://https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf (дата звернення: 23.12.2022). **6. Указ Президента України** «Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України"» від 17.09.2021 р. № 473/2021 URL:

https://www.president.gov.ua/documents/4732021-40121 (дата звернення: 23.12.2022). **7. Указ Президента України** «Про Концепцію боротьби з тероризмом в Україні» від 05.03.2019 р. № 53/2019. URL: https://zakon.rada.gov.ua/laws/show/53/2019#Text (дата звернення: 23.12.2022). **8. Вдовенко С., Даник Ю., Фараон С.** Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. *Комп'ютерні науки та кібербезпека*. 2019. № 1(12). URL: https://periodicals.karazin.ua/cscs/article/view/13080 (дата звернення: 23.12.2022). **9. Звіт про науково-дослідну роботу** удосконалення понятійно-категорійного апарату у сфері кібероборони шифр «Дефініція» (заключний) № держреєстрації 0120U103696 8.06.5.035. Київ, 2020. 203 с. **10. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В.** Інформаційна та кібербезпека: соціотехнічний аспект: підручник. Київ : ДУТ, 2015. 288 с. **11. Трофименко О.** Аналіз дефініцій різновидів інформаційних війн. URL: http://conf.inf.od.ua/doklady-konferentsii/150-trofimenko (дата звернення: 23.12.2022). **12. Закон України** «Про державну таємницю» від 21.01.1994 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12#Text (дата звернення: 23.12.2022). **13. Закон України** «Про доступ до публічної інформації» від 13.01.2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 23.12.2022). **14. Закон України** «Про інформацію» № 2938-VI. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text. **5. Указ Президента України** «Про рішення Ради національної безпеки і оборони України від 06 травня 2015 року "Про Стратегію національної безпеки України"» від 26.05.2015 р. № 287 URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text (дата звернення: 23.12.2022). **16. Живило Є.** Об'єднана підготовка персоналу складових Сил оборони сфери кібербезпеки в умовах тотальної оборони держави. URL: https://tp.kh.ua/index.php/tpdu/article/view/295/273, DOI: 10.34213/tp.21.02.16. **17. Указ Президента України** «Про рішення Ради національної безпеки і оборони України від 16 лютого 2017 року "Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури" від 16 лютого 2017 року» від 16.02.2017 р. № 37/2017. URL: https://zakon.rada.gov.ua/laws/show/n0001525-17#Text. (дата звернення: 23.12.2022).

## MODEL OF ASSESSMENT OF MILITARY COMMUNICATION AND CYBER SECURITY CAPABILITIES OF THE ARMED FORCES OF UKRAINE FOR PERFORMING TASKS OF REFLECTING MILITARY AGGRESSION IN CYBER SPACE

***Yevgen Zhyvylo (Candidate of sciences in public administration)*** [1]
***Valentyn Dokil*** [2]

[1] ***Kruty Heroes Military Institute of Telecommunications and and Information Technologies***
[2] ***National Defence University of Ukraine named after Ivan Cherniakhovskyi***

*Innovation has driven military strategy since the dawn of mankind. The invention of gunpowder, the organ cannon, and the internal combustion engine had a huge impact not only on the trends in the development of military strategy, but also on the entire chronology of world history. The 20th century was no exception. The evolving Internet continues to expand the possibilities of information technology. But, like other great inventions, its capabilities are often used to achieve negative goals and results.*

*Today, in the course of the full-scale Russian invasion of Ukraine, our society and state faced a new threat that has enormous military and geopolitical potential. In a short period of time, the vulnerabilities of unified electronic communications systems, technological process management systems have turned into an effective and probable set of real and potential threats to Ukraine's national security in cyberspace. These threats are capable of disrupting the normal functioning of communication systems of special users, including disruption and/or blocking of system operation, and/or unauthorized management of its resources.*

*At the same time, the communication and cyber security forces of the Armed Forces of Ukraine play a key role in supporting the stable functioning of such systems as part of the Security and Defense Forces of Ukraine. Thus, the procedure for organizing the assessment of capabilities in the Armed Forces of Ukraine as an element of capability-based planning is carried out taking into account the approaches adopted by NATO member states.The specified field of application covers the issue of the methodology of the process of organizing the assessment of capabilities, determining the participants of this process, the procedure and order of its implementation, the relationship with other processes, and the use of the results of this activity.*

*At the same time, due to the absence of the Law of Ukraine "On the National Security of Ukraine" (revision is underway), which will regulate the issues of assessment of capabilities, it will be premature to approve any legal framework that would regulate this area of activity. Under these conditions, representatives of the Ministry of Defense and the Armed Forces of Ukraine unanimously emphasize the need to develop appropriate methods for forecasting, identifying and assessing threats to the state's national security in cyberspace and through cyberspace. Separately, it should be emphasized the need to determine the order of organization of the assessment of capabilities, the development of a methodology for assessing the capabilities of the communications and cyber security forces of the Armed Forces of Ukraine for the performance of tasks to repel military aggression in cyberspace.*

***Keywords:*** *digital society; information and communication systems; assessment of abilities; cyber threats; cyber security; cyberspace.*

## *References*

**1. Hrytsiuk, Yu. I.** (2016). Cyber Intervention and Cybersecurity in Ukraine: Problems and Prospects for Overcoming Them. Naukovyi visnyk, 26, 8. **2. Hryshchuk, R. V., Danyk, Yu. H.** (2016). Basics of cyber security: monohrafiia. Zhytomyr : ZhNAEU, 636. **3. Dubov, D. V., Ozhevan, M. A.** (2011). Cybersecurity: global trends and challenges for Ukraine. Kyiv: Vyd-vo NISD, 30. **4. Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., Toliupa, S. V.** (2015). Information and cybersecurity: the socio-technical aspect: pidruchnyk. Kyiv : DUT, 288. **5. Kyryliuk, R., Shelest, Ye.** (2021). Cyber Forces as a Component of the National Security System Transformation. Oboronnyi visnyk : Tsentr voiennoi polityky ta polityky bezpeky, 9, 4–10. **6. Klymchyk, O. O.** (2010). Criminal Legal Qualification of the Use of Computer Technologies for Committing Terrorist Acts. Informatsiina bezpeka liudyny, suspilstva, derzhavy, 1(3), 26–30. **7. Lipkan, V. A., Lipkan, O. S.** (2008). National and international security in definitions and concepts. Kyiv : Tekst, 400. **8. Melnyk, S. V., Kashchuk, V. I.** (2013). Current Areas of Prevention of Offenses in Cyberspace as a Component of the State's Cyber Security Strategy: zb. materialiv nauk.-prakt. konf. 5 kvitnia 2013 r., m. Kyiv. Kyiv : Nauk.-vyd. tsentr NA SB Ukrainy, 416. **9. Shelomentsev, V. P.** (2012). Legal support of the cyber security system of Ukraine and the main directions of its improvement. Fighting organized crime and corruption (theory and practice), 1, 312–320. **10. Strategy of the NATO** Defence Education Enhancement Program (DEEP) in terms of distance learning. (2021). URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230208-deep-strategy-for-distance-learni-1.pdf (data zvernennia: 05.12.2022). **11. Didyk, V. O., Honcharuk, A. A., Simonenkova, I. V.** (2017). Cybersecurity in the Armed Forces of Ukraine to counter possible variants of cybercrime. Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia: mater. Vseukr. nauk.-prakt. konf. (m. Odesa, 17 lystopada 2017 r.). Odesa: Odes. derzh. un-t vnutr. spr., 94–95. **12. Voitsikhovskyi, A. V.** (2018). Cybersecurity as a direction of Ukraine's Euro-Atlantic integration. Pravo i bezpeka u konteksti yevropeiskoi ta yevroatlantychnoi intehratsii: zbirnyk statei ta tez naukovykh povidomlen za materialamy dyskusiinoi paneli II Kharkivskoho mizhnarodnoho yurydychnoho forumu, m. Kharkiv, 28 veresnia 2018 r. / redkol: Yu. H., Barabash, T. M., Anakina, D. V., Abbakumova. Kharkiv : Pravo, 42–48. **13. Law of Ukraine** «On the Basic Principles of Ensuring Cybersecurity of Ukraine», 05.10.2017, 2163-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (data zvernennia: 05.12.2022). **14. Law of Ukraine** «On Defense of Ukraine», 06.12.1991, 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (data zvernennia: 05.12.2022). **15. Decree of the President of Ukraine** «On the Regulation on the General Staff of the Armed Forces of Ukraine», 30.01.2019, 23/2019. URL: https://zakon.rada.gov.ua/laws/show/23/2019#Text (data zvernennia: 05.12.2022). **16. Decree of the President of Ukraine** «On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"», 26.08.2021, 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (data zvernennia: 05.12.2022). **17. Decree of the President of Ukraine** «On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On Urgent Measures for the State's Cyber Defense"», 26.08.2021, 446/2021. URL: https://zakon.rada.gov.ua/laws/show/446/2021#Text (data zvernennia: 05.12.2022). **18. Decree of the President of Ukraine** «On the Decision of the National Security and Defense Council of Ukraine of August 20, 2021 "On the Strategic Defense Bulletin of Ukraine"», 17.09.2021, 473/2021. URL: https://www.president.gov.ua/documents/4732021-40121 (data zvernennia: 05.12.2022).

DOI:**10.33099/2311-7249/2023-46-1-41-44**

УДК: 355.45

***Рустам Камілович Мурасов (кандидат технічних наук)***
***Ярослав Вячеславович Мельник***

***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ КІБЕРПРОСТОРУ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

*Методика оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України є надзвичайно важливою через посилення загроз кібербезпеці в Україні. Об'єкти критичної інфраструктури України, такі як енергетичні мережі, транспортні системи, банківські установи, медичні та військові заклади, системи зв'язку та інші, мають велике значення для життя і діяльності національної економіки та суспільства в цілому. Зокрема, збій в роботі цих об'єктів може призвести до серйозних наслідків, таких як відключення електропостачання, зупинка транспорту, порушення фінансової стабільності, порушення медичного обслуговування та ін. За таких умов, захист кіберпростору об'єктів критичної інфраструктури стає надзвичайно важливим завданням для держави та бізнесу. Для досягнення цієї мети необхідно мати ефективну методику оцінювання захищеності кіберпростору об'єктів критичної інфраструктури, яка дає змогу виявляти потенційні загрози та ризики, а також розробляти та впроваджувати заходи з підвищення кібербезпеки. В статті наведено теоретичні викладки, що пов'язують між собою розуміння державою принципів функціонування сучасних кібернетичних загроз та пошуку механізмів їх вирішення. Встановлено, що забезпечення національної (воєнної) безпеки поки не здійснюється за рахунок належної концепції. За результатами оцінювання захищеності кіберпростору об'єктів критичної інфраструктури визначено практичні шляхи зміцнення воєнної безпеки України через пошук ефективної стратегії кібербезпеки.*

***Ключові слова:*** *кібератака; кібербезпека; кібероборона; мінімізація наслідків надзвичайних ситуацій; дослідження причин виникнення надзвичайних ситуацій.*

## Вступ

Методика оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України є актуальною та важливою через посилення загроз у сфері кібербезпеки України, особливо у період повномасштабної російської агресії проти України. Розробка і впровадження ефективної методики оцінювання захищеності кіберпростору об'єктів критичної інфраструктури є складним завданням, що потребує врахування багатьох факторів. Для цього потрібно використовувати сучасні технології та методи аналізу, зокрема, моніторинг і аналіз кібератак, тестування на проникнення, аудит безпеки, поради фахівців тощо. Ця методика має бути адаптована до специфіки кожного об'єкта та враховувати його унікальні особливості й потенційні загрози. Важливо також враховувати міжнародні стандарти та рекомендації щодо кібербезпеки, зокрема, ISO/IEC 27001, NIST Cybersecurity Framework, ENISA Guidelines тощо. Наслідки кібератак можуть бути катастрофічними, тому важливо проводити регулярне оцінювання захищеності кіберпростору об'єктів критичної інфраструктури та приймати заходи для підвищення захищеності. Це дає змогу зменшити ризики кібератак і забезпечити безпеку функціонування критичної інфраструктури.

**Постановка проблеми.** Багато уваги надано вирішенню та оцінюванню кібербезпеки в закордонних провідних виданнях [2], традиційно в західних наукових виданнях, і останнім часом, дане питання, глибоко вивчається в цивільних і воєнних наукових сферах російської федерації [1]. Але методологія оцінювання кібербезпеки має закритий характер, а її складова більш орієнтована на комерційну діяльність направлена на надання послуг щодо моніторингу та оцінювання кібербезпеки суб'єктів господарювання.

Вищезазначене дозволяє створити власну методику оцінювання кібернетичної безпеки, яка буде враховувати реальний стан функціонування власної кібернетичної мережі та яку буде можливо оптимізувати, за умов виявлення нових складових. Ця методика має враховувати специфіку кожного об'єкта критичної інфраструктури і враховувати його унікальні особливості та потенційні загрози. Важливо також враховувати міжнародні стандарти та рекомендації щодо кібербезпеки, забезпечити регулярне оцінювання та підвищення захищеності кіберпростору об'єктів критичної інфраструктури для запобігання наслідків кібератак і забезпечення стабільності функціонування системи в цілому.

Крім того, необхідно враховувати, що загрози кібербезпеці постійно видозмінюються, тому

методика має бути гнучкою та здатною до оновлення відповідно до нових загроз і вразливостей.

**Метою статті** є проведення оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України для визначення рівня захищеності кіберпростору таких об'єктів, що забезпечить виявлення та усунення вразливостей і потенційних загроз кібербезпеці, дасть змогу запобігти можливим кібератакам та забезпечити безперебійне функціонування системи в цілому.

## Виклад основного матеріалу дослідження

У процесі вивчення наукових робіт провідних фахівців [4] у сфері кібербезпеки (IBM, Cisco та інших відомих фірм із забезпечення кібербезпеки), аналізу наукових даних, якими можна оперувати під час оцінювання стану кібербезпеки, оптимальною методикою, що пропонується в цій роботі, є методика на основі оцінювання імовірності стійкості системи у ході здійсненні кібератак, які здатні порушити роботу кібернетичної мережі [2].

$$P_{кб} = \{0; \dots\dots; 1\} \quad (1)$$

Доцільно буде зробити декомпозицію імовірностей типів кібератак (порушення стану функціонування), як незалежні події та застосувати математичний апарат теорії імовірності – теорему повної імовірності [1]. Таким чином отримуємо імовірнісну оцінку стану кібербезпеки. Складовими імовірностями будуть такі, що обрані відповідно до статистики методів здійснення кібератак для основних джерел загроз, що були заблоковані на комп'ютерах автоматизованої системи управління (далі – АСУ) (відсоток атакованих комп'ютерів АСУ за півріччя), наведених на рис. 1 та основні платформи, що використовує шкідливе програмне забезпечення (відсоток атакованих комп'ютерів АСУ), наведених на рис. 2.).


Рис. 1. Основні джерела загроз, що були заблоковані на комп'ютерах АСУ

Відповідно до статистичних даних кіберзагроз були обрані такі імовірності здійснення кібернетичних атак (табл. 1).

Для оцінювання ступеня захищеності кіберпростору України використано відомий математичний апарат, заснований на теоремах повної імовірності та множення імовірностей [1]. Теорема повної імовірності (англ. Law of Total Probability) – повна система подій, що дорівнює сумі добутків імовірностей гіпотез на умовні ймовірності події, обчислені відповідно до кожної з гіпотез. Теорема повної ймовірності дає змогу обчислити ймовірність події А, що цікавить дослідника, через ймовірність її здійснення за умов підтвердження гіпотез із заданою ймовірністю.

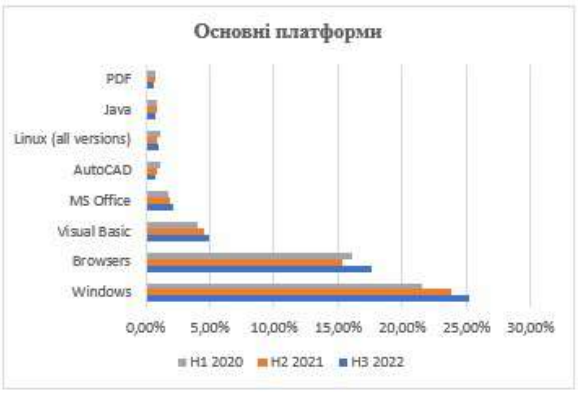



Рис. 2. Основні платформи, що використовує шкідливе програмне забезпечення у 2020, 2021 та 2022 роках

Таблиця 1

Імовірність здійснення кібернетичних атак

| Вид загрози | Умовне позначення |
|---|---|
| DDoS атака | $P_{DDoS}$ |
| Троян/вірус | $P_{virus}$ |
| Програмне забезпечення | $P_{programm}$ |
| Шпигунство/сторонній доступ | $P_{spy}$ |
| Технічні вразливості | $P_{hiker}$ |

Формула повної ймовірності застосовується, коли необхідно отримати ймовірність настання певної події, якщо ця подія залежить від кількох умов. Наприклад, можна дізнатися про ймовірність захищеності кіберпростору, знаючи, з якою ймовірністю захищено кожен її елемент. Теорема множення ймовірностей – імовірність добутку двох подій дорівнює добутку імовірностей одного з них на умовну ймовірність іншого, обчислену за умови, що перше мало місце. Іншими словами імовірність добутку двох незалежних подій дорівнює добутку імовірностей цих подій [2]:

$$P(AB) = P(A) \cdot P(B) \quad (2)$$

Застосовуючи теорему повної ймовірності та теорему множення ймовірностей, отримуємо такий вираз для ймовірність захищеності кіберпростору

$$P_{кб} = 1 - (1 - P_{DDoS})(1 - P_{virus})(1 - P_{programm})(1 - P_{spy})(1 - P_{hiker}), \quad (3)$$

Такий підхід дає змогу враховувати нові складові кібербезпеки і додавати їх під час обчислення ймовірності. Блок-схема реалізації методики оцінювання захищеності кіберпростору об'єктів критичної інфраструктури України наведено на рис. 3.

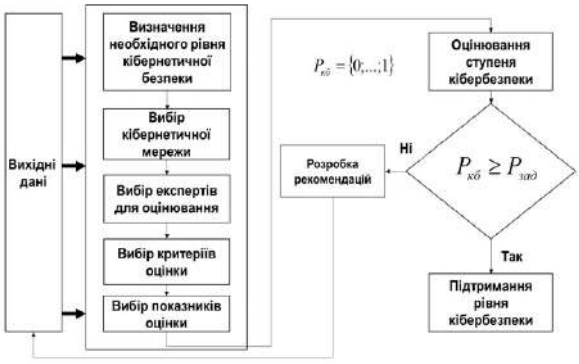



Рис. 3. Блок-схема методики оцінювання захищеності кіберпростору об'єктів критичної інфраструктури

Варто констатувати, що методи оцінювання імовірностей кіберзагроз не є доступними у загальних джерелах. Оскільки кіберсистеми мають різну архітектуру і властивості, програмне забезпечення та рівень підготовленого персоналу, доцільно застосовувати метод експертних оцінок з метою визначення ймовірностей для кожного конкретного випадку [3].

За методикою можна визначити реальний ступінь кібернетичного захисту різних систем, і як наслідок, корегувати рівень складових кібернетичного захисту, залежно від його стану, наявних кібернетичних загроз і можливостей, а також поставлених завдань.

Як приклад реалізації методики, пропонується провести практичні розрахунки оцінювання кібербезпеки кібермережі Центру імітаційного моделювання Національного університету оборони України імені Івана Черняховського. Методом експертного оцінювання пропонується обчислити значення імовірностей загроз за вихідними даними, що наведені у таблиці 2.

Таблиця 2

Обчислення значення імовірностей загроз

| Вид загрози | Умовне позначення | Значення |
|---|---|---|
| DDoS атака | $P_{DDoS}$ | 0,7 |
| Троян/вірус | $P_{virus}$ | 0,2 |
| Програмне забезпечення | $P_{programm}$ | 0,5 |
| Шпигунство/сторонній доступ | $P_{spy}$ | 0,1 |
| Технічні вразливості | $P_{hiker}$ | 0,5 |

Обчислена ймовірність кіберзагрози за виразом (3) становить $P_{кб} = 0{,}946$, що є показником вдалої кібератаки, тому потрібно застосувати заходи щодо зменшення ймовірностей успіху кібератак. Після застосування рекомендованих в роботі заходів, маємо показники наведені у таблиці 3 [4].

За результатами проведених розрахунків, ймовірність кіберзагрози зменшилася в 2,3 рази, що графічно відображено на рис. 4. Імовірність успішної кібернетичної атаки складає 0,41 що є достатньо надійним показником.

Таблиця 3

Зменшення ймовірностей успіху кібератак

| Вид загрози | Умовне позначення | Значення |
|---|---|---|
| DDoS атака | $P_{DDoS}$ | 0,3 |
| Троян/вірус | $P_{virus}$ | 0,01 |
| Програмне забезпечення | $P_{programm}$ | 0,1 |
| Шпигунство/сторонній доступ | $P_{spy}$ | 0,001 |
| Технічні вразливості | $P_{hiker}$ | 0,05 |

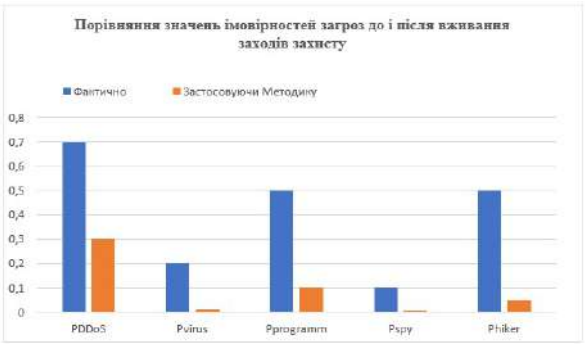



Рис. 4. Порівняння значення загроз до та після застосування заходів захисту

Після обчислень отримаємо: $P_{кб} = 0{,}41$ (рис. 5.)

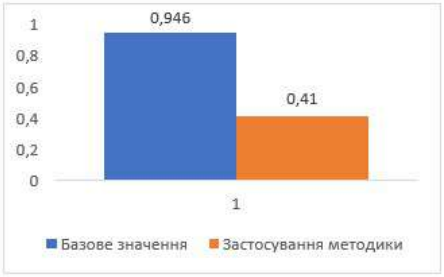



Рис. 5. Результат застосування запропонованої методики

## Висновки й перспективи подальших досліджень

Таким чином, у статті проведено визначення рівня кібербезпеки підрозділу Міністерства оборони України. На основі отриманих результатів сформовано практичні рекомендації щодо забезпечення кібернетичної безпеки до необхідного рівня, які доцільно впровадити в установах та військових частинах. Використана методика дозволяє коректувати пріоритети кіберзагроз, вносити зміни щодо наявних загроз та вразливостей для забезпечення кібероборони (відбиття воєнної агресії у кіберпросторі) України. Також за допомогою зазначеної методики є можливість аналізувати стан існуючої безпеки і шляхи її підвищення, включати і враховувати нові показники, залежно від рівня технічного оснащення, та здійснювати аналіз стану критичних показників кіберзахисту об'єктів критичної інфраструктури.

## *Література*

**1. Мохор В., Гончар С., Дибах О.** Методи оцінки сумарного ризику кібербезпеки об'єктів критичної інфраструктури. Ядерна та радіаційна безпека. 2019. №2(82). DOI: https://doi.org/10.32918/nrs.2019.2(82).01 (дата звернення: 12.12.2022). **2. Regulation (EU) of the European Parliament and of the Council «**On ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)» (Text with EEA relevance) of 17 April 2019 №2019/881. *Official Journal of the European Union*. L 151/15, 7.6.20193. **3. Указ Президента України «**Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"» від 26.08.2021 №447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 12.12.2022). **4. Мурасов Р. К., Мельник Я. В.** Імовірнісний метод прогнозування надзвичайних подій на потенційно-небезпечних об'єктах критичної інфраструктури. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. № 2(44). С. 60–64.

## ASSESSMENT OF CYBER SPACE PROTECTION OF CRITICAL INFRASTRUCTURE FACILITIES OF UKRAINE

***Rustam Murasov (Candidate of Technical Sciences)***
***Yaroslav Melnyk***

***National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine***

*The methodology for assessing the security of cyberspace of critical infrastructure objects of Ukraine is extremely important due to the strengthening of cyber security threats in Ukraine. Objects of critical infrastructure of Ukraine, such as energy networks, transport systems, banking institutions, medical and military institutions, communication systems and others, are of great importance for the life and activity of the national economy and society as a whole. In particular, a failure in the operation of these facilities can lead to serious consequences, such as power outages, traffic stoppages, disruption of financial stability, disruption of medical services, etc. Under such conditions, protecting the cyberspace of critical infrastructure objects becomes an extremely important task for the state and business. To achieve this goal, it is necessary to have an effective methodology for assessing the security of cyberspace of critical infrastructure objects, which makes it possible to identify potential threats and risks, as well as to develop and implement measures to improve cyber security. The article provides theoretical explanations that connect the state's understanding of the principles of functioning of modern cyber threats and the search for mechanisms to solve them. It has been established that the provision of national (military) security is not yet carried out at the expense of the proper concept. According to the results of the assessment of the security of the cyberspace of critical infrastructure objects, practical ways of strengthening the military security of Ukraine through the search for an effective cyber security strategy have been determined.*

***Key words***: *cyber-attack, cyber danger, cyber defense, minimization of the consequences of emergencies, investigation of the causes of emergencies.*

## *References*

**1. Mokhor, V., Gonchar, S., Dybach, O.** (2019). Methods for assessing the overall risk of cybersecurity in critical infrastructure facilitiesю Nuclear and radiation safety, 2(82). DOI: https://doi.org/10.32918/nrs.2019.2(82).01. **2. Regulation (EU) 2019/881 of 17 April 2019** on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) № 526/2013 (Cybersecurity Act). Official Journal of the European Union. L 151/15, 7.6.20193. **3. Decree of the President of Ukraine** On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine", 447/2021. **4. Murasov, R. K., Melnyk, Y. V. (**2022). A probabilistic method of forecasting emergency events at potentially dangerous objects of critical infrastructure. Modern information technologies in the sphere of security and defense, 2(44), 60–64

DOI:**10.33099/2311-7249/2023-46-1-45-50**

УДК: 65.015.3

***Олексій Ростиславович Мартинюк*** *(кандидат технічних наук, доцент)*
***Володимир Олегович Кошка***

***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# ПІДХІД ДО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ СИСТЕМИ ВИВЧЕННЯ ТА ВПРОВАДЖЕННЯ ДОСВІДУ ЗАСТОСУВАННЯ АВІАЦІЇ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

*Оцінювання ефективності роботи системи вивчення та впровадження досвіду (далі – ВВД) має значне практичне значення, оскільки ця процедура може стати інструментом для розвитку у Збройних Силах України (далі – ЗС України) дієвої системи збору, аналізу та поширення глобальної інформації про передовий воєнний досвід, що дозволить підвищити ефективність підготовки і застосування складових сил оборони держави та вказати напрями розвитку озброєння й військової техніки.*

*Необхідність оцінювання ефективності системи ВВД, задекларована керівними документами, що регламентують порядок організації вивчення та впровадження досвіду у ЗС України, але чіткого поняття ефективності ВВД у них не наведено, методику оцінювання не запропоновано.*

*Система ВВД відноситься до розряду складних систем, тому оцінювання її ефективності доцільно проводити за декількома показниками або за показником, що включає декілька часткових показників ефективності. Для цього найчастіше застосовується метод групування.*

*Варіантом реалізації методу групування є представлена у роботі [18] методика оцінювання ефективності функціонування інтегрованої системи управління військового призначення на основі декомпозиції її на підсистеми за функціональними ознаками з урахуванням вагомості, своєчасності та якості виконання завдань. Ефективність системи визначається як середнє арифметичне значення ефективності функціонування підсистем без врахування їх вагових коефіцієнтів, що може вплинути на точність результатів оцінювання.*

*Наведений у статті підхід до оцінювання ефективності роботи системи ВВД застосування авіації у ЗС України передбачає синтез показників своєчасності та якості вирішення задач функціональними підсистемами з подальшим оцінюванням ефективності підсистем з урахуванням коефіцієнтів вагомості кожної підсистеми та задачі.*

*Перевагою даного підходу є гнучкий математичний апарат, який дозволяє без проблем збільшувати (зменшувати) перелік показників ефективності функціонування системи ВВД. Крім того є можливість для кожної підсистеми застосовувати свої показники ефективності на рішення експерта.*

***Ключові слова:*** *вивчення та впровадження досвіду; Lessons learned; оцінювання ефективності; показники ефективності; підхід до оцінювання.*

## Вступ

**Постановка проблеми.** Теперішня система вивчення та впровадження досвіду у Збройних Силах України впроваджена у 2020 році, але справжня її апробація розпочалася з початком нового етапу російсько-української війни. Результати її роботи, зокрема, щодо збору, аналізу і поширення досвіду застосування авіації, ще не оцінено.

На сьогодні основними національними документами, що визначать порядок організації вивчення та впровадження досвіду в ЗС України є Доктрина з вивчення та впровадження досвіду у ЗС України (далі – Доктрина) [1] та Тимчасова інструкція вивчення та впровадження досвіду у ЗС України (далі – Тимчасова інструкція) [2].

Відповідно до Доктрини, однією з процедур процесу ВВД є оцінювання ефективності заходів (коригувальних дій) з впровадження досвіду, однак показників за якими пропонується оцінювати ефективність не визначено. Натомість зазначено, що ефективність функціонування системи ВВД має базуватися на певному «фундаменті» – готовності командувачів (командирів, начальників) усіх рівнів до обміну інформацією, висвітлення такої інформації, в першу чергу, щодо прорахунків та невдач, створенні комфортного соціального мікроклімату у ЗС України та формуванні відповідного менталітету, типу мислення, культури поведінки і спілкування особового складу.

В Тимчасовій інструкції вказано, що систематичне оцінювання ефективності роботи органів військового управління, військ (сил) щодо вивчення та впровадження досвіду є одним із

основних завдань ВВД. Також зазначено, що ефективність ВВД досягається забезпеченням своєчасної передачі та використання корисної інформації, набутого досвіду до посадових осіб, підрозділів, військових частин, органів військового управління для досягнення успіху в операції (бойових діях) та під час виконання ними визначених завдань, уникнення втрат в особовому складі, досягнення переваги над противником за рахунок більшої поінформованості та, відповідно, кращої підготовки військ (сил). Але як випливає зі змісту формалізованих донесень (додаток 9, додаток 12 до Тимчасової інструкції), під час проведення періодичного аналізу ефективності впровадження досвіду до уваги береться лише кількість вивчених та впроваджених уроків за певний період часу. Перевірка якості впровадження досвіду розглядається окремим пунктом, хоча цей показник може мати безпосередній вплив на ефективність ВВД. Критерії по яким оцінювати ефективність ВВД не сформульовано.

Загалом, у наведених керівних документах надається чимало уваги необхідності оцінювання ефективності системи ВВД, але єдиного розуміння поняття ефективності ВВД та методики оцінювання зазначеної системи не наведено.

**Аналіз останніх досліджень і публікацій.** Як відомо, вітчизняна нормативна база ВВД [1; 2] була розроблена на основі документів, що регламентують політику NATO Lessons Learned (далі – LL) [3–6]. Цей крок мав за мету досягнення максимальної функціональної сумісності з NATO LL system (далі – LLS), та є один із багатьох кроків на шляху до членства України в NATO. Тому погляди щодо того, на чому має базуватися та завдяки чому досягається ефективність ВВД є однаковими, але акцент робиться на відповідальність та підзвітність усіх учасників процесу LL.

Водночас, у Звіті за результатами аудиту NATO LL process [7] зазначено, що у ряді випадків зниження ефективності роботи LLS відбувалося внаслідок: недотримання встановлених термінів збору, аналізу і впровадження досвіду; незадовільної точності і якості впроваджених уроків.

У ряді публікацій зазначено [8–11], що ефективність LLS слід оцінювати, спираючись на результати заходів із впровадження уроків. В основі такого підходу покладена модель оцінки ефективності навчання Кіркпатріка [12]. Відповідно до цієї моделі оцінювання ефективності LLS пропонується проводити за лінійним графіком показників: зміна поведінки організації (підрозділу), продуктивність організації (підрозділу) або результативність виконання поставлених завдань. Передбачається, що зростання даних показників залежить від впливу на організацію впроваджених LL. Проте можуть існувати й інші непов'язані з LL фактори, що пояснюють підвищення ефективності організації (підрозділу), тому дана методика не завжди може відображати дійсний стан LLS.

Використання адекватного показника ефективності дозволяє правильно оцінити ефективність системи. Формальних методів вибору показника ефективності не існує, тому завжди є ризик того, що вибір показника виявиться невдалим, а результати використання цього показника – помилковими. Показники ефективності системи мають бути обчислювальними, а їх значення можуть бути розмірними або безрозмірними величинами, які дають змогу кількісно оцінювати ефект застосування системи. Основною вимогою під час визначення показника ефективності системи є відповідність цього показника меті системи [13].

У ряді публікацій [15–18] рекомендується оцінювання ефективності складних систем, якою, зокрема, є система ВВД, проводити за декількома показниками ефективності або за показником, що включає декілька часткових показників ефективності. В такому випадку виникає проблема вибору методу оцінювання.

Найчастіше застосовується метод групування [13, 16–18], що передбачає певну класифікацію задач, які вирішуються в системі на різних етапах її функціонування, з метою декомпозиції її на підсистеми. Ефективність розв'язання групи таких задач оцінюється відповідним частковим показником – показником ефективності і-ї підсистеми. Згорнувши часткові показники в один скалярний, отримують значення загальної ефективності.

Варіантом реалізації методу групування є представлена у роботі [18] методика оцінювання ефективності функціонування інтегрованої системи управління військового призначення на основі декомпозиції її на підсистеми за функціональними ознаками з урахуванням вагомості, своєчасності та якості виконання завдань. Ефективність системи пропонується визначити як середнє арифметичне значення ефективності функціонування підсистем без урахування їх важливості.

**Метою статті** є пошук підходів до оцінювання ефективності роботи системи вивчення та впровадження досвіду застосування авіації у ЗС України.

## Виклад основного матеріалу дослідження

На початковому етапі оцінювання будь-якої системи, у тому числі й системи ВВД застосування авіації, необхідно сформулювати її мету, визначити покладені на неї завдання, основні фактори, що впливають на її ефективність та умови, які обмежують можливості системи.

Отже, головною метою роботи системи ВВД застосування авіації слід вважати усунення (мінімізацію) впливу виявленого проблемного питання або нарощування впливу передового досвіду на діяльність авіаційних організаційних структур шляхом вироблення та поширення рекомендацій у сфері авіаційної діяльності (у тому числі й рекомендацій, щодо внесення змін до нормативних документів).

Для досягнення цієї мети існуюча система ВВД у ЗС України виконує наступні функціональні завдання [1]:

збір, узагальнення інформації про проблемні питання (передовий досвід);

аналіз проблемних питань і визначення головних причин їх виникнення (повторення) та шляхів вирішення;

поширення та впровадження досвіду у відповідні сфери діяльності ЗС України;

визначення дієвих прийомів і способів здійснення процесу вивчення та впровадження досвіду.

Згрупувавши їх за функціональними ознаками, систему ВВД можливо структурно зобразити у вигляді чотирьох підсистем $S_1$ – $S_4$ (рисунок 1).

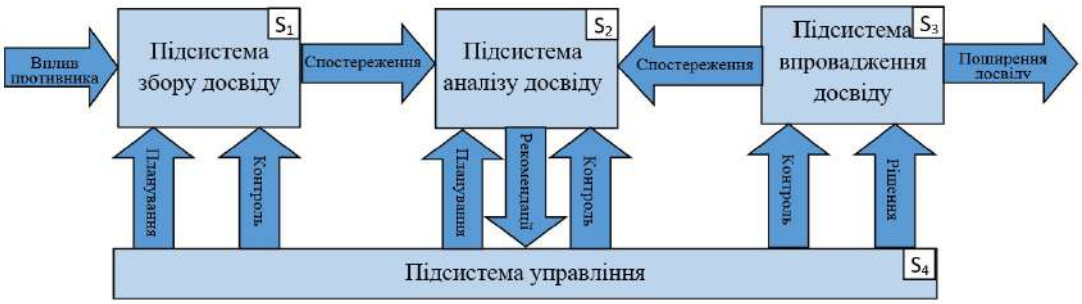



Рисунок 1. Модель системи ВВД у ЗС України

Функціональні завдання складаються із сукупності спеціальних взаємопов'язаних аналітичних, розрахункових, інформаційних та інших задач $P_j$:

$P_1$ – прийняття рішення, планування та виконання необхідних коригувальних дій для впровадження досвіду і призначення ОВУ та осіб, відповідальних за їх виконання, а також оцінювання їх ефективності;

$P_2$ – організація збору, узагальнення, аналізу інформації та визначення головних причин виникнення проблем і шляхів їх вирішення;

$P_3$ – виявлення проблемних питань щодо підготовки та застосування ЗС України під час проведення операцій (бойових дій), військових навчань (тренувань), участі у міжнародних операціях з підтримання миру і безпеки, навчаннях, повсякденної діяльності тощо;

$P_4$ – розроблення рекомендацій щодо вирішення проблемних питань та визначення заходів із впровадження досвіду (коригувальних дій);

$P_5$ – поширення інформації про вивчений та впроваджений досвід;

$P_6$ – контроль (моніторинг) за виконанням всіх процедур Процесу, насамперед, визначених заходів із впровадження досвіду (коригувальних дій);

$P_7$ – підготовка особового складу з питань ВВД.

Кожна j-та задача в системі ВВД має відповідну вагу $K_j$ ( $j = 1, \dots, 7$), яка визначається методом експертних оцінок, а множини функціональних задач $P_j$ відповідають основному призначенню підсистем $S_i$.

$$S_1 = \{\{P_2, P_3, P_7\}, \{K_2, K_3, K_7\}\};$$
$$S_2 = \{\{P_2, P_4, P_7\}, \{K_2, K_4, K_7\}\}; \quad (1)$$
$$S_3 = \{\{P_3, P_5, P_7\}, \{K_3, K_5, K_7\}\};$$
$$S_4 = \{\{P_1, P_2, P_6, P_7\}, \{K_1, K_2, K_6, K_7\}\}.$$

При розподілі результатів експертного оцінювання слід врахувати, що контрольна сума вагових коефіцієнтів $K_j$ має дорівнювати одиниці:

$$\sum_{j=1}^{7} K_j = 1. \quad (2)$$

Нормалізований запис множин елементів (1) можливо представити наступним чином:

$$S_1 = \{\{P_{1,1}, P_{1,2}, P_{1,3}\}, \{K_{1,1}, K_{1,2}, K_{1,3}\}\};$$
$$S_2 = \{\{P_{2,1}, P_{2,2}, P_{2,3}\}, \{K_{2,1}, K_{2,2}, K_{2,3}\}\}; \quad (3)$$
$$S_3 = \{\{P_{3,1}, P_{3,2}, P_{3,3}\}, \{K_{3,1}, K_{3,2}, K_{3,3}\}\};$$
$$S_4 = \{\{P_{4.1}, P_{4,2}, P_{4,3}, P_{4,4}\}, \{K_{4,1}, K_{4,2}, K_{4,3}, K_{4,4}\}\}.$$

Кожна із m задач, що вирішуються в і-й підсистемі ($P_{i,m}$) також має певну вагу $K_{P_{i,m}}$, яку визначають спираючись на результати уже проведеного експертного оцінювання:

$$\{K_{P1,1}, K_{P1,2}, K_{P1,3}\};$$
$$\{K_{P2,1}, K_{P2,2}, K_{P2,2}\}; \quad (4)$$
$$\{K_{P3,1}, K_{P3,2}; K_{P3,3}\};$$
$$\{K_{P4,1}, K_{P4,2}, K_{P4,3}, K_{P4,4}\},$$

де $K_{P_{i,m}} = K_{i,m} \times \frac{1}{\sum_{m=1}^{|K_{i,m}|} K_{i,m}}$, відповідно контрольна сума $\sum_{m=1}^{|K_{P_{i,m}}|} K_{P_{i,m}} = 1.$

Залежно від вагомості вирішуваних задач $K_{P_{i,m}}$, підсистеми $S_i$ по різному впливають на загальний процес ВВД, тобто мають свої вагові значення ($K_{S_i}$):

$$K_{S_i} = \sum_{m=1}^{|K_{i,m}|} K_{i,m} \times \frac{1}{\sum_{i=1}^{4} \sum_{m=1}^{|K_{i,m}|} K_{i,m}}, \quad (5)$$

відповідно контрольна сума $\sum_{i=1}^{4} K_{S_i} = 1$.

Оскільки підсистеми $S_i$ мають різний вплив на виконання загального процесу ВВД, тобто мають різні вагові значення, тоді ефективність системи ВВД можливо визначити як суму добутків значень ефективності підсистем та їх вагових коефіцієнтів:

$$E_{СВВД} = \sum_{i=1}^{4} K_{S_i} E_{S_i}, \quad (6)$$

де $E_{S_i}$ – значення ефективності і-ї підсистеми ВВД.

Ефективність функціонування окремої підсистеми ВВД ($E_{Si}$) пропонується визначати за двома показниками – «своєчасність» ($F_t$) та «якість» ($F_q$) виконання покладених задач (1). Так як задачі, що розв'язуються в підсистемі $S_i$ мають різний внесок у величину її значення, тому для визначення ефективності функціонування і-ї підсистеми, буде справедливий вираз:

$$E_{S_i} = \sum_{m=1}^{|P_{i,m}|} K_{P_{i,m}} F_{t_{i,m}} F_{q_{i,m}}, \quad (7)$$

де $K_{P_{i,m}}$ – ваговий коефіцієнт m-ї задачі в і-й підсистемі, $F_{t_{i,m}}$ – показник своєчасності вирішення m-ї задачі в і-й підсистемі, $F_{q_{i,m}}$ – показник якості вирішення m-ї задачі в і-й підсистемі.

$F_{t_{i,m}}$ характеризує наскільки реальний час рішення m-ї задачі $\left(T_{РВЗ_{i,m}}\right)$ відповідає часу заданому у нормативному (директивному) документі (наприклад у Табелі термінових донесень) або ж часу при ідеальних умовах функціонування $\left(T_{ЗВЗ_{i,m}}\right)$ підсистеми і визначається наступним відношенням:

$$F_{t_{i,m}} = \frac{T_{ЗВЗ_{i,m}}}{T_{РВЗ_{i,m}}}. \quad (8)$$

При $F_{t_{i,m}} \geq 1$ слід вважати що задача вирішена вчасно або завчасно, якщо $F_{t_{i,m}} < 1$ – із запізненням або взагалі не взята до виконання.

$F_{q_{i,m}}$ характеризує наскільки реальна повнота (адекватність) рішення m-ї задачі $\left(C_{РВЗ_{i,m}}\right)$ відповідає заданій повноті рішення задачі $\left(C_{ЗВЗ_{i,m}}\right)$ визначеній у нормативному (директивному) документі (наприклад, наявність у результатах рішення задачі матеріалів щодо планування, збору досвіду, узагальнення, аналізу, рекомендацій і т. п.) і визначається наступним відношенням:

$$F_{q_{i,m}} = \frac{C_{РВЗ_{i,m}}}{C_{ЗВЗ_{i,m}}}. \quad (9)$$

При $F_{q_{i,m}} = 1$, слід вважати що поставлена задача вирішена у повному обсязі, якщо $F_{q_{i,m}} < 1$ – задача вирішена не до кінця або взагалі не вирішувалася.

Отже враховуючи вираз (6), (7) загальну ефективність системи ВВД можливо визначити наступним виразом:

$$E_{СВВД} = \sum_{i=1}^{4} E_{S_i} \left( \sum_{m=1}^{|P_{i,m}|} K_{P_{i,m}} F_{t_{i,m}} F_{q_{i,m}} \right), \quad (10)$$

Якщо $E_{СВВД} \geq 1$, то ефективність системи ВВД можна оцінити задовільно, так як усі задачі виконані вчасно і у повному обсязі. За таких умов система ВВД не потребує управлінського впливу, але для досягнення високої точності результатів оцінювання ефективності доцільно періодично повторювати експертне оцінювання важливості вирішуваних задач ($P_j$).

При $E_{СВВД} < 1$ – ефективність системи ВВД є незадовільною, оскільки задачі виконані із запізненням, вирішені не до кінця або взагалі не виконувались. У такому випадку приймається управлінське рішення щодо корегування організаційної структури, вирішуваних завдань або проведення додаткової підготовки штатного персоналу ВВД тощо, проводиться повторне експертне оцінювання важливості вирішуваних задач ($P_j$).

## Висновки та перспективи подальших досліджень

В результаті проведеного дослідження знайдено підхід до оцінювання ефективності роботи системи вивчення та впровадження досвіду застосування авіації у ЗС України шляхом синтезу показників своєчасності та якості вирішення задач функціональними підсистемами та подальшим оцінюванням ефективності підсистем з урахуванням коефіцієнтів вагомості кожної задачі та підсистеми.

Перевагою даного підходу є гнучкий математичний апарат, який дозволяє без проблем збільшувати (зменшувати) перелік показників ефективності функціонування системи ВВД. Крім того є можливість для кожної підсистеми застосовувати свої показники ефективності на рішення експерта.

Подальшим напрямом розвитку даного підходу буде розробка методики оцінювання ефективності системи ВВД, для подальшої інтеграції в перспективний портал ВВД у вигляді спеціалізованого програмного забезпечення. Це дозволить використовувати бази даних порталу як джерело вихідної інформації для обчислення показників ефективності системи ВВД.

Наявність методики, що дозволить оцінювати ефективність системи ВВД за набором показників у стислі терміни матиме значне практичне значення, адже стане інструментом для створення у ЗС України дієвої системи збору, аналізу та поширення глобальної інформації про передовий воєнний досвід, що дозволить підвищити ефективність підготовки і застосування складових сил оборони держави та вказати напрями розвитку озброєння й військової техніки.

## *Література*

**1.** Доктрина з вивчення та впровадження досвіду у Збройних Силах України : рішення Начальника Генерального штабу Збройних Сил України від 03.07.2020 р. № 1928/НВГШ. *Військова керівна публікація.* 2020. № 7-00(01).01. 26 с. **2.** Тимчасова інструкція вивчення та впровадження досвіду у Збройних Силах України : наказ Генерального штабу Збройних Сил України від 15.07.2020 р. № 56. *Військова керівна публікація.* 2020. № 7-00(01).01. 69 с. **3.** Collective training and exercise directive : Bi-SC Directive of 02.10.2013 no. 075-003. URL : https://www.coemed.org/files/Branches/DH/Files_ 01/ bi-sc-75-3_final.pdf (дата звернення: 15.10.2022). **4.** Lessons Learned : Bi-SC Directive of 23.02.2018 no. 080-006. **5.** NATO Lessons Learned Policy : Document of 01.09.2011 no. PO(2011)0293. URL: https:// www.mwcoe.org/wp-content/uploads/2019/01/NATO-LL-Policy.pdf (date of access: 18.10.2022). **6.** NATO Lessons Learned Policy for release to partners : Document of 10.07.2012 no. PO(2012)0294. **7.** NATO. IBAN Performance audit report on the need to improve the effectiveness of the Lessons Learned process for NATO exercises. 2017. 43 p. URL: https://www.mwcoe.org/wp-content/uploads/2019/01/NATO-LL-Policy.pdf (date of access: 18.10.2022). **8.** Australian Emergency Management Institute. Lessons management : handbook 8. 2nd ed. Sydney : Australian Emergency Management Institute, 2013. 89 p. **9.** Center for Army Lessons Learned. Establishing a Lessons Learned Program : handbook. Fort Leavenworth : Center for Army Lessons Learned, 2011. 87 p. **10.** Joint Analysis and Lessons Learned Centre. The NATO lessons learned handbook : handbook. 4th ed. Lisboa : Joint Analysis and Lessons Learned Centre, 2022. 58 p. **11.** Air Force Lessons Learned Program : Air Force instruction of 30.07.2019 no. 10-1302. URL: https://static.e-publishing.af.mil/production/1/lemay_center/publication/afi10-1302/afi10-1302.pdf (date of access: 19.10.2022). **12. Kirkpatrick D., Kirkpatrick J.** Evaluating Training Programs: The Four Levels (3rd Edition). San Francisco: Berrett-Koehler Publishers, 2006. 229 p. **13.** Мацько О. Й., Микусь С. А. , Солонніков В. Г. та ін. Застосування сучасних інформаційних технологій в науковій діяльності: підручник. Київ : НУОУ ім. І. Черняховського, 2021. 340 с. **14. Сорока К. О.** Основи теорії систем і системного аналізу: навч. посібник. Харків : ХНАМГ, 2004. 291 с. **15. Писарчук О. О.** Оцінювання ефективності інформаційних систем за вектором критеріїв. Житомир : зб. наук. праць ЖВІ НАУ, 2010. С. 117–123. **16. Височина М. В**. Аналіз методів оцінювання ефективності управління діяльністю підприємства. *Культура народів Причорномор'я*. 2009. № 161. С. 86–89. **17. Долішня Т. І., Долішній Б. С.** Особливості методів оцінки ефективності управління діяльністю підприємства. *Наукові вісті приватного вищого навчального закладу «Галицька академія»*. 2012. № 1(20). С. 90–95. **18**. Кучеренко Ю. Ф., Носик А. М., Ткачов А. М., Шубін Є. В. Визначення ефективності функціонування системи управління військового призначення з врахуванням вагомості, своєчасності та якості виконання завдань у її підсистемах. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2019. № 4(62). С. 53–60. **19**. **Бойко Т. Г.** Огляд методів визначення вагових коефіцієнтів показників властивостей продукції. *Методи та прилади контролю якості.* 2010. № 24. С. 84–89.

## WAY OF EVALUATING THE EFFECTIVENESS OF THE AIR FORCE LESSONS LEARNED SYSTEM IN THE ARMED FORCES OF UKRAINE

***Oleksii Martyniuk*** ***(Candidate of technical sciences, docent)***
***Volodymyr Koshka***

***National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine***

*Evaluating the effectiveness of the Lessons Learned system is of great practical importance, as this procedure can become a tool for the development in the Armed Forces of Ukraine of an effective system of collecting, analyzing and disseminating global information on advanced military experience, which will allow to increase the effectiveness of training and application of the components of the state's defense forces and indicate directions for the development of weapons and military equipment.*

*The need to evaluate the effectiveness of the Lessons Learned system is declared by the governing documents that regulate the procedure for organizing the study and implementation of experience in the Armed Forces of Ukraine, but they do not provide a clear concept of the effectiveness of the internal defense system, and no evaluation methodology is proposed.*

*The Lessons Learned system belongs to the category of complex systems, therefore, it is advisable to evaluate its efficiency by several indicators or by an indicator that includes several partial indicators of efficiency. For this, the grouping method is most often used.*

*A variant of the implementation of the grouping method is presented in work [18] a method of evaluating the effectiveness of the functioning of the integrated military management system based on its decomposition into subsystems according to functional characteristics, taking into account the importance, timeliness and quality of task performance. The efficiency of the system is defined as the average arithmetic value of the efficiency of functioning of the subsystems without taking into account their weighting factors, which can affect the accuracy of the evaluation results.*

*The approach presented in the article to the evaluation of the effectiveness of the Air Traffic Control system of the use of aviation in the Armed Forces of Ukraine involves the synthesis of indicators of timeliness and quality of solving tasks by functional subsystems with further evaluation of the effectiveness of subsystems taking into account the weighting coefficients of each subsystem and task.*

*The advantage of this approach is a flexible mathematical apparatus that allows you to easily increase (decrease) the list of performance indicators of the Lessons Learned system. In addition, it is possible for each subsystem to apply its performance indicators to the expert's decision.*

***Keywords:*** *Lessons learned, effectiveness evaluation, effectiveness indicators, evaluation method.*

## *References*

**1.** Doktryna z vyvchennia ta vprovadzhennia dosvidu u Zbroinykh Sylakh Ukrainy : document of 03.07.2020 no. 1928/НВГШ. *Military management publication.* 2020. No. 7-00(01).01. 26 p. **2.** Tymchasova instruktsiia vyvchennia ta vprovadzhennia dosvidu u Zbroinykh Sylakh Ukrainy : order of the General Staff of the Armed Forces of Ukraine of 07.15.2020 no. 56. *Military management publication.* 2020. No. 7-00(01).01. 69 p. **3.** Collective training and exercise directive : Bi-SC Directive of 02.10.2013 no. 075-003. URL : https://www.coemed.org/files/Branches/DH/ Files_ 01/ bi-sc-75-3_final.pdf (дата звернення: 15.10.2022). **4.** Lessons Learned : Bi-SC Directive of 23.02.2018 no. 080-006. **5.** NATO Lessons Learned Policy : Document of 01.09.2011 no. PO(2011)0293. URL: https://www.mwcoe.org/wp-content/uploads/2019/01/NATO-LL-Policy.pdf (date of access: 18.10.2022). **6.** NATO Lessons Learned Policy for release to partners : Document of 10.07.2012 no. PO(2012)0294. **7.** NATO. IBAN Performance audit report on the need to improve the effectiveness of the Lessons Learned process for NATO exercises. 2017. 43 p. URL : https://www.mwcoe.org/wp-content/uploads/2019/01/ NATO-LL-Policy.pdf (date of access: 18.10.2022). **8.** Australian Emergency Management Institute. Lessons management : handbook 8. 2nd ed. Sydney : Australian Emergency Management Institute, 2013. 89 p. **9.** Center for Army Lessons Learned. Establishing a Lessons Learned Program : handbook. Fort Leavenworth : Center for Army Lessons Learned, 2011. 87 p. **10.** Joint Analysis and Lessons Learned Centre. The NATO lessons learned handbook : handbook. 4th ed. Lisboa : Joint Analysis and Lessons Learned Centre, 2022. 58 p. **11.** Air Force Lessons Learned Program : Air Force instruction of 30.07.2019 no. 10-1302. URL: https://static.e-publishing.af.mil/production/1/lemay_center/publication/afi 10-1302/afi10-1302.pdf (date of access: 19.10.2022). **12. Kirkpatrick D., Kirkpatrick J.** Evaluating Training Programs: The Four Levels (3rd Edition). San Francisco: Berrett-Koehler Publishers, 2006. 229 p. **13.** Matsko O.Y., Mykus S.A., Solonnikov V.G. and others. Application of modern information technologies in scientific activity: textbook. Kyiv: NDUU named after I. Chernyakhovsky, 2021. 340 p. **14. Soroka K. O.** Fundamentals of systems theory and system analysis: teaching. manual. Kharkiv: O.M. Beketov National University of Urban Economy in Kharkiv, 2004. 291 p. **15. Pisarchuk O. O.** Evaluation of the effectiveness of information systems by the vector of criteria. Zhytomyr: coll. of science Proceedings of KZMI NAU, 2010. P. 117–123. **16. Vysochyna M. V.** Analysis of methods for evaluating the effectiveness of enterprise management. *Culture of the peoples of the Black Sea region*. 2009. No. 161. P. 86–89. **17. Dolishnya T. I., Dolishnyi B. S.** Peculiarities of methods of evaluating the effectiveness of enterprise activity management. *Scientific news of the private higher educational institution "Halytska Academy"*. 2012. No. 1(20). P. 90–95. **18**. Kucherenko Y. F., Nosyk A. M., Tkachev A. M., Shubin E. V. Determining the effectiveness of the military assignment management system, taking into account the importance, timeliness and quality of task performance in its subsystems. *Collection of scientific works of the Kharkiv National University of the Air Force.* 2019. No. 4(62). P. 53–60. **19**. **Boyko T. G.** Review of methods for determining weighting coefficients of indicators of product properties. *Quality control methods and devices.* 2010. No. 24. P. 84–89.

DOI:**10.33099/2311-7249/2023-46-1-51-55**

УДК: 004.056

***Михайло Анатолійович Стрельбіцький*** *(доктор технічних наук, професор)*
***Валентин Юрійович Мазур*** *(доктор військових наук, професор)*
***Володимир Васильович Лемешко*** *(кандидат військових наук, доцент)*

***Національна академія Державної прикордонної служби України імені Богдана Хмельницького***

# ПРОТОКОЛИ ОБМІНУ «АГРЕГОВАНОЇ» ІНФОРМАЦІЇ В ІНФОРМАЦІНО–ТЕЛЕКОМУНІКАЦІЙНІЙ СИСТЕМІ

*У статті, на підставі класифікації інформації з обмеженим доступом, визначені передумови порушення її конфіденційності у ході дотримання вимог політики безпеки інформаційно-телекомунікаційної системи. Визначено, що збільшення кількості інформації може призводити до підвищення рівня обмеження доступу. Для множин інформації такого типу дано визначення як «агрегованої». Наведені умови порушення безпеки інформації, рівень конфіденційності якої залежить від її кількості. Визначені можливі канали прихованого витоку інформації з вузлів мережі без порушення політики безпеки інформаційно-телекомунікаційної системи. Запропоновано спосіб попередження несанкціонованого доступу суб'єктів інформаційної системи шляхом запровадження нового протоколу обміну між вузлами інформаційно-телекомунікаційних систем. Розроблений протокол обміну «агрегованої» інформації між вузлами мережі передбачає використання контейнеру «агрегованої» інформації, який забезпечує формування інформації з вищим рівнем доступу на захищеному вузлі інформаційно-телекомунікаційної системи.*

***Ключові слова:*** *інформація, конфіденційність, протокол, інформаційна система.*

## Вступ

Виконання Державною прикордонною службою України своїх основних функцій вимагає обробки значної кількості різнопланової інформації, в тому числі такої, що не має відповідно до законодавства грифу обмеження доступу. Разом із тим, зазначена інформація є власністю Державної прикордонної служби України (далі – Держприкордонслужба) і підлягає захисту. Безпека цієї інформації досягається дотриманням її властивостей, а саме: конфіденційності, цілісності, доступності та спостереженості [1]. Питання, що стосуються дотримання цілісності, доступності та спостереженості достатньо добре опрацьовані технологічно, зокрема, внаслідок резервування складових інформаційно-телекомунікаційних систем (далі – ІТС), розробки механізмів архівування та відновлення стану системи після збою тощо. Ключовим у підтриманні безпеки інформації залишається дотримання конфіденційності інформації.

**Постановка проблеми.** Керівними документами передбачена можливість формування кінцевого документу з вищим рівнем обмеження доступу із відомостей з нижчим рівнем. У процесі запровадження систем електронного документообігу для відомостей відкритого характеру можлива ситуація одночасного знаходження на одному вузлі мережі групи відомостей, що сукупно формують інформацію з вищим рівнем обмеження доступу. Вищенаведене вимагає пошуку процедурних і функціональних рішень унеможливлення знаходження на одному вузлі мережі такої групи інформації.

**Аналіз останніх досліджень і публікацій.** Аналіз публікацій у цій галузі [2–4] свідчить про існування багатьох методів, що регламентують доступ користувачів до ресурсів інформаційної системи. Зазначені методи формально обґрунтовані та унеможливлюють витік інформації за умов дотримання всіх вимог визначених обраним методом. У цьому контексті доцільно зауважити той факт, що доступ користувачів до ресурсів інформаційної системи є детермінований, тобто визначений до моменту ознайомлення користувача з інформацією, що є логічним. З вищенаведеного можна зробити логічний висновок, що з точки зору всіх систем розмежування доступу до ресурсів ІТС немає підстав обмежувати користувача в доступі до інформації якщо раніше такий доступ був наданий і жодних додаткових обмежень не було введено. У цьому контексті варто зауважити вимоги Зводу відомостей, що становлять державну таємницю [5], в якому за відповідними розділами регламентовано віднесення інформації до секретної та визначено її ступінь обмеження доступу. Аналіз цього документу показав, що агрегуючи інформацію з нижчим ступенем обмеження доступу, користувач ІТС може отримати інформацію з вищим ступенем обмеження доступу. Таким чином, збільшення кількості інформації в ІТС може призвести до формування даних з вищим ступенем секретності, при чому за повного дотримання вимог політики безпеки, яку визначає обрана система розмежування доступу.

**Мета статті** – визначення умов виникнення несанкціонованого каналу витоку службової інформації інформаційно-телекомунікаційних

системах Державної прикордонної служби України та формування безпечних протоколів обміну між вузлами ІТС.

## Виклад основного матеріалу дослідження

Інформаційно-телекомунікаційні системи Держприкордонслужби використовують інтранет-мережу прикордонного відомства, що базується на орендованих каналах зв'язку національних операторів. Така структура відомчої телекомунікаційної мережі не передбачає доступу до інших інформаційних ресурсів поза межами інтранет-мережі. Разом із тим, у ході використання орендованих каналів при передачі даних немає гарантії факту не перехоплення пакетів та витоку будь-якої інформації, в тому числі такої, що не відноситься до інформації з обмеженим доступом.

В умовах обробки ІТС відкритої інформації (інформації, що не відноситься до інформації з обмеженим доступом), захист якої полягає тільки в забезпеченні дотримання її трьох властивостей (цілісності, доступності та спостереженості), забезпечення конфіденційності не є обов'язковим (з причини загальнодоступності відкритої інформації). Постановою Кабінету Міністрів України зазначено, що «Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, що можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією» [6]. Зокрема, тим самим документом зазначено, що «захист інформації від витоку технічними каналами забезпечується в системі у разі, коли в ній обробляється інформація, що становить державну таємницю, або коли відповідне рішення щодо необхідності такого захисту прийнято розпорядником інформації».

Саме тому, більшість ІТС Держприкордонслужби не має спеціалізованих технічних засобів захисту інформації та розгорнутої комплексної системи захисту інформації. Такий підхід є логічним з економічної точки зору – немає сенсу захищати інформацію, якщо доступ до неї відкритий. Враховуючи вищенаведене, отримання інформації з відкритих джерел або перехоплення трафіку в інтранет-мережі Держприкордонслужби є нескладним завданням.

Розглянемо узагальнену процедуру віднесення будь-якої інформації до інформації з обмеженим доступом. Відповідно до переліку відомостей, що становлять державну таємницю [5] державні експерти з питань таємниць визначають, яка саме інформація становить державну таємницю у визначених законодавством сферах. Аналогічний підхід застосовується щодо віднесення інформації до службової, зокрема, в Переліку відомостей, що становлять службову інформацію у Державній прикордонній службі України та Інструкції із захисту публічної інформації у Державній прикордонній службі України [7] зазначено, що право на прийняття рішення щодо розповсюдження службової інформації, власником якої є відповідні органи Держприкордонслужби, надати керівникам цих органів. Таким чином, відповідність інформації хоча б одному із пунктів наведених документів є підставою відповідній посадовій особі для надання документу, виробу чи іншого матеріального носія інформації, що містить ці відомості, грифа обмеження доступу.

Проведений аналіз розділів Зводу відомостей, що становлять державну таємницю та Переліку відомостей, що становлять службову інформацію у Держприкордонслужби показав наявність пунктів, що містять «агреговане» визначення ступеня обмеження доступу. Під «агрегованим» пунктом будемо розуміти таку величину кількості інформації попереднього рівня доступу, досягнення якої призводить до підвищення загального рівня обмеження доступу.

Аналіз розділів Зводу відомостей, що становлять державну таємницю показав наявність значної кількості «агрегованих» пунктів, тобто таких, у яких ступінь обмеження доступу підвищується залежно від кількості інформації (рисунок 1).

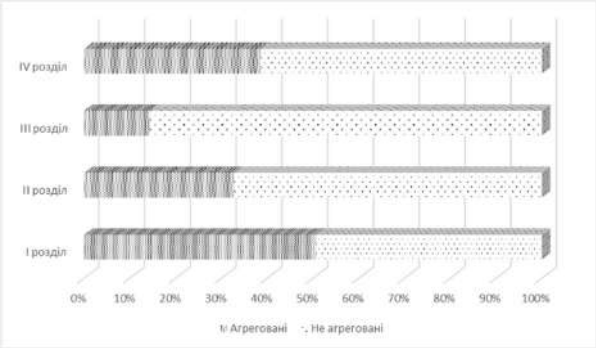



Рис. 1. Співвідношення агрегованих пунктів в ЗВДТ

Наведемо приклад «агрегації», пунктом 1.10.6 «Відомості про комплекс заходів інженерно-технічного облаштування державного кордону та прикордонної смуги…» частиною 3 «щодо ділянки відповідальності регіонального управління, органу охорони державного кордону, загону морської охорони, відділу прикордонної служби ДПС» передбачено присвоєння ступеня секретності «таємно». Разом із тим, пунктами 81 та 83 Наказу № 501 [7] передбачено віднесення інформації за окремими складовими, про заходи інженерно-технічного облаштування державного кордону на ділянці прикордонних підрозділів, до службової. Таким чином, сукупність службової інформації у кількості, що розкриває комплекс заходів інженерно-технічного облаштування державного кордону відділу прикордонної служби ДПС, повинна (відповідно вимог ЗВДТ) мати вищий рівень обмеження доступу.

У цьому контексті керівні документи, що визначають віднесення інформації до певного рівня обмеження доступу, сфокусовані на наявність

певного обсягу інформації конкретний момент часу та на конкретному носії інформації. Тут варто зауважити, що ІТС не є повними аналогами матеріальних носіїв секретної інформації, як визначено в Законі України «Про державну таємницю» від 21 січня 1994 року № 3855-XII [8]. Відмінність полягає у постійній модифікації інформації, зміни її кількості та міграції серед вузлів ІТС.

Розглянемо можливість витоку інформації через приховані канали витоку інформації через незахищений вузол ІТС (на рисунку 2 позначений node 1).

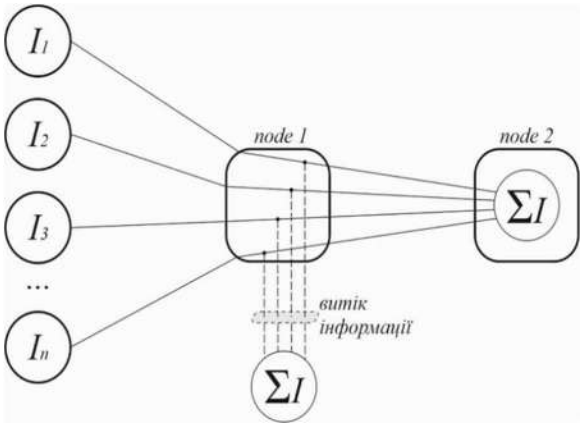



Рис. 2. Варіант витоку інформації через незахищений вузол ІТС

Типова побудова телекомунікаційної мережі передбачає наявність шлюзового вузла, через який проходить вся інформація, що стосується функціонування ІТС, які розгортаються на базі цієї мережі. Припустимо, що інформація, яка циркулює в ІТС, що нами аналізується, не має обмеження доступу. Відповідно до вимог Постанови КМУ від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» [6], наявність засобів технічного захисту інформації, зокрема, забезпечення такої властивості як «конфіденційність», не є обов'язковою. У цьому випадку можливий витік інформації, який дозволить зловмисникам отримати за певний час інформацію, що призначена для вузла node 2. З метою недопущення витоку інформації необхідно застосовувати добре розроблені та апробовані підходи до захисту інформації на вузлах мережі які не обробляють інформацію з обмеженим доступом.

Розглянемо інший варіант, який можливий в інтранет-мережі прикордонного відомства. Державна прикордонна служба України поступово переходить на систему електронного документообігу [9]. Починаючи з 2020 року документообіг Держприкордонслужби стає електронним, що передбачає зберігання електронних документів на серверах системи електронного документообігу. У цьому контексті варто зауважити, що в цій системі циркулюють тільки документи, що не мають грифу обмеження доступу, що, в свою чергу, передбачає відсутність здійснення певних заходів (створення комплексної системи захисту інформації) на вузлах системи та й для системи в цілому.

Припустимо, що вузли системи (node 1 … node n) надсилають k-му вузлу відкриту частину агрегованої інформації в різні моменти часу (рисунок 3).

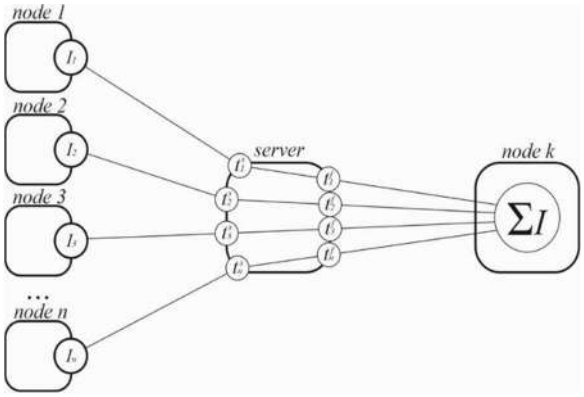



Рис. 3. Проходження інформації через сервер системи

Зазначена інформація надходить на сервер системи в моменти часу $i_i^s$ та зберігається на ньому до моменту часу $i_i^f$ (де $i$ – індекс вузла). Відкладемо на часовій діаграмі періоди знаходження складових агрегованої інформації $\sum I$. Як видно з рисунка 4, можливе існування такого періоду часу, в якому на сервері міститься вся агрегована інформація $\sum I$.

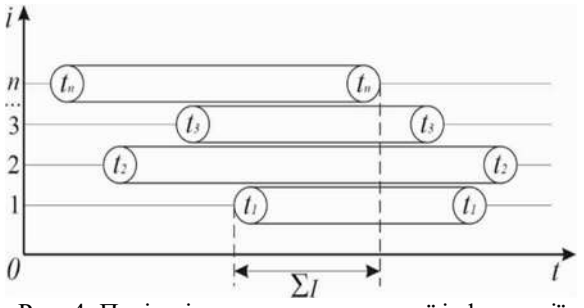



Рис. 4. Період існування агрегованої інформації

Вищенаведене дозволяє стверджувати про можливість знаходження інформації з вищим ступенем обмеження доступу на вузлі ІТС, чим це передбачено наявними дозволами та вимогами.

Аналіз існуючих моделей розмежування доступу показав відсутність врахування в них такого поняття як «агрегована» інформація, що в свою чергу не дозволяє запобігти порушенню її конфіденційності. Вирішення цієї проблеми можливе шляхом формування «агрегованого контейнеру», рівень доступу до якого визначається залежно до його заповнення необхідною інформацією. З метою формалізації цього процесу введемо поняття тематичного класифікатора агрегованого об'єкта, як сукупність підмножин нижчого рівня $\left\{T^Z\right\} = \left\{\tau_1^Z, \tau_1^Z, ..., \tau_n^Z\right\}$, де $z$ – індекс

агрегованого об'єкту, $n$ – кількість складових агрегованого об'єкту, яку визначає виконавець. Кожній складовій тематичного класифікатора та елементам підмножини визначається відповідний рівень конфіденційності, а саме відображення на множину рівнів конфіденційності $F : T^Z \to L, \tau_i^Z \to L$. Аналіз керівних документів показав, що складові $z$-го об'єкта мають однаковий рівень конфіденційності, але в загальному випадку це не є обов'язковим.

Введемо поняття «статус агрегованого контейнеру», таких статусів повинно бути два «доступний» та «критичний». Статус «агрегованого контейнеру» «доступний» присвоюється за наявності ступеня наповненості менше *n-1*. При досягненні заповнення «агрегованого контейнеру» до стану *n-1* його статус визначається як «критичний». Протокол роботи системи з такого типу контейнерами наведено на рисунку 5.

Загальний алгоритм протоколу обміну наступний, при статусі «доступний» заповнення контейнеру здійснюється без обмежень доступу до нього. У випадку переходу контейнера у статус «критичний» вузол, який ініціює заповнення контейнера, інформується про статус контейнера і передає дані на захищений вузол. В цей час, на захищений вузол сервер передає «агрегований контейнер» зі статусом «критичний». В результаті виконання цієї процедури всі вузли ІТС не порушують вимог керівних документів із захисту інформації, а інформація формується та зберігається на захищених вузлах системи.

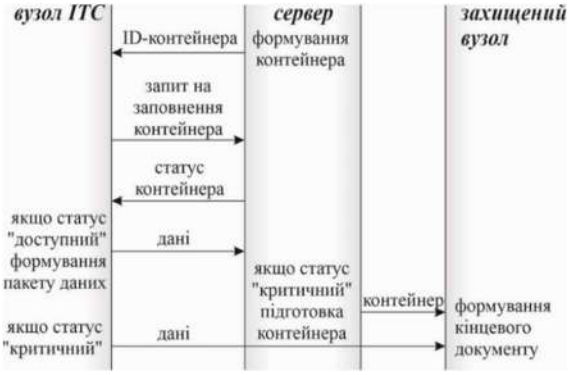



Рис. 5. Узагальнений протокол обміну інформації між вузлами ІТС

## Висновки та перспективи подальших досліджень

Аналіз нормативних документів із класифікації інформації з обмеженим доступом показав, що існуючі моделі розмежування доступу не передбачають наявність «агрегованої» інформації, рівень обмеження доступу якої зростає залежно від її кількості. Визначені можливі канали прихованого витоку інформації без порушення політики безпеки інформаційно-телекомунікаційної системи. Запропоновано спосіб попередження несанкціонованого доступу суб'єктів інформаційної системи шляхом запровадження нового протоколу обміну між вузлами ІТС. Напрямами подальших досліджень є деталізація взаємодії між захищеними та незахищеними вузлами мережі.

## *Література*

**1.** Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99. Затверджено Наказом департаменту спеціальних телекомунікаційних систем та захисту інформації служби безпеки України від "28" квітня 1999 р. № 22. Із змінами згідно наказу адміністрації Держспецзв'язку від 28.12.2012 № 806. **2. Bell D. E.** Unified Exposition and Multics Interpretation MITRE Corporation / D.E. Bell, L.J. LaPadula // Secure Computer System: (1976). [Электрон. ресурс]. – Режим доступа к ресурсу: http://csrc.nist.gov/ publications/history/bell76.pdf. **3. Biba K.** Integrity Considerations for Secure Computer Systems / K. Biba // Technical Report MTR-3153, MITRE Corporation, Bedford, MA (Apr. 1977). **4. Семенов С. Г.** Порівняльні дослідження технологій розмежування доступу для захисту даних в комп'ютерній системі / С. Г. Семенов, В. М. Зміївська, А. В. Голубенко // Системи обробки інформації – 2015. – № 3. – С. 99-102. **5.** Наказ Служби безпеки України від 23.12.2020 № 383. Зареєстровано в Міністерстві юстиції України 14 січня 2021 р. за № 52/35674 «Про затвердження Зводу відомостей, що становлять державну таємницю» https://zakon.rada.gov.ua/laws/show/z0052-21#n7 **6.** Постанова Кабінету Міністрів України від 29 березня 2006 р. № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах». **7.** Наказ Адміністрації Державної прикордонної служби України від «07» липня 2011 року № 501 «Про затвердження Переліку відомостей, що становлять службову інформацію у Державній прикордонній службі України та Інструкції із захисту публічної інформації у Державній прикордонній службі України» (з доповненнями). **8.** Закон України "Про державну таємницю" від 21 січня 1994 року № 3855-XII // Відомості Верховної Ради України (ВВР), 1994, № 16, ст.93. https://zakon.rada.gov.ua/laws/show/3855-12 **9.** Наказ АДПСУ від 08.12.2020 року № 522аг «Про введення в експлуатацію системи електронного документообігу ДПСУ».

## PROTOCOLS FOR THE EXCHANGE OF "AGGREGATED" INFORMATION IN THE INFORMATION AND TELECOMMUNICATION SYSTEM

***Mykhailo Strelbitskyi*** *(doctor of Engineering, professor)*
***Valentyn Mazur*** *(doctor of military sciences, professor)*
***Volodymyr Lemeshko*** *(candidate of military sciences, docent)*

***Bohdan Khmelnytskyi National Academy of the State Border Guard Service of Ukraine, Khmelnytskyi city, Ukraine***

*In the article, based on the classification of information with limited access, the prerequisites for violation of its confidentiality were determined in compliance with the requirements of the security policy of the information and telecommunications system. It was determined that an increase in the amount of information can lead to an increase in the level of access restriction. Sets of information of this type are defined as "aggregated". The conditions for violation of information security, the level of confidentiality of which depends on its quantity, were given. Possible channels of hidden leakage of information from network nodes without violating the security policy of the information and telecommunications system were identified. A method of preventing unauthorized access of information system subjects by introducing a new exchange protocol between nodes of information and telecommunication systems was proposed. The developed protocol for the exchange of "aggregated" information between network nodes provides for the use of an "aggregated" information container, which ensures the formation of information with a higher level of access on a protected node of the information and telecommunications system.*

***Keywords:*** *information, confidentiality, protocol, information system.*

## *References*

**1.** Criteria for evaluating the security of information in computer systems against unauthorized access. [Kryterii otsinky zakhyshchenosti informatsii v kompiuternykh systemakh vid nesanktsionovanoho dostupu] ND TZI 2.5-004-99. Approved by the Order of the Department of Special Telecommunications Systems and Information Protection of the Security Service of Ukraine dated April 28, 1999 No. 22. Amended in accordance with the Order of the State Special Communications Administration No. 806 dated December 28, 2012. **2.** Bell, D. E., LaPadula, L.J. (1976). Unified Exposition and Multics Interpretation MITRE Corporation. *Secure Computer System*, available at: http://csrc.nist.gov/publications/history/bell76.pdf. **3.** Biba K. (1976). Integrity Considerations for Secure Computer Systems, Technical Report MTR-3153, MITRE Corporation, Bedford, MA. **4.** Semenov S. H., Zmiivska V.M., Holubenko A.V. (2015). Comparative studies of access control technologies for data protection in a computer system. [Comparative studies of access control technologies for data protection in a computer system], Information processing systems , No 3, pp 99-102. **5.** On the approval of the Compendium of information constituting a state secret. [Pro zatverdzhennia Zvodu vidomostei, shcho stanovliat derzhavnu taiemnytsiu] (2021). Order of the Security Service of Ukraine dated 12/23/2020 No. 383. Registered with the Ministry of Justice of Ukraine on January 14, 2021 under No. 52/35674, available at: https://zakon.rada.gov.ua/laws/show/z0052-21#n7 **6.** On the approval of the Rules for ensuring the protection of information in information, electronic communication and information and communication systems . [Pro zatverdzhennia Pravyl zabezpechennia zakhystu informatsii v informatsiinykh, elektronnykh komunikatsiinykh ta informatsiino-komunikatsiinykh systemakh], (2006). Resolution of the Cabinet of Ministers of Ukraine dated March 29, 2006 No. 373 **7.** On the approval of the List of information constituting official information in the State Border Service of Ukraine and the Instructions for the protection of public information in the State Border Service of Ukraine" (with additions). [Pro zatverdzhennia Pereliku vidomostei, shcho stanovliat sluzhbovu informatsiiu u Derzhavnii prykordonnii sluzhbi Ukrainy ta Instruktsii iz zakhystu publichnoi informatsii u Derzhavnii prykordonnii sluzhbi Ukrainy» (z dopovnenniamy)], (2011). Order of the Administration of the State Border Service of Ukraine dated July 7, 2011 No. 501 **8.** Law of Ukraine "On State Secrets" [Zakon Ukrainy "Pro derzhavnu taiemnytsiu] (1994). available at: https://zakon.rada.gov.ua/laws/show/3855-12 **9.** On putting into operation the system of electronic document circulation of the DPSU. [Pro vvedennia v ekspluatatsiiu systemy elektronnoho dokumentoobihu DPSU] (2020). Order of the Administration of the SBGSU dated 08.12.2020 No. 522ah.

DOI:**10.33099/2311-7249/2023-46-1-56-62**

УДК: 621.762:621.396.96

***Ігор Михайлович Невмержицький*** *(кандидат технічних наук, доцент)*
***Андрій Аркадійович Гризо*** *(кандидат технічних наук, доцент)*
***Артем Олександрович Дідковський***

***Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків, Україна***

# ПРОЄКТУВАННЯ ВІЗУАЛЬНО-ІМІТАЦІЙНОГО SIMULINK-ДОДАТКА ДЛЯ МОДЕЛЮВАННЯ АДАПТИВНИХ АЛГОРИТМІВ ЗАХИСТУ РАДІОЛОКАЦІЙНИХ СТАНЦІЙ РАДІОТЕХНІЧНИХ ВІЙСЬК ВІД АКТИВНИХ ШУМОВИХ ЗАВАД

*У статті викладено загальні принципи проєктування візуально-імітаційного додатка для моделювання адаптивних алгоритмів захисту радіолокаційних станцій радіотехнічних військ від активних шумових завад. Проєктування проведено за допомогою пакета програм візуального моделювання «Simulink» системи «MATLAB». Алгоритм компенсації активних шумових завад з кореляційним зворотним зв'язком і прямим розрахунком вагових коефіцієнтів використовувався як адаптивний алгоритм захисту. Правильність результатів роботи Simulink-додатка була підтверджена під час проведення експерименту, де на вхід моделі надходили імітовані активні шумові завади, власні шуми основного та додаткового каналів прийому та ехосигнали цілі. Результати моделювання подані за допомогою компонента Scope (осцилограф) бібліотеки блоків Sinks пакета програм візуального моделювання «Simulink». Також надано рекомендації стосовно залучення запропонованого додатка до навчального процесу технічного університету як візуального дидактичного засобу навчання.*

***Ключові слова:*** *Simulink-додаток; візуально-імітаційне моделювання; компенсація завад.*

## Вступ

**Постановка проблеми.** Сьогодні для захисту радіолокаційних станцій (далі – РЛС) радіотехнічних військ (далі – РТВ) від активних шумових завад (АШЗ), використовуються автоматичні компенсатори завад, принцип роботи яких полягає у взаємній кореляції завади в основному та додаткових (компенсаційних) просторових каналах прийому сигналів. Залежно від типу РЛС це можуть бути компенсатори з кореляційним зворотним зв'язком або з прямим розрахунком вагових коефіцієнтів. Останній, здебільшого, використовується в сучасних РЛС з цифровою обробкою (наприклад, РЛС 80К6).

Сьогодні неможливо уявити собі процес проєктування, дослідження та аналізу алгоритмів роботи складних технічних систем озброєння РТВ без використання обчислювальної техніки та сучасного математичного програмного забезпечення. Особливої уваги серед інженерів і науковців займає програмне забезпечення «MATLAB». Це високопродуктивна мова для технічних розрахунків. Вона містить обчислення, візуалізацію і програмування в зручному середовищі, де завдання виражаються у формі, близькій до математичної. Типове використання «MATLAB» – це математичні обчислення, створення алгоритмів, моделювання, аналіз даних, дослідження і візуалізація, наукова інженерна графіка, розробка додатків, враховуючи створення графічного інтерфейсу [1].

Програма «Simulink» це додаток до пакету «MATLAB» (далі – Simulink-додаток), що реалізує принцип візуального програмування. Алгоритм проєктування в «Simulink» наступний – розробник візуально на екрані з бібліотеки стандартних блоків створює модель пристрою і здійснює розрахунки [1]. На відміну від класичних способів моделювання, в цьому випадку, розробнику не потрібно досконально вивчати мову програмування і числові методи математики, а достатньо загальних знань, потрібних під час роботи на комп'ютері та знань тієї області, в якій він працює. Створена Simulink-модель є достатньо самостійним інструментом «MATLAB» і під час роботи з нею зовсім не потрібно знати сам «MATLAB» та інші його додатки.

**Аналіз останніх досліджень і публікацій.** Приклади проєктування Simulink-додатків для моделювання алгоритмів роботи пристроїв завадозахисту РЛС РТВ вже наводилися в [3–6]. Так, у [3] наведено Simulink-додаток квадратурного автокомпенсатора активних шумових завад, у [4] – Simulink-додаток компенсатора імпульсних завад, у [5] – Simulink-додаток пристрою захисту від пасивних завад. У [6] розглянуто загальні підходи щодо використання створених візуально-імітаційних Simulink-додатків в освітньому процесі вищого військового навчального закладу. Разом із тим, поза увагою залишилися питання дослідження ефективності та порівняльного аналізу адаптивних алгоритмів захисту від АШЗ з кореляційним зворотним зв'язком та прямим розрахунком




*ISSN 2311-7249 (Print)/ISSN 2410-7336 (Online)*

вагових коефіцієнтів.

**Мета статті.** Враховуючи вищенаведене метою статті є розробка варіанту візуально-імітаційного додатка для моделювання адаптивних алгоритмів захисту РЛС РТВ від активних шумових завад і порівняння ефективності алгоритмів компенсації активних шумових завад з кореляційним зворотним зв'язком та прямим розрахунком вагових коефіцієнтів, а також надання рекомендацій щодо використання розробленого додатка у навчальному процесі.

## Виклад основного матеріалу дослідження

Загальний процес візуально-імітаційного моделювання засобом «Simulink» наведено в алгоритмі, що детально описаний у [3]. Згідно цього алгоритму на першому етапі проєктування необхідно провести структурний та функціональний аналіз.

Для проведення структурного аналізу алгоритмів компенсації активних шумових завад з кореляційним зворотним зв'язком та прямим розрахунком вагових коефіцієнтів слід використовувати їх структурні схеми. Структурна схема алгоритму компенсації завад з кореляційним зворотним зв'язком представлена на рис. 1 [2].

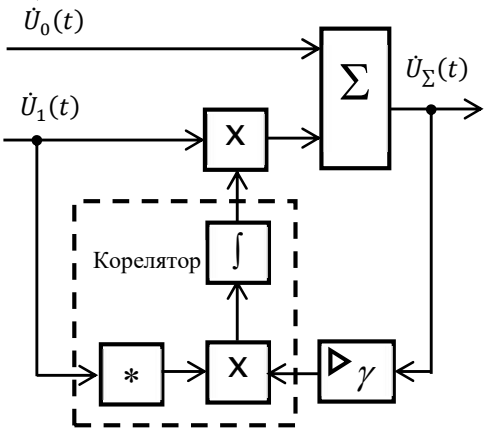



Рис. 1. Алгоритм компенсації завад з кореляційним зворотним зв'язком

Робота компенсатора з кореляційним зворотним зв'язком описується системою рівнянь (1) і (2) [2]:

$$\dot{U}_\Sigma(t) = \dot{U}_0(t) + \dot{K}(t) \cdot \dot{U}_1(t) \qquad (1)$$

$$T \cdot {d\dot{K}(t)}/{dt} + \dot{K}(t) = -\gamma \cdot \dot{U}_\Sigma(t) \cdot \dot{U}_1^*(t), \qquad (2)$$

де $\dot{U}_0(t)$ , $\dot{U}_1(t)$ , $\dot{U}_\Sigma(t)$ – комплексні обвідні процесів відповідно на вході основного і допоміжного каналів прийому сигналів та на виході автокомпенсатора; $\dot{K}(t)$ – комплексна величина керуючого (вагового) коефіцієнта; $T$ – стала часу інтегрування; $\gamma$ – коефіцієнт підсилення напруги в колі зворотного зв'язку; "*" – знак комплексного спряження.

В усталеному режимі величина керуючого коефіцієнта визначається згідно (3) [2]:

$$\dot{K} = -\gamma \cdot \overline{\dot{U}_\Sigma(t) \cdot \dot{U}_1^*(t)}, \qquad (3)$$

де "—" – знак математичного усереднення в часі.

Якщо співвідношення (1) підставити до (3), то можна знайти кінцевий вираз для керуючого коефіцієнта [2]:

$$\dot{K} = -\gamma \cdot \overline{\left[\dot{U}_0(t) + \dot{K} \cdot \dot{U}_1(t)\right] \cdot \dot{U}_1^*(t)}.$$

Розкривши дужки, отримаємо:

$$\dot{K} = -\gamma \cdot \overline{\dot{U}_0(t) \cdot \dot{U}_1^*(t)} - \gamma \cdot \dot{K} \cdot \overline{\dot{U}_1(t) \cdot \dot{U}_1^*(t)},$$

звідки (4)

$$\dot{K} = -{\gamma \cdot \overline{\dot{U}_0(t) \cdot \dot{U}_1^*(t)}}\Big/{1 + \gamma \cdot \overline{\dot{U}_1(t) \cdot \dot{U}_1^*(t)}}. \qquad (4)$$

При виборі коефіцієнта $\gamma$ таким, що $\gamma \cdot \overline{\dot{U}_1(t) \cdot \dot{U}_1^*(t)} >> 1$, згідно [2] отримаємо (5):

$$\dot{K} = -{\overline{\dot{U}_0(t) \cdot \dot{U}_1^*(t)}}\Big/{\overline{\dot{U}_1(t) \cdot \dot{U}_1^*(t)}} =$$

$$= -{\dot{\rho} \cdot \sigma_0 \cdot \sigma_1}\Big/{\sigma_1^2} = -\dot{\rho}\,{\sigma_0}/{\sigma_1}, \qquad (5)$$

де $\dot{\rho}$ – комплексний коефіцієнт кореляції процесів $\dot{U}_0(t)$ і $\dot{U}_1(t)$ ; $\sigma_0, \sigma_1$ – середньоквадратичні значення процесів $\dot{U}_0(t)$ і $\dot{U}_1(t)$.

Розрахунок коефіцієнта кореляції $\dot{\rho}$ здійснювався згідно виразу (6):

$$\dot{\rho} = {\overline{\dot{U}_{0К}(t) \cdot \dot{U}_{ДК}^*(t)}}\Big/{\sigma_{0К} \cdot \sigma_{ДК}} \qquad (6)$$

Середньоквадратичні значення процесів $\sigma_{0К}, \sigma_{ДК}$ розраховуються як корінь квадратний з дисперсії сигналів завад в основному та додатковому каналах прийому.

Позначення $U_{ДК}^*(t)$ – означає комплексне спряження.

Тоді процес на виході автокомпенсатора можна подати так (7):

$$\dot{U}_\Sigma(t) = \dot{U}_0(t) - \dot{\rho} \cdot {\sigma_0}/{\sigma_1} \cdot \dot{U}_1(t) \qquad (7)$$

Потужність (дисперсія) процесу на виході автокомпенсатора (8) [2]:

$$\sigma_\Sigma^2 = {1}/{2} \cdot \overline{\dot{U}_\Sigma(t) \cdot \dot{U}_\Sigma^*(t)}. \qquad (8)$$

Коефіцієнт придушення завад знайдемо як співвідношення потужності процесу (шумових завад) на вході автокомпенсатора до потужності процесу на його виході (9) [2]:

$$К_П = {\sigma_0^2}\Big/{\sigma_\Sigma^2} = {1}\Big/{(1 - |\dot{\rho}|^2)} \qquad (9)$$

Отримані аналітичні вираження є результатом проведеного функціонального аналізу алгоритму роботи компенсатора АШЗ. У подальшому вони використовуються для проведення візуально

імітаційного моделювання з використанням пакета «Simulink».

Перед початком моделювання необхідно налаштувати параметри моделювання. Для цього в пакеті «Simulink» потрібно встановити: час моделювання Start time: 0, Stop time: 20; метод (крок) моделювання Type: Fixed-step (фіксований); Fixed-step size (fundamental sample time): 1/1000; Solver: $ode3(Bogacki-Shampine)$. Тепер можна приступати до створення Simulink-моделі імітаторів вхідних сигналів для компенсатора АШЗ. Вхідними сигналами для компенсатора є сигнали АШЗ, власні шуми основного і додаткового каналів прийому та ехосигнали від цілі. Приклад Simulink-моделі імітатора АШЗ наведено на рис. 2.

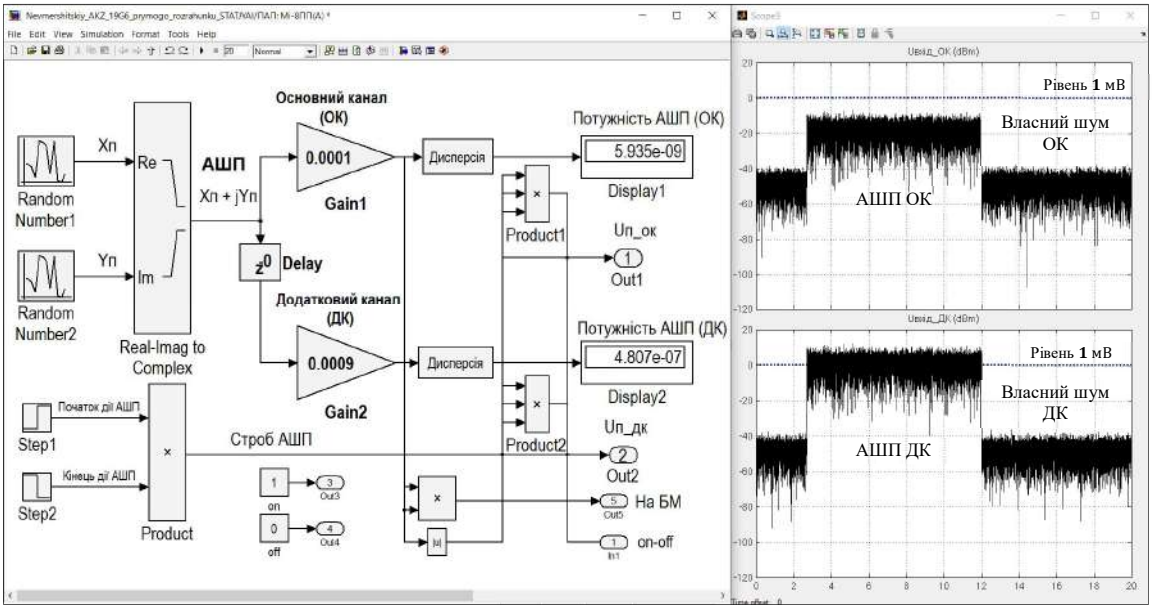



Рис. 2. Simulink-модель імітатора АШЗ

Як видно з рисунку, для імітації квадратурних складових АШЗ необхідно використовувати два блоки Random Number (бібліотека DSP System Toolbox). Для обох блоків (Random Number1 та Random Number2) необхідно встановити параметр Mean: 0; Variance: 1; Sample time: −1. Параметр Seed (зерно) для першого блока Random Number1 повинен бути Seed: 1, а для блока Random Number2 Seed: 567568 (будь-яке, але обов'язково інше).

За допомогою блока Real-Imag to Complex необхідно об'єднати квадратурні складові завади і спрямувати їх через два перемножувачі Product1 та Product2 до вихідних портів Out1 та Out2 відповідно. Для забезпечення зміни амплітуди і фази (затримки) комплексних амплітуд сигналів завад в основному та додатковому каналах прийому, до створеної схеми слід додати елементи Gain1 та Gain2 з бібліотеки Commonly Used Blocks, а також елемент затримки Delay бібліотеки DSP System Toolbox з пакета «Simulink». Для задавання інтервалу дії АШЗ під час імітації слід використовувати елементи Step1 та Step2, а також елемент Product, що формує цей інтервал (Строб АШЗ). Для вимірювання та відображення потужності сигналів, що імітуються в каналах, застосовуються блоки Дисперсія та Display1 і Display2. Результати створення Simulink-моделей імітатора власних шумів основного та додаткового каналів прийому та імітатора ехосигналів від цілі в даній статті не наводяться, але підхід щодо їх створення залишається аналогічним. Далі необхідно послідовно створити спочатку Simulink-модель компенсатора АШЗ з кореляційним зворотним зв'язком, а вже після цього, на його базі, створити Simulink-модель компенсатора з прямим розрахунком вагових коефіцієнтів.

На рисунку 3, для прикладу наведені Simulink-моделі алгоритмів компенсації АШЗ з кореляційним зворотним зв'язком та прямим розрахунком вагових коефіцієнтів відповідно. Візуалізація Simulink-моделей алгоритмів компенсації АШЗ показує, що основною відмінністю компенсатора з прямим розрахунком вагових коефіцієнтів є відсутність зворотного зв'язку (рис. 3).

Крім цього, для розрахунку комплексного коефіцієнта передачі компенсатора використовується вираз (5), де у чисельнику розраховується кореляційний момент між завадою в основному і додатковому каналах прийому $\overline{\dot{U}_{\text{ОК}} \cdot \dot{U}^*_{\text{ДК}}}$, а у знаменнику дисперсія завади, що діє у додатковому каналі прийому $\overline{\dot{U}_{\text{ДК}} \cdot \dot{U}^*_{\text{ДК}}}$.

Приклади створених Simulink-моделей фазообертача на $90^0$ та обчислювача кореляційного моменту між завадою у додатковому каналі й завадою на виході компенсатора наведено на рис. 4 і рис. 5.

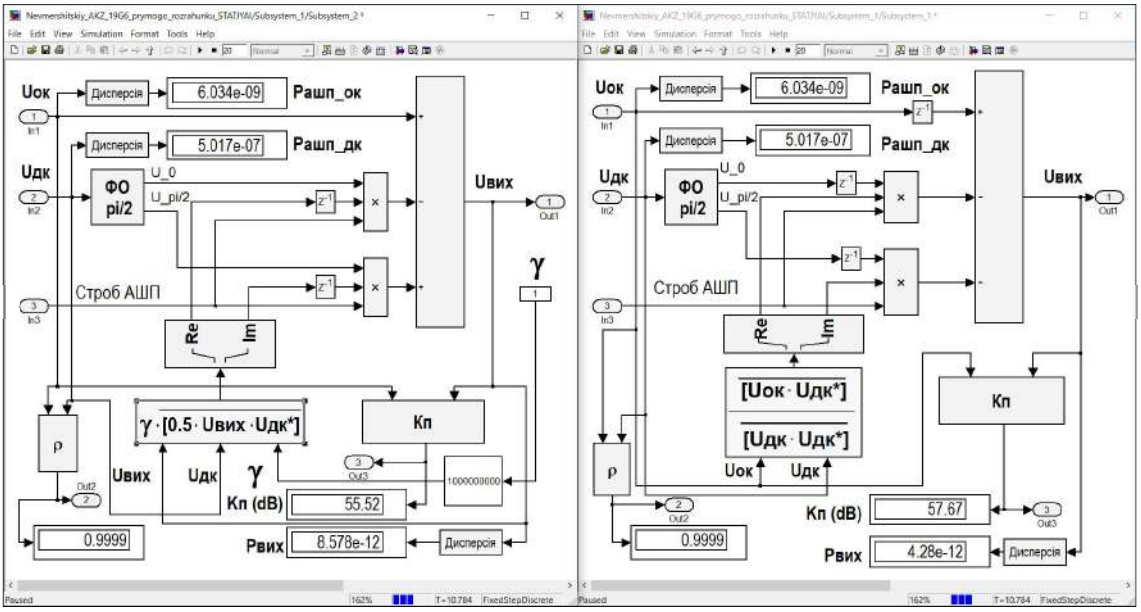



Рис. 3. Simulink-моделі алгоритмів компенсації АШЗ:
а) з кореляційним зворотним зв'язком; б) з прямим розрахунком вагових коефіцієнтів

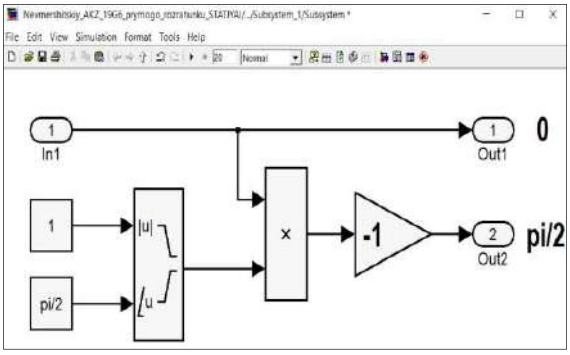



Рис. 4. Simulink-модель фазообертача на $90^0$

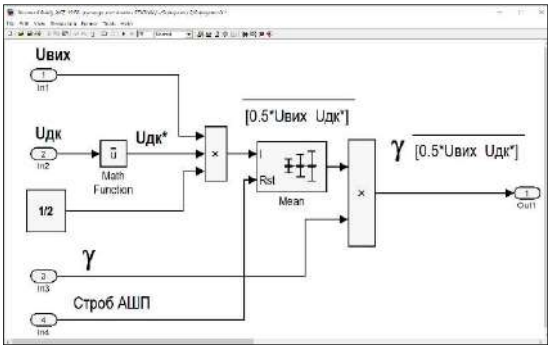



Рис. 5. Simulink-модель обчислювача кореляційного моменту між $\dot{U}_{\text{ВИХ}}$ та $\dot{U}_{\text{ДК}}$

Перед проведенням експерименту і оформленням результатів роботи компенсаторів завад, необхідно навести умови та вимоги, що ставилися перед початком проєктування.

Перше – проєктування та розробка здійснювалася компенсаторів АШЗ квадратурного типу, при цьому передбачалося, що амплітудно-частотні та фазочастотні характеристики основного і додаткового каналів компенсаторів ідентичні.

Друге – компенсатори працюють у режимі компенсації бічних пелюсток, тобто забезпечують захист від одного джерела АШЗ, що діє за бічними пелюстками діаграми спрямованості антени РЛС. Такий захист реалізується шляхом використання просторової фільтрації, що полягає у застосуванні рознесених у просторі антен. Це призводять до погіршення компенсації АШЗ, чим більша її ширина спектру [2].

Виходячи з цього, третє – набіг фази між каналами встановлений нульовим (рис. 2, параметр Delay units блока Delay задано: 0).

Четверте – власні шуми та активна шумова завада імітувалися блоками Random Number, що імітують випадковий сигнал з нормальним розподілом Ґауса (рис. 2). Власні шуми в каналах компенсатора некорельовані, тому параметр Seed блоків Random Number, що імітують квадратурні складові шумових сигналів, необхідно задавати різними для основного та компенсаційного каналів.

У якості АШЗ імітується корельований шум також з нормальним розподілом Ґауса. Параметри блоків Random Number1 та Random Number2 (рис. 2), що імітують квадратурні складові сигналу АШЗ, задані вище. Час дії АШЗ під час експерименту задавався за допомогою сигналу Строб АШЗ. За допомогою цього сигналу на вхід компенсаторів подавалися сигнали АШЗ-1 (короткотривала) та АШЗ-2 (довготривала). Потужність (дисперсія) АШЗ у основному та додатковому каналах прийому перевищувала потужність власних шумів каналів на 45– 50 дБ.

П'яте – усі імітаційні Simulink-моделі компенсаторів повинні передбачати розрахунок та відображення потужності (дисперсії) активної шумової завади на вході основного і додаткового каналів обробки ( $P_{\text{ашп\_ОК}}, P_{\text{ашп\_ДК}}$ ), та на виході автокомпенсатора $P_{\text{ВИХ}}$.

На рис. 6 наведено Simulink-модель розрахунку

дисперсії сигналів. Для створення моделі використовується блок Mean.

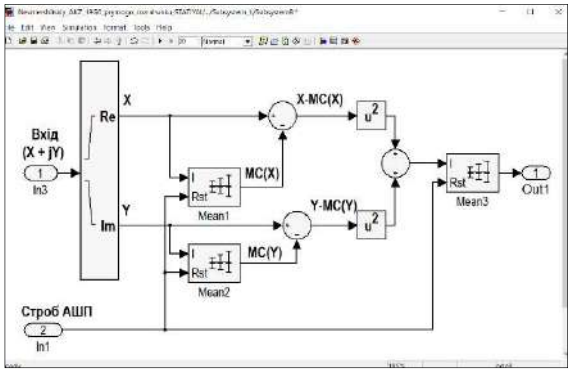



Рис. 6. Simulink-модель розрахунку дисперсії

Цей блок обчислює математичне сподівання вхідних даних векторів певної розмірності. Для того щоб блок Mean відстежував середнє значення в послідовності вхідних даних, необхідно встановити прапорець Running mean (поточне середнє). Крім цього, необхідно вказати подію скидання за допомогою параметра порту скидання Reset port: $Falling\ edge$ (скидання поточного середнього за спадом імпульсу). Таке скидання відбуватиметься щоразу, коли на додатковому порту Rst блока Mean виявляється подія скидання. У нашому випадку це імпульс Строб АШЗ. Імпульс повинен бути позитивної полярності та кратним до часу вибірки вхідного сигналу.

Шосте – необхідно передбачити розрахунок коефіцієнта кореляції АШЗ у основному та додатковому каналах прийому ( $\rho$ ). Такий розрахунок здійснюється згідно аналітичного виразу (6).

Приклад Simulink-моделі розрахунку коефіцієнта кореляції наведено на рис. 7.

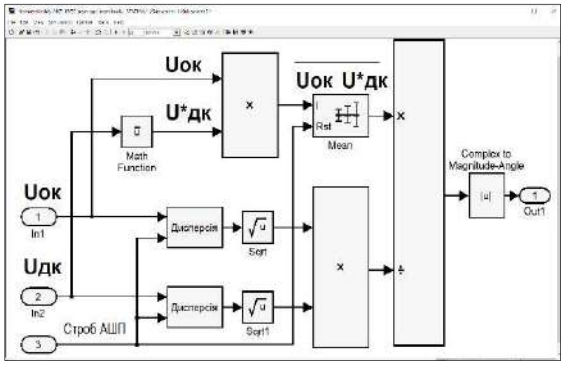



Рис. 7. Simulink-модель розрахунку коефіцієнта кореляції

Як бачимо, для отримання комплексно спряженої величини $U^*_{ДК}$ використовується блок Math Function, параметр Function якого встановлений: $conj$ (комплексне спряження). Блок Sqrt з бібліотеки математичних блоків Simulink/Math Operations призначений для визначення квадратного кореня з кожного елемента масиву вхідних даних. Параметр Function даного блока необхідно встановити: $sqrt$. Блок Complex to Magnitude-Angle з цієї ж бібліотеки приймає комплексний сигнал типу double або single. На виході цього блока маємо модуль вхідного сигналу. Для цього параметр Output даного блока необхідно встановити: $Magnitude$ (величина). Для розрахунку коефіцієнта придушення (компенсації) АШЗ використовується вираз (9). Розраховані значення коефіцієнта компенсації АШЗ наводяться в децибелах Кп$(dB)$. Simulink-модель розрахунку коефіцієнта компенсації АШЗ у даній статті не наводиться.

Сьоме – результат роботи квадратурного компенсатора АШЗ з прямим розрахунком вагових коефіцієнтів необхідно було подати порівняно з квадратурним компенсатором АШЗ з кореляційним зворотним зв'язком. Осцилограми сигналів, за результатами експерименту, необхідно було подати за допомогою компонента Scope (осцилограф) з бібліотеки блоків Simulink/Sinks.

На рис. 8 наведено результати експерименту, зокрема осцилограми сигналів на вході (*а*) та виході (*б, в*) компенсаторів з прямим розрахунком вагових коефіцієнтів та з кореляційним зворотним зв'язком відповідно. Праворуч показано результати розрахунку коефіцієнта придушення АШЗ (*г*) та осцилограма сигналу Строб АШЗ (*д*).

Результати експерименту свідчать, що компенсатор з прямим розрахунком вагових коефіцієнтів має переваги порівняно з компенсатором з кореляційним зворотним зв'язком (рис. 8). Результати імітаційного моделювання підтверджують, що компенсатор з кореляційним зворотним зв'язком має перехідні процеси при адаптації (рис. 8, *в*). Як відомо з [2] тривалість таких перехідних процесів залежить від модуля (амплітуди) напруги комплексного завадового сигналу у додатковому (компенсаційному) каналі прийому та коефіцієнта підсилення у колі зворотного зв'язку $\gamma$.

Створена Simulink-модель імітатора АШЗ (рис. 2) дозволяє задавати будь-яку величину (амплітуди) напруги комплексного завадового сигналу в додатковому каналі прийому.

Для нашого випадку, за умовою експерименту, в межах сигналів Строб АШЗ1 і Строб АШЗ2 амплітуда напруги сигналу у додатковому каналі прийому змінювалася випадково у межах: 0,1 ... 4 мВ. Також завдяки Simulink-моделі компенсатора з кореляційним зворотним зв'язком (рис. 3) є можливість задання коефіцієнта підсилення у колі зворотного зв'язку. За умовою проведеного експерименту, він становив: $\gamma = 1{,}2 \cdot 10^8$. Відображені на рис. 8 результати експерименту свідчать, що *г* стійкість роботи компенсатора завад з прямим розрахунком вагових коефіцієнтів та його швидкодія вищі за компенсатор завад з кореляційним зворотним зв'язком. Це підтверджує швидкість зростання коефіцієнта придушення завади в часі. Оскільки час дії активної завади обмежувався сигналами Строб АШЗ1 та Строб АШЗ2, то за час дії завади алгоритм адаптації компенсатора з прямим розрахунком вагових коефіцієнтів показав набагато кращий результат (рис. 8, *г, д*).

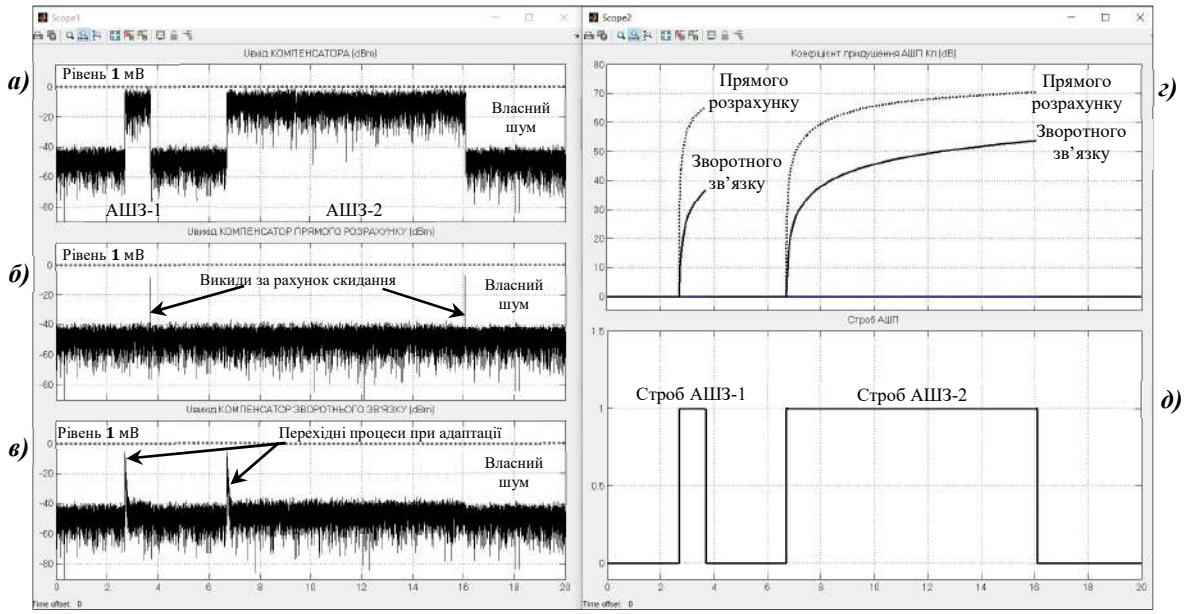



Рис. 8. Результати експерименту:
*а)* сигнали на вході компенсаторів завад; *б)* сигнали на виході компенсатора завад з прямим розрахунком вагових коефіцієнтів; *в)* сигнали на виході компенсатора завад з кореляційним зворотним зв'язком; *г)* коефіцієнт придушення АШЗ; *д)* Строб АШЗ

Візуалізовані на рис. 8, *б* результати експерименту показують, що компенсатор з прямим розрахунком вагових коефіцієнтів має два потужні викиди, що збігаються у часі зі спадами сигналів Строб АШЗ1 та Строб АШЗ2. Тривалість цих викидів дорівнює одному кроку модельного часу (у нашому випадку це $1/1000$). Такі викиди під час роботи моделі пояснюються імпульсами з порту скидання Reset port: Falling edge. Це імпульси скидання поточного середнього за спадом імпульсу блоків Mean з бібліотеки DSP System Toolbox пакета Simulink.

## Висновки та перспективи подальших досліджень

Отже, під час проєктування та розробки візуально-імітаційного Simulink-додатка, що імітує адаптивні алгоритми захисту радіолокаційних станцій радіотехнічних військ від активних шумових завад, слід використовувати принципи системного підходу. Вирішальним значенням, за такої розробки, є детальне проведення структурного та функціонального аналізу об'єкта моделювання.

Створений Simulink-додаток є потужним і універсальним засобом для дослідження та оцінки ефективності адаптивних алгоритмів захисту радіолокаційних станцій радіотехнічних військ від активних шумових завад. Наведені результати експерименту, із застосуванням створеного Simulink-додатка, підтверджують його працездатність та не суперечать вже відомим результатам. Водночас експеримент засвідчив, що адаптивний алгоритм захисту радіолокаційних станцій від активних шумових завад з прямим розрахунком вагових коефіцієнтів має переваги порівняно з адаптивним алгоритмом захисту радіолокаційних станцій від активних шумових завад з кореляційним зворотним зв'язком. Стійкість роботи алгоритму з прямим розрахунком вагових коефіцієнтів та його швидкодія вищі за алгоритм з кореляційним зворотним зв'язком.

Висока наочність Simulink-додатка та результатів його роботи відкриває широкі можливості для викладачів стосовно його використання як дидактичного засобу навчання. Так, візуалізація процесів компенсації активних шумових завад, в реальному масштабі часу, сприяє розвитку творчих здібностей курсантів (студентів) завдяки індивідуалізації навчання та появи можливості самостійно виконувати й намагатися ухвалювати власні технічні рішення, що перетворює навчальний процес у захоплююче заняття.

Наприкінці зазначимо, що перспективними можуть стати дослідження спрямовані на вирішення актуального наукового завдання щодо створення нових та модернізації вже існуючих адаптивних алгоритмів захисту радіолокаційних станцій радіотехнічних військ від активних шумових завад.

## *Література*

**1. Дэбни Дж., Харман Т.** Simulink® 4. Секреты мастерства / пер. с англ. М. Л. Симонова. Москва : БИНОМ. Лаборатория знаний, 2003. 403 с.
**2. Ширман Я. Д., Манжос В. Н.** Теория и техника обработки радиолокационной информации на фоне помех. Москва : Радио и связь, 1981. 416 с.
**3. Невмержицький І. М., Гризо А. А., Малишев О. А., Купрій В. М.** Моделювання елементів систем озброєння

радіотехнічних військ засобами візуально-імітаційного моделювання Simulink. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2009. № 1(19). С. 66–69. **4. Невмержицький І. М., Гризо А. А., Калініченко І. І., Клименко Р. Ю.** Візуально-імітаційне моделювання цифрового компенсатора несинхронних імпульсних завад, що реалізує подвійне перетворення Хартлі. *Системи озброєння і військова техніка*. 2010. № 4(24). С. 141–145. **5. Невмержицький І. М., Гризо А. А., Матвійчук М. А., Семенов В. С., Гуйда Е. І.** Проєктування візуально-імітаційних додатків для моделювання алгоритмів селекції рухомих цілей існуючих та модернізованих РЛС РТВ за допомогою пакету Simulink. *Наука і техніка Повітряних Сил Збройних Сил України*. 2017. № 2(27). С. 105–109. **6. Невмержицький І. М., Дацків Ю. І., Сидоренко Д. С., Оленин О. М.** Досвід використання в освітньому процесі університету Simulink-додатків для візуально-імітаційного моделювання алгоритмів перешкодозахисту радіолокаційних станцій радіотехнічних військ. *Системи обробки інформації*. 2019. № 1(156). С. 112–117.

## DESIGNING OF A VISUAL SIMULATION SIMULINK APPLICATION FOR MODELING ADAPTIVE ALGORITHMS FOR THE PROTECTION OF RADARS OF RADIO ENGINEERING TROOPS AGAINST ACTIVE NOISE INTERFERENCE

***Igor Nevmerzhitsky*** *(Candidate of Technical Sciences, Associate Professor*
***Andrii Hryzo*** *(Candidate of Technical Sciences, Associate Professor)*
***Artem Didkovskyi***

***Kharkiv national Air Force University named after I. Kozhedub, Kharkiv, Ukraine***

*The article gives the general principles for designing a visual simulation application for modeling adaptive algorithms for protecting radar stations of the radio engineering troops against active noise interference. The designing was made using the Simulink visual modeling software package of the MATLAB system. As adaptive protection algorithms, an active noise interference compensation algorithm with correlative feedback connection and direct calculation of weight coefficients was used. The correctness of the results of the Simulink application was confirmed during the experiment, where the simulated active noise interference, intrinsic noises of the main and additional receiving channels and echo signals of the target were input to the model. Simulation results are presented using the Scope component (oscilloscope) of the Sinks block library of the Simulink package. Recommendations are also given on the inclusion of the proposed application in the educational process of a technical university as a visual didactic learning tool.*

***Keywords:*** *Simulink application; visual simulation modeling; interference compensation.*

## *References*

**1. Dabney, J., Harman, T.** (2003) Simulink® 4. Mastering Simulink 4. Translated from English by M. Simonova. Moscow: BINOM. Laboratoriya znaniy, 403. **2. Shirman, Ya. D., Manzhos, V. N.** (1981) Theory and technique of processing radar information against the background of interference, Radio i svyaz, Moscow, 416. **3. Nevmerzhitsky, I. M., Hryzo, A. A., Malyshev, O. A. and Kuprii, V. M.** (2009), Modelling of elements of systems of arms of radio engineering armies by means of visual - imitating modelling Simulink. Scientific Works of Kharkiv National Air Force University, 1(19), 66–69. **4. Nevmerzhitsky, I. M., Hryzo, A. A., Kalinichenko, I. I., Klimenko R. Ju.** (2010) Visual-imitating modelling of the digital equalizer of the nonsynchronous pulse handicaps realizing double discrete transformation Hartly. Systems of Arms and Military Equipment, 4(24), 141–145. **5. Nevmerzhitsky, I. M., Hryzo, A. A., Matviychuk, M. A., Semenov, V. S. and Guyda, E. I.** (2017) Designing visual-imitating applications for modeling algorithms of selection of moving targets for existing and modernized RTV radars with Simulink package. Science and Technology of the Air Force of Ukraine, 2(27), 105–109. **6. Nevmerzhitsky, I. M., Datskiv, Y. I., Sidorenko, D. S., Olenin, O. N.** (2019) Experience of use in the educational process of the university Simulink-applications for visual-imitation modeling of interference protection algorithms of radiolocation stations of radiotechnical troops. Information Processing Systems, 1(156), 112–117.

DOI:**10.33099/2311-7249/2023-46-1-63-68**

УДК: 519.81

***Наталія Олександрівна Королюк*** **(*кандидат технічних наук*)**

***Харківський національний університет Повітряних Сил імені Івана Кожедуба, Харків, Україна***

# ПІДХІД ЩОДО АВТОМАТИЗАЦІЇ ШТУРМАНСЬКИХ РОЗРАХУНКІВ ДЛЯ УПРАВЛІННЯ ЛІТАКАМИ ВИНИЩУВАЛЬНОЇ АВІАЦІЇ

*У статті запропоновано загальний порядок виконання попередніх штурманських розрахунків із визначення відстаней рубежу введення винищувачів у бій. Проаналізовано, що застосування сил і засобів збройної боротьби, в ході широкомасштабного вторгнення рф на територію України, свідчить про перехід від концепції «платформо-центричної війни», де основний акцент робиться на кількості озброєння та військової техніки, у бік «мережецентричної війни», основою якої є інтеграція всіх сил і засобів у єдиному інформаційному просторі. Підвищення ефективності управління можливе за рахунок практичної організації єдиного бойового управління всіма військами і силами авіації та протиповітряною обороною. Існуюча методика виконання попередніх штурманських розрахунків, що реалізована в спеціальному математичному та програмному забезпеченні комплексів засобів автоматизації посадовими особами бойової обслуги командного пункту, не враховує конфігурацію радіолокаційного поля залежно від рельєфу місцевості та висот польоту засобів повітряного нападу, зон виявлення та ураження зенітних ракетних комплексів, напрямку польоту засобів нападу. Обмеження впливають на точність їх виконання та обґрунтоване прийняття рішення на бойові дії. Розроблено алгоритм виконання розрахунків із визначення відстані рубежу введення винищувачів у бій. Обґрунтовано порядок розрахунку рубежу введення винищувачів у бій з урахуванням напрямку польоту повітряних цілей відносно заданого рубежу. Впровадження запропонованої методики розрахунку рубежів введення винищувачів у бій в автоматизовану систему дозволить оперативно та ефективно оцінити бойові можливості винищувальної авіації щодо виконання бойового завдання з перехоплення повітряних цілей на заданих рубежах.*

***Ключові слова**: попередні штурманські розрахунки; навігаційно-тактичні рубежі; програма польоту; рубіж введення у бій; перехоплення; автоматизація.*

## Вступ

**Постановка проблеми.** В умовах збройної агресії російської федерації з 2014 року, коли під окупацію потрапили Донецька, Луганська області та Автономна Республіка Крим, що трансформувалася у широкомасштабне вторгнення з 24 лютого 2022 року, особлива увага військових науковців і воєнних практиків надається пошуку адекватної відповіді на щоденні виклики. Можливість віднайти такі відповіді виникає лише за умов належного теоретико-методологічного осмислення сутності сучасних збройної боротьби та зіткнень. Крім того, необхідним у цьому процесі є постійний аналіз, вивчення, узагальнення світового досвіду протистояння воєнним загрозам [1]. Найважливішим стратегічним завданням державної політики залишається забезпечення національної безпеки, захист державного суверенітету, відновлення територіальної цілісності. В умовах загострення військово-політичного стану питання національної безпеки набувають важливого і особливого значення.

Аналіз застосування засобів і сил збройної боротьби в ході широкомасштабного вторгнення свідчить, що основною тенденцією застосування військ є перехід від концепції «платформо-центричної війни», де акцентовано головну увагу на кількості озброєння і військової техніки, у бік «мережецентричної війни», основою якої є інтеграція сил і засобів у єдине інформаційне середовище. Отже це дозволяє суттєво підвищити ефективність бойового застосування сил і засобів протиповітряної оборони (далі – ППО) шляхом зменшення тривалості циклу бойового управління. Підвищення ефективності управління можливе завдяки практичній організації єдиного бойового управління всіма військами і силами авіації і ППО [1–4]. Як показав досвід, угруповання сил та засобів повітряного нападу (далі – ЗПН) здатні виконувати оперативні, тактичні та стратегічні завдання, які обумовлюють підвищення значення боротьби у повітряному просторі для досягнення успіху в окремих операціях збройних сил та у війні в цілому [1; 2]. Аналіз збройних конфліктів та форм агресії російської федерації з 2014 року дозволив визначити наступні особливості повітряних операцій:

завчасне та старанне планування наступальних операцій з використанням нових інформаційних технологій;

висока динамічність бойових дій з використанням всіх видів розвідки, безпілотних літальних апаратів, авіації, ракетних військ, засобів радіо-електронної боротьби;

застосування нових тактичних прийомів;

невизначеність обстановки перед початком і в ході ведення бойових дій, що ускладнює своєчасне прийняття обґрунтованих рішень та їх корегування.

Використання ЗПН передбачає зростання вимог до процесу управління з пунктів управління (далі – ПУ) підпорядкованими силами та засобами [3]. Однією з вимог щодо ефективної боротьби з повітряним противником (далі – ПП) є оперативна оцінка повітряної обстановки (далі – ПО) та прийняття рішення щодо подальших дій підпорядкованими силами та засобами ППО.

Швидкоплинність та зростаюча динамічність бойових дій, високий ступінь невизначеності обстановки, необхідність оперативного аналізу, жорсткі часові межі та врахування значної кількості різнорідних факторів свідчать про необхідність підвищення рівня автоматизації процесів оцінки ПО, визначення задуму ПП та реалізації штурманських розрахунків для управління літаками винищувальної авіації.

Під час підготовки та в ході ведення бойових дій посадові особи бойової обслуги командного пункту (далі – КП) повинні виконати низку штурманських розрахунків із визначення бойових можливостей винищувальної авіації щодо виконання бойового завдання з прикриття особливо важливих об'єктів держави та угрупувань військ, необхідних командиру для прийняття рішення. Важливість розрахунків полягає у визначенні навігаційно-тактичних рубежів [1; 4]. На основі проведених штурманських розрахунків обираються способи бойових дій, місце розташування зон чергування в повітрі, розглядаються питання перебазування підрозділів авіації на передові (оперативні) аеродроми, дислокація підрозділів радіотехнічних військ, які забезпечують збір, обробку та видачу радіолокаційної інформації про повітряну обстановку [4].

Наявна методика виконання попередніх штурманських розрахунків, що реалізована в спеціальному математичному та програмному забезпеченні комплексів засобів автоматизації посадовими особами бойової обслуги КП не враховує конфігурацію радіолокаційного поля залежно від рельєфу місцевості та висот польоту ЗПН, зон виявлення та ураження зенітних ракетних комплексів, напрямок польоту ЗПН. Обмеження впливають на точність їх виконання та обґрунтоване прийняття рішення на бойові дії. Таким чином, виникають помилки, пов'язані з неврахуванням вищезазначених особливостей, що може призвести до зменшення ймовірності виконання бойового завдання з прикриття особливо важливих об'єктів держави, а в деяких випадках взагалі до його невиконання [3; 5]. Автоматизація проведення оперативно-тактичних розрахунків та подальше моделювання бойових дій, дозволить підвищити оперативність виконання вищезазначених розрахунків, якість, ефективність прийнятих рішень відповідальною особою на виконання бойового завдання.

**Аналіз останніх досліджень і публікацій.** В роботах [1; 2] розглянуто загальний порядок визначення потрібного та можливого рубежу введення у бій. У праці [4] визначена методика розрахунку навігаційно-тактичних рубежів, яка дозволяє оцінити бойові можливості винищувальної авіації щодо виконання перехоплення ПП. Але в наведеній методиці не враховано напрямок польоту повітряної цілі, конфігурація радіолокаційного поля залежно від рельєфу місцевості та висоти польоту ЗПН. Це не дозволяє бойовій обслузі КП оцінити бойові можливості винищувальної авіації щодо перехоплення повітряних цілей на заданих рубежах.

**Мета статті.** Опис Автоматизація виконання розрахунку навігаційно-тактичних рубежів з урахуванням напрямку, висоти польоту засобів повітряного нападу з метою підвищення точності виконання розрахунків та якості прийнятого рішення.

## Виклад основного матеріалу дослідження

Визначення схеми польоту на знищення повітряної цілі дає змогу автоматизувати процес виконання розрахунків щодо визначення дистанції рубежів введення у бій. Припустимо, на видаленні $D_ц$ від аеродрому вильоту винищувачів виявлена ціль, що летить до нього на висоті $H_ц$ зі швидкістю $V_ц$. Далі приймається рішення щодо її знищення, у визначений час подається команда на зліт винищувачів на перехоплення. Надалі, політ винищувачів до рубежу введення у бій виконується за доцільною програмою, що являє собою певну послідовність зміни висоти і швидкості польоту, при якій досягається набір заданої висоти (розгін літака за мінімальний час). На початку виконання розрахунків щодо визначення відстані можливих рубежів введення винищувачів у бій, необхідно визначити програму польоту на перехоплення повітряної цілі.

Основними характеристиками програми польоту є величини $S_\Sigma$ і $t_\Sigma$, де $S_\Sigma$ – величина відстані винищувача від аеродрому (зони чергування) за час $t_\Sigma$ польоту по програмі. Час $t_\Sigma$ відраховується від моменту подачі команди на зліт (початку наведення) винищувача. Під час польоту винищувачів для знищення повітряної цілі на малих, середніх та великих висотах величини $S_\Sigma$ та $t_\Sigma$ розраховуються за формулами:

$$t_\Sigma = t_{пас} + t_н + t_р + t_м + t_г + t_{пр},$$

$$S_\Sigma = S_н + S_р - L_{см} - S_г \text{ (для задньої півсфери)}, \quad (1)$$

$$S_\Sigma = S_н + S_р + S_г + V_к t_{пр} \text{ (для передньої півсфери).}$$

де $t_{пас}$ - час прийняття рішення на ПУ,

$t_н$, $S_н$ – час та відстань набору висота та швидкості;

$t_р$ , $S_р$ – час та відстань розвороту;

$t_м$ – час маневру;

$t_г$ , $S_г$ – час та відстань польоту в горизонтальній площині;

$t_{пр}$ – час для приводу літака.

Величини $S_\Sigma$ і $t_\Sigma$ за відповідної програми польоту постійні, не залежать від дальності виявлення цілі, якщо виконується умова

$$D_ц + \Delta l_0 - V_ц t_\Sigma > S_\Sigma \qquad (2)$$

де $D_ц$ – дальність до цілі;

$\Delta l_0$ – дистанція виходу на ціль по закінченню розвороту;

$V_ц$ – швидкість цілі.

В цьому випадку відстань рубежу введення винищувача у бій розраховується за виразом:

$$S_{РВБ} = \frac{D_ц + \Delta l_0 - V_ц t_\Sigma + nS_\Sigma}{1+n}. \qquad (3)$$

де $n = \frac{V_ц}{V_в}$ – відношення швидкості цілі до швидкості горизонтального польоту винищувачів у режимі максимальної дальності. Під час атаки у задню півсферу $\Delta l_0$ береться зі знаком «+», а в передню – зі знаком «–». Якщо виникає ситуація, що

$$D_ц + \Delta l_0 - V_ц t_\Sigma < S_\Sigma , \qquad (4)$$

то ділянка горизонтального польоту в режимі максимальної дальності буде відсутня. Основна програма польоту з $S_\Sigma$ і $t_\Sigma$ стане нездійсненною. Тоді необхідно буде знайти таку траєкторію, яка відрізняється від основної меншим значенням $S^*_\Sigma$ і для якої справедлива умова:

$$D_ц + \Delta l_0 - V_ц t_\Sigma = S_\Sigma . \qquad (5)$$

Необхідну програму польоту можна знайти, якщо буде відомий зв'язок між $t^*_\Sigma$ і $S^*_\Sigma$ . Цю програму можна виразити лінійною залежністю:

$$t^*_\Sigma = t_\Sigma - k_\Sigma (S_\Sigma - S^*_\Sigma) , \qquad (6)$$

де $k_\Sigma = \frac{\Delta t_\Sigma}{\Delta S_\Sigma}$ – коефіцієнт, що характеризує зміну $t^*_\Sigma$ і зміну $S^*_\Sigma$ . Під час атаки у задню напівсферу $k_\Sigma$ береться зі знаком «+», а в передню – зі знаком «–». Тоді відстань рубежу введення винищувачів у бій, що визначає програму польоту за відсутності горизонтальної ділянки на режимі максимальної дальності, потрібно розраховувати за формулою:

$$S_{РВБ} = S^*_\Sigma = \frac{D_ц + \Delta l_0 - V_ц t_\Sigma + k_\Sigma V_ц S_\Sigma}{1 + k_\Sigma V_ц} \qquad (7)$$

або, якщо $n^* = k_\Sigma V_ц$ , тоді

$$S_{РВБ} = S^*_\Sigma = \frac{D_ц + \Delta l_0 - V_ц t_\Sigma + n^* S_\Sigma}{1 + n^*}. \qquad (8)$$

Вихідними даними для розрахунку є швидкість польоту цілі ( $V_ц$ ), відстань від аеродрому рубежу виявлення цілі, швидкість винищувачів ( $V_в$ ), характеристики програми польоту на перехоплення $t_\Sigma$ , $S_\Sigma$ , $k_\Sigma$ , $\Delta l_0$ .

Порядок розрахунку відстаней рубежів введення у бій зводиться до такого: визначається величина $S^* = D_ц + \Delta l_0 - V_ц t_\Sigma$ , яка порівнюється з величиною $S_\Sigma$ , і якщо є умова (1), то розрахунок виконується за формулою (2), в іншому випадку – за формулою (3).

Блок-схема алгоритму розрахунку рубежів введення у бій винищувачів наведена на рис. 1.

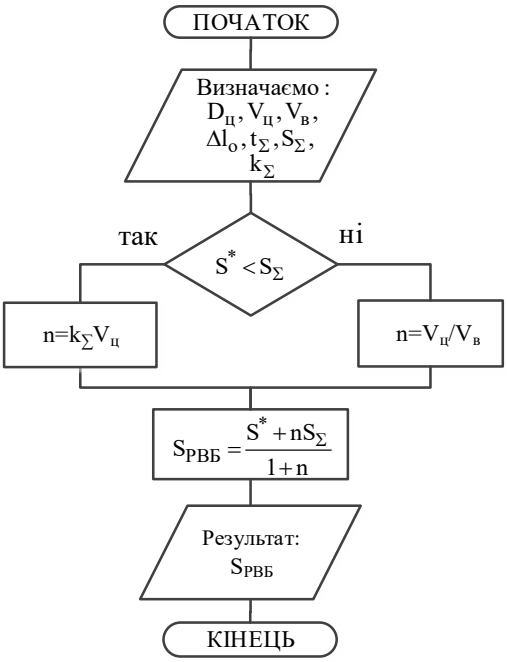



Рис. 1. Блок-схема алгоритму розрахунку рубежів введення у бій

У випадках, коли ціль прямує не на аеродром зльоту винищувачів, а з деяким курсом $\gamma_ц$ (рис. 2), відстань рубежу введення у бій розраховується за формулою

$$S_{РВБ} = \frac{n\hat{S} - \sqrt{\hat{S}^2 + (1-n^2)y^2}}{n^2 - 1}, \quad (9)$$

де

$$\hat{S}^2 = D_ц \cos\alpha - V_ц t_\Sigma + \Delta l_0 + nS_\Sigma \quad (10)$$

$$y = D_ц \sin\alpha,\ n = \frac{V_ц}{V_в},\ \text{якщо}\ D_ц \sin\alpha \geq S_\Sigma, \quad (11)$$

або

$$n = D_ц \cos\alpha - V_ц t_\Sigma + \Delta l_0 \geq \sqrt{S_\Sigma^2 - y^2},\ \text{якщо}\ D_ц \sin\alpha < S_\Sigma \quad (12)$$

$$n = k_\Sigma V_ц,\ D_ц \cos\alpha - V_ц t_\Sigma + \Delta l_0 < \sqrt{S_\Sigma^2 - y^2},\ \text{якщо}\ D_ц \sin\alpha < S_\Sigma, \quad (13)$$

$$\alpha = A_ц - \gamma_ц - 180^0, \quad (14)$$

де $A_ц$ – азимут цілі.

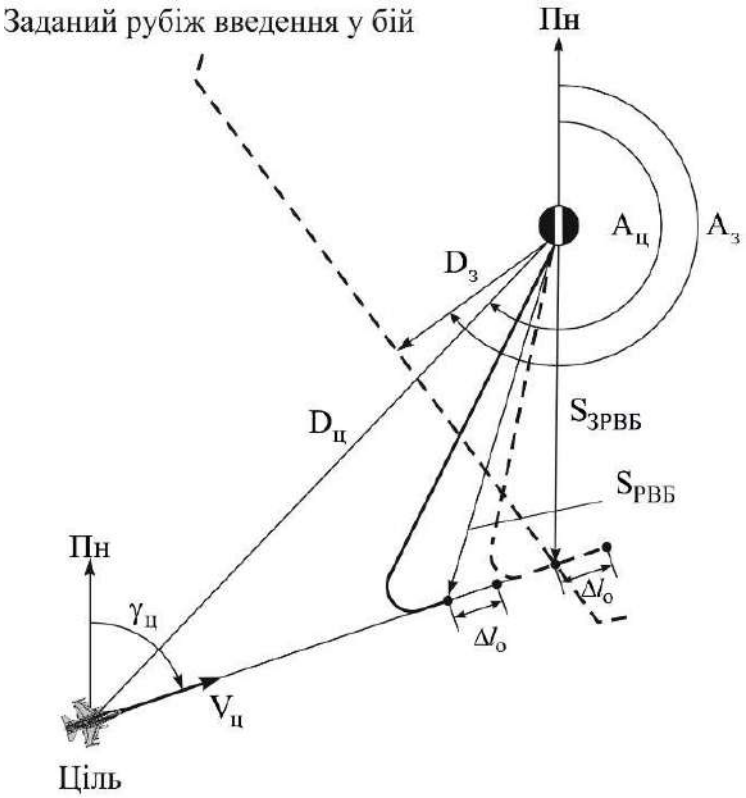



Рис. 2. Схема визначення $S_{РВБ}$

Відстань точки заданого рубежу введення у бій від аеродрому вильоту винищувачів залежить від напрямку її польоту, її положення у момент входу до радіолокаційного поля виявлення і розраховується за формулою:

$$S_{ЗРВБ} = \sqrt{\left(\frac{D_з - D_ц \sin\alpha\cos\beta}{\sin\beta}\right)^2 + y^2} \quad (15)$$

де $D_з$ – найкоротша відстань від аеродрому зльоту до заданого рубежу:

$$\beta = \gamma_ц - A_з - 90^o, \quad (16)$$

$A_з$ – азимут найближчий до аеродрому точки заданого рубежу $S_{ЗРВБ}$.

Порівняння відстаней $S_{РВБ}$ та $S_{ЗРВБ}$ дає підставу припустити, що введення у бій винищувачів на заданому рубежі можливе, якщо значення $\Delta S_{РВБ} = S_{РВБ} - S_{ЗРВБ}$ позитивно, і неможливо, якщо негативно.

Загальний алгоритм визначення рубежу введення винищувачів у бій наведений на рис. 3

Тому, запропонований підхід щодо автоматизації виконання розрахунку навігаційно-тактичних рубежів з урахуванням напрямку, висоти польоту засобів повітряного нападу з метою підвищення точності виконання розрахунків та якості прийнятого рішення. Запропонований підхід сприятиме збільшенню ймовірності виконання бойового завдання з прикриття особливо важливих об'єктів держави.

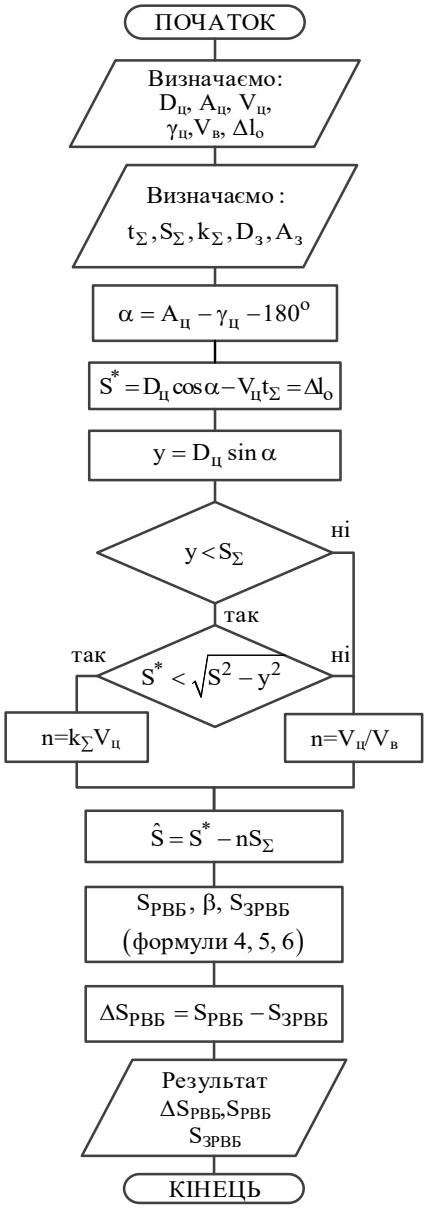



Рис. 3. Загальний алгоритм розрахунку РВБ

## Висновки та перспективи подальших досліджень

Узагальнюючи зазначимо, що у статті запропоновано підхід визначення рубежів введення винищувачів у бій з урахуванням напрямку та висоти польоту повітряної цілі. Крім того, розроблено алгоритм розрахунку рубежів введення винищувачів у бій. Варто акцентувати увагу, що впровадження запропонованої методики для автоматизації проведення оперативно-тактичних розрахунків і моделювання бойових дій дозволить підвищити оперативність виконання вищезазначених розрахунків та ефективність прийнятих рішень командиром щодо виконання бойового завдання з перехоплення повітряних цілей на заданих рубежах. Водночас, точність проведення розрахунків дає змогу стверджувати, що якість прийнятих рішень, на виконання завдань винищувачами, значно зросте.

## *Література*

**1. Alimpiev A., Berdnik P., Korolyuk N., Korshets O., Pavlenko M.** Selecting a model of unmanned aerial vehicle to accept it for military purposes with regard to expert data Eastern-European. *Journal of Enterprise Technologies*. 2017. Vol. 1. № 9(85). P. 53–60**. 2. Чернов В. Г., Волобуєв В. А., Желем О. К.** Наведення літаків на повітряні та наземні цілі : навчальний пособник. Харків : ХУПС, 2004. 131 с. **3.** Command and Control of Joint Air Operations. Joint Publication/3-3010, February 2014. **4. Королюк Н. О., Першин О. В., Грідньова Т. О., Шевченко С. О.** Обґрунтування сучасного підходу щодо автоматизації процесів прийняття рішень по управлінню авіацією. Збірник наукових праць. 2019. №1(59). С. 32–39. **5. Королюк Н. О., Корольов Р. В., Коршець О. А.** Процедура формалізації даних, які використовуються при описі процесу управління рухом повітряних об'єктів. *Збірник наукових праць ХНУПС*. 2017. № 4(53). С. 103-106. **6. Камінський В. В**., **Тюрін В. В., Корщець О. А., Королюк Н. О.** Аналіз застосування безпілотних літальних апаратів в сучасних збройних

конфліктах та АТО на Сході України. *Наука і оборона*. 2017. № 3(4). С. 4–8. **7. Субботин С.А., Олейник А. А., Гофман Е. А.** Интеллектуальные информационные технологии проектирования автоматизированных систем диагностирования и распознавания образов: монографія. Харків : ООО «Компания Смит», 2016. 317 с. **8. Пермяков О. Ю. Королюк Н. О.** Інформаційно-телекомунікаційні технології і сучасна збройна боротьба. *Актуальні проблеми інформаційних технологій* : збірник матеріалів наук.-техн. конф. молод. уч. (20–21 листопада 2018 року, м. Київ). Київ : НУОУ, 2018. С. 5–6. **9. Mendel J., Hagras H., John R.I.** Standard Background Material About Interval Type-2 Fuzzy Logic Systems. 2010. *IEEE CIS Standards Committee.* URL: http://ieee-cis.org/technical/standards/ (дата звернення: 13.12.2022). **10. Скорик А. Б., Воронин В. В., Зверев А. А., Галицкий О. Ф.** Актуальные вопросы оценки эффективности противовоздушного боя. *Збірник наукових праць Харківського університету Повітряних Сил*. 2010. Вип. 3 (25). С. 8–14. **11. Wu D., Mendel J. M.** Enhanced Karnik-Mendel Algorithms. *IEEE Transactions on Fuzzy Systems*. August 2009. Vol. 17. № 4. P. 923–934. **12. Mendel J. M.** On centroid calculations for Type-2 Fuzzy Sets. *Appl. Comput. Math*. 2011. V. 10. № 1, Special Issue. P. 88–96. **13.** Світова гібридна війна: український фронт / за заг. ред. В. П. Горбуліна; Нац.ін-тстратег.дослідж. Київ : НІСД, 2017. 496 с. URL: http://resource.history.org.ua/item/0013707 (дата звернення: 10.01.2022). **14. Чернов В. Г., Мажара І. П., Сургай В. М., Телятник Б. А.** Аналіз помилкових дій офіцерів бойового управління під час наведення винищувачів на повітряні цілі. *Новітні технології для захисту повітряного простору* : тези допов. наук. конф., 18–19 квіт. 2012 р. Харків : Харківський університет Повітряних Сил імені Івана Кожедуба, 2012. С. 61.

## APPROACH TO THE AUTOMATION OF NAVIGATION CALCULATIONS FOR FIGHTER AVIATION AIRCRAFT CONTROL

***Natalia Korolyuk***

***Kharkiv national Air Forces University named after I. Kozhedub, Kharkiv, Ukraine***

*The article proposes a general procedure for performing preliminary navigational calculations for determining the distances of the boundary of the introduction of fighters into battle. It was analyzed that the use of forces and means of armed struggle during the large-scale invasion of the Russian Federation on the territory of Ukraine indicates a transition from the concept of "platform-centric war", where the main emphasis was placed on the number of weapons and military equipment, towards "network-centric war". the basis of which is the integration of all forces and means in a single information space. Increasing the effectiveness of management is possible due to the practical organization of unified combat management of all troops and forces of aviation and air defense. The existing method of performing preliminary navigational calculations, which is implemented in the special mathematical and software of the complexes of automation means by officials of the combat service of the command post, does not take into account the configuration of the radar field depending on the topography of the area and the altitude of the flight of air attack vehicles, the detection and defeat zones of anti-aircraft missile systems, the direction of flight of attack vehicles. Restrictions affect the accuracy of their execution and reasoned decision-making on combat operations. An algorithm has been developed for calculating the distance to the line of entry of fighter jets into battle. The procedure for calculating the boundary of the introduction of fighters into battle is substantiated, taking into account the direction of flight of air targets relative to the given boundary. The implementation of the proposed methodology for calculating the boundaries of the introduction of fighters into battle in the automated system will allow to quickly and effectively assess the combat capabilities of fighter aircraft in the performance of the combat task of intercepting air targets at the specified boundaries.*

***Keywords:*** *preliminary navigator calculations, navigational and tactical milestones, flight program, engagement milestone, interception, automation.*

## *References*

**1. Alimpiev, A. Berdnik, P., Korolyuk, N., Korshets, O., Pavlenko, M.** (2017). Selecting of a model of unmanned aerial vehicle to accept it for military purposes with regard to expert data of Eastern – European. Journal of of Enterprise Technologies, 1, 9 (85), 53–60. **2. Chernov, V. G. Volobuev, V. A., Jelly, O. K.** (2004). Aiming of aircraft at air and ground targets: study guide. Kharkiv : HUPS, 131. **3.** Command of and of Control of of of Joint Air Operations. Joint Publication/3-3010, February 2014. **4. Korolyuk, N., Pershin, A.** (2019). Ground of modern method in relation to the ав-томатизації processes of making decision for by the aviation. Collection of scientific works, 1 (59), 32–39. **5. Korolyuk, N., Korolev R., Korshes, O.** (2017). Procedure of formalization of data, what used at description of process of traffic of air objects. Collection of scientific works. HNUPS, 4(53), 103–106. **6. Kaminskiy, V. V., Turin, V. V.** (2017). Analysis of application of UAF in modern armed conflicts on East of Ukraine. Science and defensive, 3 (4), 4–8. **7. Subbotin, S., Gofman, E.** (2016). Intellectual to of informative technology of planning of the ASC of diagnosticating characters: monograph. Kharkiv : LTD. «Company Смит», 317. **8. Permiakov, O., Korolyuk, N.** (2018). Information and telecommunication technologies and modern armed struggle. Actual problems of information technologies: Scientific and technical conference of young scientists. Kiev, MD, 5–6. **9. Mendel, J.M., Hagras, H., John, R. I.** (2010). Standard Background Material About Interval Type-2 Fuzzy Logic Systems. IEEE CIS Standards Committee. URL : http://ieee-cis.org/technical/standards/. **10. Wu, H., Mendel, J. M. (**October, 2002). Uncertainty Bounds and Their Use in the Design of Interval Type-2 Fuzzy Logic Systems. IEEE Transactions on Fuzzy Systems, 10, 5, 622–639. **11. Wu, D., Mendel, J.M.** (2009). Enhanced Karnik-Mendel Algorithms. IEEE Transactions on Fuzzy Systems, August, , 17, 4, 923-934. **12. Mendel, J. M.** (2011). On centroid calculations for Type-2 Fuzzy Sets. Appl. Comput. Math, 10, 1, Special Issue, 88–96. **13.** World hybrid war: the Ukrainian front (2017). By General. ed. V. P. Horbulina; National University strategist research Kyiv: NISD. URL: http://resource. history.org.ua/item/0013707 (date of application: 10.01.2022). **14. Chernov, V. G., Mazhara, I. P., Surgai, V. M., Telyatnik, B. A.** (2012). Analysis of erroneous actions of combat control officers during the guidance of fighters on aerial targets. The latest technologies for the protection of air space: theses of nauk. conference, April 18-19, 2012, Kharkiv : Kharkiv Air Force University named after Ivan Kozhedub, 61..

DOI:**10.33099/2311-7249/2023-46-1-69-72**

УДК 004.94:355

***Олексій Анатолійович Кільменінов*** *(кандидат технічних наук)*[1]
***Дмитро Анатолійович Чопа*** *(кандидат технічних наук, старший науковий співробітник)*[2]

***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# ВИКОРИСТАННЯ СИСТЕМИ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ «JCATS» ДЛЯ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ БОЙОВОГО ЗАСТОСУВАННЯ ЗРАЗКІВ ОЗБРОЄННЯ

*Під час будівництва і розвитку Збройних Сил України формування необхідного вигляду і визначення параметрів систем озброєння є ключовою проблемою, що розглядається в процесі програмно-цільового планування розвитку озброєння та військової техніки. Обґрунтування тактико-технічних вимог спонукає до проведення досліджень зразків озброєння та військової техніки з метою перевірки відповідності їх характеристик, що пред'являються не лише як до окремих бойових засобів, а й як до засобів, що діють у складі бойових систем через оцінювання ефективності застосування відповідних підрозділів. Кількісно-якісним відображенням властивостей зразків озброєння та військової техніки є їх тактико-технічні характеристики. Від повноти переліку та обґрунтування їх рівня прямо залежать бойові якості перспективних зразків. Тому обґрунтоване і повне формування кількісних показників, що описують функціонування окремого зразка озброєння та військової техніки в імітаційному середовищі Системи імітаційного моделювання «Joint Conflict and Tactical Simulation», є важливим етапом під час проведення оцінювання ефективності застосування зразка озброєння та військової техніки. У статті, на підставі аналізу наявних підходів щодо визначення показників оцінювання ефективності окремих зразків озброєння і військової техніки, структури та змісту складових бази даних Системи імітаційного моделювання «Joint Conflict and Tactical Simulation» розглянуті деякі аспекти формування (визначення) потрібних чисельних характеристик показників, що описують зразок озброєння та військової техніки для оцінювання ефективності його застосування в імітаційному середовищі.*

***Ключові слова:*** *оцінювання ефективності застосування; система імітаційного моделювання бойових дій; тактико-технічні вимоги до зразків озброєння та військової техніки; ймовірність влучення та ураження.*

## Вступ

Кількісно-якісним відображенням властивостей зразків ОВТ є їх тактико-технічні характеристики (далі – ТТХ). Від повноти переліку та обґрунтування їх рівня прямо залежать бойові якості перспективних зразків ОВТ.

Відповідність зразків озброєння та військової техніки (далі – ОВТ) вимогам, що до них висуваються, забезпечуються сукупністю їх властивостей і характеризують якість матеріальної складової бойового потенціалу підрозділу.

Сучасні досягнення в галузі інформаційних технологій, зростання можливостей обчислювальної техніки, динамічний розвиток технологій програмування і моделювання відкрили широкі можливості для опису та дослідження процесів функціонування різних складних систем, до яких відносяться сучасні зразки озброєння. Провідну роль у цьому посідає розподілене імітаційне моделювання, яке, на відміну інших методів, практично не має обмежень.

**Постановка проблеми.** Аналіз наявних підходів щодо визначення системи показників, що використовуються для опису зразків ОВТ та використовуються в існуючій системі формування тактико-технічних вимог (далі – ТТВ), не повною мірою відповідають змісту (набору показників) бази даних Системи імітаційного моделювання «Joint Conflict and Tactical Simulation» (далі – СІМ «JCATS»), в якій створюється зразок ОВТ для подальшого моделювання його функціонування в імітаційному середовищі. Це, своєю чергою, обумовлює невідповідність зразка ОВТ, функціонування якого буде відтворюватися в імітаційному середовищі, реальному зразку, до якого необхідно кількісно обґрунтувати ТТВ.

**Аналіз останніх досліджень і публікацій.** У Збройних Силах України (далі – ЗС України) майже 20 років використовується СІМ «JCATS», але цей сучасний інструментарій розглядався як засіб забезпечення практичної підготовки, наприклад, для проведення командно-штабних навчань (далі – КШН). Варто зазначити, що до нині СІМ «JCATS» не отримала широкого застосування під час проведення наукових досліджень. У деяких роботах [1] проводився аналіз існуючих науково-методичних підходів до моделювання бойових дій. Було визначено певні обмеження їх застосування для моделювання процесів, що характерні для сучасної збройної боротьби. Для цієї мети запропоновано використовувати розподілену імітаційну СІМ «JCATS». Автори роботи [2]

розглядали загальні питання теоретико-експериментальних досліджень ОВТ з використанням імітаційної моделі СІМ «JCATS». У роботах [3; 4] проаналізовано можливості СІМ «JCATS», структура та зміст складових її бази даних, що дало змогу визначити підходи до формування вихідних даних для створення обрису перспективних (тих, що модернізуються) зразків ОВТ в імітаційному середовищі. Проте автори розглядали загальні питання можливості використання СІМ «JCATS» для проведення наукових досліджень, що пов'язані з оцінюванням ефективності застосування зразків ОВТ.

Сьогодні питання формування (визначення) потрібних чисельних характеристик показників, що описують зразок ОВТ для оцінювання ефективності його застосування в імітаційному середовищі науковцями, не розглядалися.

**Мета статті.** На підставі аналізу існуючої системи показників оцінювання ефективності зразків ОВТ (на прикладі окремого зразка стрілецької зброї), а також системи показників, що використовуються в базі даних СІМ «JCATS», розглянути підхід щодо визначення кількісних значень показників для створення (опису) зразка ОВТ в імітаційному середовищі.

## Виклад основного матеріалу дослідження

У СІМ «JCATS» реалізована об'єктно-орієнтовна архітектура моделей, що забезпечує модульність та достатню гнучкість. З точки зору використання математичного апарату для формалізованого опису процесів ведення збройної боротьби СІМ «JCATS» являє собою дворівневу ієрархічну модель.

Перший рівень – деталізований опис взаємодії на рівні окремих об'єктів з використанням метода Монте-Карло. При цьому враховуються: склад і ТТХ ОВТ й засобів прицілювання, типи боєприпасів та їх здатність ураження, габаритні розміри об'єктів, діапазони швидкісних характеристик техніки, характеристики місцевості, дорожніх та погодних умов, пори року, час доби, стан особового складу і рівень його підготовки.

Послідовність і зміст етапів створення боєприпасу калібром 5,45-мм до автомату АК-74 в базі даних СІМ «JCATS» було розглянуто авторами в [4].

Виходячи з мети статті, постає актуальне наукове завдання щодо дослідження визначення(формування) послідовності кількісних показників для створення зразка ОВТ (на прикладі 5,45-мм патрона до АК–74) в імітаційному середовищі для подальшого оцінювання ефективності його застосування, зокрема кількісні показники ймовірності влучення (далі – Ph) та ймовірності ураження (далі – Pk).

Аналіз розглянутих джерел свідчить, що ймовірність влучення може бути визначена порівнянням площі цілі з площею серцевини розсіювання, за шкалою розсіювання, таблицею значень імовірностей і сіткою розсіювання.

Якщо ціль за своєю формою відрізняється від прямокутника, то знайдену ймовірність влучення необхідно помножити на коефіцієнт фігурності (1):

$$P = \Phi(\frac{y}{Bв_{сум}})\Phi(\frac{z}{Bб_{сум}})K \ , \qquad (1)$$

де $P$ – ймовірність влучення в ціль;

$\Phi$ – ймовірність влучення в смугу, що дорівнює висоті та ширині цілі відповідно;

$y$ – половина висоти цілі;

$z$ – половина ширини цілі;

$Bв_{сум}$ і $Bб_{сум}$ – сумарні серединні відхилення відповідно за висотою та бічним напрямом;

$K$ – коефіцієнт фігурності.

Розміри цілі та коефіцієнти фігурності визначаються залежно від типу цілі. Дані про них є у спеціальних довідниках. Сумарні серединні відхилення $Bв_{сум}$ і $Bб_{сум}$ відповідно за висотою та бічним напрямом також надаються у збірниках Таблиць стрільб [5].

Таким чином, для будь-якого зразка стрілецької зброї, можна розрахувати значення ймовірності влучення відповідного боєприпасу для різних цілей на різних відстанях з подальшим заповненням таблиці показників Ph в базі даних СІМ «JCATS».

Інформацію про вогневу потужність, що має боєприпас залежно від дистанції пострілу по цілі, що має певні рівні захисту, можна отримати з балістичних випробувань реального зразка, або з полігонних випробувань, або з конструкторсько-технічної документації щодо конкретного типу боєприпасу. Тобто в таблиці показників Pk бази даних СІМ «JCATS», ймовірнісні показники ураження будуть відображати стан цілі після влучного пострілу. Слід зазначити, що СІМ «JCATS» враховує положення цілі та положення вогневого засобу, а також умови вогневого контакту, це відображається в таблиці Ph кількісними значеннями імовірнісних показників для певних видів положення цілі та вогневого засобу і умов вогневого контакту (рис. 1).

Значення стану об'єкту, що здійснює постріл:

S (Stationary) – об'єкт нерухомий;

M (Moving) – об'єкт знаходиться в русі.

Значення стану цілі:

S (Stationary) – ціль нерухома;

M (Moving) – ціль рухається.

Значення стану захисту цілі:

E (Exposed) – схильна до впливу;

D (Defilade) – знаходиться в укритті.

Значення кутів влучення боєприпасу в ціль:

H (Head) – боєприпас потрапляє в ціль під кутом 90 градусів (лобовий постріл);

F (Flank) – боєприпас потрапляє в ціль під іншими кутами (постріли з флангу).

Наприклад, SSEH – постріл з автомату АК-74 кулею калібру 5,45-мм здійснюється з місця (S) по цілі, яка не рухається (S) не в укритті (E) розташована перпендикулярно лінії прицілювання (H). Далі вибираємо дистанцію пострілу з таблиці. В таблиці можливо змінювати не лише кількісні значення імовірнісних показників, а й умови, що визначають положення цілі, відстані до неї тощо. Підкреслимо, що така гнучкість системи дає змогу

не тільки створювати в імітаційному середовищі існуючі (штатні) зразки ОВТ, а й перспективні, для яких відсутні дані полігонних випробувань, або досвід застосування. Під час стрільби зі стрілецької зброї по поодиноких цілях одне влучання зазвичай дає ураження цілі. Тому під імовірністю ураження поодинокої цілі розуміють імовірність отримання хоча б одного влучання при заданій кількості пострілів. Імовірність ураження цілі при поодинокому пострілі ($P_1$) буде дорівнювати імовірності влучання в ціль ($p$), тому розрахунок імовірності ураження цілі за такої умови зводиться до визначення імовірності влучання по цілі.

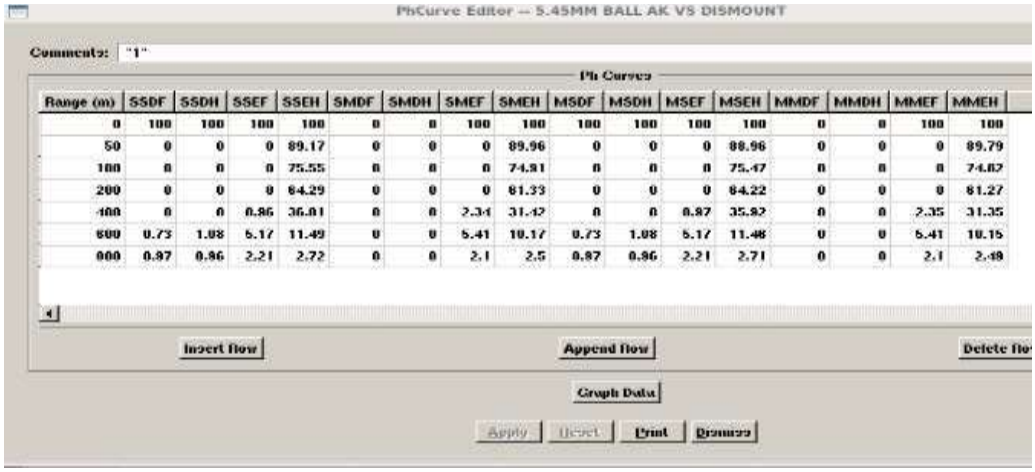



Рис. 1. Скриншот таблиці показників Ph

Імовірність ураження цілі $P_1$ під час декількох поодиноких пострілах однією чергою або декількома чергами, коли імовірність влучання для всіх пострілів однакова, буде визначатися за виразом:

$$P_1 = 1-(1-p)^n, \qquad (2)$$

де $(1-p)$ — імовірність промаху;

$p$ – імовірність влучання в ціль;

$n$ – кількість пострілів.

Визначена за виразом (2) імовірність ураження цілі характеризує такий термін як «надійність стрільби», тобто відображає в скількох випадках із ста в середньому ціль в даних умовах буде уражена не менш ніж при одному влучанні. Стрільба вважається достатньо надійною, якщо імовірність ураження цілі не менш ніж 80%.

Імовірність ураження цілі під час декількох пострілів однією чергою або декількома чергами, коли імовірність влучання перших та наступних куль змінюється від пострілу до пострілу доцільно визначати:

а) для однієї черги:

$$P_1 = 1-(1-p_{пер})(1-p_{наст})^{n-1}, \qquad (3)$$

б) для декількох черг (імовірність влучання від черги до черги не змінюється):

$$P_1 = 1-(1-p_{пер})^k(1-p_{наст})^{n-k}, \qquad (4)$$

де $p_{пер}$ –

$p_{наст}$ –

$n$ – загальна кількість пострілів;

$к$ – кількість черг

в) для декількох черг (імовірність влучання від черги к черзі змінюється):

$$P_1 = 1-(1-p_1)^{S_1}(1-p_2)^{S_2}\ldots(1-p_2)^{Si}, \qquad (5)$$

де $S_1$, $S_2$, $Si$ – кількість пострілів в черзі;

$p_1$, $p_2$ – мовірність влучання при одному пострілі першої, другої, і т.д. черг [6].

Використовуючи наведені вирази (3–5), формується таблиця враження цілей (рис. 2).

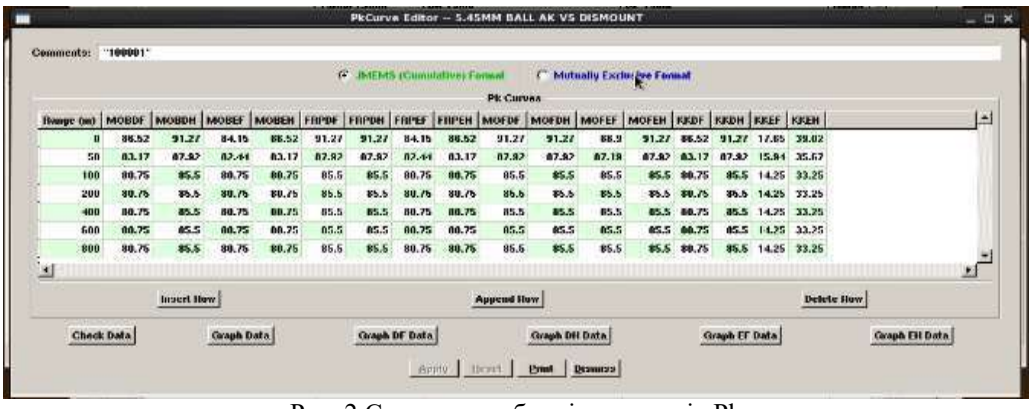



Рис. 2 Скриншот таблиці показників Pk

Водночас зазначимо, що в базі даних CIM «JCATS» можна впливати не лише на властивості боєприпасів і зброї, що їх використовує, а також створювати групи цілей, по яких ці боєприпаси

застосовуються. Це дає змогу побудувати гнучке імітаційне середовище з різними групами боєприпасів та цілей, описати їх залежність, а саме, головне, окремо для кожної групи визначити імовірність влучання та імовірність ураження.

## Висновки й перспективи подальших досліджень

На підставі аналізу існуючої системи показників оцінювання ефективності зразків стрілецької зброї, а також структури і змісту таблиць бази даних СІМ «JCATS», в яких містяться дані для створення (опису) зразка ОВТ в імітаційному середовищі, розглянуто підхід щодо визначення кількісних показників ефективності зразка ОВТ (на прикладі зразка стрілецької зброї) для його опису в імітаційному середовищі з використанням відомого математичного апарату.

Також варто зазначити, що перспективним напрямом подальших досліджень є розгляд можливих підходів стосовно визначення кількісних показників ефективності зразків артилерійського озброєння відповідно до системи показників ефективності, що використовуються для опису зазначеного класу ОВТ в базі даних СІМ «JCATS».

## *Література*

**1. Купрієнко А.М., Голуб В.А., Гумінський Р.В.** Можливості застосування імітаційної системи JCATS в наукових дослідженнях. *Військово-Технічний Збірник*. 2014. № 11. С. 89–98. **2.** Основы военно-технических исследований. Теория и приложения: монография : в 10 т. Т.9. / Прикладные аспекты испытаний и теоретико-экспериментальных исследований вооружения и военной техники / И.Б. Чепков, С.В. Лапицкий и др.; под ред. С.В. Лапицкого. – Киев:Издательский дом Дмитрия Бураго, 2015.373–400 с. **3. Звіт про НДР** «Методика застосування засобів імітаційного моделювання бойових дій для оцінки тактико-технічних вимог до перспективних зразків озброєння та військової техніки» шифр «МЕТОДИКА ІМ» (остаточний). Київ: НУОУ, 2019. **4. Кільменінов О.А., Чопа Д.А., Мельник Я.В.** Використання можливостей системи імітаційного моделювання JCATS для обґрунтування тактико-технічних вимог до перспективних зразків озброєння та військової техніки. *Сучасні інформаційні технології в сфері безпеки та оборони.* 2020. № 2(38). С. 125–132. **5. Таблицы стрельб** по наземным целям из стрелкового оружия калибров 5,45 и 7,62 мм. Издание второе, дополненное. Москва: МО СССР, 1977. 6. **Наставление по стрелковому делу**. Москва : МО СССР, 1985.

## SOME ASPECTS OF CONDUCTING RESEARCH TO EVALUATE THE EFFICIENCY OF WEAPONS IN THE JCATS SIMULATION SYSTEM ENVIRONMENT

***Oleksii Kilmeninov** (Candidate of technical sciences)*
***Dmytro Chopa** (Candidate of technical sciences, Senior Research Fellow)*

***National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine***

*When solving the problems of construction and development of the Armed Forces of Ukraine, the formation of the necessary type and determination of the parameters of weapons systems is a key problem considered in the process of program-target planning for the development of weapons and military equipment. The substantiation of tactical and technical requirements requires research of weapons and military equipment samples in order to verify the conformity of their characteristics, which are presented not only as separate combat weapons, but also as weapons operating as part of combat systems through an assessment of the effectiveness of the use of the corresponding units. A quantitative and qualitative reflection of the properties of weapons and military equipment samples is their tactical and technical characteristics. The combat qualities of promising samples directly depend on the completeness of the list and the justification of the level. Therefore, the justified and complete formation of quantitative indicators describing the functioning of a separate sample in the simulation environment of the JCATS simulation system is an important stage in conducting research to evaluate the effectiveness of the a separate sample of weapons and military equipment. In the article, the authors, based on an analysis of existing approaches for determining indicators for evaluating the effectiveness of individual samples of weapons and military equipment, the structure and content of the components of the JCATS database, consider some aspects of the formation (definition) of the necessary numerical characteristics of indicators describing the sample of weapons and military equipment to assess the effectiveness of its use in a simulation environment.*

***Key words:** evaluation of application effectiveness; combat simulation system; tactical and technical requirements for weapons and military equipment; the probability of hitting and killing.*

## *References*

1. Kuprienko, A., Holub, V., Huminskyi, R. (2014). Possibilities of using the JCATS simulation system in scientific research. Viiskovo-Tekhnichnyi Zbirnyk, Lviv: NASV, 2014, 11, 89–98. 2. Chepkov, I., Lapytskyi, S., Grebennyk, A., Rasstrygin, A. (2015). Fundamentals of military-technical studies, theory and applications. Volume 9. Applied aspects of tests and theoretical-experimental studies of weapons and military equipment : monohrafyia. Kyiv: TsNDI OVT ZS Ukrainy. 3. Report on the NDR. «The method of using combat simulation tools to assess the tactical and technical requirements for promising samples of weapons and military equipment» shyfr «METODYKA IM» (ostatochnyi) (2019). Kyiv: NUOU. 4. Kilmeninov, O., Chopa, D., Melnyk, Y. (2020) Using the capabilities of the JCATS simulation modeling system to justify the tactical and technical requirements for promising samples of weapons and military equipment. Modern information technologies in the sphere of security and defence, 2 (38), 125–132. 5. Tables of shooting at ground targets from small arms calibers 5,45 y 7,62 mm (1977) Edition second, supplement, Moskva : MO SSSR**.** 6. Shooting instraction (1985) Moskva : MO SSSR.

DOI:**10.33099/2311-7249/2023-46-1-73-77**

УДК 004.94:355

***Валерій Олександрович Крайнов*** *(кандидат технічних наук, доцент)*
***Олександр Васильович Лаврінчук*** *(кандидат технічних наук, с.н.с.)*
***Роман Іванович Грозовський*** *(кандидат військових наук)*

***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# ОСНОВНІ ПІДХОДИ ЩОДО ВИБОРУ ЛОГІЧНОЇ СТРУКТУРИ БАЗИ ДАНИХ ДЛЯ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНУ ВІЙСЬКОВОГО УПРАВЛІННЯ

*Наявні вимоги до якості прийняття рішень у різних сферах військового управління призвели до необхідності розроблення та використання спеціалізованого програмного забезпечення, яке дозволило б здійснювати накопичення, зберігання та аналіз доступних об'ємів інформації, які забезпечують вирішення завдань, що стоять перед органом військового управління. Однак, сучасні автоматизовані інформаційні системи органу військового управління, що орієнтовані на конкретні програми, не відповідають вимогам офіцерів-користувачів, оскільки процес оброблення масивів даних ними є недосконалий. Ці обставини обумовили необхідність розроблення такої бази даних, застосування якої має сприяти їх інтенсивному використанню. Створення баз даних та управління ними здійснюються на основі обраної логічної моделі даних, яка виступає невід'ємним елементом створення та реалізації сучасних баз даних та систем управління ними. Під логічною моделлю даних розуміється модель, що відображає логічні взаємозв'язки між різними елементами даних без їх фізичної організації та змісту. У цьому логічна модель розробляється під конкретну реалізацію системи управління базами даних і, навіть, враховуючи специфіку конкретної предметної області з урахуванням її концептуальної моделі. Можливості системи управління базами даних значною мірою обумовлені вибором моделі представлення даних, формування яких одна із найважливіших напрямів досліджень у галузі проєктування баз даних. Можна стверджувати, що поява баз даних стала одним із найважливіших досягнень у галузі програмного забезпечення. У статті розглянуто основні підходи до вибору логічної структури баз даних для автоматизованої інформаційної системи органу військового управління, особливість яких базується на розробленні єдиного інтегрованого підходу до проєктування, який на етапі логічного проєктування не буде залежати від специфіки конкретної системи управління базою даних і в той же час буде формально охоплювати весь цикл проєктування.*

***Ключові слова:*** *база даних; автоматизована інформаційна система; система управління; орган військового управління.*

## Вступ

Розвиток обчислювальної техніки і поява ємних зовнішніх пристроїв прямого доступу, що запам'ятовують, зумовили інтенсивний розвиток автоматичних і автоматизованих систем різного призначення і масштабу. Насамперед, такий прогрес помітний в роботі органів військового управління. Такі системи працюють з великими обсягами інформації, яка зазвичай має досить складну структуру, потребує оперативності в обробці, часто оновлюється і водночас потребує тривалого зберігання. Прикладами таких систем є автоматизовані інформаційні системи органу військового управління (далі – АІС ОВУ). Це призвело до появи нової інформаційної технології інтегрованого зберігання та обробки даних – концепції баз даних, в основі якої лежить механізм надання обробній програмі з усіх даних, що зберігаються, тільки тих, які їй необхідні, і у формі, що необхідна саме цій програмі. Водночас сама форма (структура даних, і формати полів, що входять до цієї структури) описується на логічному, тобто, «видимому» з програми, рівні. До того ж, оскільки різні програми можуть по-різному «бачити» (а, отже, і використовувати) одні й ті самі дані, то система має зробити невидимими («прозорими») для програми всі дані, крім тих, які для неї є «своїми» [1–5].

Якість і терміни створення баз даних (далі – БД) багато в чому визначаються методами і засобами, що застосовуються для проєктування, характеристиками, що істотно залежать від прийнятої архітектури інформаційної системи, а також засобами моделювання предметної області та умовами функціонування АІС ОВУ [6–11].

Побудована логічна модель даних є джерелом інформації для етапу фізичного проєктування та забезпечує розробника фізичної бази даних засобами знаходження необхідних, для досягнення поставленої мети, компромісів, що є дуже важливим для ефективного проєктування. Логічна модель даних також відіграє важливу роль на етапі експлуатації та супроводу вже готової системи. За правильно організованого супроводу, підтримувана в актуальному стані модель даних дозволяє точно і наочно уявити будь-які зміни, що вносяться до бази даних, а також оцінити їх вплив на прикладні програми і використання даних, що вже є в базі.

**Постановка проблеми.** Логічна схема є результатом об'єднання локальних уявлень користувачів і являє собою інтегральне, несуперечливе, незалежне від системи управління базами даних (далі – СУБД) визначення даних, що підлягають зберіганню у БД з метою використання для всього комплексу оперативно-тактичних завдань. Характерною особливістю баз даних є сталість, а саме:

дані постійно накопичуються та використовуються;

склад і структура даних, необхідних для вирішення певних прикладних завдань, зазвичай, є постійними та стабільними за часом;

окремі або навіть усі елементи даних можуть змінюватися (прояв сталості) – постійна актуальність.

Безпосереднє об'єднання локальних уявлень може призвести до виникнення суперечливості й надмірності в зв'язках між атрибутами. Виявлення та усунення суперечливих і надлишкових зв'язків є однією з основних задач вибору логічної структури БД у її проєктуванні. Тому вся сукупність вихідних зв'язків повинна бути проаналізована з метою подолання суперечливості і надмірності завдяки видаленню деяких зв'язків і заміни одних зв'язків іншими. Водночас має бути забезпечена незалежність від кожного конкретного додатку (запиту), яка може бути досягнута в разі, якщо логічна схема буде відображати лише найсуттєвіші зв'язки, з яких виводяться всі інші. Тобто, концептуальна схема повинна містити мінімальну кількість зв'язків, що одночасно забезпечують інформаційні потреби кожної посадової особи ОВУ.

**Аналіз остатніх досліджень і публікацій.** Теоретичні основи проєктування баз даних у своїх працях розглядали В. Карпуша, Б. Панченко, С. Діго, С. Здонік, Г. Гайна, Д. Майер, Т. Конноллі, К. Бегг, У. Вольфенгаген, Л. Кузін, В. Саркісян [1]. Проблеми проєктування баз даних досліджували Є. Зіндер, Л. Калініченко, Дж. Мартін, В. Меллінг, Д. Цикриітзиіс, Ф. Лоховскі. Проблемам проєктування й опрацювання баз даних присвячені роботи Г. Цибко, Т. Щепакіної, М. Ареф'євої, А. Змитровича, Є. Морозова, Г. Ревункова, Ю. Рамського, Н. Сазонової, О. Ткачева, В. Фреймана. Формування проєктувальних умінь майбутніх інженерів-педагогів досліджували В. Кошелева, В. Беспалько.

## Виклад основного матеріалу дослідження

Як показано в дослідженнях щодо функціонування БД [1–5], на етапі логічного проєктування БД здійснюється відображення отриманої концептуальної схеми на модель даних СУБД. У розглянутому випадку (формально) ця процедура втратила власні особливості, оскільки на етапах концептуального і логічного проєктування використовується одна і та ж реляційна модель даних. Однак, звернемо увагу на те, що ставлення у третій нормальній формі забезпечують необхідні функціональні можливості за поданням даних, але не в повній мірі враховують часові параметри їх обробки за реалізації запитів користувачів. З огляду на той факт, що створювана база даних є елементом системи військового призначення, для якої ці параметри відіграють істотну роль, вважається доцільним розумно відійти від оптимального ненадмірного покриття, отриманого в результаті концептуального проєктування з метою досягнення компромісу, пов'язаного з підвищенням оперативності АІС ОВУ.

Вирішення цієї проблеми залежить від використання тимчасових характеристик, які визначаються не тільки параметрами БД, але і особливостями програмного і технічного забезпечення, які виділяються ресурсами, розмірами і числом буферів СУБД і т.п., тобто факторами, конкретні дані про які на етапі логічного проєктування, як правило, не відомі. Тому, під час синтезу логічної структури БД, розробники зазвичай вводять деякі припущення, до числа яких можна віднести [4–7]:

розглядається обробка незалежних за часом запитів;

відносною оцінкою часу обробки запиту є сумарна кількість логічних записів (далі – кортежів), які обираються строком на шляху доступу до цільовогоїзапису даного запиту;

зміною середнього часу доступу до кортежів різних файлів (типів відносин) можна знехтувати, оскільки домінуючу роль відіграє час обміну із зовнішньою пам'яттю.

В результаті зазначеного визначення середнього часу, виконання запитів посадових осіб ОВУ в процесі оперативно-тактичних розрахунків може бути обчислено таким виразом:

$$T_{\text{ср}} = \tau_{\text{ср}} \sum_{i=1}^{N} f_i \sum_{k=1}^{s} \sum_{l=1}^{m} n_{ikl} X_{kl} \qquad (1)$$

де $\tau_{\text{ср}}$ – середній час вибірки кортежу з БД;

$f_i$ – кількість запитів $i$-го типу, які необхідно обслужити в процесі оперативно-тактичних розрахунків;

$n_{ikl}$ – середня кількість кортежів, вибірка яких здійснюється в процесі виконання $i$-го запиту з $k$-го файлу при його реалізації $l$-им способом;

$$X_{kl}\begin{cases}1 & \text{– при } k\text{-тій відносині обраний } l\text{-тий варіант реалізації;}\\ 0 & \text{– в іншому варіанті.}\end{cases}$$

Мінімізація значення $T_{\text{ср}}$ під час зроблених припущеннях зводиться до мінімізації середнього (через безліч запитів) числа вибірок кортежів, необхідних для реалізації запитів. З цією метою для кожного запиту моделюється процес його навігації в логічній структурі за різних варіантів організації відносин (далі – файлів) бази даних. Для моделювання та визначення значень $n_{ikl}$ можуть бути використані запропоновані в роботах [5; 7] алгоритми декомпозиції та імітації процесів навігації запитів у базах даних. Таким чином можна уникнути необхідності залучати для оцінювання варіантів логічних структур бази даних детальні характеристики зв'язку часових параметрів з параметрами фізичної організації даних під час використання конкретної СУБД.

У випадках, коли на етапі логічного проєктування відомо значення обсягу пам'яті, що виділяється в АІС ОВУ для розміщення бази даних, можуть бути використані наступні варіанти перетворення концептуальної схеми під час використання в складі АІС ОВУ сучасних СУБД для персональних електронних обчислювальних машин (далі – ПЕОМ) [3; 11]:

виділення в окремі файли кортежів, ідентифікованих атрибутами, як пошукові ознаки;

застосування засобів вторинного індексування цих атрибутів.

Обидва варіанти організації даних, забезпечуючи прискорення доступу до певних (найчастіше використовуваних) кортежів, створюють додаткові системні витрати: збільшують пам'ять, інтенсифікують завантаження буферів СУБД і т.п. Це може призвести до такого неконтрольованого збільшення $\tau_{\text{ср}}$ (яке в натуральному виразі (1) покладається константою), що ефект прискорення доступу до даних, який досягається за рахунок різних варіантів організації відносин (файлів) в базі даних, може бути скомпенсованим збільшенням $\tau_{\text{ср}}$. Через це завдання з мінімізації $\tau_{\text{ср}}$ необхідно вирішувати за умови обмеження використання зовнішньої пам'яті, яка вимагається для розміщення БД. Це обмеження є узагальненим відображенням основних чинників, здатних зробити істотний негативний вплив на $\tau_{\text{ср}}$, і може бути задано нерівністю:

$$\sum_{k=1}^{S} P_k V_{kl} X_{kl} \le V_{\text{доп}}$$

де $P_k$ – середня кількість кортежів в $k$-му відношенні (фото) бази даних;

$V_{kl}$ – середній розмір кортежу (в байтах) в $k$-му відношенні (фото) при $l$-му варіанті його реалізації.

Для визначення значень параметрів, що входять до цього обмеження, використовуються об'ємні характеристики даних, що містяться в концептуальну схему, а також системні характеристики внутрішнього представлення даних, що підтримується СУБД на ПЕОМ.

Інформації про типи і кількість запитів, які повинні бути обслуговані АІС ОВУ в процесі оперативно-тактичних розрахунків, також береться з результатів концептуального проєктування. Такі цифри задаються з аналізу даних навчань, штабних ігор і тренувань, а також досвіду офіцерів ОВУ [6; 10].

Обчислювальні проблеми розв'язання задачі мінімізації функцій (1) пов'язані з розрахунком значень $T_{\text{ср}}$ для різних сполучень варіантів організації відносин, специфіковані в концептуальну схему. Якщо побудувати схему розрахунку таким чином, щоб з кожним варіантом логічної організації $k$-тих відносин зіставлялася частка $T_{\text{ср}}$, яку вносить пов'язаними з цим ставленням запитом (за визначення цієї частки має враховуватися вибірка кортежів не тільки даного файла, але і всіх інших, заданих в запиті), то можна говорити про те, що функція (1) має властивість адитивності відносно своїх компонентів. Так, в процесі виконання запиту, обробка кортежів відносин, пов'язаних з умовами запиту, не залежить від організації відносин, з якими запит не пов'язаний. Це очевидно в разі, коли атрибути індексуються, і часто виконуються тоді, коли пошукові атрибути виділяються в окремий файл [6].

З урахуванням наведених міркувань, для формалізації і розв'язання задачі вибору оптимального варіанту логічної структури бази даних АІС ОВУ, може бути запропонований наступний підхід. Припустимо, в процесі організації роботи АІС ОВУ може обслужити $N$ різних типів запитів посадових осіб ОВУ, причому відома кількість запитів $i$ - го типу $f_i$, які повинні виконуватися в процесі ОТР, $i\,\{1,\ \dots\ ,\ N\}$. Під час обслуговування запитів з бази даних вибираються кортежі (записи), які зберігаються в $S$ незалежних один від одного відносинах (файлах). Кожне $k$-те відношення, $k\,\{1,\ \dots\ ,\ S\}$, може бути реалізовано в $M$ варіантах, і для $k$-того варіанта організації відносин відомі обсяги займаної зовнішньої пам'яті $V_{kl}$ і середня кількість кортежів, вибірку яких необхідно провести з $k$-тої відносини при виконанні і-го запиту, $l\,\{1,\ \dots\ ,\ M\}$.

Нехай, $X[x_{ki}]SM$ – рішення задачі, де:

$$X_{kl}\begin{cases}1 & \text{– при } k\text{-тій відносині обраний перший варіант реалізації } l;\\ 0 & \text{– в іншому варіанті.}\end{cases}$$

Тоді для визначення оптимального, за запропонованим в [11] цільовим показником, варіанту логічної структури бази даних АІС ОВУ необхідне рішення наступного завдання: знайти $X[x_{ki}]$, за якого функція (1) досягає мінімуму, і виконуються обмеження:

$$\sum_{k=1}^{S} P_k V_{kl} X_{kl} \le V_{\text{доп}}; \quad (2)$$

$$\sum_{l=1}^{M} x_{kl} = 1,\ k = \overline{1,\ S}; \quad (3)$$

$$x_{kl}\{0,\ 1\};\ k = \overline{1,\ S}; i = \overline{1,\ N};\ l = 1. \quad (4)$$

Нерівність (1) забезпечує виконання вимоги по витраті зовнішньої пам'яті для варіантів логічної структури бази даних, а умова (2) означає можливість вибору тільки одного варіанту організації файлу в базі даних.

Завдання (1) – (4) відноситься до класу задач цілочисельного лінійного програмування. Через те, що параметри $N,\ S$ і $M$, зазвичай, не беруть великих значень, для його вирішення можуть бути використані ефективні алгоритми, що реалізують метод гілок і меж [2; 10]

## Висновки й перспективи подальших досліджень

Зауважимо, що ставлення як модель об'єкта, в загальному випадку, не є загальним. Так, в предметній області артилерії існують об'єкти, властивості яких характеризуються векторами значень. Наприклад, щодо об'єкта «З'єднання ракетних військ і артилерії» атрибуту «Умови зберігання боєприпасів» відповідає не один, а кілька значень кортежів («в сховищі», «на відкритому майданчику», «на рухомих засобах» і т.п.). Природним способом придушення надмірності за подання об'єктів такого роду є виокремлення кожної характеристики (разом з атрибутом об'єкта) окремим ставленням. З'єднання таких відносин по атрибуту-ідентифікатору об'єкта не призводить до спотворення інформації в БД: в силу незалежності характеристик усі комбінації значень характеристик, які при цьому утворюються,

З точки зору теоретичних результатів, отриманих в області проєктування реляційних баз даних, найбільш повне і ефективне придушення надмірності пов'язано з приведенням відносин на основі обробки багатозначних залежностей існуючих між атрибутами в предметній області, що підлягає аналізу. Для цієї мети сформульовані аксіоми (правила виводу) для багатозначних залежностей і базуються на них алгоритми обробки такого роду залежностей [1]. Проте для реалізації проєкту розробки персональних електронних обчислювальних машин п'ятого покоління [4; 5] ці результати мають, переважно, теоретичне значення.

## *Література*

**1. Коннолли Т., Бегг К.** Базы данных. Проектирование, реализация и сопровождение. Теория и практика. 3-тє вид. Вильямс, 2017. 1440 с. **2. Шаров С. В., Осадчий В. В.** Бази даних та інформаційні системи : навч. посіб. Мелітополь : МДПУ ім. Б. Хмельницького, 2014. 352 с. **3. Дейт К. Дж.** Введення в системи баз даних : підручник. Вільямс, 2017. 328 с. **4. Берко А. Ю., Верес О. М., Пасічник В. В.** Системи баз даних та знань : підручник. Львів : Магнолія-06, 2015. 440 с. **5. Берко А. Ю., Верес О. М., Пасічник В. В.** Системи баз даних та знань. Системи управління базами даних та знань : навч. посіб. Львів : Магнолія-06, 2012. 584 с. **6. Павленко П. М. та ін.** Інформаційні системи і технології : навч. посіб. Київ : НАУ, 2013. 324 с. **7. Шаров С. В., Осадчий В. В.** Бази даних та інформаційні системи : навч. посіб. Мелітополь : МДПУ ім. Б. Хмельницького, 2014. 352 с. **8. Микусь С. А. та ін.** Інформаційні технології інформаційно-аналітичного забезпечення органів управління військами (силами): підручник. Київ : НУОУ, 2018. 352 с. **9. Микусь С. А. та ін.** Організація інформаційно-аналітичного забезпечення органів управління військами (силами): підручник. Київ : НУОУ, 2019. 237 с. **10. Микусь С. А. та ін.** Застосування сучасних інформаційних технологій у наковій діяльності: підручник. Київ: НУОУ, 2019. 237 с. **11. Крайнов В. О.** Основні підходи щодо вибору показників якості при проектуванні концептуальної бази даних для автоматизованої інформаційної системи органу військового управління. *Збірник наукових праць ВІКНУ ім. Тараса Шевченко*. 2021. № 75. С. 120–125.

## MAIN APPROACHES TO THE CHOICE OF THE LOGICAL STRUCTURE OF THE DATABASE FOR THE AUTOMATED INFORMATION SYSTEM OF THE MILITARY GOVERNANCE AUTHORITY

***Valerii Krainov** (Candidate of technical sciences, associate professor)*
***Oleksandr Lavrinchuk** (Candidate of technical sciences, senior research associate)*
***Roman Hrozovskyi** (Candidate of military sciences)*

***National Defense University of Ukraine named after Ivan Chernyakhovskyi, Kyiv, Ukraine***

*The currently existing requirements for the quality of decision-making in various areas of military management led to the need to develop and use specialized software that would allow for the accumulation, storage and analysis of available volumes of information that provide solutions to the tasks facing the body military administration. However, the existing automated information systems of the military management body, which are focused on specific programs, do not meet the requirements of officer-users, since the process of processing data arrays by them is imperfect. These circumstances necessitated the development of a database, the use of which would facilitate their intensive use. The creation and management of databases is carried out on the basis of the selected logical data model, which acts as an integral element of the creation and implementation of modern databases and their management systems. A logical data model is a model that reflects logical relationships between various data elements without their physical organization and content. In this, a logical model is developed for a specific implementation of a database management system, and even taking into account the specifics of a specific subject area, taking into account its conceptual model. The capabilities of the database management system are largely determined by the choice of the data representation model, the formation of which is one of the most important areas of research in the field of database design. It can be argued that the advent of databases has become one of the most important advances in the field of software.*

*The article considers the main approaches to the selection of the logical structure of databases for the automated information system of the military management body, the peculiarity of which is based on the development of a single integrated approach to design, which at the stage of logical design will not depend on the specifics of a specific database management system and in the same time will formally cover the entire design cycle.*

***Key words**: logical structure of the database, automated information system, database, database design, military administration.*

## *References*

**1. Konnolly, T., Behh, K.** (2017). Database. Design, implementation and support. Theory and practice. 3rd view. Vyliams, 1440. **2. Sharov, S. V., Osadchyi, V. V.** (2014). Databases and information systems: navch. posib. Melitopol: MDPU im. B. Khmelnytskyi, 352. **3. Deit, K. Dzh.** (2017). Introduction to database systems: pidruchnyk. Viliams, 328. 4**. Berko, A. Yu., Veres, O. M., Pasichnyk, V. V.** (2015). Database and knowledge systems: pidruchnyk. Lviv: Mahnoliia-06, 440. **5. Berko, A. Yu., Veres, O. M., Pasichnyk, V. V.** (2012). Database and knowledge systems. Database and knowledge management systems: navch. posib. Lviv : Mahnoliia-06, 584. **6. Pavlenko, P. M. ta in.** (2013). Information systems and technologies: navch. posib. Kyiv: NAU, 324. **7. Sharov, S. V., Osadchyi, V. V.** (2014). Databases and information systems: navch. posib. Melitopol: MDPU im. B. Khmelnytskyi, 352. **8. Mykus, S. A. ta in.** (2018). Information technologies for information and analytical support of troops (forces) management bodies: pidruchnyk. Kyiv: NUOU, 352. **9. Mykus, S. A. ta in.** (2019). Organization of information and analytical support for the management of troops (forces): pidruchnyk. Kyiv: NUOU, 237. **10. Mykus, S. A. ta in.** (2019). The use of modern information technologies in business activities: pidruchnyk. Kyiv: NUOU, 237. **11. Krainov, V. O.** (2021). The main approaches to the selection of quality indicators when designing a conceptual database for the automated information system of the military management body. Zbirnyk naukovykh prats VIKNU im. Tarasa Shevchenko, 75, 120–125.

DOI:**10.33099/2311-7249/2023-46-1-78-82**

УДК 355.45

***Микола Якович Павлунько*** *(кандидат військових наук, доцент)*[1]
***Олег Ігорович Богатов*** *(кандидат технічних наук, доцент)*[2]
***Вікторія Петрівна Марко***[1]

[1] ***Національний університет оборони України імені Івана Черняховського, Київ, Україна***
[2] ***Харківський Національний автомобільно-дорожній університет, Харків, Україна***

# ОЦІНЮВАННЯ ПОХИБОК ВИМІРЮВАННЯ ШВИДКОСТІ В СПОЛУЧЕНИХ РАДІОТЕХНІЧНИХ СИСТЕМАХ В УМОВАХ ВПЛИВУ НЕУЗГОДЖЕНОСТЕЙ ЗА ЧАСОМ

*У статті, на основі масового застосування шумоподібних сигналів для передачі інформації з синхронним забезпеченням в системах засобів зв'язку під час їх руху, а також радіолокації, радіонавігації та управління космічними апаратами, проаналізовано вимоги до методів передачі інформації та до характеристик пристроїв її обробки. Визначено особливості використання цифрових технологій під час передачі та обробки інформації в радіотехнічних, телеметричних системах і системах зв'язку, що є причиною широкого впровадження складних сигналів для забезпечення адресної передачі в умовах довільного доступу, а також скритності систем передачі даних. Виявлено потреби в підвищенні ступеня захисту інформації, що найгостріше проявилися з розвитком мікроелектроніки, створенням елементної бази з надвеликим ступенем інтеграції. Проведено оцінювання залежності ймовірності достовірного виявлення сигналів (помилкової тривоги), що визначатимуть якість функціонування і роботу різних систем від забезпечення інформаційної безпеки каналів збору інформації, їх завадостійкості. Враховано функціональні зв'язки між вимірювальними каналами радіотехнічних суміщених систем і проведено оцінювання показників якості їх функціонування в умовах впливу загальних неузгодженостей шкал часу та частоти засобів єдиного часу. Визначені межі неузгодженості за часом, при яких забезпечується заданий рівень точності вимірів радіальної швидкості з урахуванням впливу зсуву за часом. Здійснено кількісне оцінювання впливу похибок схеми спостереження за затримкою каналу вимірювання дальності на похибки каналу вимірювання радіальної швидкості та показників якості функціонування каналу вимірювання швидкості суміщених систем з урахуванням впливу загальних неузгодженостей.*

***Ключові слова:*** *показники якості функціонування; сумісна радіотехнічна система; широкосмуговий шумоподібний сигнал.*

## Вступ

Шумоподібні сигнали (далі – ШПС) – це сигнали в яких база сигналу B є результатом перемноження ширини спектра F на тривалість T ($B = F \times T$) і є більше одиниці. Ці сигнали досить часто використовуються для передачі інформації і забезпечення синхронізації у системах зв'язку з рухомими об'єктами, управління космічними апаратами, радіолокації та радіонавігації.

Сьогодні спостерігається швидке зростання кількості комплексів і систем управління та зв'язку, збільшення обсягу переданої ними інформації, що накладає жорсткі вимоги до методів передачі інформації і до характеристик пристроїв її обробки. Розвиток мікроелектроніки, створення елементної бази з надвеликим ступенем інтеграції призвели до широкого використання цифрових технологій під час передачі й обробки інформації в радіотехнічних, телеметричних системах і системах зв'язку. Особливістю цифрових систем передачі інформації (далі – СПІ) є широке використання складних сигналів, що забезпечують можливість адресної передачі та вибору абонентом потрібного сигналу в умовах доступу багатьма станціями (довільного доступу), скритності роботи СПІ, підвищеної стійкості до навмисних завад і ефективного використання каналів зв'язку.

Іншим актуальним завданням є підвищення рівня конфіденційності інформації, що передається радіоканалом. В умовах мирного часу, посилення конкурентної боротьби зростає роль захисту інформації в радіоканалах, що використовуються комерційними структурами. Забезпечення інформаційної безпеки каналів збору інформації стає ще більш актуальним в межах декларованої програми посилення антитерористичної діяльності та під час бойових дій.

Дослідження і підвищення завадостійкості систем, що використовують ШПС, є важливим завданням, тому що від цього залежить якість роботи багатьох систем: GPS, ГЛОНАСС, Galileo, закритих каналів передачі інформації, радіолокації, управління космічними і літальними апаратами та ін. Від завадостійкості таких каналів залежить ймовірність правильного виявлення сигналів

(помилкової тривоги), які й визначають якість роботи і безпеку різних систем.

**Постановка проблеми.** Аналіз існуючих методів оцінювання похибок вимірювальних каналів суміщених радіотехнічних систем (далі – СРС) з широкосмуговим шумоподібним сигналом (далі – ШШС) внаслідок загальних неузгодженостей [16–17] свідчить, що вони мають суттєві недоліки, наприклад:

зазначені методи не дають чіткого уявлення про фізику процесів, що відбуваються в СРС;

деякі розрахунки згідно формул, що застосовують ці методи, можуть призвести до прямо протилежних висновків стосовно функціонування реальних СС;

квадратична залежність зниження відношення сигнал/шум від неузгодженостей призводить до можливості збільшення цього відношення при $\Delta f^{22}T^2 > 2$.

Зазначимо, що ці неузгодженості виникають внаслідок впливу похибок засобів єдиного часу і (або) через взаємний вплив у каналах систем. Тому доцільно здійснити кількісне оцінювання впливу похибок схеми спостереження за затримкою (далі – ССЗ) каналу вимірювання дальності на похибки каналу вимірювання радіальної (променевої) швидкості.

**Аналіз останніх досліджень і публікацій.** Теорія ШПС, а саме побудова сигналів, синтез методів, алгоритмів і пристроїв обробки досить широкого поширення набули з середини XX-го століття. Загальна теорія досить детально викладена в роботах В. Б. Пестрякова, В. П. Афанасьева, В. Л. Гурвіча, А. Л. Алєксєєва, Н. І. Смирнова, Уидроу Б., Стирнз С. [1–6]. Добре відомі й широко використовуються ШПС – лінійні рекурентні послідовності максимального періоду, окремим випадком яких є послідовності Хаффмена або М-послідовності.

Простота їх формування і прийнятні кореляційні властивості зумовили впровадження сигналів у системи і комплекси управління, зв'язку, радіолокації і радіонавігації [16–17]. Використання ШПС з великою базою дає змогу підвищити надійність систем управління і зв'язку та збільшити роздільну здатність по відстані в системах виміру дальності [1; 2; 5–6]. Однак під час пошуку ШПС з великою базою виникає низка проблем, пов'язаних з мінімізацією часу входження в кодовий синхронізм. Серед методів пошуку і синхронізації ШПС, що не потребують окремого еталону часу (це дає змогу безпосередньо визначити затримку сигналу за часом) мінімальний час синхронізації, при невеликих значеннях сигнал/ шум, мають методи паралельного аналізу сигналу з використанням багатоканальних кореляторів або узгоджених фільтрів, що розроблені в [1; 2; 5–7].

Наведені у згаданих вище джерелах методи розроблялися стосовно задачі обробки сигналу на тлі ідеалізованої завади – білого шуму і не враховують взаємовпливу використовуваних в СПІ сигналів. Так, рівень стійкості багатоканальних пристроїв на основі кореляторів знижується при одночасній наявності на вході декількох сигналів [1; 2; 5; 6]. Відомі оптимальні методи обробки сигналів, за наявності завад від декількох абонентів, складні в реалізації і описанні [8; 9].

Однак, у деяких випадках, на вході приймального пристрою діють негауссівські завади різного виду і потужності. Крім завад природного походження (атмосферних і космічних шумів), в СПІ присутні взаємні (системні) завади, поява яких обумовлена квазіортогональністю прийнятих сигналів. Можуть спостерігатися також вузькосмугові завади від різних радіопристроїв, що працюють з системою зв'язку в загальному частотному діапазоні і штучні завади (постановочні), що створюють для придушення джерела інформації і мають значну потужність [1; 5; 6]. Оцінювання надійності роботи СПІ в умовах дії внутрішніх (системних) або зовнішніх (природних чи навмисних) завад можлива на основі загальносистемного підходу [1; 2; 5; 6; 10–12]. У [5; 6] наведено, що для СПІ з ШПС найбільш небезпечними є потужні гармонійні завади та завади, що за структурою подібні до корисного сигналу (подібні завади).

Розроблення оптимальних пристроїв в системах передачі інформації і управління, що працюють в умовах дії негауссівських, вузькосмугових і структурних завад, призводить до створення складних за побудовою нелінійних пристроїв [11; 12]. Простішим рішенням є введення до складу СПІ пристроїв додаткової обробки сигналу з придушенням завад конкретного виду [13–15].

**Метою статті** є оцінювання показників якості функціонування каналу вимірювання швидкості суміщених систем з урахуванням впливу загальних неузгодженостей.

## Виклад основного матеріалу дослідження

Як наведено в [18], поява похибок синхронізації в одному каналі СРС призводить до додаткових похибок в іншому каналі цієї системи (рис. 1).

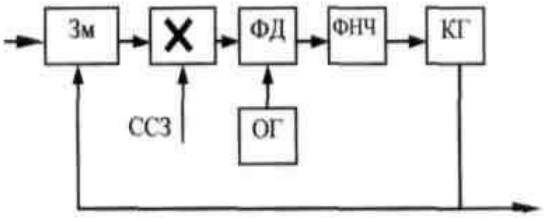



Рис 1. Вимірювальний канал СРС

На рис. 1 позначені: Зм – змішувач; ФД – фазовий детектор; ФНЧ – фільтр нижніх частот; КГ – керований генератор; ОГ – опорний генератор. Пропонуємо визначати взаємний вплив каналів таким чином: зміна за часом в схемі спостереження за затримкою призводить до зсуву прийнятого ШШС і опорного сигналу з виходу цієї схеми. Водночас не здійснюється повне згортання сигналу, і не отримується «чиста» несуча частота сигналу (рис. 2).

Як видно з рис. 2 з появою часового зсуву ΔТ сигнал, який надходить до входу фазового детектора схеми фазового автопідлаштування частоти (ФАПЧ) буде зрізаним на межах переходів від однієї серії символів до другої. Ці зрізи вносять похибки до вимірювань частоти ФАПЧ.

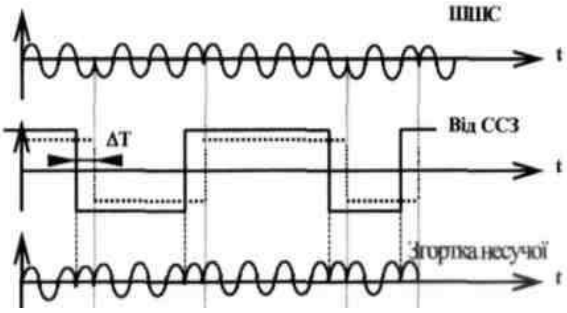



Рис 2. Епюри сигналів

Як видно з рис. 2 з появою часового зсуву ΔТ сигнал, що надходить до входу фазового детектора схеми фазового автопідлаштування частоти (далі – ФАПЧ) буде зрізаним на межах переходів від однієї серії символів до другої. Ці зрізи вносять похибки до вимірювань частоти ФАПЧ.

Таким чином, за інтервали ΔТ буде накопичуватись похибка вимірювання, яка зменшує співвідношення сигнал/шум (тобто збільшує шумові складові вхідної суміші), пропорційно тривалості інтервалу ΔТ. Водночас нове значення похибки буде пропорційним величині:

$$\delta^2 \sim \frac{(1+\Delta T/T_{ПВП})}{\mu_0} \qquad (1)$$

де $\mu_o$ – співвідношення сигнал/шум для ідеального випадку;

$T_{ПВП}$ – тривалість псевдовипадкової послідовності (далі – ПВП).

У подальшому потрібно відзначити, що кількість таких інтервалів (ΔТ) протягом довжини ПВП, що модулює, буде дорівнювати кількості переходів від однієї серії символів до другої, тобто кількості так званих «серій» одиниць і нулів у періоді ШШС. Ця кількість визначається за виразом [2]:

$$L_1 = 2^{n-1}, \qquad (2)$$

де n – кількість розрядів групи ПВП, що формує послідовність.

Припускаючи рівноймовірність розподілення серій за термін спостереження сигналу Тінт, можна знайти кількість переходів із співвідношення:

$$L = \frac{2^{n-1}}{T_{ПВП}} \cdot T_{інт.} \qquad (3)$$

Оскільки в СРС під час вимірювань використовуються послідовності, що моделюються, достатньо великої довжини (n≥10), то вираз (3) можна подати у вигляді:

$$L = \frac{2^{n-1}}{T_{ПВП}} \cdot T_{інт} = \frac{2^{n-1}}{r_0(2^n-1)} \cdot T_{інт} \approx \frac{T_{інт}}{2\tau_0} \qquad (4)$$

При цьому зменшення співвідношення сигнал/шум буде характеризуватись виразом:

$$\frac{L\cdot\Delta T}{T_{ПВП}} = \frac{\Delta T}{\tau_0^2}\frac{T_{інт}}{2^{n+1}} \qquad . \qquad (5)$$

Таким чином, можна записати загальний вираз для флуктуаційної похибки вимірювання радіальної швидкості з урахуванням впливу зсуву за часом.

$$\sigma^2_{флД} = \frac{C^2\left(1+\frac{\Delta T\cdot T_{інт}}{r_0^2\cdot 2^{n+1}}\right)}{32\pi^2 f_0^2 T_{інт}^2 \mu_0} \qquad (6)$$

Величину часового зсуву ΔТ визначимо так. Припустимо, що нестабільність частоти генератора становить величину $\Delta f/f_0 = 10^{-8}$ за 10 годин. Тоді за термін сеансу зв'язку t=10 хв стабільність приблизно можна вважати:

$$\Delta f/f_0 \cdot t/T \approx 10^{-8}\cdot 1/60 = 0{,}16\cdot 10^{-9}. \qquad (7)$$

У цьому випадку ΔТ знаходиться за виразом:

$$\Delta T = T_{ПВП}\cdot 0{,}16\cdot 10^{-9} = 0{,}16\cdot 10^{-9} N/f_T. \qquad (8)$$

Зокрема, для N=1023, $f_T=10^6$ отримаємо $\Delta T = 0{,}164\cdot 10^{-12}$ с для систем із запитом, але для систем без запиту розходження шкал може бути порядку $10^{-8}$ с. Тоді похибка вимірювання зросте у:

$$1+\frac{\Delta T}{\tau_0^2}\frac{T_{інт}}{2^{n+1}} \approx 1+\frac{30\cdot 10^{-3}\cdot 10^{-8}}{10^{-12}\cdot 2048} = 1{,}3 \quad \text{рази.}$$

З виразу (6) можна зробити висновок, що для зменшення вищенаведеного впливу слід використовувати сигнали з великою базою B>1000. Оскільки СРС під час вимірювання параметрів руху також приймає інформацію, то слід урахувати також похибки пов'язані з впливом інформаційної модуляції на точність вимірювань.

Відомо, що флуктуаційна похибка вимірювання радіальної швидкості під час впливу інформаційної модуляції зростає пропорційно величині $1 + 0{,}5\, N_0 П_ф / P_c$ ($N_0$ – спектральна щільність потужності шумів; $П_ф$ – смуга пропускання фільтрів, що фактично дорівнює швидкості передавання інформації, тобто $R_{інф} = П_ф$; $P_c$ – потужність сигналу на вході вимірювального каналу). Фізично це відбувається за рахунок впливу неповного згортання «несучої» частоти вхідного сигналу, обумовленого інформаційними посилками (інверсною модуляцією).

Водночас дисперсія загальної похибки слідкування (флуктуаційна та динамічна) буде:

$$\sigma^2_{ДΣ} = \frac{\tau_{0N_0}^2\left(1+\frac{N_0 R_{інф}}{2P_c}\right)\left(1+\frac{\Delta T T_{інт}}{\tau_0^2 2^{n+1}}\right)}{P_c\pi^2 T_{інт}^3} + 0{,}25\ddot{Д}\, T_{інт}^2 \qquad (9)$$

де $\ddot{Д}$ – третя похідна від функції дальності.

Відзначимо, що без урахування похибок за рахунок впливу неузгодженостей вираз (9) не має множника в других дужках чисельника. В цьому випадку оптимальне значення $T_{інт}$ (з погляду мінімуму дисперсії) визначається за виразом:

$$T_{інт} = \sqrt[7]{\frac{3\lambda_0^2 N_0\left(1+\frac{N_0 R_{інф}}{2P_c}\right)\cdot}{P_c\pi^2\ddot{Д}^2}} \qquad (10)$$

Для знаходження оптимального значення $T_{інт}$ у випадку впливу неузгодженостей використаємо такий вираз:

$$\frac{d\sigma_\Sigma^2}{dT_{інт}} = 0.$$

При цьому отримаємо:

$$-\frac{3A\left(1+BT_{інт}'\right)}{T_{інт}^4} + \frac{AB}{T_{інт}^3} + \dddot{Д}^2 T_{інт}^2 = 0' \qquad (11)$$

де $A = \frac{\lambda_0^2 N_0\left(1+\frac{N_0 R_{інф}}{2P_c}\right)}{P_c \pi^2}$; $B = \frac{\Delta T}{\tau_0^2 2^{n+1}}$.

Оптимальне значення $T_{інт}$ доцільно визначати методом ітераційних обчислень:

$$T_{інт} = \sqrt[7]{\frac{\lambda_0^2 N_0\left(1+\frac{N_0 R_{інф}}{2P_c}\right)\left(3+2\frac{\Delta T T_{інт}}{\tau_0^2 2^{n+1}}\right)}{P_c \pi^2 Д^2}} \quad (11)$$

З виразу (11) можна зробити висновок, що неузгодженість з ΔТ призводить до суттєвого збільшення похибок вимірювання радіальної швидкості. Для забезпечення припустимого рівня похибок слід обмежувати величину $\Delta T \le 0{,}05\text{-}0{,}1\ \tau_0$. У протилежному випадку слід зменшувати швидкість передачі інформації.

## Висновки й перспективи подальших досліджень

Таким чином, в статті була розглянута залежність похибок вимірювання при співвідношенні сигнал/шум, що збільшується в умовах змішування сигналів у вимірювальних каналах СРС з появою часового зсуву ΔТ.

Під час моделювання псевдовипадкової послідовності з достатньо великою її довжиною (n≥10) визначено загальний вираз (6) для флуктаційної похибки вимірювання радіальної (променевої) швидкості з урахуванням впливу зсуву за часом.

У статті розраховано збільшення похибки вимірювання для цифрових систем без запиту, яку можна зменшити, використовуючи сигнал з великою базою (В>1000).

На основі наведених виразів можна визначати оптимальні терміни спостереження сигналів у випадку впливу неузгодженостей за часом у вимірювальних каналах СРС.

Також враховано функціональні зв'язки між вимірювальними каналами СРС та проведено оцінювання показників якості їх функціонування в умовах впливу загальних неузгодженостей шкал за часом та частоти засобів єдиного часу. Визначено межі неузгодженостей за часом, при яких забезпечується потрібний рівень точності вимірювання радіальної швидкості.

Напрямами подальших досліджень слід вважати визначення сигналів у складних системах, за використання псевдовипадкової перебудови робочої частоти, а також удосконалення методів вимірювання ширини займаної смуги частот за критерієм співвідношення потужностей широкосмугових та над широкосмугових систем з метою створення загороджувальної завади радіоелектронним засобам, що використовують сигнали з великою кількістю стрибків під час перебудови робочої частоти.

## *Література*


**1. Пестряков В. Б., Афанасьев В. П., Гурвич В. Л. и др**. Шумоподобные сигналы в системах передачи информации / под ред. В. Б. Пестрякова. Москва : Сов. радио, 1973. 424 с. **2. Алексеев А. И., Шереметьев А. Г., Тузов Г. И., Глазов Б. И.** Теория и применение псевдослучайных сигналов. Москва : Наука, 1969. 368 с. **3. Смирнов Н. И., Горгадзе С. Ф.** Фазоманипулированные сложные сигналы с прямоугольными спектрами мощности. *Радиотехника и электроника*. Т. 39. 1994. №12. С. 2028–2036. **4. Уидроу Б., Стирнз С.** Адаптивная обработка сигналов : пер с англ. / под ред. В.В. Шахгильдяна. Москва : Радио и связь, 1988. 440 с. **5. Диксон Р. К.** Широкополосные системы : пер. с англ. Москва : Связь, 1979. 502 с. **6. Варакин Л. Е.** Системы связи с шумоподобными сигналами. Москва : Радио и связь, 1985. 384 с. **7. Журавлев В. И.** Поиск и синхронизация в широкополосных системах связи. Москва : Радио и связь, 1986. 40 с. **8. Малыгин И. Н.** Коды, коды, коды. *Технологии и средства связи*. 1999. № 3. С. 68. **9. Fakatselis J., Belkerdid M. A.** Processing Gain for Direct Sequence Spread Spectrum Communication Systems and PRISM™. Application Note 9633, Harris Semiconductor, August 1996. URL: https://fcc.report/FCC-ID/NM5WL2400-PCM/85424.pdf (дата звернення: 20.12.2022). **10**. Цифровые методы в космической связи / под ред. С. Голомба. Пер. с англ./ под ред. В. И. Шляпоберского. Москва : Связь, 1969. 272 с. **11. Treichler J.** Transient and convergent behavior of the adaptive line enhancer, IEEE Trans. *Ac-coust, Speech &Signal Process* (*ASSP-27).* №1. Feb. 1979. P. 53–62. **12. Тузов Г.И., Урядников Ю.Ф., Прытков В.И. и др.** Адресные системы управления и связи. Вопросы оптимизации / под ред. Г. И. Тузова. Москва : Радио и связь, 1993. 384 с. **13. Li L. and Milstein L.B..** Rejection of narrow-band interference in PN spread spectrum systems using dicision-feedback filters, «IEEE Trans. Commun». Vol. COM-31. Apr., 1983. P. 473–483. **14. Омура Т., Татибана Я.** Адаптивный цифровой фильтр для подавления гармонического шума. *Дэнси цусин гаккай ромбунси.* 1981. V. 64. № 9. P. 767–774. **15. Петров Е. П., Частиков А. В.** Адаптивный подавитель помех. *Адаптивные устройства обработки информации в радиолокационных и радионавигационных системах*: сб. научн. тр. МАИ. Москва : МАИ, 1984. С. 26–30. **16. Варакин Л. Е.** Системы связи с ШПС. Москва : Радио и связь, 1985. С. 384. **17. Чердынцев В. А.** Радиотехнические системы. Минск : Высшая школа, 1988. С. 370. **18. Чумак Б. О., Роянов О. М., Лисаченко І. Г.** Оцінка якості роботи радіотехнічних станцій при виявленні та супроводі космічних об'єктів. *Системи обробки інформації*. Харків : ХУПС. 2005. Вип. 4 (44). С. 96–103.


## ERRORSESTIMATION OF SPEED MEASUREMENTS IN THE COMBINED RADIO ENGINEERING SYSTEMS IN THECONDITIONS OF INFLUENCE OF INCONSISTENCIES IN TIME


***Mykola Pavlunko*** *((Candidate of Military Sciences, associate professor)*[1]
***Oleg Bogatov*** *(Candidate of Technical Sciences, associate professor)*[2]
***Victoria Marco***[1]

*[1]National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine*
*[2]Kharkiv National Automobile and Highway University, Kharkiv, Ukraine*

*Based on the mass application of noise-like signals for the transmission of useful information with synchronous provision in many systems of means of communication during their movement, as well as radiolocation, radio navigation and control of spacecrafts, the requirements for both information transmission methods and characteristics of processing devices were analyzed. The peculiarities of the use of digital technologies in the transmission and processing of information in radio engineering, telemetry systems and communication systems are determined, which is the reason for the widespread implementation of complex signals to ensure address transmission in conditions of arbitrary access, as well as secrecy of data transmission systems. The identified need to increase the degree of information protection was most acutely manifested with the development of microelectronics, the creation of an elemental base with an extremely high degree of integration. The dependence of the probability of reliable detection of signals (false alarms) that will determine the quality of work and the operation of various systems on the provision of information security of information collection channels and their immunity to interference is estimated. The functional connections between the measuring channels of radio-technical connected systems are taken into account, and the quality indicators of their functioning under the influence of general inconsistencies of the time scales and the frequency of the unified time means are evaluated. Limits of inconsistencies in time, at which a given level of accuracy of speed measurements is ensured, are determined. A quantitative evaluation of the effect of the errors of the range measurement channel delay monitoring scheme on the errors of the radial velocity measurement channel was carried out, and the indicators of the quality of the functioning of the velocity measurement channel of the combined systems were estimated, taking into account the influence of general inconsistencies.*

**Keywords:** indicators of the quality of functioning, combined radio engineering system, broadband noise-like signal.

## *References*

**1. Pestrjakov, V. B., Afanas'ev, V. P., Gurvich, V. L. i dr. (**1973) Noise-like signals in information transmission systems / pod red. V. B. Pestrjakova. Moskva : Sov. radio, 424. **2. Alekseev, A. I., Sheremet'ev, A. G., Tuzov, G. I., Glazov, B. I.** (1969) Theory and application of pseudorandom signals. Moskva : Nauka, 368. **3. Smirnov, N. I., Gorgadze, S. F. (**1994) Phazomani-polished complex signals with rectangular power spectra. *Radiotehnika i jelektronika,* 39 ,12, 2028–2036. **4. Uidrou, B., Stirnz, S.** (1988) Adaptive signal processing: per s angl. / pod red. V.V. Shahgil'djana. Moskva : Radio i svjaz', 440. **5. Dikson, R. K.** (1979) Broadband systems: per. s angl. Moskva : Svjaz', 502. **6. Varakin, L. E. (**1985) Communication systems with noise-like signals. Moskva : Radio i svjaz', 384. **7. Zhuravlev, V. I.** (1986) Search and Timing in Broadband Communications Systems. Moskva : Radio i svjaz',. 40. **8. Malygin, I. N.** (1999) Codes, codes, codes. *Tehnologii i sredstva svjazi*, 3, 68. **9. Fakatselis, J., Belkerdid, M. A. (**August 1996) Processing Gain for Direct Sequence Spread Spectrum Communication Systems and PRISM™. Application Note 9633, Harris Semiconductor. URL: https://fcc.report/FCC-ID/NM5WL2400-PCM/85424.pdf (data zvernennja: 20.12.2022). **10.** Digital methods in space communication. (1969) / pod red. S. Golomba. Per. s angl. / pod red. V. Shljapoberskogo. Moskva : Svjaz',. 272. **11. Treichler, J.** (Feb. 1979) Transient and convergent behavior of the adaptive line enhancer, IEEE Trans. *Ac-coust, Speech &Signal Process* (*ASSP-27),*1, 53–62. **12. Tuzov, G. I., Urjadnikov, Ju. F., Prytkov, V. I. i dr**. Address management and communication systems. Questions of optimization / pod red. G. I. Tuzova. Moskva : Radio i svjaz', 1993. 384. **13. Li, L. and Milstein L., B. (**Apr. 1983) Rejection of narrow-band interference in PN spread spectrum systems using dicision-feedback filters, «IEEE Trans. Commun», COM-31, 473–483. **14. Omura, T., Tatibana, Ja.** (1981) Adaptive digital filter for suppression of harmonic noise. *Djensi cusin gakkaj rombunsi,* 64, 9, 767–774. **15. Petrov, E. P., Chastikov, A. V.** (1984) Adaptive interference suppressor. Adaptive information processing devices in radar and radio navigation systems: sb. nauchn. tr. MAI. Moskva : MAI, 26–30. **16. Varakin, L. E.** (1985) Communication systems with ShPS. Moskva : Radio i svjaz', 384. **17. Cherdyncev, V. A.** (1988) Radio engineering systems. Minsk : Vysshaja shkola, 370. **18. Chumak, B. O., Roianov, O. M., Lysachenko, I. H.** (2005) Assessment of the quality of work of radio technical stations in the detection and tracking of space objects. *Systemy obrobky informatsii*. Xarkiv : KhUPS, 4 (44), 96–103.

DOI:**10.33099/2311-7249/2023-46-1-83-88**

УДК 004.81

***Олександр Вікторович Зайцев*** *(кандидат технічних наук, доцент)*[1]
***Михайло Олексійович Попов*** *(доктор технічних наук, професор, член-кореспондент НАН України)*[2]
***Сергій Сергійович Стефанцев*** [3]

[1]***Воєнна академія імені Євгенія Березняка, Київ, Україна***
[2]***Державна установа «Науковий центр аерокосмічних досліджень Землі Інституту геологічних наук Національної академії наук України», Київ, Україна***
[3]***Воєнна академія імені Євгенія Березняка, Київ, Україна***

# ПІДХІД ДО ОЦІНЮВАННЯ СТАНУ ОБ'ЄКТІВ НА ОСНОВІ СПІЛЬНОГО ВИКОРИСТАННЯ ПОТОЧНИХ РОЗВІДУВАЛЬНИХ ДАНИХ І ПОПЕРЕДНЬОЇ ІНФОРМАЦІЇ

*В сучасних умовах значна частина розвідувальних завдань вирішується шляхом комплексного оброблення даних, отриманих як технічними засобами розвідки, так й когнітивним (аналітичним) шляхом. Як правило, дані від різних типів джерел відрізняються надійністю, точністю, рівнем невизначеності, тобто є гетерогенними. Гетерогенність подібних даних утворює серйозну проблему при їх зведенні та комбінуванні. У статті запропоновано підхід до оцінювання стану об'єктів інтересу розвідки на основі комбінування ймовірнісних даних від різних типів розвідувальних джерел за допомогою модифікованого правила Байеса. Модифікація складається у тому, що часткові ймовірності стану об'єкта інтересу у відношенні правдоподібності розглядаються як випадкові змінні з бета-законом розподілу. В силу властивостей бета-розподілу таким чином значно поширюються можливості моделювання і обробки ймовірнісних даних від технічних засобів розвідки. Передбачається, що кожний технічний засіб розвідки містить у своєму складі зв'язані послідовно приймач, класифікатор і вирішальний блок. Приймач реєструє сигнали, що продукує об'єкт інтересу, ті сигнали обробляються, аналізуються і за підсумками формується відповідна часткова ймовірнісна байесівська оцінка. Для моделювання невизначеності ймовірнісних оцінок людини, заснованих на апостеріорній інформації, використовується інструментарій теорії свідчень Демпстера-Шейфера. Стисло розглянуто математичний інструментарій дослідження, після чого наведено суть запропонованого підходу. Наступними кроками дослідження мають бути технологізація розробленого підходу і розробка його програмного забезпечення.*

***Ключові слова****: об'єкт інтересу; оцінювання стану; розвідувальні дані; апостеріорна інформація; модифіковане правило Байеса; теорія свідчень Демпстера-Шейфера.*

## Вступ

**Постановка проблеми.** Успіхи в розробці нових ефективних сенсорів і технологізації інформаційно-пошукових процесів, які демонструються в світі, дозволяють поступово збільшувати обсяг і складність завдань, які воєнній розвідці вдається вирішувати шляхом залучення різноманітних технічних засобів. До таких завдань відносяться виявлення об'єктів, оцінювання їх стану, викриття замаскованих та хибних об'єктів тощо.

**Аналіз останніх досліджень і публікацій.** Для успішного вирішення подібних завдань воєнна розвідка має цілий набір технічних засобів з арсеналу MASINT, SIGINT, IMINT/GEOINT та ін. [1, 2]. У якості даних, що здобуваються за допомогою технічних засобів розвідки (далі – ТЗР), можуть бути знімки, спектрограми власного або відбитого електромагнітного випромінювання, повідомлення, коди тощо. Дані щодо об'єкта вивчення, отримані за допомогою ТЗР, допомагають сформувати заключення про його тип, стан тощо або прийняти інше рішення щодо об'єкта.

Одним з ефективних шляхів підвищення достовірності такого рішення є залучення раніше відомої інформації або експертних оцінок щодо розглядуваного об'єкта. Однак попередня інформація може бути застарілою, а оцінкам експертів притаманні, принаймні, когнітивні помилки. Таким чином, під час підготовки інформаційних документів використовуються два типи даних – чіткі та однозначні (hard) від ТЗР і дані з елементом невизначеності (soft) від інших джерел. Гетерогенність даних створює серйозну проблему при їх зведенні і комбінуванні.

У статті запропоновано підхід до оцінювання стану об'єктів на основі спільного використання поточних розвідувальних даних і попередньої інформації, в якому проблема гетерогенності даних вирішується за допомогою використання спеціального математичного інструментарію.

Матеріал статті організований наступним чином. В розділі 2 стисло викладено мотивацію на проведення роботи. Методологія, покладена в основу дослідження, описана в розділі 3. Розділ 4 містить опис запропонованого підходу. У розділі 5 наведено висновки.

*Мотивація.* Будемо під ТЗР розуміти засіб, що містить у своєму складі зв'язані послідовно приймач, класифікатор і вирішальний блок. Приймач реєструє сигнали, що продукує об'єкт інтересу, ті сигнали аналізуються, класифікуються і за підсумками класифікування у вирішальному блоці приймається відповідне рішення.

При вирішенні відносно простих завдань (наприклад, детектування об'єктів) ТЗР часто здатен працювати в автоматичному режимі. Але складні завдання (а оцінювання поточного стану об'єкта є саме таким завданням) потребують іншої організації процесів добування і обробки даних. Зокрема, в подібних випадках до вирішення завдання залучають, як правило, кілька ТЗР, а також є затребуваною деяка інша інформація щодо розглядуваного об'єкта.

**Мета статті**. У даній статті пропонується вирішення проблеми зведення даних різних типів (hard і soft) шляхом застосування математичного інструментарію теорії Байеса [3] і теорії свідчень Демпстера-Шейфера (далі – ТСДШ) [4]. Наявність такого вирішення обумовила можливість розробити новий підхід до оцінювання поточного стану об'єктів інтересу.

## Виклад основного матеріалу дослідження

*Математичний інструментарій дослідження. 1. Зведення даних за Байесом.* Припустимо, за допомогою N сенсорів вивчається деякий об'єкт, при цьому будь-який n-ий сенсор формує своє бачення поточного стану об'єкта незалежно від інших сенсорів і у такому вигляді:

$$\left\{\left\langle H_1, p_1^{(n)}\right\rangle,...,\left\langle H_k, p_k^{(n)}\right\rangle,...,\left\langle H_K, p_K^{(n)}\right\rangle\right\} \qquad (1)$$

де $H_k$ – гіпотеза про перебування об'єкта в k-му стані; $p_k^{(n)}$ – ймовірність, яка присвоєна гіпотезі $H_K$ за даними n-го сенсора; n=1,2,…,N.

Оскільки кожна гіпотеза має N оцінок ймовірності її реалізації (по числу сенсорів), то постає проблема зведення цих часткових оцінок до одного числа. Згідно з модифікованим правилом Байеса [5], зведена ймовірність гіпотези може бути розрахована за формулою:

$$P_k^{ps} = \left\{1 + \left[\frac{P_k^{(pr)}}{1-P_k^{(pr)}} \cdot \frac{\prod_{n=1}^{N}\psi^{(n)}(p_k^{(n)})}{\prod_{n=1}^{N}\psi^{(n)}(\overline{p}_k^{(n)})}\right]^{-1}\right\}^{-1} \qquad (2)$$

де $\psi^{(n)}(\cdot)$ – щільність ймовірностей станів; $P_k^{pr}$ – апріорна ймовірність k-го стану; $\overline{p}_k^{(n)} = \sum_{\substack{i-1 \\ i\neq k}}^{K} p_i^{(n)}$; k=1,2,…K.

У формулі (2) дріб

$$\frac{\prod_{n=1}^{N}\psi^{(n)}(p_k^{(n)})}{\prod_{n=1}^{N}\psi^{(n)}(\overline{p}_k^{(n)})} \qquad (3)$$

складає відношення правдоподібності. В [5] пропонується розглядати ймовірність $p_k^{(n)}$ у відношенні правдоподібності як випадкову змінну з бета-законом розподілу.

Щільність розподілу $\psi()$ змінної $p$, яка належить до сімейства бета-розподілів, визначається як [6]:

$$\psi(p) = \frac{p^{\alpha-1}\cdot(1-p)^{\beta-1}}{B(\alpha,\beta)}, \qquad (4)$$

де $B(\alpha,\beta) = \frac{\Gamma(\alpha)\cdot\Gamma(\beta)}{\Gamma(\alpha+\beta)}$ – бета-функція; $\Gamma(\cdot)$ – гама-функція; $\alpha,\beta$ – параметри; $\alpha>0, \beta>0$.

Якщо скористатися бета-розподілом для ймовірності як випадкової величини та зафіксувати значення параметрів $\alpha$ та $\beta$, то при відомих часткових ймовірностях і визначеній моделі бета-правдоподібності (symmetric beta likehood model) можна за формулою (2) розрахувати зведену ймовірність для кожної гіпотези.

Скористаємося симетричною моделлю бета-правдоподібності [5], за якою відношення правдоподібності для будь-якої k-ої гіпотези визначається наступним чином:

$$\frac{\psi^{(n)}(p_k^{(n)})}{\psi^{(n)}(\overline{p}_k^{(n)})} = \frac{(p_k^{(n)})^{\alpha_{n-1}}\cdot(1-p_k^{(n)})^{\beta_{n-1}})}{(p_k^{(n)})^{\beta_{n-1}}\cdot(1-p_k^{(n)})^{\alpha_{n-1}})} = \left(\frac{p_k^{(n)}}{1-p_k^{(n)}}\right)^{\alpha_n-\beta_m} \qquad (5)$$

при цьому $\alpha>\beta$.

Враховуючи (5), формула (2) набуває вигляду:

$$P_k^{ps} = \left\{1 + \left[\frac{P_k^{(pr)}}{1-P_k^{(pr)}} \cdot \prod_{n=1}^{N}\left(\frac{p_k^{(n)}}{1-p_k^{(n)}}\right)^{\alpha_n-\beta_m}\right]^{-1}\right\}^{-1} \qquad (6)$$

З формули (6) видно, що зведена ймовірність будь-якої гіпотези щодо стану об'єкта визначається:

частковими ймовірностями, які присвоюються цієї гіпотезі ТЗР;

параметрами бета-розподілу;

апріорними ймовірностями можливих станів об'єкта.

Оцінки апріорних ймовірностей можливих станів об'єкта, що розглядається, базуються на двох основних джерелах. Перше джерело – це наявні аналітичні матеріали, пов'язані з даним об'єктом.

Друге джерело – відомості, отримані раніше самими різними шляхами. На жаль, в силу різних причин (старіння інформації, ненадійність окремих джерел, неповнота даних тощо) інформація від обох зазначених джерел може бути неточною, неоднозначною й навіть суперечливою. Ефективний математичний апарат для опрацювання подібної інформації розроблений в ТСДШ [4].

*2. Теорія свідчень.* Ключовим в ТСДШ є поняття «основа аналізу» (далі – ОА). Під ОА розуміють множину з K взаємно незалежних елементів, що разом складають вичерпну групу. У даній роботі у якості елементів ОА розглядаються гіпотези щодо можливих станів об'єкта, а ОА складається з K гіпотез і записується як $\theta = \{H_1,...,H_k,...,H_K\}$.

З елементів ОА можуть формуватися більш складні утворення, наприклад, кон'юнкції типу $H_1 \cup H_2$ або ін. Сукупність «всі елементи з ОА» + будь-які кон'юнкції з елементів ОА + «пуста множина» (остання позначається як $\varnothing$) утворюють так звану «показову множину» $P(\theta)$. Показова множина містить $2^\theta$ простих та складних елементів:

$$P(\theta) = \{\varnothing, H_1,...,H_k,...,H_K, H_1 \cup H_2, H_1 \cup H_3,...,H_1 \cup H_2 \cup H_3,...,\theta\}.$$

Кожна підмножина $H$ в множині $P(\theta)$ характеризується певним числом $m(H)$, яке називається масою елемента $H$. Маса $m(A)$ показує ступень суб'єктивної довіри до елемента А з множини $P(\theta)$. Маси елементів $A \subseteq P(\theta)$ задовольняють умовам:

$$\left.\begin{array}{l} 0 \le m(A) \le 1; \\ m(\varnothing) = 0; \\ \sum\limits_{A \subset P(\theta)} m(A) = 1 \end{array}\right\}. \qquad (7)$$

Маси елементів показової множини, взяті разом, складають так званий розподіл базових ймовірностей (далі – РБІ). На основі цього розподілу обчислюються дві важливі в ТСДШ функції: функція довіри Bel і функція правдоподібності Pl.

Для всіх $A \subseteq \theta$ функція довіри визначається як

$$Bel(A) = \sum_{B \subseteq A} m(B). \qquad (8)$$

Функція довіри $Bel(A)$ показує рівень існуючої підтримки елемента А. Для всіх $A \subseteq \theta$ функція правдоподібності визначається як

$$Pl(A) = 1 - Bel(\overline{A}) = \sum_{B \cap A \neq \varnothing} m(B), \qquad (9)$$

де $\overline{A}$ – доповнення до елемента $A$. Функція правдоподібності $Pl(A)$ показує рівень максимально можливої підтримки елемента $A$. З визначень (8) і (9) легко побачити, що співвідношення між функціями довіри і правдоподібності таке: $Pl(A) \ge Bel(A)$.

Маса дозволяє характеризувати одним числом не тільки синглтони, а й комбінації з кількох гіпотез, що дуже зручно у процесі роботи з невизначеностями. Проте, у процесі виходу на етап прийняття рішення, дослідникові бажано мати окрему оцінку для кожної гіпотези. Щоб реалізувати таку потребу, Ф. Сметс (Ph. Smets), в 1990 році запропонував перетворення [7], за яким отримується, так звана, пігністична ймовірність (від латинського pignus = парі) будь-якого синглтона $A$ з множини ОА ( $A \subseteq \theta$ ):

$$BetP(A) = \sum_{A \in B \subseteq \theta} \frac{|A \cap B|}{|B|} \cdot m(B), \qquad (10)$$

де $|B|$ – кардинальне число множини $B$.

Пізніше в [8] було вказано на такий недолік формули Сметса (10). Справа у тому, що синглтон, для якого обчислюється пігністична імовірність, може також входити до складу деяких багатоелементних підмножин показової множини, й у подібних випадках до базової маси синглтона за формулою (10) додатково включається частка маси кожної зазначеної багатоелементної підмножини. Ця частка береться як маса багатоелементної підмножини, що рівномірно розподілена по всіх її складових елементах. Таким чином, не враховується існуюча різниця в масах між окремими елементами.

В роботах [9, 10] були запропоновані різні шляхи усунення цього недоліку, але найбільш ефективне рішення було нещодавно описано в роботі [11]. Суть його у наступному. Припустимо, $m(A)$ – це РБІ, визначений на множині ОА, а $m(H)$ – це РБІ для підмножини $H \subset P(\theta)$. Тоді удосконалене пігністичне перетворення для елемента $A$ визначається таким чином:

$$NBetP(A) = \gamma R_{Bel} + (1-\gamma) R_{Pl}, \qquad (11)$$

де $R_{Bel} = \sum\limits_{A \subset H \subset P(\theta)} \left( \frac{m(A)}{\sum\limits_{B \subseteq H} m(B)} \cdot m(H) \right), \qquad (12)$

$$R_{Pl} = \sum_{A \subset H \subset P(\theta)} \left( \frac{Pl(A)}{\sum\limits_{B \subseteq H} Pl(B)} \cdot m(H) \right), \qquad (13)$$

$\gamma$ – коефіцієнт визначеності,

$$\gamma = \sum_{\substack{C \subseteq \theta; \\ |C|=1}} m(C) \qquad (14)$$

На викладених математичних положеннях базується запропонований авторами підхід до оцінювання стану об'єктів.

*Запропонований підхід*

Розглянемо суть запропонованого підходу за допомогою наступного допоміжного прикладу (рис. 1).

Нехай, є деякий об'єкт $\Omega$ з трьома можливими станами $\Pi = (\pi_1, \pi_2, \pi_3)$ і необхідно встановити, у якому саме з них об'єкт $\Omega$ перебуває. До виконання цього завдання залучені два ТЗР, які працюють незалежно один від одного. Кожен ТЗР реєструє сигнали об'єкта і формує своє бачення поточного стану об'єкта $\Omega$ у вигляді $\left\langle H_k, p_k^{(n)} \right\rangle$, де $H_k$ – гіпотеза про перебування об'єкта в стані $\pi_k$; $p_k^{(n)}$ – ймовірність, яка присвоєна гіпотезі $H_k$ за даними n-го ТЗР; k=1,2,3; n=1,2.

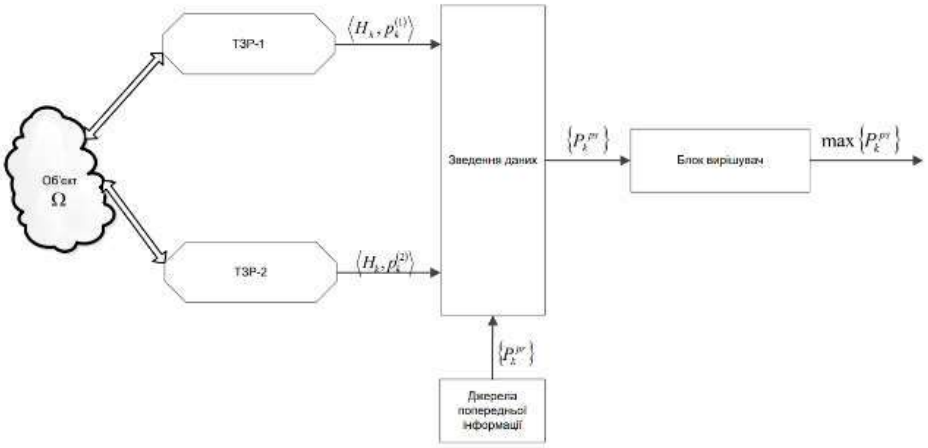



Рис.1. Запропонований підхід до оцінювання стану об'єктів на основі спільного використання поточних розвідувальних даних і попередньої інформації

Щоб вирішити поставлене завдання, необхідно:

1. Отримати бачення поточного стану об'єкта кожним з ТЗР.

2. Мати інформацію щодо апріорних ймовірностей можливих станів об'єкта.

3. Розрахувати зведені ймовірності кожної з гіпотез щодо стану об'єкта.

4. Визначити найбільш ймовірний стан об'єкта.

*Часткові ймовірності стану об'єкта* $\Omega$. Припустимо, під час вивчення об'єкта інтересу бачення ТЗР виявилось таким:

ТЗР-1: $p_{\pi_1}^{(1)} = 0.8; p_{\pi_2}^{(1)} = 0.1; p_{\pi 3}^{(1)} = 0.1;$

ТЗР-2: $p_{\pi_1}^{(2)} = 0.1; p_{\pi_2}^{(2)} = 0.7; p_{\pi 3}^{(2)} = 0.2;$

*Апріорні ймовірності можливих станів об'єкта* $\Omega$. Припустимо, результатом вивчення інформації з доступних джерел стали такі маси для станів об'єкта:

$$m(\pi_1) = 0.20;\ m(\pi_2) = 0.15; \qquad m(\pi_3) = 0.18;$$

$$m(\pi_1 \cup \pi_2) = 0.25;\ m(\pi_2 \cup \pi_3) = 0.22;$$

Необхідно перейти від нечітких мас до однозначних оцінок апріорних ймовірностей $P_{\pi 1}^{pr}$, $P_{\pi 2}^{pr}$, $P_{\pi 3}^{pr}$. Перехід здійснюється по-кроково за наступною процедурою:

1. За формулою (12) для кожного з можливих станів об'єкта $\Omega$ обчислити суму $R_{Bel}$:

$$R_{Bel}(\pi_1) = m(\pi_1) + m(\pi_1 \cup \pi_2) = 0.20 + 0.25 = 0.45;$$

$$R_{Bel}(\pi_2) = m(\pi_2) + m(\pi_1 \cup \pi_2) + m(\pi_2 \cup \pi_3) =$$

$$0.15 + 0.25 + 0.22 = 0.62;$$

$$R_{Bel}(\pi_3) = m(\pi_3) + m(\pi_2 \cup \pi_3) = 0.18 + 0.25 = 0.40.$$

2. Визначити функції правдоподібності, користуючись формулою (9):

$$Pl(\pi_1) = m(\pi_1) + m(\pi_1 \cup \pi_2) = 0.20 + 0.25 = 0.45;$$

$$Pl(\pi_2) = m(\pi_2) + m(\pi_1 \cup \pi_2) + m(\pi_2 \cup \pi_3) =$$

$$0.15 + 0.25 + 0.22 = 0.62;$$

$$Pl(\pi_3) = m(\pi_3) + m(\pi_2 \cup \pi_3) = 0.18 + 0.25 = 0.40.$$

3. За формулою (13) для кожного з можливих станів об'єкта $\Omega$ обчислити суми $R_{Pl}$:

$$R_{Pl}(\pi_1) = m(\pi_1) + \frac{Pl(\pi_1)}{Pl(\pi_1) + Pl(\pi_2)} \cdot m(\pi_1 \cup \pi_1) =$$

$$0.20 + \frac{0.45}{0.45 + 0.62} \cdot 0.25 = 0.305;$$

$$R_{Pl}(\pi_2) = m(\pi_2) + \frac{Pl(\pi_2)}{Pl(\pi_1) + Pl(\pi_2)} \cdot m(\pi_1 \cup \pi_2) +$$

$$\frac{Pl(\pi_2)}{Pl(\pi_2) + Pl(\pi_3)} \cdot m(\pi_2 \cup \pi_3) = 0.15 +$$

$$+ \frac{0.62}{0.45 + 0.62} \cdot 0.25 + \frac{0.62}{0.62 + 0.40} \cdot 0.22 = 0.429;$$

$$R_{Pl}(\pi_3) = m(\pi_3) + \frac{Pl(\pi_3)}{Pl(\pi_2) + Pl(\pi_3)} \cdot m(\pi_2 \cup \pi_3) =$$

$$0.18 + \frac{0.40}{0.62 + 0.45} \cdot 0.22 = 0.266.$$

4. Обчислити коефіцієнт визначеності за формулою (14):

$$\gamma = m(\pi_1) + m(\pi_2) + m(\pi_3) = 0.20 + 0.15 + $$
$$+ 0.18 = 0.53$$

5. Користуючись формулою (11), розрахувати апріорні ймовірності станів об'єкта $\Omega$ через відповідні пігністичні ймовірності:

$$P^{pr}_{\pi_1} = NBetP(\pi_1) = 0.53 \cdot 0.343 + 0.47 \cdot 0.303 =$$
$$= 0.325;$$

$$P^{pr}_{\pi_2} = NBetP(\pi_2) = 0.53 \cdot 0.357 + 0.47 \cdot 0.429 =$$
$$= 0.391;$$

$$P^{pr}_{\pi_3} = NBetP(\pi_3) = 0.53 \cdot 0.300 + 0.47 \cdot 0.266 =$$
$$= 0.284.$$

*Зведені ймовірності кожної з гіпотез щодо стану об'єкта.* Розрахунки здійснюються за формулою (6). Приймемо, що показник ступеню у формулі (6) дорівнює $\alpha - \beta = 0.5$, і проводимо розрахунки:

$$P^{ps}_1 = \left\{1 + \left[\frac{P^{(pr)}_1}{1 - P^{(pr)}_1} \cdot \prod_{n=1}^{2} \left(\frac{p^{(n)}_1}{1 - p^{(n)}_1}\right)^{0.5}\right]^{-1}\right\}^{-1} =$$

$$= \left\{1 + \left[\frac{0.325}{1 - 0.325} \cdot \left(\frac{0.8}{1 - 0.8}\right)^{0.5} \cdot \left(\frac{0.1}{1 - 0.1}\right)^{0.5}\right]^{-1}\right\}^{-1} =$$
$$= 0.32;$$

$$P^{ps}_2 = \left\{1 + \left[\frac{0.391}{1 - 0.391} \cdot \left(\frac{0.1}{1 - 0.1}\right)^{0.5} \cdot \left(\frac{0.7}{1 - 0.7}\right)^{0.5}\right]^{-1}\right\}^{-1} =$$
$$= 0.24;$$

$$P^{ps}_3 = \left\{1 + \left[\frac{0.284}{1 - 0.284} \cdot \left(\frac{0.1}{1 - 0.1}\right)^{0.5} \cdot \left(\frac{0.2}{1 - 0.2}\right)^{0.5}\right]^{-1}\right\}^{-1} =$$
$$= 0.07.$$

*Найбільш ймовірний стан об'єкта* визначається тією гіпотезою $H_k \cdot$, яка має найбільшу серед інших зведену імовірність:

$$P^{ps}_k \cdot = \max_{k=1,2,..3} \left\{P^{ps}_k\right\} = \left|k^{\cdot} = 1\right| = P^{ps}_1.$$

Тобто, найймовірніше, що об'єкт $\Omega$ перебуває у стані $\pi_1$.

У підсумку відзначимо, що хоча суть підходу було викладено за допомогою допоміжного числового прикладу, це не заважає використовувати розроблений підхід до оцінювання стану об'єктів в умовах будь-якої кількості станів і чисельності залучених ТЗР.

## Висновки й перспективи подальших досліджень

Таким чином, в статті запропонований підхід до оцінювання стану об'єктів на основі спільного використання поточних розвідувальних даних і попередньої інформації. Проблема, обумовлена гетерогенністю і невизначеністю зазначених даних, вирішується за допомогою математичного апарату теорії Байеса і теорії свідчень Демпстера-Шейфера. Суть розробленого підходу висвітлено на основі допоміжного прикладу.

Подальші дослідження мають бути спрямовані на технологізацію розробленого підходу і розробку його програмного забезпечення.

## *Література*

**1. HUMINT,** Commanders Guide to Human Intelligence: HANDBOOK. U.S. Army Intelligence Center of Excellence, 2012, № 12–17, 42 p. **2. Doctrine,** JP 2-0 Joint Intelligence. Publ. of the U.S. Army, 22 October 2013. 144 p. **3. Ash R. B.** Basic Probability Theory. New York: Dover Publications, 2008. 337 p. **4. Shafer G. A.** Mathematical Theory of Evidence. Princeton: Princeton University Press, 1976. 297 p. **5. Krzystofowicz R., Long D.** Fusion of Detection Probabilities and Comparison of Multisensor Systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. 1990. Vol. 20. № 3. P. 665–677. DOI: 10.1109/21.57281. **6. Krishnamoorthy K.** Handbook of Statistical Distributions. Boca Raton, FL : Chapman & Hall / CRC, 2006. P. 195–206. **7. Smets Ph.** Constructing the pignistic probability function in a context of uncertainty. In: Uncertainty in Artificial Intelligence / M. Henrion, J. F. Lemmer, L. N. Kanal, R. D. Shachter (Eds). Amsterdam : North Holland. Vol. 5. 1990. P. 29–39. **8. Daniel M.** Probabilistic Transformations of Belief Functions / L. Godo (Ed.): ECSQARU 2005, LNAI 3571. Heidelberg: Springer-Verlag, 2005. P. 539–551. **9. Cobb B. R., Shenoy P. P.** A comparison of methods for transforming belief functions models to probability models. In: Symbolic and quantitative approaches to reasoning with uncertainty (ECSQARU 2003); Lecture Notes in Artificial Intelligence – 2711. T.D. Nielsen, N.L. Zhang (Eds). Berlin : Springer-Verlag, 2003. P. 255–266. **10. Deng Z., Wang J.** Conflicting evidence combination method based on evidence distance and belief entropy. 2020 IEEE International Conference on Networking, Sensing and Control (ICNSC). 2020. P. 1–6. DOI: 10.1109/ICNSC48988.2020.9238076. **11. Zhao Y. X., Jia R. F., Liu C.** Transformation method of decision-making probability based on the certainty degree. *Journal of Harbin Engineering University.* 2015. Vol. 36. № 6. P. 801–804.

## AN APPROACH TO THE STATE OF THE OB'ECTS ASSESSING BASED ON THE USING CURRENT INTELLIGENCE DATA AND PREVIOUS INFORMATION

***Oleksandr Zaitsev (candidate of technical sciences, associate professor)[1]***
***Mykhailo Popov (doctor of technical sciences, professor, NAS Corresponding Member)[2]***
***Serhii Stefantsev[3]***
***[1]Military Academy named after Yevheniy Bereznyak, Kyiv,Ukraine***
***[2]State Institution "Scientific Centre for Aerospace Research of the Earth of the Institute of Geological Sciences of the National Academy of Sciences of Ukraine", Kyiv, Ukraine***
***[3]Military Academy named after Yevheniy Bereznyak, Kyiv,Ukraine***

*In modern conditions, a significant part of intelligence tasks is solved by complex processing of data obtained both by technical means of intelligence and by cognitive (analytical) means. As a rule, data from different types of sources differ in reliability, accuracy, and level of uncertainty, i.e. they are heterogeneous. The heterogeneity of such data creates a serious problem when combining and combining them. The article offers an approach to assessing the state of objects of intelligence interest based on combining probabilistic data from different types of intelligence sources using a modified Bayes rule. The modification consists in the fact that partial probabilities of the state of the object of interest in relation to likelihood are considered as random variables with the beta distribution. Due to the properties of the beta distribution, the possibilities of modeling and processing probabilistic data from technical intelligence tools are significantly expanded in this way. It is assumed that each technical means of intelligence contains in its composition a receiver, a classifier and a decisive block connected sequentially. The receiver registers signals that produce an object of interest, those signals are processed, analyzed, and a corresponding partial Bayesian probability estimate is formed based on the results. The Dempster-Schafer evidence theory toolkit is used to model the uncertainty of human probabilistic estimates based on a posteriori information. The mathematical tools of the study are briefly considered, after which the essence of the proposed approach is presented. The next steps of research should be the technologization of the developed approach and the development of its software.*

***Key words:*** *object of interest, state assessment, intelligence, a posteriori information, modified Bayes rule, Dempster-Schaefer evidence theory.*

## *References*

**1. HUMINT (**2012). Commanders Guide to Human Intelligence: HANDBOOK. U.S. Army Intelligence Center of Excellence, 12–17, 42. **2. Doctrine (**22 October 2013). JP 2-0 Joint Intelligence / Publ. of the U.S. Army, 144. **3. Ash, R. B.** Basic Probability Theory. New York: Dover Publications, 2008. 337. **4. Shafer, G. A.** Mathematical Theory of Evidence. Princeton: Princeton University Press, 1976. 297. **5. Krzystofowicz, R., Long, D. (**1990). Fusion of Detection Probabilities and Comparison of Multisensor Systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 20, 3, 665–677. DOI: 10.1109/21.57281. **6. Krishnamoorthy, K.** (2006). Handbook of Statistical Distributions. Boca Raton, FL: Chapman & Hall. CRC, 195–206. **7. Smets, Ph.** (1990). Constructing the pignistic probability function in a context of uncertainty. In: Uncertainty in Artificial Intelligence, 5, / M. Henrion, J. F. Lemmer, L. N. Kanal, R. D. Shachter (Eds). Amsterdam: North Holland; 29–39. **8. Daniel, M.** Probabilistic Transformations of Belief Functions / L. Godo (Ed.): ECSQARU 2005, LNAI 3571. Heidelberg: Springer-Verlag. 2005, 539–551. **9. Cobb, B. R., Shenoy, P. P.** (2003). A comparison of methods for transforming belief functions models to probability models / In: Symbolic and quantitative approaches to reasoning with uncertainty (ECSQARU 2003); Lecture Notes in Artificial Intelligence – 2711. T.D. Nielsen, N.L. Zhang (Eds). Berlin: Springer-Verlag, 255–266. **10. Deng, Z., Wang, J.** (2020). Conflicting evidence combination method based on evidence distance and belief entropy / 2020 IEEE International Conference on Networking, Sensing and Control (ICNSC), 1–6. DOI: 10.1109/ICNSC48988.2020.9238076. **11. Zhao, Y. X., Jia, R. F., Liu, C.** (2015). Transformation method of decision-making probability based on the certainty degree / Journal of Harbin Engineering University, 36, 6, 801–804.

DOI:**10.33099/2311-7249/2023-46-1-89-94**

УДК 004.75

***Ольга Володимирівна Андрощук*** *(кандидат психологічних наук)*
***Руслан Михайлович Черевко*** *(доктор філософії)*
***Микола Васильовитч Петрушен***
***Максим Юрійович Голобородько*** *(кандидат технічних наук, с.н.с.)*

***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# АКТУАЛЬНІ ПІДХОДИ ДО ПОБУДОВИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ ХМАРНИХ ТЕХНОЛОГІЙ З ВИКОРИСТАННЯМ РЕФЕРЕНСНОЇ АРХІТЕКТУРИ

*У статті проведено аналіз актуальних підходів до побудови інформаційної інфраструктури на основі хмарних технологій з використанням референсної архітектури. Теоретично проаналізовано розробки в галузі управління інформаційними технологіями. Досліджено перехід від детального опису кожного процесу до загальних цілей і принципів, які є важливими для управління інформаційними технологіями. Визначено, що існує ряд понять термінів, які можуть охоплювати ті чи інші процеси. Особлива увага була приділена вивченню використання технологій в державних установах, які стали основою для інформаційної системи, що розробляється. Дослідження базується на зарубіжному досвіді. Метою статті є аналіз і систематизація теоретичних й практичних аспектів використання референсних архітектур. Відповідно до поставленої мети статті запропоновані такі завдання: визначення загальних принципів роботи інформаційної інфраструктури, референсних архітектур на базі IT4IT; аналіз побудови інформаційної інфраструктури на основі хмарних технологій для створення єдиної інформаційної системи управління оборонними ресурсами Збройних Сил України. Використання референсних архітектур під час створення єдиної інформаційної інфраструктури потребує всебічного дослідження шляхів його виконання. Водночас, ця стаття присвячена дослідженню перспектив використання референсних архітектур під час побудови хмарних технологій для створення інформаційної інфраструктури державних організацій.*

***Ключові слова:*** *IT-інфраструктура; ЦОД; IT4IT; IT-стратегії; IT-служби; СОА; технічна архітектура; референсна архітектура; інформаційне забезпечення.*

## Вступ

Сьогодні ми є свідками безпрецедентного зростання мережевих інформаційних технологій. Напередодні повномасштабної російської агресії Верховна Рада України схвалила Закон, який дозволяє державним органам влади зберігати та обробляти дані у хмарі [1]. Крім того, Кабінет Міністрів України дозволив державним установам в умовах воєнного стану користуватися хмарними ресурсами і дата-центрами, що розташовані за межами України [2; 3].

**Постановка проблеми.** Сучасна Україна живе в умовах нової реальності, тому керівний склад держави змушений ухвалювати блискавичні рішення у відповідь на актуальні виклики. Таким чином, крок до цифрової трансформації став питанням безпеки, адже критично важливі для держави дані й досі зберігаються лише на фізичних серверах. Дата-центри стають привабливою мішенню не лише для численних хакерських атак ворога, але й для російських ракет. Збройні Сили України (далі – ЗС України) повинні розробити і застосувати нові сучасні підходи до розвитку власного інформаційного простору, забезпечення його стійкості та безпеки. Інформатизація ЗС України вимагає динамічного розподілу ресурсів і постійного збільшення трафіку, що викликано необхідністю використання мобільних пристроїв та відеоматеріалів.

**Аналіз останніх досліджень і публікацій.** Наразі інформаційні технології значно впливають на розвиток суспільства, тому дослідження спрямовані на подальший розвиток цих технологій здійснюються у достатній мірі як в нашій країні, так і за кордоном. Питання щодо ефективного функціонування мереж та управління станом компонентів мереж досліджувалися в роботах К. Шеннона, Л. Н. Беркман, Н. В. Лукової-Чуйко, О. Г. Оксіюка, І. Ю. Субача, В. О. Хорошка та ін. Функціональну стійкість інформаційних систем досліджували в своїх роботах Л. М. Артюшин, О. В. Барабаш, Ю. В. Кравченко, О. А. Кононов, В. А. Машков, О. А. Машков, С. А. Микусь, С. В. Нікіфоров, С. М. Неділько, Д. М. Обідін, Н. В. Руденко, В. А. Савченко, В. В. Собчук та ін. Питання стійкості систем щодо зовнішніх впливів досліджувались І. В. Рубан, О. Г. Оксіюк, С. В. Толюпа та ін. Управління інформаційними системами з урахуванням динаміки розвитку процесів досліджували О. С. Бичков, О. І. Лисенко, В. В. Онищенко.

**Мета статті.** В результаті теоретичного дослідження джерел присвячених побудові інформаційної інфраструктури на основі хмарних технологій під час побудови єдиної інформаційної системи управління оборонними ресурсами ЗС України було проведено аналіз та систематизація теоретичних і практичних аспектів використання раніше не розглянутих референсних архітектур.

## Виклад основного матеріалу дослідження

Використання хмарних технологій має підвищити взаємодію споживачів інформації, забезпечити швидке досягнення нових інформаційних спроможностей та покращити процес обміну інформацією. Як фундаментальну організацію системи було розглянуто стандарт ДСТУ ISO/IEC/IEEE 42010:2018 «Інженерія систем і програмних засобів. Опис архітектури», що складається із сукупності компонентів, зв'язків між ними і зовнішнім середовищем та принципи, якими керуються під час їх створення та розвитку [4]. Формування політики цифрової трансформації в системі Міністерства оборони України (далі – МО України), визначило низку стратегічних цілей. Зокрема, йде робота над створенням:

інформаційної системи оперативного (бойового) управління ЗС України;

єдиної інформаційної системи управління оборонними ресурсами (Defense Resources Management Information System) (далі –DRMIS).

У межах МО України основою щодо створення інформаційної інфраструктури стало створення DRMIS, яка має задовільнити існуючі інформаційні потреби структурних підрозділів щодо функціональних процесів управління оборонними ресурсами. Створення такої всеосяжної інформаційної системи досить складне, тому на цей час функціонують декілька різних інформаційних систем, що вирішують окремі, не пов'язані між собою, групи завдань. Одним із шляхів створення DRMIS є вдосконалення функціональної взаємодії існуючих та перспективних інформаційних систем на основі побудови інформаційної інфраструктури, що дозволить інтегрувати розрізнені інформаційні системи в єдину, яка в структурованому вигляді консолідується з інформацією, забезпечує оперативний доступ до інформації для аналізу і прийняття рішень. Успішність та ефективність DRMIS та інформаційної інфраструктури багато в чому визначаються рівнем розвитку, стабільністю й безпекою базової ІТ-інфраструктури, яка є основою для впровадження прикладних інформаційних систем і автоматизації функціональних процесів.

Сучасні практики створення ІТ-інфраструктури розглядають моделі зрілості ІТ-інфраструктури, які дозволяють оцінити поточні витрати на ІТ-інфраструктуру, виділити основні ІТ-процеси та технології, що потребують модернізації чи оновлення, а також дозволяють визначити шляхи та методи, які забезпечать зниження загальної вартості. Найпоширенішими у використанні є: Capability Maturity Model Integration (CMMI); Infrastructure Optimization Model (IOM); Infrastructure Optimization Initiative (IOI); Maturity Model; Process Capability Model [5]. Усі ці бібліотеки пропонують методики, за якими можна оцінити поточний стан ІТ-інфраструктури: наскільки наявні ІТ-засоби та ІТ-процеси ефективні з погляду інформаційних технологій, наскільки безпечна ІТ-інфраструктура, яка вартість ІТ.

Базова ІТ-інфраструктура має бути цілісною, максимально надійною, мати великий запас потужності, відповідати не лише поточному стану, а й враховувати його розвиток у майбутньому. Правильне її проєктування дозволить: знизити витрати на ІТ; спростити модернізацію існуючої інфраструктури; звести до мінімуму ймовірність простоїв у роботі або виходу систем з ладу; підтримувати безпеку інфраструктури на належному рівні; забезпечити просте управління ІТ-інфраструктурою; підвищити надійність ІТ-інфраструктури.

До основних компонентів ІТ-інфраструктури можна віднести:

центри обробки даних (далі – ЦОД), інженерну інфраструктуру ЦОД;

обчислювальну інфраструктуру (сервери);

інфраструктуру управління даними (системи зберігання даних, системи резервного копіювання та відновлення даних);

служби каталогу облікових записів користувачів;

моніторинг та управління.

Зазначене підтверджується положеннями, затвердженої Міністром оборони України 03 листопада 2021 р. під № 17549/з Концепції розвитку ІТ-інфраструктури МО України та ЗС України (далі – Концепція). Вона призначена для впровадження поглядів щодо подальшого розвитку ІТ-інфраструктури МО та ЗС України і визначає мету, основні принципи, напрями, цілі і завдання розвитку ІТ-інфраструктури МО та ЗС України.

Стрімкий розвиток інфокомунікаційних мереж з хмарною технологією відкриває безліч можливостей для користувачів. Користувачам «хмари» надаються необхідні сервіси «віддалено» за допомогою технології віртуалізації. Проте важливим аспектом у наданні хмарних послуг є швидкість надання цих сервісів, наявність вільних каналів для їх надання, щоб задовольнити потреби користувачів. Обробку всіх запитів користувачів здійснює ЦОД, який повинен забезпечити єдиний інформаційний ресурс з гарантованими рівнями достовірності, доступності та безпеки даних. Однак «нестійка» структура ЦОД, внаслідок міграції віртуальних машин, вноситиме затримки під час обслуговування запитів на надання сервісу.

Вважаємо за необхідне, охарактеризувати термін «Центр обробки даних» (ЦОД), який являє собою цілий комплекс інженерних та ІТ-систем, який є невід'ємною частиною безлічі телекомунікаційних структур. ЦОД повинен забезпечити єдиний інформаційний ресурс з гарантованими рівнями достовірності, доступності

та безпеки даних. У хмарних мережах ЦОД містяться не лише сервери зберігання даних, але й фізичні сервери, які здійснюють обробку запитів на надання сервісів. На кожному такому сервері може міститися від однієї до кількох десятків віртуальних машин, які здатні обробляти та задовольняти відповідними компонентами чи додатками запити на надання сервісу. Інженерна інфраструктура ЦОД складається з:

електричних систем, джерел безперебійного живлення та систем кондиціювання;

структурованої кабельної мережі;

приміщення та займані площі.

Архітектура інформаційної інфраструктури є важливим критичним елементом, що пов'язує інформаційні технології і процеси стратегічного планування щодо їх розвитку, прикладні інформаційні системи та процеси їх супроводу. Процес розробки архітектури інформаційної інфраструктури дає можливість гнучко підходити до змін та розробляти мінімальну кількість документів управління. Першочерговими завданнями проєкту побудови архітектури інформаційної інфраструктури стали:

організація необхідних структур із залученням керівництва, функціональних підрозділів і планування робіт;

розуміння стратегії розвитку;

формування загальних IT-вимог до цільової архітектури;

розробка принципів побудови архітектури.

Під час створення складних, розподілених інформаційних систем, проєктуванні архітектури інформаційної інфраструктури, виборі компонентів і зв'язків між ними слід враховувати, крім загальних (відкритість, масштабованість, переносимість, мобільність, захист тощо), низку специфічних концептуальних вимог таких, як:

висока доступність – забезпечує комфортний, максимально спрощений доступ користувачів до сервісів і результатів функціонування інформаційних систем на основі сучасних графічних засобів, мнемосхем та наочних користувальницьких інтерфейсів;

кросплатформність – суттєво скорочує витрати на розробку нового або адаптацію існуючого програмного забезпечення;

масштабовність – здатність системи обробити більший обсяг роботи або бути легко розширеною;

відмовостійкість та безпека – забезпечує безпеку системи за різних видів загроз і надійний захист даних від помилок проєктування, руйнування або втрати інформації, а також авторизацію користувачів, керування робочим завантаженням, резервуванням даних і обчислювальних ресурсів, максимально швидким відновленням функціонування інформаційних систем;

гнучкість – забезпечує відносно простий, без докорінних структурних змін, розвиток інфраструктури і зміну конфігурації використовуваних засобів, нарощування функцій і ресурсів інформаційних систем відповідно до розширення сфер і завдань її застосування.

Істотний вплив на формування стратегії розвитку прикладних інформаційних систем надає IT-архітектура, яка є тим фундаментом, на якому будуються і функціонують прикладні системи. В рамках IT-архітектури встановлюються принципи функціонування апаратної платформи, операційних систем, систем управління базами даних, засобів розробки, мов програмування, прикладних систем проміжного прошарку, систем безпеки, мережевої інфраструктури.

Однією із перспективних моделей розвитку IT-архітектури є сервісна модель взаємодії між інформаційними системами в межах сервісно-орієнтованої архітектури (далі – СОА). Вона являє собою стиль побудови архітектури, орієнтований на сервіси. Найбільш загальне формулювання СОА наводиться міжнародним консорціумом The Open Group, який є розробником референсної архітектури IT4IT [6]. На даний час відкритий стандарт IT4IT є одним із найновіших стандартів щодо управління архітектурою IT-інфраструктури [6]. Він не скасовує існуючі стандарти і кращі практики бібліотеки інфраструктури інформаційних технологій (далі – ITIL), відкритої організаційної структури (TOGAF), Зводу знань з управління проєктами (PMBoK) і т. ін., а виступає у якості «надбудови», що дозволяє з'єднати їх разом [7; 8]. IT4IT можна використовувати для оцінювання поточного стану та планування гармонійного розвитку управління IT-інфраструктурою – як у частині функціональних процесів, так і їх автоматизації.

Референсна архітектура IT4IT забезпечує «еталонну, повторювану, модель» для створення екосистеми управління IT. Вона призначена для того, щоб допомогти адаптуватися до змін у технології, процесах і методах без необхідності змінювати архітектуру управління відповідно до кожної зміни [9]. Референсна архітектура IT4IT проводить відповідність між функціональними компонентами, пов'язаними об'єктами даних та ланцюжками цінності, тим самим описуючи процес надання IT-сервісів та формулюючи загальний концепт.

У стандарті IT4IT слід розділяти поняття термінів «процес» і «потік», оскільки саме на цьому і будується основна концепція стандарту. *Потоки* створення цінностей за своєю суттю не є *процесами*, але ними підтримуються. Основні потоки створені для сфери управління, планування, розподілу ресурсів, створення та надання IT-сервісів. Можна виділити чотири основні потоки створення цінності цільового стану:

планування (Strategy to Portfolio, S2P) – отримує стратегічні запити на нові або покращені IT-сервіси і розробляє концепцію сервісу для представлення нової або покращеної послуги, згідно запиту;

побудова (Requirement to Deploy, R2D) – отримує концепцію IT-сервісу, проєктує та розробляє логічну послугу з більш детальними

вимогами, що описують порядок розроблення щойно запитаної послуги та її компоненти;

випуск (Request to Fulfill, R2F) – отримує план випуску ІТ-сервісу та створює записи в каталозі послуг, що надають опис порядку надання послуги;

запуск (Detect to Correct, D2C) – забезпечує структуру для інтеграції, моніторингу, управління, відновлення та інших операційних аспектів, пов'язаних із реалізованими сервісами та/або тими, що розробляються.

Наступним основоположним питанням побудови архітектури інформаційної інфраструктури є визначення ІТ-стратегії на основі референсної архітектури. У завданні вибору ІТ-стратегії можна виділити такі складові елементи:

визначення стратегії розвитку прикладних ІС;

визначення стратегії управління та експлуатації ІТ-інфраструктури.

Розбіжностями напрямів ІТ-стратегії є різні підходи до їх оцінки. Стратегія розвитку прикладних інформаційних систем (далі – ІС) тісно пов'язана з функціональними процесами, тому під час її оцінювання увага має бути сфокусована на якість підтримки функціональних процесів відповідними прикладними ІС і, отже, відповідність ІТ-служби в цілому потребам користувачів. Для реалізації складової ІТ-стратегії, пов'язаної з управлінням ІТ-інфраструктурою, стандартними підходами є управління на основі методології ITIL і аудит діяльності ІТ-підрозділу за допомогою стандарту «Control Objectives for Information and Related Technology» (COBIT) [7; 10].

Під час розроблення ІТ-стратегії необхідно відштовхуватися від поточного стану інформаційної інфраструктури та існуючих прикладних ІС. На підставі аналізу існуючих ІС і цільової функціональності можна отримати опис якої функціональності бракує, яку зараз слід реалізовувати в межах впровадження нових ІС, тобто визначити цільові елементи стратегії за допомогою аналізу ситуацій AS-IS – «як зараз» і TO-BE – «як має бути».

СОА – це модель, в якій різні функціональні модулі компонентів взаємодіють за допомогою уніфікованих інтерфейсів. ІТ-сервіси можуть виступати як прикладні системи, або їх окремі функціональні модулі, або віддалені програмні компоненти, що надаються у вигляді сервісу. За таких умов, важливим є той факт, що всі функції ІС (як локальних, так і віддалених) мають бути визначені як ІТ-сервіси з чітко визначеними завданнями і можливостями повторного використання іншими системами. Реалізація сервісно-орієнтованої моделі як референсної архітектури інформаційної інфраструктури несе як стратегічну, так і тактичну цінність. Стратегічними перевагами СОА є:

скорочення часу реалізації ІТ-проєктів;

застосування єдиного підходу до оцінки ризиків та вибору компонентів, складових ІТ-архітектури;

підвищення продуктивності ІС;

більш швидка і менш дорога інтеграція;

гнучкість у зміні та налаштуванні;

уніфікація доступу до даних і забезпечення цілісності даних;

можливість об'єднувати інформаційні системи від декількох виробників;

можливість одночасного використання різних способів придбання ІС в межах єдиної інформаційної інфраструктури;

відповідність всіх компонентів ІТ-архітектури єдиній політики інформаційної безпеки.

Тактична цінність використання СОА полягає в:

простоті розробки та впровадження ІС;

гнучкості в зміні різних процесів для задоволення специфічних потреб;

можливості повторного використання компонентів;

можливості безперервного поліпшення якості кожного з ІТ-сервісів окремо.

Вибір ІТ-сервісів може розглядатися як процес прийняття рішення про те, за допомогою яких апаратно-програмних засобів буде здійснюватися підтримка і автоматизація ключових функціональних процесів. Результатом некоректного вибору можуть бути неприємні наслідки, починаючи від даремно витрачених коштів і часу до зміни обраного курсу розвитку. Окрім того, у процесі вибору ІТ-сервісів вирішується також задача про спосіб реалізації ІС. Якщо раніше це питання вирішувалося шляхом закупівлі апаратно-програмних засобів ІС і розміщення їх у замовника, то сучасний рівень розвитку ІТ характеризується зростанням ринку ІТ-послуг та ІТ-аутсорсингу з використанням послуг сторонніх ЦОД, а також хмарних послуг.

Різні типи хмарних архітектур можуть бути реалізовані за допомогою різних моделей обслуговування, базовими серед яких є: IaaS (послуги інфраструктури), PaaS (послуги платформи) та SaaS (послуги прикладних програм) (рис. 1).

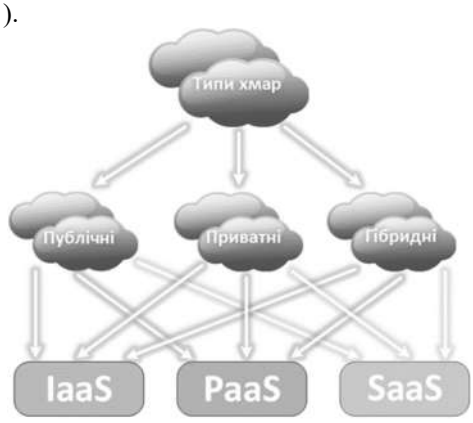



Рис. 1. Типи хмар і моделі їх обслуговування

IaaS (Infrastructure-as-a-Service) – модель «інфраструктура-як-сервіс» передбачає надання користувачеві ІТ-ресурсів з певною обчислювальною потужністю та обсягами пам'яті.

PaaS (Platform-as-a-Service) – модель обслуговування «платформа-як-сервіс» передбачає надання доступу споживачу до операційних систем, засобів розробки і тестування програмного забезпечення, і надає послуги як: сховище даних, програмне забезпечення, система управління базами даних (далі – СУБД), інтеграція, робоче місце, безпека тощо.

SaaS (Software-as-a-Service) – модель обслуговування «програмне забезпечення як послуга», за якої програми та сервіси надає і обслуговує провайдер, розміщує їх в хмарі і пропонує до використання через браузер або веб-додаток.

У процесі розробці такого роду систем важливим питанням є вибір технічної складової (технічної архітектури), яка зможе забезпечити надійне, відмовостійке, безпечне і продуктивне середовище функціонування всіх підсистем.

Технічна архітектура (Technical Architecture) – є першим рівнем загальної архітектури ІС та складає її основу (базис). Вона описує всі апаратні засоби, що використовуються під час виконання заявленого набору функцій, а також включає засоби забезпечення мережевої взаємодії та надійності. Технічна архітектура – це сукупність програмно-апаратних засобів, методів і стандартів, які забезпечують ефективне функціонування системи та подають інфраструктуру в цілому.

Важливим аспектом, на етапі проєктування ІС та системи зв’язку в цілому, є вибір технологічного рішення за допомогою якого майбутня або існуюча система буде виконувати ті вимоги, які висуваються до неї та завдання, які на неї покладаються. Відмова сервера або вузла кластеру, що зазвичай відбувається несподівано та у відповідальний момент, тягне за собою серйозні наслідки, що особливо актуально для систем спеціального призначення у військовій сфері діяльності.

Проблеми недостатньої продуктивності сервера (вузла) через зростання навантаження можна вирішувати шляхом нарощування потужності сервера, або оптимізацією використовуваних алгоритмів, програмних кодів і т.д. Іншим способом підвищення продуктивності серверів є їхнє об’єднання у кластер, у якому навантаження розподіляється між серверами (вузлами) за допомогою комплексу спеціальних методів та алгоритмів балансування навантаження. Крім вирішення проблеми високих навантажень, технологія кластеризації допомагає також забезпечити резервування серверів, ефективність якого знову ж таки залежить від того, як розподіляється (балансується) навантаження між вузлами кластера.

Балансування навантаження може здійснюватися за допомогою апаратних і програмних інструментів та може бути реалізоване на мережевому, транспортному й прикладному рівнях моделі взаємозв'язку відкритих систем (The Open Systems Interconnection Model (OSI)).

Балансування навантаження кластерної системи на мережевому рівні передбачає таке підключення сервера до мережі, за якого його кожна IP-адреса (в тому числі віртуальна) обслуговується різними фізичними серверами (вузлами кластера), тобто передбачає вирішення наступного завдання: потрібно зробити так, щоб за одну конкретну IP-адресу сервера відповідали різні фізичні машини. Зниження навантаження на сервер на транспортному рівні передбачає використання балансувальника, який розподіляє запити по пулу відповідно до заданих алгоритмів.

Як ще один приклад інструменту балансування на практичному рівні можна розглянути pgpool – проміжний шар між клієнтом і сервером СУБД PostgreSQL. За його допомогою можна розподіляти запити між серверами баз даних залежно від їх вмісту: наприклад, запити на читання будуть передаватися на один сервер, а запити на запис – на інший.

## Висновки й перспективи подальших досліджень

Розуміння вищезазначеного переконує в тому, що вибір та застосування якогось одного алгоритму в майбутній або існуючій системі, особливо розподіленій, не повною мірою може забезпечити надійне та відмовостійке функціонування системи, що в подальшому призведе до порушення роботи як окремих модулів, так і всієї системи в цілому. Тому, основою створення єдиного інформаційного простору Міністерства оборони України та Збройних Сил України має стати сервісно-орієнтована архітектура інформаційно-технологічної-інфраструктури, яка забезпечує доступ до інформації, та надає доступ до автоматизованих функціональних процесів у вигляді інформаційно-технологічних сервісів. Надання таких сервісів із використанням хмарних технологій має підвищити взаємодію споживачів інформації, забезпечити швидке досягнення нових інформаційних спроможностей та покращити процес обміну інформацією.

Подальші дослідження, на нашу думку, буде доцільно спрямувати на більш глибокий розгляд та аналіз можливостей референсної архітектури інформаційної інфраструктури на базі бібліотеки IT4IT.

## *Література*

**1. Закон України** «Про хмарні послуги» від 17.02.2022 № 2075-IX URL : https://zakon.rada.gov.ua/laws/show/2075-20#Text (дата звернення 01.12.2022). **2. Постанова Кабінету Міністрів України** «Деякі питання забезпечення функціонування інформаційно- комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану» від 12.03.2022 № 263. URL : https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text (дата звернення 01.12.2022). **3. Закон України** «Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-

комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів» від 15.03.2022 № 2130-IX. URL : https://zakon.rada.gov.ua/laws/show/2130-20#Text (дата звернення 01.12.2022). **4. ДСТУ ISO/IEC/IEEE 42010:2018** «Інженерія систем і програмних засобів. Опис архітектури» (ISO/IEC/IEEE 42010:2011, IDT). 2018. URL : http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=77960 (дата звернення 01.12.2022). **5. Голобородько М. Ю., Федорієнко В. А., Кірпічніков Ю. А. [та ін.]** Теоретичні підходи щодо визначення місця інформаційної інфраструктури Міністерства оборони України у розумінні рамкових архітектурних методологій. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. 2016. № 3(58). С. 136–141. **6. Open Group IT4IT™** Reference Architecture, Version 2.1. URL : https://pubs.opengroup.org/it4it/refarch21/index.html (дата звернення 01.12.2022). **7. What is ITIL** Best Practice. ITIL. AXELOS. URL : https://www.axelos.com/best-practice-solutions/itil/what-is-itil (дата звернення 01.12.2022). **8. TOGAF**, an Open Group standard. URL : http://www.opengroup.org/subjectareas/enterprise/togaf (дата звернення 01.12.2022). **9. Андрощук О. В., Петрушен, М. В., Литовченко Г. Д., Капілевич В. О.** Практика використання референсної архітектури інформаційної інфраструктури. *Молодий вчений: збірник наукових праць*. 2022. № 9(109). С. 1–5. **10. COBIT an ISACA Framework.** URL : http://www.isaca.org/cobit (дата звернення 01.12.2022).

## CURRENT APPROACHES TO BUILDING INFORMATION INFRASTRUCTURE BASED ON CLOUD TECHNOLOGIES USING REFERENCE ARCHITECTURE

***Olha Androshchuk** (Ph.D. of Psychological Sciences)*
***Ruslan Cherevko** (Ph.D. of Engineering Sciences)*
***Mykola Petrushen***
***Maxim Holoborodko** (Ph.D.)*

***The National Defense University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine***

*The article analyzed current approaches to building information infrastructure based on cloud technologies using reference architecture. Developments in field of information technology management are theoretically analyzed. The transition from a detailed description of each process to general goals and principles that are important for IT management is explored. It was determined that there are a number of concepts that can cover certain processes. Special attention is paid to study of use technologies in state institutions and as the basis developed information system. Study based on foreign experience. The purpose of this study is analysis and systematization of theoretical and practical aspects use of reference architectures. In accordance with set goal, tasks of article were to determine general principles of information infrastructure, reference architectures based on IT4IT. Analysis of construction information infrastructure based on cloud technologies during construction of a unified information system for management of defense resources in the Armed Forces of Ukraine. The use of reference architectures during creation of a unified information infrastructure requires a comprehensive study the ways of its implementation. A valid article is devoted to study of prospects using reference architectures in the construction cloud technologies for the creation of information infrastructure state organizations.*

***Keywords:** IT infrastructure; data center; IT4IT; IT strategies; IT services; SOA; technical architecture; reference architecture; information support.*

### *References*

**1. Law of Ukraine** «On Cloud Services» № 2075-IX (17.02.2022). URL : https://zakon.rada.gov.ua/laws/show/2075-20#Text (accessed on December 01, 2022). **2. Resolution of the Cabinet of Ministers of Ukraine** «Some issues of ensuring the functioning of information and communication systems, electronic communication systems, public electronic registers under martial law» № 263 (12.03.2022). URL : https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text (accessed December 01, 2022). **3. Law of Ukraine** «On Amendments to Certain Laws of Ukraine on Ensuring the Functioning of Information and Communication Systems, Electronic Communication Systems, Public Electronic Registers» № 2130-IX (15.03.2022). URL : https://zakon.rada.gov.ua/laws/show/2130-20#Text (accessed December 01, 2022). **4. DSTU ISO/IEC/IEEE 42010:2018** «Systems and software engineering. Architecture description» (ISO/IEC/IEEE 42010:2011, IDT). (2018). URL : http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=77960 (accessed 01.12.2022). **5. Goloborodko M.Y., Fedorienko V.A., Kirpichnikov Y.A. [et al.**] (2016). Theoretical approaches to determining the place of the information infrastructure of the Ministry of Defense of Ukraine in the understanding of architectural methodologies Zbirnyk naukovykh pracj Centru vojenno-strateghichnykh doslidzhenj Nacionaljnogho universytetu oborony Ukrajiny imeni Ivana Chernjakhovsjkogho, 3(58), 136–141. **6. Open Group IT4IT™** Reference Architecture, Version 2.1 URL : https://pubs.opengroup.org/it4it/refarch21/index.html (accessed 01.12.2022). **7. What is ITIL Best Practice**. ITIL. AXELOS URL : https://www.axelos.com/best-practice-solutions/itil/what-is-itil (accessed 01.12.2022). **8. TOGAF**, an Open Group standard URL : http://www.opengroup.org/subjectareas/enterprise/togaf (accessed 01.12.2022). **9. Androshhuk, O. V., Petrushen, M. V., Lytovchenko, Gh. D., Kapilevych, V. O.** (2022). Practice of using the reference architecture of information infrastructure Molodyj vchenyj : zbirnyk naukovykh pracj, 9(109), 1–5. **10. COBIT an ISACA Framework** URL : http://www.isaca.org/cobit (accessed 01.12.2022).

DOI:**10.33099/2311-7249/2023-46-1-95-98**

УДК: 355.415

***Олег Михайлович Воробйов*** *(доктор технічних наук, професор)*[1]
***Володимир Васильович Ткаченко***[1]
***Михайло Порфирійович Бамбуляк***[2]
***Сергій Віталійович Тягай*** *(кандидат військових наук)*[2]

[1] ***Національний університет оборони України імені Івана Черняховського, Київ, Україна***
[2] ***Кам`янець-Подільський національний університет імені Івана Огієнка, Кам`янець-Подільський,***

# ВИБІР ТА ОБҐРУНТУВАННЯ ПОКАЗНИКІВ ЕЛЕКТРОМАГНІТНОЇ СТІЙКОСТІ РАДІОЕЛЕКТРОННОЇ АПАРАТУРИ ІНФОРМАЦІЙНИХ СИСТЕМ ДО ЗОВНІШНІХ ЕЛЕКТРОМАГНІТНИХ ВПЛИВІВ

*У статті окреслено низку питань, що актуалізують наявні проблеми забезпечення захисту радіоелектронної апаратури інформаційних систем технічних засобів Збройних Сил України від зовнішніх електромагнітних впливів. Здійснено аналіз наукових робіт в цій сфері і визначено, що напрямом створення захисту буде розробка комплексного методу створення такого захисту, який складається з двох складових, а саме захисту радіоелектронної апаратури інформаційних систем технічних засобів та захисту об'єкту зберігання цих засобів від зовнішнього електромагнітного впливу. Обґрунтовано узагальнений кількісний показник електромагнітної стійкості радіоелектронної апаратури інформаційних систем технічних засобів у межах якого вона спроможна виконувати свої функції і зберігати параметри в межах, встановлених у технічному завданні, під час і після електромагнітного впливу із заданими параметрами. Відповідно цих вимог, обрано і обґрунтовано часткові показники. Серед такої широкої групи показників визначено основні, що найбільш співпадають із досягненням кількісних величин, що відповідають меті – зниженню уражаючої дії зовнішнього електромагнітного впливу на об'єкти ураження до рівня їх граничної електромагнітної стійкості. В подальшому пропонується на основі визначених та обґрунтованих показників електромагнітної стійкості обґрунтувати технічні вимоги до створення захисту радіоелектронної апаратури інформаційних систем технічних засобів.*

***Ключові слова****: інформаційні системи, радіоелектронна апаратура, електромагнітна стійкість.*

## Вступ

В сучасних умовах на озброєнні Збройних Сил України (далі – ЗС України) перебуває досить велика номенклатура матеріальних засобів. До їх складу входять технічні засоби, що обладнані інформаційними системами до складу яких входить радіоелектронна апаратура (далі – РЕА), що досить уразлива до зовнішніх електромагнітних впливів (далі – ЕМВ). Тому питання захисту цих об'єктів стає все більш актуальним.

**Постановка проблеми.** З досвіду російсько-української війни та проведення операції Об'єднаних сил [1] у ЗС України все частіше поширюється використання інформаційних технологій і, як функціональна їх складова, різного роду інформаційні системи, що розміщують як на стаціонарних, так і на технічних засобах. Крім того, через перехід на стандарти НАТО тенденція до збільшення кількості таких об'єктів поширюється. Слід зазначити, що до складу цих систем входить велика кількість РЕА, яка досить уразлива до сучасних видів перспективної зброї і заснована на використанні ЕМВ.

Тому вирішення питання щодо пошуку шляхів захисту інформаційних систем технічних засобів та їх впровадження є актуальною проблемою в сучасних умовах бойового використання ЗС України.

**Аналіз останніх досліджень і публікацій** свідчить, що проблемам захисту РЕА інформаційних систем від ЕМВ різного виду походження надається значна увага як в нашій країні, так і в світі. Це пов'язано, в першу чергу, з тим, що до систем управління, керування, спеціального, робочого обладнання та інформаційних систем сучасних зразків технічних засобів входить велика кількість РЕА і ця тенденція з часом поширюється з одного боку, а імовірність ураження цих агрегатів з боку противника, терористичних груп чи ЕМВ природнього походження збільшується з іншого боку [2; 3].

В роботах [4; 5] визначено фізичні механізми впливу потужного ЕМВ на елементну базу РЕА і запропоновано розробити комплексний метод створення захисту, який складається з двох складових, а саме захисту самого зразка технічних засобів та захисту об'єкту зберігання цих засобів від зовнішнього ЕМВ. Однак, в цих роботах, на думку авторів, не достатньо чітко були вибрані та обґрунтовані показники і критерії електромагнітної стійкості (далі – ЕМС) бо саме за цими параметрами формуються технічні вимоги до створення захисту РЕА інформаційних систем.

**Метою статті** є обґрунтування показників

електромагнітної стійкості радіоелектронної апаратури інформаційних систем до зовнішніх електромагнітних впливів.

## Виклад основного матеріалу дослідження

Рішення цього завдання пов'язане з необхідністю обґрунтувати узагальнений кількісний показник ЕМС радіоелектронної апаратури в межах якого РЕА спроможна виконувати свої функції і зберігати параметри в межах, встановлених у технічному завданні, під час і після ЕМВ із заданими параметрами. Відповідно цих вимог необхідно вибрати і обґрунтувати часткові показники.

На нашу думку, обрані часткові показники мають врахувати: параметри критичного навантаження РЕА і його математичні імовірнісні характеристики; екрануючі властивості РЕА; показники ЕМС радіоелектронної апаратури (максимальні значення енергії, напруги, струму, за яких з заданим рівнем ймовірності ще забезпечується робота РЕА у нормальному режимі) [6; 7].

З метою розроблення ефективного захисту РЕА логістичного забезпечення на ОЦЗ, пов'язаних з зовнішнім ЕМВ необхідно визначити показники і критерії, які характеризують об'єкти ураження (кіл електрообладнання і РЕА), джерело ЕМВ та механізм їх взаємодії.

До першої групи показників і критеріїв, що характеризують об'єкти ураження, а це саме структурні елементи РЕА, слід віднести наступні [7]:

а) режим роботи (ввімкнений стан; вимкнений стан);

б) характеристика приймальних пристроїв (ширина діаграми спрямованості приймальних пристроїв радіоелектронної апаратури; рівень бокових пелюсток засобів, які працюють в діапазоні довжин хвиль (радіолокаційні, навігаційні, зв'язку); коефіцієнт підсилення приймальних антен; робоча довжина хвилі приймальних пристроїв; ширина смуги пропускання приймальних пристроїв);

в) граничні рівні потужності (енергії), при яких наступає функціональне ураження елементів РЕА;

г) ступінь захищеності елементної бази (характеристика пристроїв екранування; характеристика захисних пристроїв);

д) монтаж кабелів та дротів живлення (функціонального зв'язку між електронними блоками (вузлами, тощо)), їх довжина та ступінь екранування тощо.

Для даної групи показників перш за все необхідно мати інформацію щодо граничних рівнів потужності (енергії) ураження РЕА, на яку передбачається ЕМВ.

Із всієї номенклатури елементів електронної техніки найбільш уразливими є чутливі елементи приймальних пристроїв (різноманітні детектори та змішувальні надвисокочастотні діоди, фотоприймачі), а також інші елементи сучасної мікроелектроніки (польові транзистори, інтегральні мікросхеми тощо). Стійкість елементів електронної техніки залежить як від конструктивно-технологічного виконання, так і від параметрів потужності джерела ЕМВ (друга група показників).

Під час розгляду питань, пов'язаних зі стійкістю РЕА до впливу магнітних полів, необхідно враховувати її антенні властивості, режими роботи, екранування, розміщення, особливості проходження сигналів, що впливають, тощо. На підставі цих даних можна оцінити оптимальні параметри випромінювання, які дадуть можливість вірогідно оцінити вплив на електронне обладнання та оцінити можливості протидії джерелам потужного ЕМВ.

До критеріїв і показників, які характеризують джерело потужного ЕМВ відносяться такі:

а) режим роботи (безперервне випромінювання; випромінювання серії (пачки) імпульсів; випромінювання поодинокого імпульсу);

б) форма імпульсу, що випромінюється (відео імпульс (електромагнітна зброя));

в) характеристики імпульсу, що випромінюється (тривалість імпульсу; тривалість фронтів відео імпульсу або тривалість зростання та спаду надвисокочастотного (далі – НВЧ) – імпульсу; полярність для відео імпульсу; довжина хвилі (діапазон довжин хвиль) випромінювання (для оптичного і НВЧ-випромінювання) або несуча частота (частота запобігання); потужність (енергія, інтенсивність) випромінювання;

г) характеристики системи випромінювання (форма та ширина діаграми спрямованості випромінювання (для радіодіапазону); розходження променю лазерного випромінювання, тощо).

До характеристик, які обумовлюють взаємозв'язок між джерелом потужного ЕМВ і приймального пристрою, на яке воно діє, відносяться такі:

а) взаємна орієнтація діаграм спрямованості джерела потужного випромінювання та приймального пристрою, на який здійснюється вплив;

б) відстань між джерелом і апаратурою, на яку воно діє. Відстань між джерелом випромінювання та об'єктом впливу можна поділити на зони А, Б, В, Г, Д (рис. 1);

в) збіг довжин величини хвилі випромінювання, що діє, і робочої довжини хвилі засобу, на який здійснюється вплив (в оптичному і мікрохвильовому діапазоні);

г) смуговий або поза смуговий вплив тощо.

Серед такої широкої групи вищезазначених характеристик необхідно визначити основні, що найбільш співпадають із досягненням кількісних величин, які відповідають меті щодо зниження уражальної дії зовнішнього ЕМВ на об'єкти ураження до рівня їх граничної ЕМС. Тобто мова йде про критерій ЕМС, який являє собою

відношення величин і умов, що за результатами випробувань дозволяють (з використанням розрахункових і експериментальних даних) з визначеним ступенем достовірності стверджувати, що імовірність збереження робочого стану кіл електрообладнання і РЕА від ЕМВ буде не менше допустимого значення.

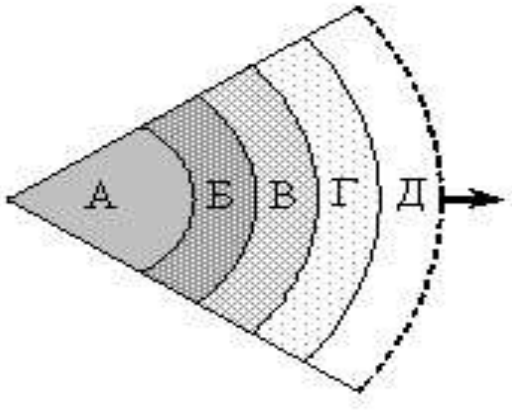



Рис. 1. Умовні зони дії потужного електромагнітного впливу на радіоелектронну апаратуру інформаційних систем:
А – досягнення функціонального ураження всієї радіоелектронної апаратури; Б –досягнення часткового функціонального ураження та тривалого функціонального подавлення; В – досягнення тривалого та короткочасного функціонального подавлення; Г – досягнення короткочасного або часткового функціонального подавлення; Д – безпечна [6].

ЕМС окремих кіл електрообладнання і РЕА інформаційних систем технічних засобів включає в себе поняття їх працездатності і безпеки. Працездатність – це спроможність кіл РЕА виконувати свої функції і зберігати параметри в межах заданих норм, а безпека – це властивість даної апаратури, що полягає у відсутності її спрацювання у випадку коли може трапитись поразка об'єкту. Тому якісними основними критеріями ЕМС радіоелектронної апаратури є такі:

а) збереження робочого стану РЕА інформаційних систем під час дії ЕМВ;

б) відсутність несанкціонованого спрацювання РЕА інформаційних систем від ЕМВ.

Кількісні критерії ЕМС окремих РЕА інформаційних систем можна використовувати співвідношення параметрів струмів і напружень, що наводяться в колах виробів, що оцінюються ( $x_i$ ) з допустимим значенням ( $x_{iД}$ ):

за збереженням працездатності $max x_i \le x_{iД} / u_p$, де $u_p$ – заданий квантіль рівня імовірності; по безпеці $max\, x_i \le 0{,}1 x_{iД}$.

Параметри $x_{iД}$ відповідають параметрам критичного навантаження. Слід зазначити, що будь-який ЕМВ являється для РЕА навантаженням, яке складається з діючого первинного навантаження (Z), і діючого вторинного навантаження (X), що виникає в даній апаратурі під дією первинного навантаження. З цієї точки зору нас цікавить вторинне навантаження, яке є реакцією РЕА інформаційних систем на зовнішній вплив (Z) і представляється за виразом:

$$x(t) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \dot{G}(\omega)\ \ \dot{K}(\omega) \cdot e^{\omega t} d\omega ,$$

де $\dot{G}(\omega)$ – спектральна функція зовнішнього впливуZ;

$\dot{K}(\omega)$ – комплексний коефіцієнт передачі РЕА.

Під час оцінювання ЕМС окремих РЕА інформаційних систем в загальному випадку величина вторинного навантаження $x(t)$ розглядається як випадкова величина, що розподіляється за нормальним законом. Під рівнем вторинного навантаження приймаємо значення його енергії в відповідному спектрі частот. Рівень вторинного навантаження, що викликає відказ РЕА інформаційних систем, називають критичним навантаженням ( $\gamma$ ).

## Висновки та перспективи подальших досліджень

Виходячи з цих міркувань, приймаємо узагальнений кількісний показник ЕМС радіоелектронної апаратури як ймовірність (Рст), що РЕА інформаційних систем спроможні виконувати свої функції і зберігати параметри в межах, встановлених у технічному завданні, під час і після ЕМВ із заданими параметрами. Як часткові кількісні критерії ЕМС радіоелектронної апаратури пропонується використовувати такі показники:

параметри критичного навантаження РЕА інформаційних систем;

математичне сподівання критичного навантаження $m_\gamma$;

його середньоквадратичне відхилення $\sigma_\gamma$;

коефіцієнт варіації відхилення $\sigma_\gamma$, що дорівнює $\sigma_\gamma / m_\gamma$;

коефіцієнт запасу стійкості $\eta = m_\gamma / m_X$, де замість математичного сподівання критичного $m_\gamma$ і діючого $m_X$ навантаження використовується їх середнє значення; екрануючі властивості РЕА інформаційних систем;

показники ЕМС кіл електрообладнання і РЕА (максимальні значення енергії, напруги, струму, за яких з заданим рівнем ймовірності ще забезпечується робота РЕА інформаційних систем у нормальному режимі) [8].

На основі визначених та обґрунтованих показників ЕМС, в подальшому проведемо обґрунтування вимог до створення захисту РЕА інформаційних систем технічних засобів, що лежать в основі запропонованого захисту.

## *Література*

**1. Середа Ю. О.** Створення пошарового захисту об'єкту зберігання технічних засобів логістичного забезпечення від зовнішнього електромагнітного впливу. *Проблеми управління та застосування сил і засобів логістичного забезпечення в операціях (бойових діях) за досвідом відбиття збройної агресії росії та проведення операції Об'єднаних сил (АТО)*: Тези доп. наук.-практ. сем. (Київ, 23 черв. 2022). Київ, 2022. С. 82. **2. Ковтуненко О. П., Богучарський В. В., Слюсар В. І., Федоров П. М.** Зброя на нетрадиційних принципах дії (стан, тенденції, принцип дії та захист від неї) : [монографія]. Полтава, 2006. 247 с. 3**. Кравченко В. И.** Оружие на нетрадиционных физических принципах. Электромагнитное оружие. Харків : [ХНМТ], 2009. 266 с. **4. Кравченко В. И.** Электромагнитное оружие : [монография]. Хаків : [ХПИ], 2008. 185 с. **5. Сівак В. А., Воробйов О. М., Середа Ю. О.** Порівняння енергетичних показників впливу сучасної електромагнітної зброї і критеріїв стійкості електрообладнання та радіоелектронної апаратури технічних засобів логістичного забезпечення. *Збірник наукових праць Національної академії державної прикордонної служби України імені Богдана Хмельницького*. 2021. № 1(84). С. 254–271. **6. Авчинников Є. А.** Науково технічні проблеми розробки електромагнітної зброї. *Системи озброєння і військова техніка*. 2008. № 2(14). С. 18–22. **7. Балюк Н. В., Кечиев Л. Н., Степанов П. В.** Мощный электромагнитный импульс: воздействие на электронные средства и методы защиты. Москва: ООО «Группа ИДТ». 2007. 478 с.

## SELECTION AND JUSTIFICATION OF INDICATORS OF ELECTROMAGNETIC RESISTANCE OF RADIO ELECTRONIC EQUIPMENT OF INFORMATION SYSTEMS TO EXTERNAL ELECTROMAGNETIC INFLUENCES

***Oleh Vorobiov** (Doctor of Technical Sciences, Professor)* [1]
***Volodymyr Tkachenk*** [1]
***Mykhailo Bambulyak*** [2]
***Serhiy Tygai** (Candidate of Military Sciences)* [2]

[1] ***National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine***
[2] ***Kamiyanets-Podilskyi National University named after Ivan Ohienko, Kamyanets-Podilskyi, Ukraine***

*The article is devoted to solving the problems of ensuring the protection of radio-electronic equipment of information systems of the technical means of the Armed Forces of Ukraine from external electromagnetic influences. The analysis of scientific works in this field was carried out and it was determined that the direction of creating protection will be the development of a complex method of creating protection, which consists of two components, namely the protection of radio-electronic equipment of information systems of technical means and the protection of the object of storage of these means from external electromagnetic influence. The article is devoted to solving the problems of ensuring the protection of radio-electronic equipment of information systems of the technical means of the Armed Forces of Ukraine from external electromagnetic influences. The analysis of scientific works in this field was carried out and it was determined that the direction of creating protection will be the development of a complex method of creating protection, which consists of two components, namely the protection of radio-electronic equipment of information systems of technical means and the protection of the object of storage of these means from external electromagnetic influence. In the future, it is proposed to justify the technical requirements for the creation of protection of radio-electronic equipment of information systems of technical means on the basis of determined and substantiated indicators of electromagnetic resistance.*

***Key words**: information systems; radio-electronic equipment; electromagnetic stability.*

## *References*

**1. Sereda. Y. A.** Creation of layer-by-layer protection of the object of storage of technical means of logistic support against external electromagnetic influence. Problems of management and application of forces and means of logistical support in operations (combat operations) based on the experience of repelling armed aggression of Russia and conducting the operation of the United Forces (ATO): Thesis of the addendum. science and practice family (Kyiv, June 23, 2022). Kyiv, 2022, 82. **2. Kovtunenko, O. P., Bogucharskyi, V. V., Slyusar, V. I., Fedorov, P. M.** Weapons based on non-traditional principles of action (status, trends, principle of action and protection against it): [monograph]. Poltava, 2006, 247. **3. Kravchenko, V. I.** Weapons based on unconventional physical principles. Electromagnetic weapons. Kh.: [KhNMT], 2009, 266. **4. Kravchenko, V. I.** Electromagnetic weapons: [monograph]. Kh.: [KhPI], 2008. 185. **5. Sivak, V. A.** Rowing of energy indicators in addition to the current electromagnetics and criteria for the efficiency of electrical control and radioelectronic equipment of technical problems in logical safety, Book of Science Works of the National Academy of State Bridging Service of Ukraine named after Bohdan Khmelnitsky, 2021, 1(84), 254–271. **6. Avchinnikov, Є. A.** Scientific and technical problems of the development of electromagnetics. Systems of health and safety and technology, 2008, 2(14), 18–22. **7. Balyuk, N. V., Kechiev, L. N., Stepanov, P. V.** Powerful electromagnetic impulse: impact on electronic means and methods of protection. Moscow: IDT Group LLC, 2007, 478.

DOI:**10.33099/2311-7249/2023-46-1-99-106**

УДК [378.147+355.233]:004.358

***Людмила Анатоліївна Заїка*** *(кандидат педагогічних наук, старший дослідник)*
***Олександр Васильович Лаврінчук*** *(кандидат технічних наук, старший науковий співробітник)*
***Сергій Васильович Лук'яненко***

***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# СУЧАСНИЙ СТАН І ПЕРСПЕКТИВИ РОЗВИТКУ ПІДГОТОВКИ ТА ПРОВЕДЕННЯ КОМАНДНО-ШТАБНИХ НАВЧАНЬ ІЗ ВИКОРИСТАННЯМ СИСТЕМ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ

*Досвід нинішньої російсько-української війни, розвиток нових форм і способів ведення бойових дій вимагає подальших змін у системі підготовки офіцерських кадрів усіх рівнів та ланок управління. Напрям розвитку такої підготовки непорушно ґрунтується на стандартах підготовки НАТО, впровадження яких, у Збройних Силах України, вже демонструє високоякісні результати на полі бою. Відповідно, поглиблення і розширення такої практики є підґрунтям майбутніх перемог. Акцентовано увагу на особливостях розвитку тенденцій переходу українського війська від методик проведення командно-штабних навчань із використанням комп'ютерів до методик комп'ютерних навчань (тренувань) (Computer Assisted Exercises) за стандартами НАТО. Ядро таких тренувань складають сучасні імітаційні системи і технології. Світовий досвід подібних практик дає змогу проаналізувати проблемні питання організації, і проведення комп'ютерних навчань (тренувань), порівняти можливості створення федерацій на різних рівнях управління з підтримки подібних тренувань (проведення багатоступеневих навчань) із власними спроможностями. Проаналізовано подібні федерації, що застосовуються у країнах НАТО під час багатонаціональних комп'ютерних навчань (тренувань). Отримані результати можуть бути використані для нарощування зусиль щодо розвитку підходів до організації і проведення практичних навчань (тренувань) із використанням систем імітаційного моделювання, а також технічної та технологічної бази підрозділів імітаційного моделювання як Збройних Сил, так й інших складових сил безпеки і оборони України.*

***Ключові слова****: Computer Assisted Exercises; системи імітаційного моделювання; конструктивне моделювання; JTLS; JCATS.*

## Вступ

Сучасні Збройні Сили виконують завдання в складних бойових умовах. Сьогодні військові підрозділи мають бути готовими ефективно діяти в умовах швидкої зміни обстановки, а командири – скорочувати час, потрібний для її оцінювання й прийняття ефективних управлінських рішень. У середовищі військових дій (навчань, тренувань) своєчасне забезпечення інформацією та надійне функціонування добре структурованих управлінських процесів на всіх рівнях і напрямах стають критичними факторами успішності виконання поставлених завдань. Світові технологічні досягнення у військовій сфері сприяють не лише вирішенню завдань повсякденної діяльності, але й суттєво впливають на стандарти підготовки військ (сил). Водночас традиційні підходи, як правило, важко модифікуються і є негнучкими з багатьох поглядів.

**Постановка проблеми.** Під час проведення командно-штабних навчань з використанням комп'ютерів у ході підготовки органів військового управління Збройних Сил України (далі – ЗС України) різних рівнів все більшого розповсюдження набуває використання сучасних систем імітаційного моделювання військового призначення. Вони вже набули широкого розповсюдження завдяки своїм технічним спроможностям з відтворення реалістичного середовища професійної військової діяльності на всіх рівнях. Підготовка і проведення таких навчань (тренувань) за стандартами НАТО із використанням імітаційних систем та мереж мають певні методичні, технічні й технологічні особливості.

**Метою статті** є проведення аналізу сучасних тенденцій підготовки і проведення комп'ютерних командно-штабних навчань та перспектив їх розвитку та надання рекомендацій для використання в інтересах ЗС України та інших складових сил безпеки і оборони України.

## Виклад основного матеріалу дослідження

Комп'ютерні командно-штабні навчання (тренування) (Computer Assisted Exercises) (далі – CAX) – із концепцією «*train as you fight*» проводяться в країнах НАТО під час колективної підготовки як для відпрацювання окремих тактичних завдань, так і штабних процедур на всіх трьох рівнях прийняття рішень та управління

(тактичному, оперативному і стратегічному). Використання імітаційного моделювання дає змогу військовим фахівцям покращувати свої знання та удосконалювати практичні навички через практику виконання функцій посадових осіб органів управління та командирів підрозділів під час моделювання бойових дій за різними сценаріями. При цьому CAX стали невід'ємною складовою практичної підготовки військових фахівців у країнах-учасницях НАТО.

Сьогодні процес організації CAX добре структурований та розвинений.

Розглянемо структуру CAX, що складається з двох основних компонентів: навчальної аудиторії (Training Audience) (далі – TA), первинної навчальної аудиторії (Primary Training Audience (PTA)) або вторинної навчальної аудиторії (Secondary Training Audience) (STA)) та групи керівництва навчанням (Exercise Control (далі – EXCON)). Кожне CAX створюється для певної ТА на підставі навчальних цілей (Training Objectives (TO)). Під час навчання (тренування) від початку його специфікації до аналізу проведених дій (After Action Review (далі – AAR)) вся увага концентрується саме на них. ТА в ході навчань може прибувати та розміщуватись в одному навчальному центрі (навчальному закладі) або різні частини ТА можуть бути розташовані в географічно віддалених місцях (у різних навчальних центрах, країнах, континентах тощо). Тренування, у яких компоненти ТА розташовані таким чином, називаються розподіленими (Distributed Exercises (DE)). Розподілене інтерактивне моделювання (Distributed Interactive Simulation (далі – DIS)) та розподілене тренування – це різні речі. Розподілене тренування може підтримуватися або централізованою системою моделювання, або розподіленою. Розташування клієнтських робочих станцій на віддалених сайтах ще не робить моделювання розподіленим – під час розподіленого моделювання об'єкти одного і того ж синтетичного імітаційного середовища моделюються у різних програмних модулях і на різних комп'ютерах та згодом взаємодіють один з одним [4].

Так, наприклад, під час проведення багатонаціонального розподіленого навчання «SABER GUARDIAN – 2016» за участю наших військових взаємодія між елементами навчання, що знаходились на території різних країн та населених пунктів, була організована за допомогою динамічного віртуального тунелю, серверу та повторювачів самого засобу імітаційного моделювання (рис. 1).

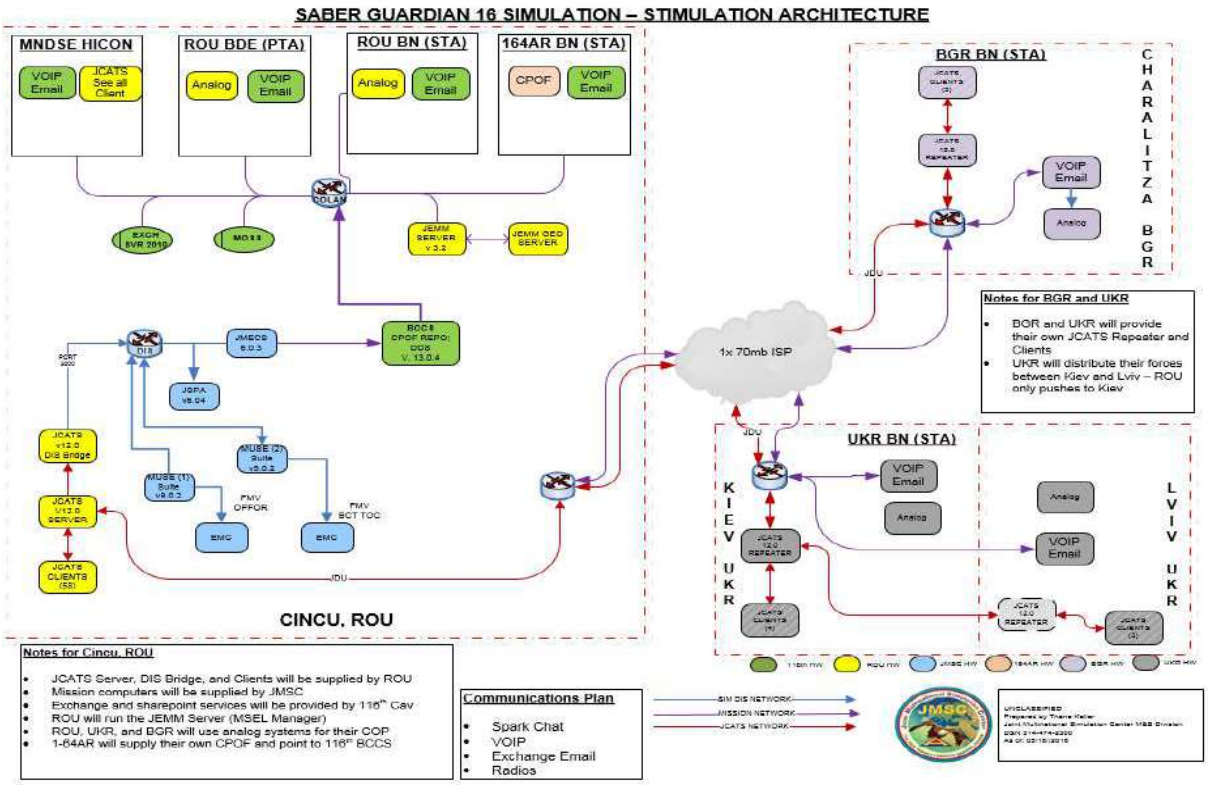



Рис. 1. Архітектура розподіленого багатонаціонального навчання «SABER GUARDIAN – 2016»

Другим компонентом CAX є EXCON (рис. 2) [5]. Тренувальна команда (Training Team (далі – TT)) складається з наставників, спостерігачів/тренерів (Observer/Trainers (O/T)), експертів з предметних питань (Subject Mater Experts (SME))та аналітиків. TT розташовується з ТА, спостерігає за ТА, інструктує, збирає дані для AAR та оцінювання ТА. До групи забезпечення навчань (Support) входять: групи забезпечення життєдіяльності (Real Life Support (RLS)) та безпеки (Security), громадський інформаційний центр (Public Information Center (PIC)), бюро по

роботі з відвідувачами (Visitor Officer bureau (VOB)) й інші. Група з організації зв'язку та інформаційних технологій (Information Technology/Communications and Information Systems (IT/CIS)) відповідає за організацію та належну роботу засобів імітації та зв'язку. Експериментальна група (Experimentation Team) проводить експерименти, що заплановані разом із тренуванням.

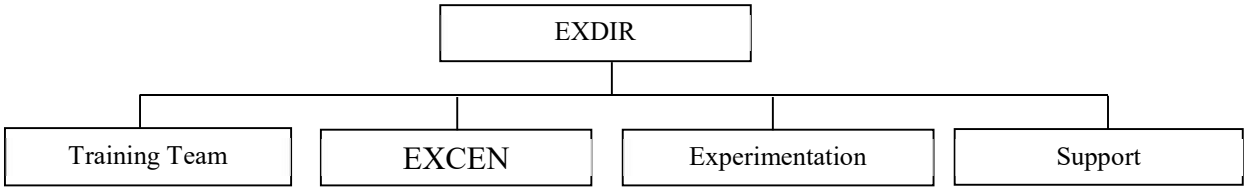



Рис. 2. Структура групи керівництва навчанням (EXCON)

Центр навчання (Exercise Center (далі – EXCEN)) (рис. 3) [5] відповідає за послідовний і узгоджений його хід у відповідності до визначених цілей. Функції EXCEN розділені між ситуаційним центром (SITCEN) та елементами групи імітації (Response Cells (далі – RC)): вищими підрозділами і штабами (Higher Control (далі – HICON)), підлеглими підрозділами і штабами (Lower Control (далі – LOCON)), ситуаційними силами (Situational Forces (далі – SITFOR)). Під час тренування RC відіграють роль HICON або LOCON, кількість яких визначається сценарієм і ТА. Головними цілями для такого тренування є підтримка процесу прийняття рішення та, у процесі його виконання, досягнення здатності ефективно прогнозувати подальші дії.

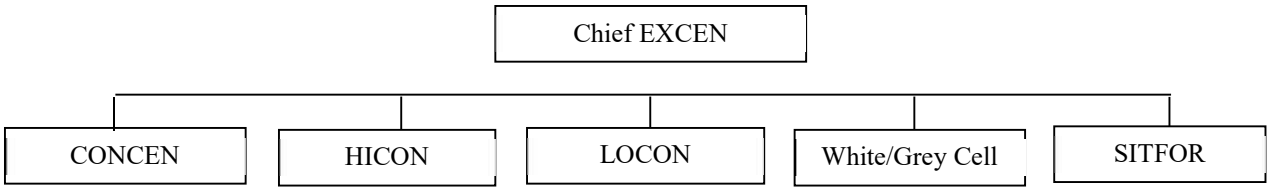



Рис. 3. Структура центру навчання (EXCEN)

У класичному випадку RC складаються з координатора сценарію (інцидентів) (Master Events List/Master Incidents List (далі – MEL/MIL)), офіцерів штабу відповідного рівня, оперативного чергового штабу (Battle Captain), який ознайомлений з можливостями системи імітаційного моделювання та декількох її операторів. Є два способи взаємодії між ТА та симуляцією, і обидва вони непрямі. Перший – через RC, що діють як LOCON для ТА. ТА віддає наказ, а рольові гравці RC як підпорядковані штабу підрозділу, отримують наказ. Потім планувальники в RC координують і планують виконання наказу, а після стандартних процедур системи управління Command and Control (далі – C2), передають плани дій операторам робочих станцій, що реалізують їх у відповідній системі моделювання. Отримані кількісні результати моделювання (звіти, обстановка) відповідно передаються і трансформуються (з дотриманням стандартних процедур та форматів) у дані й накази для ТА.

Другий спосіб – це автоматична взаємодія через C2. Системи імітаційного моделювання можуть бути пов'язаними з оперативними системами C2 ТА за допомогою посередницького програмного забезпечення. Наприклад, визначені повітряні місії (завдання для авіаційних підрозділів), виконані в системі C2, можуть бути доведені та подані до системи моделювання через засоби функціонального сервісу (Functional Area Services (далі – FAS)). Можливий і зворотний напрям.

Таким чином, подібна структура САХ є продуманою і чутливою до впливу результатів імітаційного моделювання, а тому і результативною під час підготовки особового складу. RC є основним компонентом, що безпосередньо працює з імітаційними засобами у САХ. Використання системи імітаційного моделювання дає змогу виконати наступні важливі завдання: обрахувати можливі наслідки та результати прийнятих ТА рішень; імітувати ситуації та умови, що не контролюються ТА або EXCON; підтримувати отримання послідовної достовірної інформації відповідно до можливостей розвідки та зусиль сторін; активувати систему C2, що використовується ТА. Незважаючи на застосування імітаційного моделювання для виконання перших двох завдань, можливе його використання і як методу навчання у повністю сценарних тренуваннях, де плани ТА не моделюються, а результати їх рішень під час вправи прогнозуються відповідно до ситуації, що розвивається. У так званих динамічних сценаріях (dynamic scripting) ТА виконують ввідні дані на основі досвіду та інтуїції EXCON, і ризик того, що вони непослідовні та нереалістичні, є високим. Внаслідок цього ТА може отримати так званий досвід «негативного навчання» (negative training). Зазначений метод і досі є усталеною практикою проведення командно-штабних навчань у ЗС України.

Виходячи з вищевикладеного, необхідно

зазначити, що верифіковані та валідовані засоби імітаційного моделювання з перевіреними базами даних й відповідними технічними можливостями є запорукою успішності навчання та значно зменшують ризик отримання негативного досвіду.

У своїй праці [5] професор Erdal Cayircі наводить ілюстративну, на нашу думку, таблицю щодо відомої класифікації реального, віртуального, конструктивного (далі – LVC) імітаційного моделювання військового призначення (табл. 1).

Таблиця 1

Класифікація імітаційного моделювання військового призначення

| Категорія | Люди | Системи |
|---|---|---|
| Реальне | Реальні | Реальні |
| Віртуальне | Реальні | Зімітовані |
| Конструктивне | Зімітовані | Зімітовані |

Моделі, отримані в результаті конструктивного моделювання, залежно від функціональних можливостей, розподіляють на такі категорії: Service Models – видові моделі, що розроблені на потребу окремого роду військ; Joint Models – відповідають вимогам всіх родів військ чи федерацій, що складаються з видових моделей; Expert Models – експертні моделі, що розробляються спеціально для імітації певних функцій, таких, як логістика, розвідка, радіоелектронна боротьба, внутрішня безпека чи космічні операції [5]. На сьогодні ми маємо змогу зупинитися лише на двох конструктивних об'єднаних (Joint Models) системах імітаційного моделювання (CIM): Joint Conflict and Tactical Simulation (далі – CIM «JCATS»), досвід використання якої нами нараховує вже майже два десятиліття, та Joint Theater Level Simulation (далі – CIM «JTLS»), впровадження якої наразі триває.

JCATS – це CIM високої роздільної здатності, із відповідними властивостями рельєфу та даними навколишнього середовища, з можливістю об'єднання модельованих одиниць в один агрегат (підрозділ) та управління ним на рівні взводу, роти чи батальйону. Деталізація даних рельєфу (Terrain) може проводитися до рівня планів окремих будівель, однак змодельована місцевість часто обмежується районом 200 км х 200 км. CIM «JCATS» зазвичай використовується у навчаннях і тренуваннях на тактичному рівні (до бригади включно), сьогодні являється єдиною широко розповсюдженою програмою конструктивного моделювання для колективної підготовки у ЗС України.

JTLS – це високоагрегована CIM, що найкраще підходить для моделювання дій оперативного рівня (оперативне командування, армійський корпус), повітряних місій, кораблів (фрегатів, підводних човнів тощо). Дані місцевості використовуються з нижчим рівнем деталізації, але можуть складати великі території, розміром до континентів. Дослідження румунських військових [6] засвідчують недостатню кількість центрів моделювання (підготовки) у Європі, оснащених CIM «JTLS» (Багатонаціональна дивізія Південь-Схід (MND-SE) Штаб-квартири НАТО, центр імітаційного моделювання НАТО у м. Ставангері, Норвегія, тощо). Особливий попит на симулятор подібного рівня виникає під час об'єднаних багатонаціональних навчань і тренувань на оперативному та стратегічному рівнях, кількість яких зростає щороку.

Сучасні тенденції розвитку підготовки військових фахівців шляхом проведення CAX все більше ґрунтуються на Концепції федерацій багатороздільної здатності (Multi-resolution federations concept) – одночасно швидкому та економічно ефективному способі організації середовища конструктивного моделювання з розширеними його можливостями. Федерації з різною роздільною здатністю – це федерації, що інтегрують високоагреговане моделювання та моделювання з високою роздільною здатністю в розподілену систему моделювання, як правило, за допомогою архітектур високого рівня (далі – HLA). Віртуальні та реальні системи моделювання також можуть стати елементами (федератами) у федераціях багатороздільної здатності. Дослідник Erdal Cayircі пропонує не відрізняти багатороздільні федерації від федерацій «Наживо, віртуально та конструктивно» (Live, Virtual, & Constructive (далі – LVC)). Така диференціація систем моделювання має місце, при цьому і LVC федерації та федерації багатороздільної здатності часто створюються окремо [5].

Започаткований Federation Object Model (далі – FOM) підхід у HLA ґрунтується на нових методах створення об'єктів FOM, що може містити як платформи реального часу Real-Time Platform Reference (далі – RPR), так й інші моделі, більш придатні для федерацій багатороздільної здатності. Сьогодні вже напрацьовані еталонні архітектури, що можна використовувати як для LVC, так і до подібних федерацій. Однак, більшість федерацій розроблено та реалізовано окремо від об'єднань LVC. Деякими прикладами таких реалізацій є Об'єднана федерація багатосторонніх резолюцій (Joint Multi Resolution Federation (JMRF)) та Модель з кількома роздільними здатностями (Multi Resolution Model (далі – JMRM)) у США, еталонна архітектура мережі моделювання програми «Партнерство заради миру» (P2SN) між країнами-партнерами НАТО, федерація KORA та SIRA (KOSI) у Німеччині, ALLIANCE у Франції, тощо. Федерації розвиваються та не завжди використовуються у великих тренуваннях. Так, тренувальна федерація НАТО (NTF) – це багатороздільна HLA федерація, що походить від JMRM, успішно використовується під час великих навчань НАТО з 2008 року. Початкова NTF мала дві моделі бойових дій, а саме CIM «JTLS» і CIM «JCATS» [7].

NTF є наочним прикладом використання властивості взаємосумісності засобів моделювання.

Так, під час САХ із ТА нижчою або відповідною рівню органу управління армійського корпусу, СІМ «JCATS» забезпечує кращу достовірність результатів моделювання. Але через високу роздільну здатність робота з ним потребує високої деталізації. Таким чином, використання виключно СІМ «JCATS» у тренуваннях, де задіяна значна кількість підрозділів у масштабному театрі дій, наприклад, корпусних навчаннях та вище, не є доцільною. Для такого рівня краще підходить СІМ «JTLS». Однак, часом сценарії навчань (тренувань) вимагають планування із використанням інструментарію високої роздільної здатності, що недоступне в СІМ «JTLS». Саме організація NTF дає змогу поєднати системи імітаційного моделювання «JTLS» і «JCATS». Під час таких двох симуляцій атрибути одиниць і підрозділів (угруповань) оновлюються одночасно в обох моделях, але деякі одиниці моделюються за допомогою СІМ «JCATS», а деякі підрозділи (угруповання) – за допомогою СІМ «JTLS». Одиниці в СІМ «JCATS» можуть взаємодіяти з підрозділами в СІМ «JTLS». Наприклад, літальний апарат у СІМ «JCATS» може запустити ракету для ураження корабля в СІМ «JTLS». Через це у [8] зазначається, що часом постає питання про вибір одиниць або підрозділів моделювання у тій чи іншій системі. Організація NTF дає можливість час від часу «перемикати право власності» між системами імітаційного моделювання «JTLS» і «JCATS» на змодельовані об'єкти, що позитивно впливає на способи реалізації сценарію та хід взаємодії між учасниками САХ. Дослідники виокремлюють кілька таких способів, які пропонується розглянути докладніше.

*Спільне використання одиниць і підрозділів на основі району місцевості.* Право моделювання дій у певній зоні може бути надане СІМ «JCATS», тоді як всі інші регіони будуть за СІМ «JTLS». Водночас СІМ «JCATS» також може відповідати за декілька районів місцевості та діяти в них.

*Спільне використання підрозділів і одиниць на основі компонентів*. Може бути проведений розподіл моделювання бойових дій, наприклад, повітряних, морських, наземних, спеціальних операцій тощо, за однією системою моделювання (симуляцією), тоді як інші підрозділи та одиниці (компоненти) моделюються іншою. Наприклад, все, що стосується компоненти спеціальних операцій, імітується у СІМ «JCATS», а всі інші – у СІМ «JTLS». У цьому випадку в одному районі місцевості можуть бути одиниці, змодельовані в СІМ «JCATS», і підрозділи (угруповання), змодельовані в СІМ «JTLS». Це збільшує ймовірність того, що одиниці у СІМ «JCATS» взаємодіятимуть із підрозділами в СІМ «JTLS».

*Спільне використання одиниць і підрозділів на основі національних сил*. Під час багатонаціональних тренувань одиниці та підрозділи однієї національної сили можуть моделюватися в одній системі моделювання, тоді як штаб-квартира альянсу та сили інших країн – в іншій.

*Спільне використання одиниць і підрозділів на основі родів військ*. Усі підрозділи певного роду військ моделюються в одній СІМ, а інших родів військ – в іншій. Наприклад, ми можемо використовувати одну з симуляцій для імітації дій морських сил і засобів, а іншу – для наземних і повітряних.

*Спільне використання одиниць і підрозділів на основі видів операцій*. Одні типи операцій (виконання завдань), наприклад, розмінування місцевості, глибинна розвідка, відновлення особового складу, переправа через річку, десантування, боротьба із заворушеннями, можуть бути змодельовані в СІМ «JCATS», а інші – в СІМ «JTLS».

Таким чином, стає очевидним, що незважаючи на відповідність вимогам тактичного рівня, моделювання із високою роздільною здатністю є корисним для тренувань вищого рівня. Під час тренувань стратегічного рівня, MEL/MIL може містити ввідні (інциденти), що вимагають імітації завдань високої роздільної здатності, наприклад, відновлення особового складу, розгортання водних переправ чи організації блок-постів. Проілюструємо особливості виконання подібного завдання, що відпрацьовувався на САХ оперативного рівня [5].

Командування об'єднаних сил (основна ТА) отримало розвідувальну інформацію про знаходження підрозділу противника в невеликому селищі, який залишиться там протягом кількох годин. ТА оцінює ситуацію та можливі варіанти дій. Один із них – віддати наказ про авіаудар. Оскільки ризик супутніх втрат є високим, такий варіант не було обрано. Інший – віддати наказ про снайперську атаку – оцінено як доцільний. Командування сил спеціальних операцій, що входить до складу основної ТА, отримує наказ спланувати та провести операцію. Їх план включає розгортання гелікоптерів для евакуації та безпосередньої підтримки з повітря у разі ескалації зіткнення та втрат. Командування передає накази своїм підлеглим через рольових гравців RC. Під час подальшого планування виявляється, що із запланованих позицій пряма видимість району інциденту відсутня і, відповідно, снайперська команда повинна переміститися на кращу позицію, що знаходиться майже за 2 км від позиції початкового плану, та останню частину шляху долати повзком. Розглянемо можливий хід тренування у випадках, якщо:

симуляція відсутня;

є лише високоагрегована симуляція (СІМ «JTLS»);

є лише моделювання високої роздільної здатності (СІМ «JCATS»);

є федерація багато роздільної здатності (NTF).

*Симуляція відсутня*. ТА (RC) виконує всі обчислення вручну та звітує Командуванню сил спеціальних операцій щодо:

наявності повітряних засобів, палива,

боєприпасів і персоналу для місії, засобів для безпосередньої підтримки з повітря та евакуації;

оцінки прямої видимості та відстані;

загроз (виявлення, ураження, ймовірності ураження та знищення);

часу, необхідного для розгортання дій у повітрі;

засобів управління для всіх переміщень, можливостей із зв'язку;

часу, необхідного для подолання додаткових останніх 2 км;

загрози (виявлення, ведення бою, ймовірність попадання та знищення у разі бойових дій) та їхній вплив протягом подолання цих 2 км;

ідентифікації цілі;

залучення особового складу та техніки, ймовірність ураження чи знищення, побічні втрати.

Необхідно також запланувати усе вищезазначене на зворотній шлях (повернення до району базування). Забезпечення прямих відеострімів з безпілотних літальних апаратів (далі – БпЛА) є неможливим.

*Високоагрегована симуляція (CIM «JTLS»).* RC виконує всі наведені нижче дії вручну, оскільки високоагреговані симуляції не мають необхідної роздільної здатності для їх точного моделювання:

оцінки прямої видимості та відстані;

часу, необхідного для подолання додаткових останніх 2 км;

загроз (виявлення, ураження, ймовірності ураження та знищення), у тому числі протягом останніх 2 км;

ідентифікації цілі;

залучення особового складу та техніки, ймовірності ураження чи знищення, побічних втрат.

Забезпечення прямих відеострімів з БпЛА є неможливим.

*Моделювання високої роздільної здатності (CIM «JCATS»).* Симуляції з високою роздільною здатністю можуть моделювати точно та з необхідним рівнем деталізації все, що перераховано вище. Однак підготовка бази даних і робота з моделлю може стати занадто громіздкою через загальний високий рівень тренування. Крім того, система конструктивного моделювання з високою роздільною здатністю може не мати засобів візуалізації для позитивної ідентифікації та відеострімів з БпЛА.

*Федерація багатороздільної здатності (NTF).* Таке поєднання є доцільним. Щоразу, коли потрібна більша деталізація дій – виконання передається до моделювання із високою роздільною здатністю. Дані БпЛА (відеострими з БпЛА) можуть надаватися через систему імітаційного моделювання, наприклад, Virtual Battle Space (далі – VBS). ТА отримує результати розвідки щодо бойового зіткнення. Подібна федерація забезпечує взаємодію та повторюваність.

Разом із тим, використання федерацій з багатороздільною здатністю є корисними під час тренувань на тактичному рівні, коли їх сценарії передбачають транспортування на далекі відстані, масштабні логістичні процедури тощо.

Таким чином, дослідивши досвід практики організації та використання федерацій багатороздільної здатності в ході практичних навчань (тренувань), можна зробити наступні висновки:

1. Зазначене середовище моделювання дає змогу більш реалістично моделювати ввідні (інциденти) та різні ситуації сценарію із використанням систем високої роздільної здатності під час навчань (тренувань) оперативного та стратегічного рівня.

2. Суттєво розширюються можливості зі взаємодії та повторюваності симуляції через усталені й найсучасніші CIM шляхом використання федерацій, що значно зменшує залежність від специфіки окремо взятого засобу, робить тренування більш універсальним.

3. Підвищується здатність багаторівневості тренувального середовища, особливо під час об'єднаних операцій для підтримання навчання декількох рівнів навчальної аудиторії, що мають різні навчальні цілі.

4. Розширюється інформаційна підтримка системи С2: можливість отримання результатів моделювання із використанням засобів багатороздільної здатності може надавати високоагреговану звітну інформацію і більш деталізовані її результати.

5. З'являється можливість з віртуалізації і візуалізації оперативних дій та процесів. CIM, наприклад, VBS-3, можуть візуалізувати процес та надавати такі дані розвідки, як аерофотознімки, відеострими з БпЛА тощо.

Разом із тим, основна концепція CAX «*train as you fight*» передбачає не тільки імітаційний супровід процесів прийняття рішень та управління силами і засобами, а й потребує отримання навичок із використання інших систем та ресурсів ланки С2. В країнах НАТО стандартні програми, відомі як FAS, вже складають оснащення кожної військової частини, а їх важливість для життєдіяльності підрозділів зумовлена доступом (на своєму рівні) до загальних баз даних. Більшість із таких програм можуть експортувати свої бази даних у MISSION SECRET мережу під час запуску та функціонування NATO SECRET мережі. Подібна комутація в реальних місіях (завданнях) важлива з причини необхідності захисту даних, при цьому для CAX рівень секретності зазвичай є NATO UNCLASSIFIED і всі дані вправ часто не є реальними.

Системи FAS є зазвичай інтероперабельними. Наприклад, Система функціональних зон логістики (Logistics Functional Area System (далі – LOGFAS)), що активно впроваджується у ЗС України, Інтелектуальна функціональна система (Intelligence Functional System (INTEL-FS)), Інструмент для оперативного планування, активації сил та моделювання (Tool for Operational Planning, Force Activation and Simulation (TOPFAS)) чи Об'єднана система наведення (Joint Targeting System (JTS)). За

рахунок додаткового допоміжного модуля управління спільними навчаннями» (Joint Exercise Management Module (JEMM)) ТА отримує ввідні (події та інциденти), що відбуваються під час тренувань. Результатом загальної роботи таких систем є створення оперативної картини у Службі загальної оперативної картини НАТО (NATO Common Operational Picture (NCOP)). Розподілені права доступу до баз даних, хоча і тренувальних, отримання навичок роботи з ними є важливою складовою будь-яких САХ. Таким чином, ТА, що використовує результати конструктивного моделювання під час тренування, не працюючи на його засобах, а лише отримуючи звітну інформацію, напряму працює з сервісами функціональної області FAS. Їх метою є надання якнайбільше інформації для забезпечення роботи органу управління у процесі прийняття рішень та управління підпорядкованими силами і засобами. Для цього необхідні синхронізація бази даних моделювання та FAS, функціональна сумісність і пов'язаність між всіма сервісами для створення загальної оперативної картини.

Аналіз практики застосування подібних мереж засвідчує наявність ряду технічних питань передачі даних. Так, польські науковці досліджували причини помилок під час безперервної передачі даних з бази даних CIM «JTLS» до LOGFAS протягом кількох днів САХ, проблематичність поєднання CIM «JTLS» та CIM «JCATS» [9]. На сьогодні інтеграція різних систем моделювання у об'єднану симуляцію HLA під час підготовки тренувань та експериментів ще вимагає значних зусиль з точки зору часу та персоналу.

## Висновки й перспективи подальших досліджень

Для покриття потреб війська, зберігаючи філософію «*train as you fight*», військові фахівці провідних країн світу все більше звертаються до сучасних технологій для забезпечення безперервних віртуальних середовищ навчання. Останні розробки використовують сучасні методики і технічні можливості для об'єднання віртуального та фізичного світу з метою покращити навчальну реальність у безпечному, доступному середовищі.

За результатами проведеного аналізу можна зробити такі висновки:

1. Системи імітаційного моделювання дають змогу створювати складний віртуальний світ, що імітує реальну картину бойових дій у ході реалізації сценарію САХ під час процесу прийняття рішення та управління визначеними силами і засобами, аналізу його результатів, ефективного прогнозування дій. Наявність RC (на рівнях HICON чи LOCON) та їх здатність реалізовувати різноманітні сценарії в імітаційному середовищі є основною перевагою та особливістю такого виду військових навчань. Розглянута структура САХ дає змогу результативно підтримувати всі його етапи і досягати цілей навчання (тренування).

2. Розподілене навчання (тренування) визначає інфраструктуру для пов'язування моделей різних типів у різних місцях для створення реалістичних і складних віртуальних світів з метою моделювання високоінтерактивних заходів. Ця інфраструктура об'єднує системи, побудовані для окремих цілей, технології, продукти від різних постачальників і платформ від різних служб і дозволяє їм взаємодіяти.

Під час сучасних САХ, які проводяться НАТО, існують дві основні мережі. Перша – мережа моделювання, що може бути організована DIS через основний сервер з ретранслятором та клієнтськими серверами, розташованими у різних країнах (частинах світу). Друга – операційна мережа, що підтримує FAS сумісність. DIS відіграє важливу роль у САХ, які визначають інфраструктуру мережі моделювання.

3. Програми конструктивного моделювання і служби FAS НАТО довели свою ефективність завдяки підвищенню швидкості реакції користувачів системи та сприяють можливості розподілу професійних функцій у ході виконання завдань під час проведення САХ.

Зазначені результати засвідчують потребу трансформаційних зрушень і змін у підготовці та проведенні командно-штабних навчань (тренувань), відпрацюванні завдань професійної військової підготовки. Результати проведеного аналізу можуть бути корисними для подальшого спрямування зусиль щодо розвитку технічної та технологічної бази підрозділів імітаційного моделювання як Збройних Сил, так і інших складових сил безпеки і оборони України, ревізії існуючого методичного підґрунтя підготовки та проведення командно-штабних навчань з використанням комп'ютерів, створення мережевих федерацій різних рівнів під час участі у міжнародних САХ.

## *Література*

**1. Cayirci E., Marincic D.**. Computer Assisted Exercises and Training: A Reference Guide. USA : Wiley & Sons, 2009. 312 p. **2. Cayirci E.** (2007). Exercise Structure for Distributed Multi-resolution NATO Computer Assisted Exercises. ITEC'2007, May. **3. NATO.** Bi-SC 75–3 Collective Training and Exercise Directive, 2013. **4**. Engineering Principles of Combat Modeling and Distributed Simulation. (2012). https://doi.org/10.1002/9781118180310. **5. Cayirci E.** (2007). Multi-Resolution Exercise Control Structure for NATO Education and Training Network, MN-MSG-056-12. **6. Bârsan G., Zinca (Neagoe) D-I.** (2018) Constructive Simulation Programs And Nato Functional Area Services Applied In Computer Assisted Exercises Land Forces Academy Review Vol. XXIII, No 2(90), p.160-166. **7. Cayirci E., Ersoy C.** (2002). Simulation of Tactical Communications Systems by Inferring Detailed Data from the Joint Theater Level Computer Aided Exercises. SCS Simulation Journal, 78: 475-484. **8. Cayirci E.** Distributed Multi-resolution Computer Assisted Exercises. *NATO Modelling and Simulation Conference, October 2007,* p. 1787–1797. URL: https://www.researchgate.net/

publication/224123704_Multi-resolution_federations_in_support_of_operational_and_higher_level_combinedjoint_computer_assisted_exercises (дата звернення: 15.12.2022). **9**. **Kozioł M.** (2020). Interoperability and data flow between JTLS-GO simulation system and LOGFAS logistic system during CAX (Computer Assisted Exercise) exercises. Economics and Organization of Logistics 5 (1), p.65–78.

## CURRENT STATUS AND DEVELOPMENT PROSPECTS OF PLANNING AND CONDUCTING COMMAND POST EXERCISES USING SIMULATION SYSTEMS

***Liudmyla Zaika*** *(candidate of pedagogical sciences, senior researcher)*
***Oleksandr Lavrinchuk*** *(candidate of technical sciences, senior researcher)*
***Serhii Lukianenko***

***National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine***

*The article discusses the issue of the implementation of NATO standards in the system of professional training of officers of all levels of management. Today, in the Armed Forces of Ukraine, there is a steady trend of the transition of the Ukrainian army from the methods of conducting command and staff exercises with the use of computers to the methods of Computer Assisted Exercises (CAX). Professional training based on NATO standards is already showing excellent results on the battlefield. The authors emphasize that modern simulation systems and technologies are the core of such training. The purpose of the study is to conduct a partial analysis of the foreign experience of similar practices of conducting CAX, their structural and methodological features with the use of constructive simulation. The technical and technological issues of the organization of distributed training and simulation, federations of different resolutions are covered. Special attention is paid to the simulation systems JCATS and JTLS, the organization of the structural modeling environment with its extended capabilities using high-level architecture (HLA). Ways of using the property of interoperability of simulation systems in NATO training federations (NTF) are considered, and an example of the implementation of the scenario during the CAX, the use of other systems and resources of the command and control chain is given. The result of the analysis attests to the transformational shifts needed today in the development and conduct of command and staff training, working out the tasks of professional training. The highlighted observations can be useful for the timely direction of efforts to develop the technical and technological base of simulation modeling centers, the revision of the existing methodological basis for the preparation (conducting) of command and staff exercises using computers, the creation of network federations of various levels during participation in international CAXs. Further research could be focused on the timely direction of efforts to develop the technical and technological base of simulation centers in the interests of both the National Defense University of Ukraine and the Armed Forces of Ukraine.*

***Key words:*** *CAX, simulation systems, constructive simulation, JCATS, JTLS.*

## *References*

**1. Cayirci, E., Marincic, D.** (2009). Computer Assisted Exercises and Training: A Reference Guide. Wiley & Sons. **2. Cayirci, E.** (2007). Exercise Structure for Distributed Multi-resolution NATO Computer Assisted Exercises. ITEC'2007. May. **3. NATO.** Bi-SC 75–3 Collective Training and Exercise Directive, 2013. **4. Engineering** Principles of Combat Modeling and Distributed Simulation. (2012). https://doi.org/10.1002/9781118180310. **5. Cayirci, E.** (2007). Multi-Resolution Exercise Control Structure for NATO Education and Training Network, MN-MSG-056-12. **6. Bârsan, G., Zinca, (Neagoe) D-I.** (2018) Constructive Simulation Programs And Nato Functional Area Services Applied In Computer Assisted Exercises Land Forces Academy Review Vol. XXIII, 2(90), 160-166. **7. Cayirci, E., Ersoy, C.** (2002). Simulation of Tactical Communications Systems by Inferring Detailed Data from the Joint Theater Level Computer Aided Exercises. SCS Simulation Journal, 78: 475-484. **8. Cayirci, E.** (2007). Distributed Multi-resolution Computer Assisted Exercises. NATO Modelling and Simulation Conference, October, 1787–1797. URL: https://www.researchgate.net/publication/224123704_Multi-resolution_federations_in_support_of_operational_and_higher_level_combinedjoint_computer_assisted_exercises. **9. Kozioł, M.** (2020). Interoperability and data flow between JTLS-GO simulation system and LOGFAS logistic system during CAX (Computer Assisted Exercise) exercises. Economics and Organization of Logistics 5 (1), 65–78.

DOI:**10.33099/2311-7249/2023-46-1-107-114**

УДК 519.6

***Олександр Олександрович Шапран***
***Євгеній Петрович Махно***

***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# АНАЛІЗ ПРОЦЕСІВ ІНТЕЛЕКТУАЛІЗАЦІЇ СИСТЕМИ ДИСТАНЦІЙНОГО НАВЧАННЯ У ЗБРОЙНИХ СИЛАХ УКРАЇНИ

*Упровадження технологій штучного інтелекту в освітню сферу спонукало започаткуванню нових напрямів інтелектуалізації в освітньому процесі. Застосування штучного інтелекту відкриває нові перспективи в освіті. Водночас завдяки своїм перевагам і актуальності, на перший план вийшло дистанційне навчання. Але поява можливості розвитку нових напрямів інтелектуалізації в сфері освіти залишає відкритими питання про їх першочерговість. Досить часто можливість отримання фінансових вигід на розробленні та впровадженні продукту програмного забезпечення переважає цінність його призначення та користь від його застосування. Як зрозуміти які саме напрями та задачі в освітній сфері є найактуальнішими? Отже, це дослідження бере за мету провести дослідження для знаходження найактуальніших напрямків і задач освітнього процесу дистанційного навчання, що потребують першочергової інтелектуалізації. Висвітлити перспективи подальшого розвитку системи дистанційного навчання. А також, підкреслити важливість і необхідність продовження існуючих та провадження нових досліджень штучного інтелекту в освіті.*

***Ключові слова:*** *штучний інтелект; інтелектуалізація; адміністрування; система дистанційного навчання.*

## Вступ

З розширенням і доступністю інформаційних технологій штучний інтелект (далі – АІ) стає дедалі важливішим для програмно-технічної підтримки інноваційного та ефективного навчання. АІ може забезпечити покращення якості навчання та досліджень, допомагаючи слухачам і викладачам отримувати швидкі, бажані результати та необхідні компетентності, а також забезпечувати індивідуальні потреби кожного, хто навчається. Нові можливості в освітній сфері, пов’язані зі штучним інтелектом, вражають свідомість. Технології, що здатні імітувати людський інтелект, дозволяють робити висновки, певні прогнози, генерувати судження, надавати слухачам персональні поради, підтримку, забезпечувати зворотний зв'язок, надавати допомогу викладачам у прийнятті рішень [13]. Завдяки роботі алгоритмів АІ з’явилася можливість автоматичного прийняття рішень. Таким чином, відбувається повна трансформація філософії і вигляду освіти, при цьому змінюються способи навчання та викладання.

Особлива увага приділяється аналізу впливу штучного інтелекту на результативність та якість навчання, а також на перспективи майбутнього розвитку освітньої галузі в умовах швидкої технологічної еволюції [1].

Впровадження АІ в освітній процес у формі дистанційного навчання стало поштовхом до зародження та розвитку інноваційних освітніх напрямів. Значно розширилися можливості щодо автоматизації та інтелектуалізації освітніх процесів. Навчання стає більш персоналізованим і адаптивним. З першого погляду все відбувається закономірно, гармонійно та лаконічно. Але повстає питання пріоритетності розвитку й інтелектуалізації напрямів. виходячи з цього виникає необхідність проведення дослідження для визначення найактуальніших напрямків інтелектуалізації освітнього процесу дистанційного навчання.

**Постановка проблеми.** Наразі вже активно застосовуються численні напрями впровадження штучного інтелекту в дистанційне навчання та в сферу освіти в цілому. Нові розробки, що стосуються АІ, постійно тестуються, аналізуються, трансформуються та вдосконалюються. Проте дистанційне навчання передбачає набагато ширший спектр напрямів інтелектуалізації порівняно з діючими у навчальному процесі. Окремої уваги заслуговують процеси адміністрування системи дистанційного навчання. Також, іноді, вибір напрямів інтелектуалізації не є системним явищем. Зокрема, зусилля спрямовуються на другорядні, сумнівні, суперечливі напрями. Періодично порушується зв'язок між розробниками програмних продуктів і кінцевими користувачами (викладачами, слухачами). Таким чином, спостерігається відсутність системності у пошуці та визначенні актуальних напрямів інтелектуалізації освітніх процесів у дистанційному навчанні.

**Аналіз останніх досліджень і публікацій.** Впровадження новітніх інформаційних технологій в освітню сферу забезпечило нові прояви та

можливості у системах дистанційного навчання. Завдяки застосуванню AI в освіті (далі – AIEd) з'явилися інструменти для проєктування викладання й навчання. Оцінюючи переваги застосування технологій AI в освіті можна зазначити, що нові напрями інтелектуалізації надають нові можливості та перспективи покращення якості освітнього процесу.

Наразі науковцями-освітянами напрацьовано низку нових освітніх напрямів для застосування у системах дистанційного навчання з багатообіцяючими прогнозами завдяки інноваційним технологіям AI [14]. Серед них такі освітні напрями як: формування навичок саморегулювання навчання (Fan та ін., 2021) [2]; надання підтримки в режимі реального часу (Лукас та ін. , 2021, Мартінес-Мальдонадо та ін., 2021) [2]; інформаційні технології для запису мікроповедінкових даних, слухачів, під час виконання навчальної діяльності на цифровій навчальній платформі Хван, Спікол та Лі (2018), (Cantabella, Martínez-España, Ayuso, Yáñez, & Muñoz, 2019), Chen and Wang (2020) [3]; додатків AIEd для різних цілей, таких як профілювання учнів, прогнозування успішності, оцінювання, персоналізація, адаптивне навчання (Zawacki-Richter та ін., 2019); Roschelle, Lester, & Fusco, 2020) [3]; автоматичний підрахунок балів і формальне оцінювання (Zhu, Liu, & Lee, 2020) [4]; системи для повторення матеріалу у процесі навчання (Lee et al., 2019) [4]; розумне репетиторство (Zawacki-Richter, Marin, Bond, & Gouverneur, 2019) [4]; інтелектуальні системи зворотного зв'язку (Cutumisu, Chin, & Schwartz, 2019) [4]; голосовий інтерактивний багатомовний чат-бот, здатний реагувати на настрій, тон і мову учнів Ralston et al. (2019) [5]; класи з віртуальною реальністю (Arici та ін., 2019; Radianti та ін., 2020) [6]; персоналізовані освітні налаштування (Moreno-Guerrero та ін., 2020; Мусавінасаб та ін., 2018; Smutny & Schreiberova, 2020); (Bhutoria, 2022; Hwang, 2014; Kabudi та ін., 2021) [6]; інтелектуальні системи навчання (Holmes, Bialik, & Fadel, 2019); (Conati, Barral, Putnam, & Rieger, 2021; Mousavinasab et al., 2021), Pai et al. (2020); (Serban et al. (2020) [7]; платформи гейміфікації (Zou, Huang, & Xie, 2019); (Дермевал та ін., 2019) [7]; адаптивні системи навчання (Kabudi, Pappas, & Olsen, 2021; Tang, Chang, & Hwang), (Pliakos та ін., 2019; Xie та ін., 2019); (Cavalcanti et al., 2021; Вукович та ін., 2021) [8]; саморегульоване навчання (SRL) (Brezovszky та ін., 2019; McLaren та ін., 2022; Ruipérez-Valiente & Kim, 2020) [9]; мультимедійні та онлайн-платформи з відстеженням навчальної поведінки (Pishtari, G. et al., 2020; Xia, X ., 2020a) [10]; автоматизовані рішення зворотного зв'язку між викладачем та студентом (Keuning та ін., 2018; Лю та ін., 2017; Ма та ін., 2017); Villal'on та ін., 2008; Wijewickrema та ін., 2018) [11]; технології штучного інтелекту, для забезпечення персоналізованого навчання (Daghestani, Ibrahim, Al-Towirgi, & Salman, 2020) [12].

**Мета статті.** З огляду на значну кількість нових напрямів розвитку застосування штучного інтелекту в освітніх процесах дистанційного навчання метою статті є проведення дослідження для знаходження найактуальніших напрямків і завдань освітнього процесу дистанційного навчання, які потребують першочергової інтелектуалізації.

## Виклад основного матеріалу дослідження

Досягнення поставленої мети потребує проведення аналізу для визначення актуальних напрямів і завдань освітнього процесу у формі дистанційного навчання, що потребують першочергової інтелектуалізації. У зв'язку з цим проведено науково-дослідну роботу «Удосконалення системи дистанційного навчання Збройних Сил України: цифровізація та інтелектуалізація». У процесі дослідження взяли участь наукові та науково-педагогічні працівники (далі – НПП) вищих військових навчальних закладів України загальною кількістю 249 осіб.

У межах дослідження було проведено анонімне опитування, що складалося з трьох блоків. Щодо досвіду використання технологій дистанційного навчання – 47,1% опитаних мають досвід використання до 3 років; 33,3% респондентів – від 3 до 5 років досвіду; 8,4% – 5 – 10 років; 4,8% – більше 10 років та 6,4% опитаних не використовують такі технології зовсім.

У другому блоці питань проведено опитування НПП вищих військових навчальних закладів з метою подальшого аналізу їхнього ставлення до інтелектуалізації дистанційного навчання, що являє собою розроблення, впровадження та використання у відповідних програмних продуктах (наприклад, Moodle) алгоритмів штучного інтелекту для автоматизованого вирішення складних завдань освітнього процесу в умовах невизначеності.

Блок містить три уточнюючих питання для деталізації аналізу:

1. «На Вашу думку, чи можна покращити якість освітнього процесу, запроваджуючи технології штучного інтелекту (інтелектуалізації) у дистанційному навчанні?»

Цим питанням з'ясовувалося саме відношення до впровадження технологій штучного інтелекту в освітні процеси дистанційного навчання. Запропоновано два варіанти відповіді: «Так», «Ні» (рис. 1).

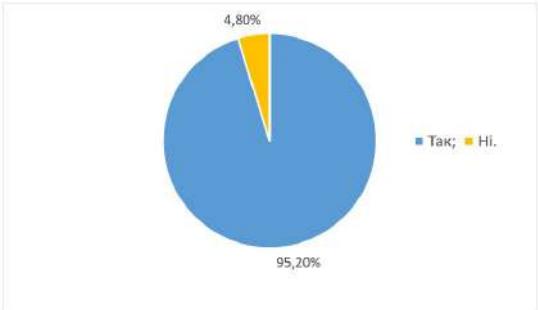



Рис. 1. Ставлення НПП до покращення освітнього процесу за допомогою технологій штучного інтелекту

У результаті 95,2% відповідей були позитивними, 4,8% – негативними.

Наступним було питання з множинним вибором:

2. «Визначте до 5 переваг інтелектуалізації дистанційного навчання». Запропоновано 14 найрозповсюдженіших варіантів відповідей (рис. 2).

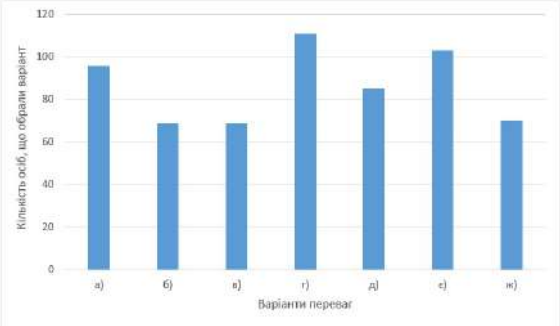



Рис. 2. Переваги інтелектуалізації дистанційного навчання

Найчастіше обиралися варіанти, що стосуються персоналізації освітнього процесу:

а) зростання персоналізованої направленості в освіті;

б) виявлення та відслідковування перешкод і проблемних ситуацій для слухачів (курсантів, студентів) в процесі навчання;

в) впровадження поточної адаптивності в освітній процес на основі аналізу поведінки слухача (курсанта, студента);

г) відслідковування індивідуальних навчальних потреб та надання необхідних рекомендацій;

д) адаптація освітньої траєкторії шляхом врахування індивідуальних особливостей, особистої направленості (уподобань, хобі) слухачів (курсантів, студентів);

є) підвищення об'єктивності оцінювання знань;

ж) створення позитивного емоційного стану слухачів (курсантів, студентів) в освітньому процесі, враховуючи індивідуальні вподобання.

Також поширеними були варіанти, що стосувалися скорочення, або прогнозування часу (рис. 3):

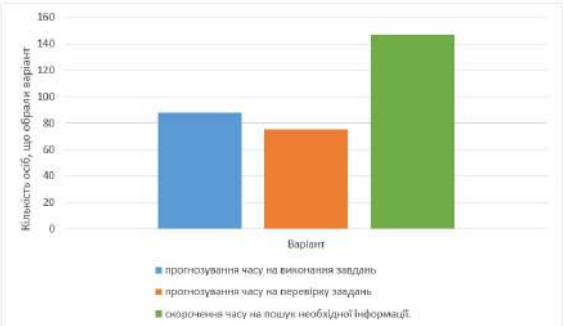



Рис. 3. Скорочення та прогнозування часу

а) прогнозування часу на виконання завдань;

б) прогнозування часу на перевірку завдань;

в) скорочення часу на пошук необхідної інформації.

А також – варіанти щодо об'єктивності оцінювання знань (рис. 4):

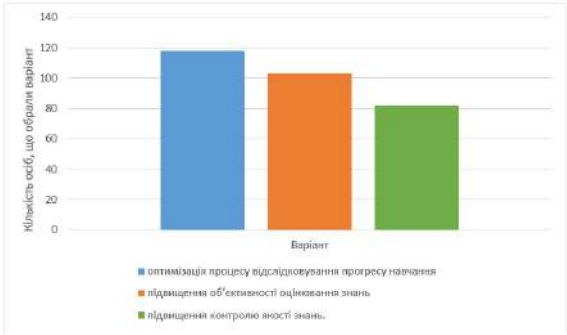



Рис. 4. Об'єктивність оцінювання знань

а) оптимізація процесу відслідковування прогресу навчання;

б) підвищення об'єктивності оцінювання знань;

в) підвищення контролю якості знань.

Прикінцевим питанням пропонувалося подати завдання, що потребують вирішення з допомогою технологій штучного інтелекту:

3. «Запропонуйте, які завдання, на Вашу думку, потрібно вирішити запроваджуючи технології штучного інтелекту (інтелектуалізації) у дистанційному навчанні з метою покращення якості освітнього процесу». Для прикладу було запропоновано три варіанти завдань:

прогноз необхідного часу на виконання будь-якого завдання для окремого слухача (індивідуально) залежно від різних факторів (складності завдання, терміновості виконання, рівня підготовки слухача тощо);

формування інформаційного поля спілкування між слухачами групи (питання до колег за темою, співбесіди тощо);

формування індивідуального навчального плану дистанційного курсу для окремого слухача з урахуванням особистих компетентностей, якості та швидкості виконання поточних завдань слухачем тощо.

Отримані результати запропонованих завдань були проаналізовані, узагальнені та розподілені на групи за напрямами застосування.

Завдання AI в освітньому процесі:

*1. Форуми*

Формування інформаційного поля спілкування між слухачами групи (університету) (питання до колег за темою, співбесіди тощо) визначення рівня відповідності тематичній групі спілкування залежно від: рівня успішності на однакових з іншими студентами курсах, рівня однакових компетентностей на різних курсах, кількості збігів у тематичних Інтернет-пошукових запитах.

вхідні змінні: спільні курси, модулі, дисципліни, компетентності, пошукові запити браузера, активність у соціальних мережах тощо;

вихідні параметри: необхідний рівень певного вхідного параметру для об'єднання тих, хто має цей рівень у групи спілкування. Формування рекомендацій щодо входження до певних груп.

Формування інформаційного поля спілкування

між слухачами і викладачами (рекомендації та організація комунікації з фахівцями предметної галузі, які нададуть якісну допомогу в опануванні певного матеріалу курсу (дисципліни), враховуючи навчальне навантаження викладачів).

Визначення ступеня рекомендації щодо можливої консультативної допомоги фахівцем предметної галузі з проблемних питань студента залежно від: рівня успішності на курсі (модулі), рівня компетентностей слухача на курсі(ах), кількості й форми проведених занять викладачем за проблемними темами слухача, рівня навчального навантаження викладача.

Формування інформаційного поля для викладачів з метою автоматично згенерованих рекомендацій щодо необхідності в індивідуальних консультаціях із слухачами, які мають таку потребу, відповідно до їх рівня опанування навчальної програми курсу (дисципліни).

Визначення рівня необхідності надання допомоги слухачеві залежно від його успішності на курсі, швидкості виконання завдань, якості виконання завдань, рівня активності на форумі курсу.

Використання даних з браузерів та соцмереж, а також анкетні дані, що вибудовують соціальний портрет, за яким можна групувати за напрямами чи спільними інтересами слухачів (курсантів, студентів).

Формування соціального портрету слухача залежно від кількості пошукових запитів в інтернеті за напрямами навчання, кількості пошукових запитів за конкретними темами навчальної програми, рівня спільних інтересів на основі аналізу активності у соціальних мережах та Інтернеті.

Формування груп у віртуальному середовищі за спільними інтересами залежно від повноти збігів соціальних портретів.

*2. Чат-боти*

Використання слухачами та викладачами інтелектуальних чат-ботів для підготовки та надання рекомендацій з оптимальної поведінки на основі соціальних, психологічних, правових та інших алгоритмів/протоколів дій.

*3. Персоналізація*

Формування індивідуального навчального плану дистанційного курсу для окремого слухача з урахуванням рівня набутих компетентностей в межах курсу, якості та швидкості виконання поточних завдань слухачем. Індивідуальні навчальні плани – набір варіантів навчальних планів та критеріїв переходу до кожного з них. Перехід до певного варіанту навчального плану за певного рівня відповідності критеріям залежно від рівня набутих компетентностей в межах курсу, якості та швидкості виконання поточних завдань.

Формування індивідуальної програми підготовки (комбінація додаткових дистанційних курсів, що закривають певні компетентності, які необхідні для виконання функціональних обов'язків (навчального плану)) для окремого працівника (слухача) з урахуванням особистого поточного рівня компетентностей.

Визначення інтенсивності (кількості курсів і їх тривалості) індивідуальної програми підготовки для набуття необхідного рівня компетентностей для якісного виконання функціональних обов'язків (навчального плану) залежно від поточного рівня компетентностей та заданого рівня компетентностей для цієї посади (навчального плану).

Персоналізація навчання з урахуванням індивідуальних особливостей і уподобань слухачів (курсантів, студентів) використовуючи дані з браузерів, соцмереж, анкетні дані тощо.

Індивідуальний підбір навчальних дисциплін (курсів) залежно від поточного і заданого рівня компетентності (компетентностей).

Формування індивідуальних завдань для кожного слухача з урахуванням його особистого рівня знань.

Поточне корегування інтенсивності проходження та інформаційного навантаження дистанційного курсу окремо для кожного курсанта (студента, слухача) залежно від успішності його проходження.

Для реалізації адаптивного плану використовувати сенсори, вбудовані в смартфони для отримання особистих даних слухачів (курсантів, студентів) про їх фізіологічний стан. Цей технологічний прийом вже реалізовано на практиці індивідуалізованого лікування та/або профілактики патологічних станів пацієнтів.

Розроблення програми пошуку та визначення вроджених індивідуальних задатків і здібностей та їх подальший розвиток.

Побудова структури навчання за зразком «дерева навчання», що буде мати можливість враховувати особисті компетентності слухача, рівень його підготовки, психологічні особливості.

Формування індивідуальної траєкторії вдосконалення знань за фахом для набуття необхідних компетентностей.

Відслідковування активності слухачів (курсантів, студентів) у процесі навчання з метою вироблення заохочувальних рекомендацій для викладача.

*4. Рекомендаційна система*

Формування моніторингової системи відслідковування індивідуальних навчальних потреб студента та надання рекомендацій студенту щодо індивідуальної освітньої траєкторії.

Формування рекомендацій щодо вдосконалення знань за фахом шляхом визначення індивідуальної траєкторії набуття компетентностей.

Інформування викладача про ефективність певних блоків (модулів) курсу на основі їх відпрацювання студентами (швидкості відпрацювання завдань і порівняння з їх якістю виконання та кількістю студентів, хто відпрацював швидко і якісно (якщо таких багато, то завдання надто легке), тривалістю та частотою перегляду навчальних матеріалів (якщо більшість

відкривають щось і закривають, значить це нецікаво. Або взагалі не відкривають і не користуються).

Інформування викладача про найбільш популярні та найменш популярні навчальні матеріали курсу.

Формування рейтингу навчальних матеріалів відповідно до: частоти звертання до них, тривалості перегляду, аналізу рівня їх якості у відгуках в опитуваннях. Формування рекомендацій щодо покращення навчального матеріалу курсу залежно від рівня у рейтингу.

Створення рекомендаційної системи щодо додаткових курсів, інформаційного матеріалу в Інтернеті з метою кращого опанування навчального матеріалу з урахуванням індивідуальних особливостей слухачів (курсантів, студентів) та рівня їх поточних компетентностей.

Рекомендаційна система щодо підбору інформаційних джерел, необхідних слухачу для засвоєння певної теми, курсу (дисципліни).

Відслідковування активності слухачів (курсантів, студентів) у процесі навчання з метою вироблення заохочувальних рекомендацій для викладача.

Залежно від якості виконання завдань слухачем, швидкості виконання завдань, соціальної активності на курсі (активність на форумах, блогах курсу) формування рекомендацій більш слабкому в навчанні слухачу (за тими ж критеріями) щодо сильних слухачів (курсантів, студентів), які мають високі показники і можуть допомогти у навчанні.

*5. Вдосконалення інтерфейсу (сервісу)*

Удосконалення інтерфейсу системи (колір, розміщення певних елементів тощо) на основі індивідуальних уподобань, навчальної завантаженості, невербальних знаків та сигналів.

Формування мотиваційних чинників до навчання для слухачів (курсантів, студентів) на основі результатів опанування навчального плану курсу.

Формування у курсантів зацікавленості до отримання знань шляхом відображення мотиваційних чинників.

Відслідковування активності слухачів (курсантів, студентів) у процесі навчання з метою вироблення заохочувальних рекомендацій для викладача залежно від якості та швидкості виконання завдань слухачем, соціальної активності на курсі (активність на форумах, блогах курсу) формування рекомендацій викладачу щодо рівня та частоти заохочувальних відзнак цьому слухачу.

Відслідковування активності слухачів (курсантів, студентів) у процесі навчання з метою вироблення попереджувальних рекомендацій для викладача для активізації їхньої роботи.

Формування комфортного навчального середовища.

Формування рекомендацій щодо використання інструментів гейміфікації залежно від мети і форми проведення навчального заняття.

Аналіз проблемних ситуацій, опрацювання викликів і створення позитивного інформаційного простору з урахуванням результатів вищезазначених етапів.

Розроблення консультативної системи з ефектом присутності живого викладача під час виявлення необхідності надання допомоги в опануванні певного навчального матеріалу курсу (дисципліни) для підвищення ефективності сприйняття інформації.

Формування завдань, максимально наближених до реальних ситуацій на основі практичного досвіду за певною предметною галуззю.

Створення інтелектуальної тренувальної системи для удосконалення практичних навичок, необхідних для успішного засвоєння курсу «Вищої математики».

Розроблення системи прогнозування результатів та очікувань від навчання та надання рекомендацій щодо покращення навчання або заохочення (залежно від динаміки навчання конкретного слухача).

Формування рекомендацій щодо використання навчального презентаційного матеріалу з метою надання можливості слухачу усвідомити реалістичність вивчення матеріалу.

Рекомендаційна система забезпечення організації самостійної навчально-дослідницької діяльності та можливостей самореалізації окремого слухача і викладача на основі індивідуальних вподобань та вимог.

*6. Розрахунок часу*

Прогноз необхідного часу на виконання будь-якого завдання для окремого слухача.

Формування рекомендацій щодо необхідного часу на відпочинок слухачеві залежно від результатів, темпу навчання та невербальних реакцій.

Інтелектуалізація розрахунку часу для науково-педагогічних працівників на розроблення методичного забезпечення матеріалів дистанційних курсів.

Прогнозування часу на виконання завдань для кожного з курсантів визначеної спеціальності залежно від співвідношення питань завдання.

*7. Об'єктивність оцінювання*

Формування індивідуальної траєкторії роботи, тестування (опитування) в кінці кожного заняття (теми, модуля, курсу), залежно від результатів навчання.

Автоматизована система контролю знань на основі наданих відповідей та роботи протягом практичного заняття.

Інтелектуалізація процесу надання творчих завдань з їх автоматичним оцінюванням.

Оцінювання процесу вирішення завдання не лише за кінцевим статичним значенням, а за всім процесом прийняття рішення.

Програма визначення спроможності слухача засвоювати матеріал певної теми, модуля (дисципліни).

Розроблення системи уточнення (визначення) освітніх компетентностей відповідно до

професійної діяльності за посадою.

Визначення рівня підготовки слухачів (курсантів, студентів) для формування окремих підгруп в подальшому навчанні.

Створення програми пошуку прогалин у пройденому навчальному матеріалі за результатами аналізу засвоєння знань.

Запровадження єдиної системи відбору суб'єктів на навчання, враховуючи увесь спектр їх знань, навичок, умінь, що допоможе раціональніше використати їх інтелектуальний ресурс, а також розвинути його, а потім знову здійснити перерахунок отриманого чи витраченого ресурсу з метою встановлення результатів навчання та особистісного розвитку, його доцільності продовження навчання.

Надання окремому слухачеві курсу можливості реалізації механізмів самоконтролю з метою визначення рівня засвоєння матеріалу (курсу) та формування індивідуального інформаційного поля.

*8. База даних*

Формування бази довідкових матеріалів, що визначає необхідність і пропонує потрібну інформацію конкретному слухачеві.

Автоматизація підбору тем, що необхідно вивчити студенту (курсанту) на основі результату контролю якості знань.

Формування каталогу курсів із зазначенням компетентностей, що вони розвивають. В подальшому це спростить формування AI пошуку інформації та персоналізованого напряму розвитку.

Розробка програми прийняття рішень на основі напрацьованих баз даних, існуючих моделей, типових ситуацій.

Створення інтелектуальної системи для скорочення часу на пошук інформації, що необхідна для підготовки до занять на основі пошукових запитів, тематики завдань тощо.

*9. Антиплагіат*

Створення системи для розвитку творчих здібностей для уникнення механічного переписування інформації.

Усунення можливості дублювання (плагіату) виконаної роботи іншими учасниками освітнього процесу.

Результати аналізу та узагальнення інформації щодо використання AI в освітньому процесі засвідчили наявність 65 завдань, що були розподілені на 9 груп (рис. 5).

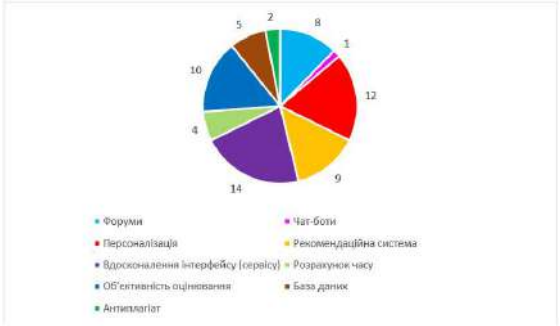



Рис. 5. Завдання штучного інтелекту в освітньому процесі

Найчисельнішими виявилися групи, що стосуються персоналізації освітнього процесу, вдосконалення інтерфейсу (сервісу), а також об'єктивності оцінювання на основі персонального підходу.

Водночас в опитуванні взяли участь і закордонні фахівці загальною кількістю 13 осіб. Проведений аналіз їхніх відповідей свідчить, що:

на перше питання другого блоку: «На Вашу думку, чи можна покращити якість освітнього процесу, запроваджуючи технології штучного інтелекту (інтелектуалізації) у дистанційному навчанні?». Всі відповіли стверджувально (рис. 6);

на питання з множинним вибором: «Визначить до 5 переваг інтелектуалізації дистанційного навчання», було запропоновано 14 поширених варіантів відповідей.

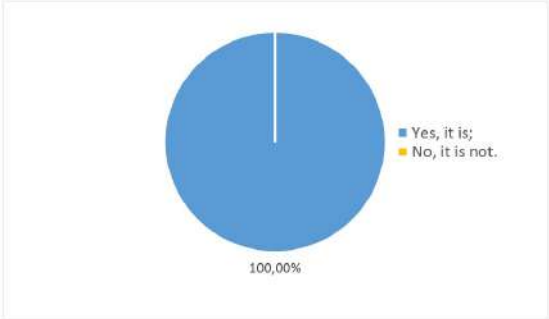



Рис. 6. Ставлення іноземних НПП до покращення освітнього процесу за допомогою технологій AI

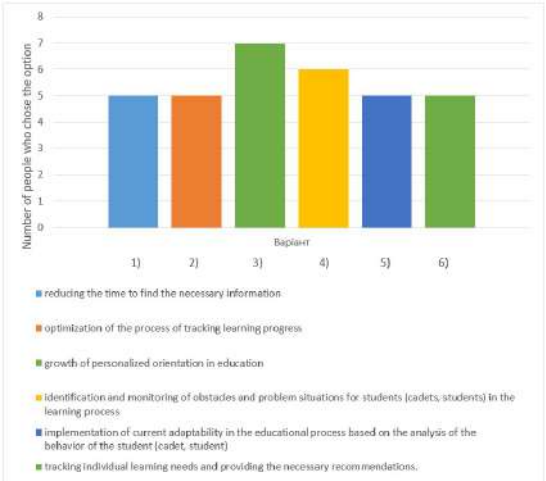



Рис. 7. Переваги інтелектуалізації дистанційного навчання

Найчастіше обиралися наступні варіанти:

а) скорочення часу на пошук необхідної інформації;

б) оптимізація процесу відслідковування прогресу навчання;

в) зростання персоналізованої направленості в освіті;

г) виявлення та відслідковування перешкод і проблемних ситуацій для слухачів (курсантів, студентів) в процесі навчання;

д) впровадження поточної адаптивності в освітній процес на основі аналізу поведінки

слухача (курсанта, студента);

е) відслідковування індивідуальних навчальних потреб та надання необхідних рекомендацій.

На прикінцеве питання: «Запропонуйте, які завдання, на Вашу думку, потрібно вирішити запроваджуючи технології штучного інтелекту (інтелектуалізації) у дистанційному навчанні з метою покращення якості освітнього процесу», було запропоновано низку завдань.

Завдання AI в освітньому процесі, запропоновані іноземними фахівцями:

1. Забезпечення персоналізованих курсів, що будуть точно відповідати потребам кожного студента. Курс може змінюватися залежно від рівня знань студента, його розкладу, аналізу його навчального прогресу, індивідуальних потреб.

2. Адаптація темпу навчання, відповідної навчальної програми до навичок слухача, забезпечення якості виконання завдань.

3. Визначення часу, необхідного для виконання будь-якого завдання для кожного студента (індивідуально) залежно від різних факторів (складність завдання, терміновість виконання завдання, компетентність студента, тощо).

4. Адаптація навчального процесу до індивідуального темпу навчання кожного слухача.

5. Створення інтерактивного контенту, який буде адаптований для кожного студента шляхом збору інформації про мотивацію, залученість та зацікавленість студентів під час проходження курсу, а також вхідних даних для визначення рівня компетентностей слухачів (курсантів, студентів).

6. Створення мікронавчальних модулів, що активуються під час виявлення недостатньої обізнаності слухачів (курсантів, студентів).

Результати аналізу розглянутих завдань свідчать, що відповіді й пропозиції вітчизняних і закордонних фахівців загалом співпадають. Що говорить про постійну співпрацю, обмін досвідом та інтеграцію українського, військового науково-освітнього простору до загальноєвропейського.

Виходячи з загальної мети статті щодо проведення аналізу для знаходження найактуальніших напрямів і завдань, що потребують першочергової інтелектуалізації освітніх процесів у формі дистанційного навчання доцільно зробити такий висновок. За підсумками другого блоку опитування, більшої уваги заслуговують напрями персоналізації освітнього процесу, а також розрахунку та прогнозування часу на виконання будь-якого завдання залежно від різних факторів.

## Висновки й перспективи подальших досліджень

Таким чином, технології AI в освітньому процесі у формі дистанційного навчання надає нові можливості для покращення якості викладання та навчання. Проте дистанційне навчання в нашій країні перебуває лише на початку свого розвитку. Завдяки AI починають свій розвиток нові напрями цієї сфери. Одним з таких напрямів, що заслуговує першочергової уваги в дистанційному навчанні, є напрям адміністрування. Інтелектуалізація процесів адміністрування підніме дистанційне навчання на принципово новий рівень. Крім того, саме адміністрування дистанційного навчання завдяки зростанню можливостей, новим вимогам, ускладненню і розгалуженню адміністративних процесів потребує трансформації та розширення відповідно до його нових напрямів і завдань.

Отже напрямом подальших досліджень слід вважати проведення аналізу процесів адміністрування системи дистанційного навчання з подальшим створенням концептуальної моделі інтелектуалізації адміністрування навчання для кращого розуміння загального функціонування запропонованої системи. Це, в свою чергу, дасть змогу виконати низку завдань щодо інтелектуалізації освітнього процесу дистанційного навчання визначених найбільш актуальними за результатами проведеного дослідження. Це може значно підвищити ефективність навчання та забезпечити краще засвоєння матеріалу слухачами та підготувати їх до виконання складних завдань у реальних умовах. AIEd продовжить дивувати новими можливостями для інновацій в освітній сфері.

## *Література*

**1.** Walcutt, J.J. & Schatz, S. (Eds.) (2019). Modernizing Learning: Building the Future Liarning Ecosystem. Washington, DC: Government Publishing Office. License: Creative Commons Attribution CC BY 4.0 IGO Міжнародний стандартний номер книжки в Україні ISBN: 978-617-7187-61-4 (2021 рік) **2.** Carvalho L. How can we design for learning in an AI world? Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X2200008X (дата звернення: 15.02.2023) **3.** Chih-Ming C. Developing a computer-mediated communication competence forecasting model based on learning behavior features. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X20300047 (дата звернення: 16.01.2023) **4.** Zhang K. AI technologies for education: Recent research & future directions. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X21000199 (дата звернення: 23.01.2023) **5.** Xieling C. A multi-perspective study on Artificial Intelligence in Education: grants, conferences, journals, software tools, institutions, and researchers. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X20300059 (дата звернення: 30.01.2023) **6.** Kabudi T. AI-enabled adaptive learning systems: A systematic mapping of the literature. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X21000114 (дата звернення: 06.02.2023) **7.** Tan Y. Developing a gamified AI-enabled online learning application to improve students' perception of university physics. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X21000266 (дата звернення: 22.02.2023) **8.** Ferguson C. AI-Induced guidance: Preserving the optimal Zone of Proximal Development. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X22000443 (дата звернення: 14.02.2023) **9.** Ingkavara T. The use of a personalized learning approach to implementing self-regulated online learning. Computers

and Education: Artificial Intelligence. URL: https://www.sciencedirect.com/science/article/pii/S2666920X22000418 (дата звернення: 17.02.2023) **10.** Xia X. Diversion inference model of learning effectiveness supported by differential evolution strategy. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X22000261 (дата звернення: 20.02.2023) **11.** Osakwe I. Towards automated content analysis of educational feedback: A multi-language study. Computers and Education: Artificial Intelligence. URL: https://www.sciencedirect.com/science/article/pii/S2666920X22000145 (дата звернення: 22.02.2023) **12.** Hwang G. A fuzzy expert system-based adaptive learning approach to improving students' learning performances by considering affective and cognitive factors. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X20300035 (дата звернення: 27.02.2023) **13.** Kravchenko Y., Afanasyeva O.,Tyshchenko M., Mykus S. Intellectualisation of decision support systems for computer networks: Production-logical F-inference. CEUR Workshop Proceedings, 2021, vol. 2845, pp. 117–126. **14.** Авторський колектив. Теорія і практика дистанційного навчання у Збройних Силах України. Ч. 2: Система електронного навчання вищих військових навчальних закладів та військових навчальних підрозділів закладів вищої освіти: навч.-метод. / колектив авторів; за заг. ред. А.М.Сиротенка. – К.:НУОУ ім. Івана Черняховського. – 2021. С. 3-35.

## ANALYSIS OF THE PROCESSES OF INTELLECTUALIZATION OF THE DISTANCE LEARNING SYSTEM IN THE ARMED FORCES OF UKRAINE

***Oleksandr Shapran***
***Yevhenii Makhno***

***The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine***

*The introduction of artificial intelligence technologies in the educational sphere has prompted the emergence of new areas of intellectualization in the educational process. The use of artificial intelligence in education continues to inspire with its prospects. At the same time, due to its advantages and relevance, distance learning has come to the fore. However, the emergence of the possibility of developing new areas of intellectualization in education has overshadowed the question of their priority. Quite often, the opportunity to make money on the development and implementation of a software product outweighs the value of its purpose and the benefits of its use. How can we understand which areas and tasks in the educational sector are the most relevant? Therefore, this study aims to research to find the most relevant areas and tasks of the educational process of distance learning that require priority intellectualization. To highlight the prospects for further development of the distance learning system. Also, to emphasize the importance and necessity of continuing existing and conducting new research on artificial intelligence in education.*

***Keywords:*** *artificial intelligence; intellectualization; administration; distance learning system.*

### *References*

**1.** Walcutt, J.J. & Schatz, S. (Eds.) (2019). Modernizing Learning: Building the Future Liarning Ecosystem. Washington, DC: Government Publishing Office. License: Creative Commons Attribution CC BY 4.0 IGO Міжнародний стандартний номер книжки в Україні ISBN: 978-617-7187-61-4 (2021 year) **2.** Carvalho L. How can we design for learning in an AI world? Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X2200008X (date of application: 15.02.2023) **3.** Chih-Ming C. Developing a computer-mediated communication competence forecasting model based on learning behavior features. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X20300047 (date of application: 16.01.2023) **4.** Zhang K. AI technologies for education: Recent research & future directions. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X21000199 (date of application: 23.01.2023) **5.** Xieling C. A multi-perspective study on Artificial Intelligence in Education: grants, conferences, journals, software tools, institutions, and researchers. Computers and Education: Artificial Intelligence. URL: https://www.sciencedirect.com/science/article/pii/S2666920X20300059 (date of application: 30.01.2023) **6.** Kabudi T. AI-enabled adaptive learning systems: A systematic mapping of the literature. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X21000114 (date of application: 06.02.2023) **7.** Tan Y. Developing a gamified AI-enabled online learning application to improve students' perception of university physics. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X21000266 (date of application: 22.02.2023) **8.** Ferguson C. AI-Induced guidance: Preserving the optimal Zone of Proximal Development. Computers and Education: Artificial Intelligence. URL: https://www.sciencedirect.com/science/article/pii/S2666920X22000443 (date of application: 14.02.2023) **9.** Ingkavara T. The use of a personalized learning approach to implementing self-regulated online learning. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X22000418 (date of application: 17.02.2023) **10.** Xia X. Diversion inference model of learning effectiveness supported by differential evolution strategy. Computers and Education: Artificial Intelligence. URL:https://www.sciencedirect.com/science/article/pii/S2666920X22000261 (date of application: 20.02.2023) **11.** Osakwe I. Towards automated content analysis of educational feedback: A multi-language study. Computers and Education: Artificial Intelligence. **12.** Hwang G. A fuzzy expert system-based adaptive learning approach to improving students' learning performances by considering affective and cognitive factors. Computers and Education: Artificial Intelligence. **13.** Kravchenko Y., Afanasyeva O.,Tyshchenko M., Mykus S. Intellectualisation of decision support systems for computer networks: Production-logical F-inference. CEUR Workshop Proceedings, 2021, vol. 2845, pp. 117–126. **14.** Avtorskyi kolektyv. Teoriya I praktyka dystanciynogo navchannia u Zbroinyh Sylah Ukrayiny. P 2. Systema elektronnogo navchannia vyshchyh viyskovyh navchalnyh zakladiv ta pidrozdiliv zakladiv vyshchoi osvity: navch.-metod. / kolektyv avtoriv; za zag. red. A.M.Syrotenka. – K.:NUOU im. Ivana Cherniakhovskogo. – 2021. P. 3-35.

DOI:**10.33099/2311-7249/2023-46-1-115-123**

УДК 355.23(477):378.5

***Дмитро Анатолійович Чопа*** *(кандидат технічних наук, с.н.с.)*[1]
***Анатолій Йосипович Дерев'янчук*** *(кандидат технічних наук, професор)*[2]
***Денис Русланович Москаленко***[2]
***Дмитро Степанович Максимчук***[3]

[1]***Національний університет оборони України імені Івана Черняховського, Київ, Україна***
[2]***Сумський державний університет, Суми, Україна***
[3]***Військова академія, Одеса, Україна***

# ВІДДАЛЕНІ ВІРТУАЛЬНІ РЕМОНТНІ ЛАБОРАТОРІЇ ОЗБРОЄННЯ ТА ВІЙСЬКОВОЇ ТЕХНІКИ: ВИМОГИ СЬОГОДЕННЯ ТА ПЕРСПЕКТИВИ

*Сучасні умови застосування Збройних Сил України, що пов'язані з відсіччю збройної агресії російської федерації проти нашої держави, визначають нові вимоги до організації навчання та підготовки військових фахівців різних спеціальностей. Висока інтенсивність бойових дій обумовлює необхідність виконання значного обсягу ремонтно-відновлювальних робіт озброєння та військової техніки. Крім того, воєнно-технічна допомога від наших іноземних партнерів, зумовлює потребу опанування знаннями і навичками стосовно технічного обслуговування і ремонту озброєння та військової техніки іноземного виробництва в короткі строки. Тому заходи щодо прискореної та якісної підготовки спеціалістів для ремонтно-відновлювальних підрозділів, за умов відсутності традиційної навчально-матеріальної бази, потребують зміни поглядів та застосування інноваційних підходів у системі підготовки зазначених фахівців. Одним із таких, запропонованих у статті, інноваційних підходів є створення та використання віддалених віртуальних ремонтних лабораторій для підготовки відповідних фахівців із застосуванням технологій 3D моделювання. Авторами, на підставі практичного досвіду, розглянуто етапи створення та використання запропонованого програмного продукту.*

***Ключові слова:*** *ремонтно-відновлювальні роботи; віддалені віртуальні ремонтні лабораторії; технології 3D моделювання.*

## Вступ

Нейтралізація загроз національним інтересам України в мирний час, успішне ведення бойових дій під час війни або воєнного конфлікту потребують цілого комплексу заходів із підвищення боєздатності Збройних Сил України (далі – ЗС України) і обороноздатності держави в цілому. Однією з важливих складових такого комплексу є система технічного обслуговування і ремонту, що забезпечує необхідний рівень технічної готовності озброєння та військової техніки (далі – ОВТ) до їхнього застосування. Під час відступу російських військ на півночі нашої країни та, особливо, у ході наступальних дій ЗС України на Харківщині, де ворогом було залишено велику кількість ОВТ, особливо гострою стала потреба у підготовці висококваліфікованих фахівців. Частково, залишені зразки підлягали швидкому відновленню завдяки поточному ремонту, інші – виступали «донорами».

Крім того, в Україну надходить ОВТ, що постачають наші західні партнери. Слід зазначити, що таке ОВТ умовно можна поділити на дві групи, зокрема це системи (комплекси): розроблені ще за радянських часів у СРСР і країнах соцтабору; західного виробництва, серед яких є новітні або відносно нові зразки, і застарілі, що після тривалого зберігання також підлягають ремонту. Тому, за умов сучасної війни стратегічним напрямом удосконалення знань і практичних навичок військових фахівців з ремонту ОВТ є застосування інформаційних технологій, що відкривають нові, ще недосліджені високотехнологічні варіанти відновлення озброєння, пов'язані з унікальними можливостями комп'ютеризації ремонтних процесів.

**Постановка проблеми.** Існуюча система ремонту ОВТ у мирний час, в цілому, задовольняла потреби військ у забезпеченні бойової готовності ОВТ. Однак, в ході бойових дій в Україні, виконання завдань щодо своєчасного та якісного ремонту ОВТ перетворились в одну з найважливіших проблем, яка, першочергово, пов'язана з підготовкою фахівців для ремонтно-відновлювальних підрозділів.

В умовах недостатньої кількості навченого та досвідченого особового складу, певних часових обмежень, недостатнього матеріально-технічного забезпечення питання своєчасного ремонту ОВТ, відправлення його у війська, а також забезпечення безпеки робіт є достатньо критичними.

Крім того, надходження зразків ОВТ від наших іноземних партнерів обумовлює необхідність опанування в найкоротші терміни знаннями та

навичками щодо технічного обслуговування і ремонту відповідного ОВТ. Тому часткове вирішення зазначених проблемних питань, враховуючи досвід проведення антитерористичної операції, а згодом – операції об'єднаних сил та вже набутого досвіду в процесі відбиття агресії російської федерації, можна забезпечити за допомогою сучасних інформаційних технологій.

**Аналіз останніх досліджень і публікацій.** Сьогодні, досвід відновлення ОВТ в ЗС України є досить вагомим. Однак, фахівці та науковці констатують недосконаліть існуючих технічних підходів стосовно ремонту і відновлення ОВТ з урахуванням сучасних умов. Про актуальність даного питання свідчить значна кількість наукових публікацій, зокрема Державного науково-дослідного інституту випробовувань і сертифікації ОВТ і Національного університету Повітряних сил імені Івана Кожедуба. Враховуючи численні наявні дослідження, що присвячені застосуванню різних методів відновлення та ремонту ОВТ, жодна з них не розглядає застосування 3D технологій під час підготовки фахівців і в процесі організації ремонту ОВТ. Автори розглянутих публікацій концентрують свою увагу на різноманітних аспектах створення математичних моделей функціонування системи відновлення [1; 2] та методик оцінювання ефективності відновлення ОВТ [3; 4], удосконалюють вже існуючі методики [5; 6], оцінюють економічну ефективність ремонту зразків ОВТ [7], удосконалюють підходи стосовно прогнозування пошкоджень ОВТ [8; 9], доводять, що використання результатів зазначених досліджень здатні суттєво покращити стан ремонтної системи тощо [10; 11]. Разом із тим, проблема створення ефективної системи розроблення та впровадження технологій 3D моделювання для забезпечення прискореного та якісного ремонту ОВТ, залишається не вирішеною.

**Мета статті.** Здійснити науковий аналіз проблем, що пов'язані з підготовкою фахівців для ремонтно-відновлювальних підрозділів, і на його основі цього запропонувати підхід до створення віддалених віртуальних ремонтних лабораторій для підготовки зазначених фахівців із застосуванням 3D технологій.

## Виклад основного матеріалу дослідження

Сьогодні у ЗС України відбувається поступовий перехід на стандарти Організації Північноатлантичного договору (далі – НАТО). Варто констатувати, що запровадження таких стандартів під час проведення ремонту ОВТ наразі досить проблематичне через відсутність експлуатаційної документації і досвідчених фахівців. Зважаючи на той факт, що українських військових залучають до міжнародних навчань окремими структурними одиницями або у складі багатонаціональних сил, то наші підрозділи мають бути повністю сумісними з військовими формуваннями країн-членів НАТО, зокрема, й під час проведення відновлювальних робіт на військовій техніці в польових умовах.

Наявні підходи, що застосовуються у процесі організації та проведенні ремонту ОВТ, не відповідають сучасним вимогам. Наразі застосовують орієнтовно таку методику відновлювального ремонту ОВТ, зокрема, іноземного виробництва: ремонтні підрозділи ремонтують ОВТ в безпосередній близькості від лінії бойового зіткнення або в так званій «сірій» зоні; іноземні фахівці допомагають у ремонті дистанційно по захищених каналах передачі інформації; частина озброєння ремонтується за кордоном. За таких обставин важко вести мову про якість та своєчасність ремонту. Це стосується і системи підготовки фахівців з ремонту ОВТ.

Як відомо, сучасний зразок ОВТ, наприклад, артилерійський комплекс (далі – АК) являє собою сукупність складних систем, для яких характерна велика кількість складових, що поєднані для вирішення певних завдань, у першу чергу, вогневих [12]. На рис. 1 наведена структурно-функціональна схема сучасного типового АК. Через надходження до ремонтних органів військових частин у великій кількості несправних пускових установок, самохідних і причіпних гармат, мінометів, розглянемо один з основних компонентів АК – засоби доставки боєприпасів до цілі.

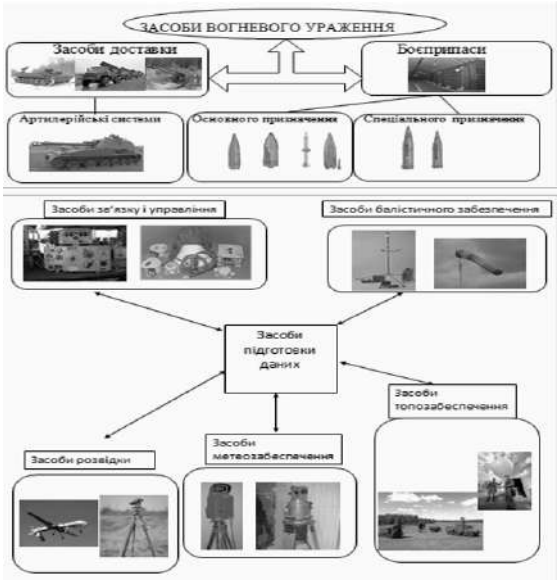



Рис. 1 Структурно-функціональна схема типового АК

Через надходження до ремонтних органів військових частин у великій кількості несправних пускових установок, самохідних і причіпних гармат, мінометів, розглянемо один з основних компонентів АК – засоби доставки боєприпасів до цілі.

Відомо, що під час бойових дій була знищена значна кількість конструкторської та експлуатаційної документації, наукові розробки, технічна література, навчально-матеріальна база, в тому числі й ремонтно-відновлювальних

підрозділів. Тому варіант інтенсивної підготовки фахівців ремонтних органів з використанням 3D моделей зразків артилерійського озброєння (далі – АО) необхідної деталізації, на наш погляд, є найбільш доцільним. Під час реалізації такого варіанту виникає питання: з одного боку – де взяти ІТ спеціалістів достатньої кваліфікації, з іншого – як швидко буде відпрацьований необхідний програмний продукт. Із наведеного вище виникає необхідність у підготовці відповідних фахівців для створення 3D моделей АО, розроблення спеціального контенту для навчання, алгоритмів і моделей, які б сприяли вирішенню проблеми. Водночас, така постановка завдання вимагає пошуку взаємозв'язку між створеним інтерактивним комплексом з ремонту ОВТ і суб'єктом навчального процесу. Для реалізації цього пропонуються такі етапи:

1. Створення мультимедійного продукту окремих зразків ОВТ.
2. Створення інтерактивного комплексу з ремонту ОВТ.
3. Комплексне застосування вищеназваних програмних засобів.

Створення мультимедійного продукту окремих зразків ОВТ є найбільш складною й відповідальною операцією. Узагальнюючи досвід кафедри військової підготовки Сумського державного університету у сфері розроблення тривимірних моделей АО, пропонується загальна схема та етапи створення мультимедійних продуктів для підготовки фахівців ремонтних органів (рис. 2).

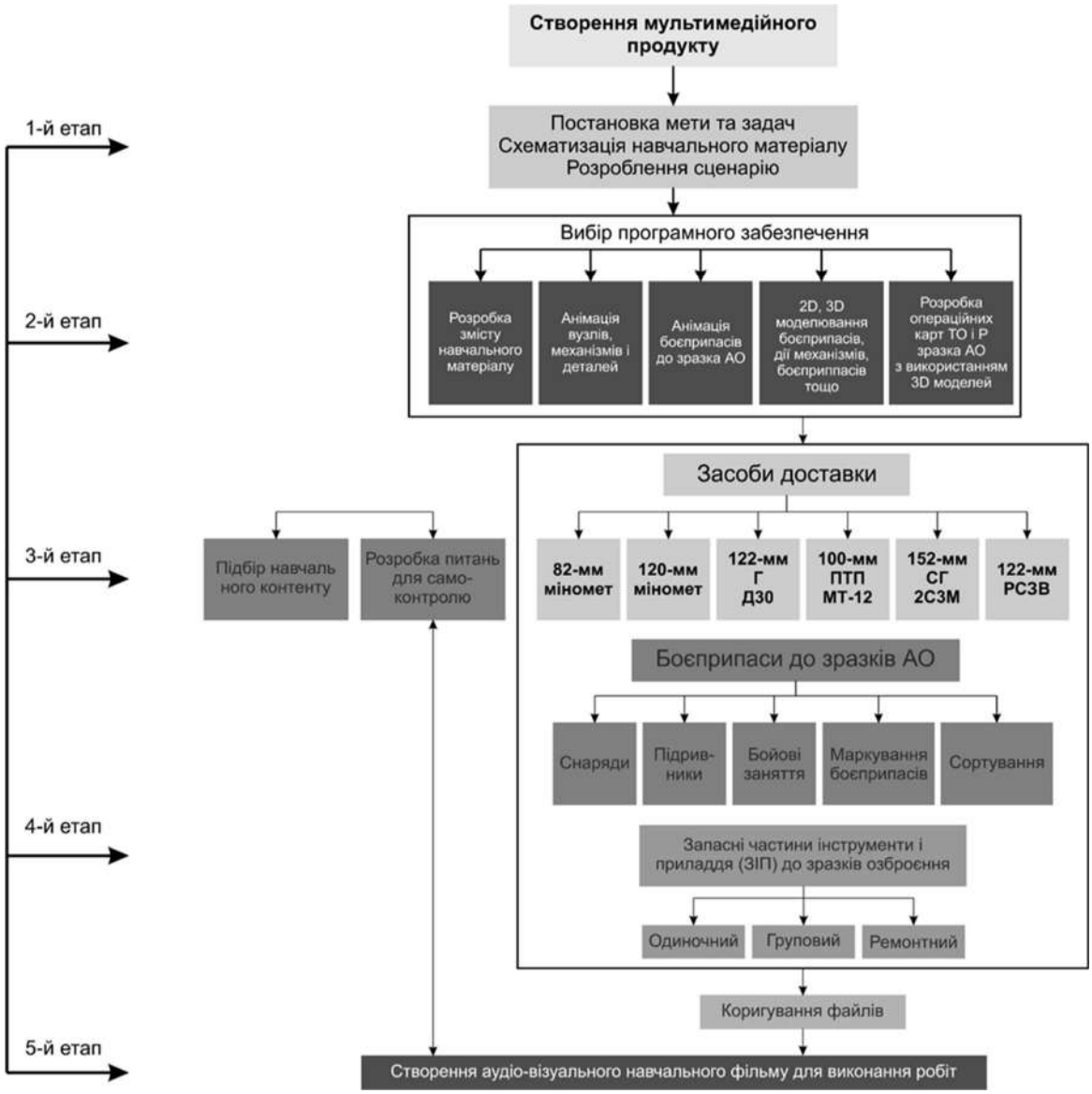



Рис. 2 Загальна схема та етапи створення мультимедійних продуктів для фахівців ремонтних органів

Під час розроблення мультимедійного продукту для його комплексного застосування необхідно враховувати те, що інтерфейс має бути максимально наближеним до реального зразка ОВТ і 3D модель має враховувати основні реальні процеси взаємодії вузлів і механізмів зразка озброєння, прицільних пристроїв, противідкотних пристроїв, підривників і бойових зарядів тощо. Для

подальшого вирішення завдань стосовно створення мультимедійного продукту окремих зразків ОВТ, щонайперше, визначимо об'єкти, які становлять сутність системи навчання, тобто функціональний зв'язок між її складовими (блоками). До них віднесемо функціональні блоки, що надані на рис. 3.


Рис. 3 Функціональний зв'язок між блоками системи навчання фахівців

Під час розроблення мультимедійного продукту для його комплексного застосування необхідно враховувати те, що інтерфейс має бути максимально наближеним до реального зразка ОВТ і 3D модель має враховувати основні реальні процеси взаємодії вузлів і механізмів зразка озброєння, прицільних пристроїв, противідкотних пристроїв, підривників і бойових зарядів тощо. Для подальшого вирішення завдань стосовно створення мультимедійного продукту окремих зразків ОВТ, щонайперше, визначимо об'єкти, які становлять сутність системи навчання, тобто функціональний зв'язок між її складовими (блоками). До них віднесемо функціональні блоки, що надані на рис. 3.

Так, навчальний блок – реалізує засоби оцінки фахівця та зорієнтований на певну галузь знань (міномети, причіпна артилерія, самохідна артилерія тощо). Контролюючий блок – реалізує засоби оцінки ефективності навчання у вигляді тестів або іншого способу контролю. Блок бази даних – інформує користувача про місце зберігання інформації та можливий доступ до неї. Блок засобів інтерфейсу з користувачем (фахівцем) – реалізує засоби аудіо візуальної взаємодії з користувачем (фахівцем). Аналіз функції блоків, наведених вище, дає можливість виокремити об'єкти, що беруть участь у процесі навчання і створити об'єктну модель підготовки фахівця (рис.4).

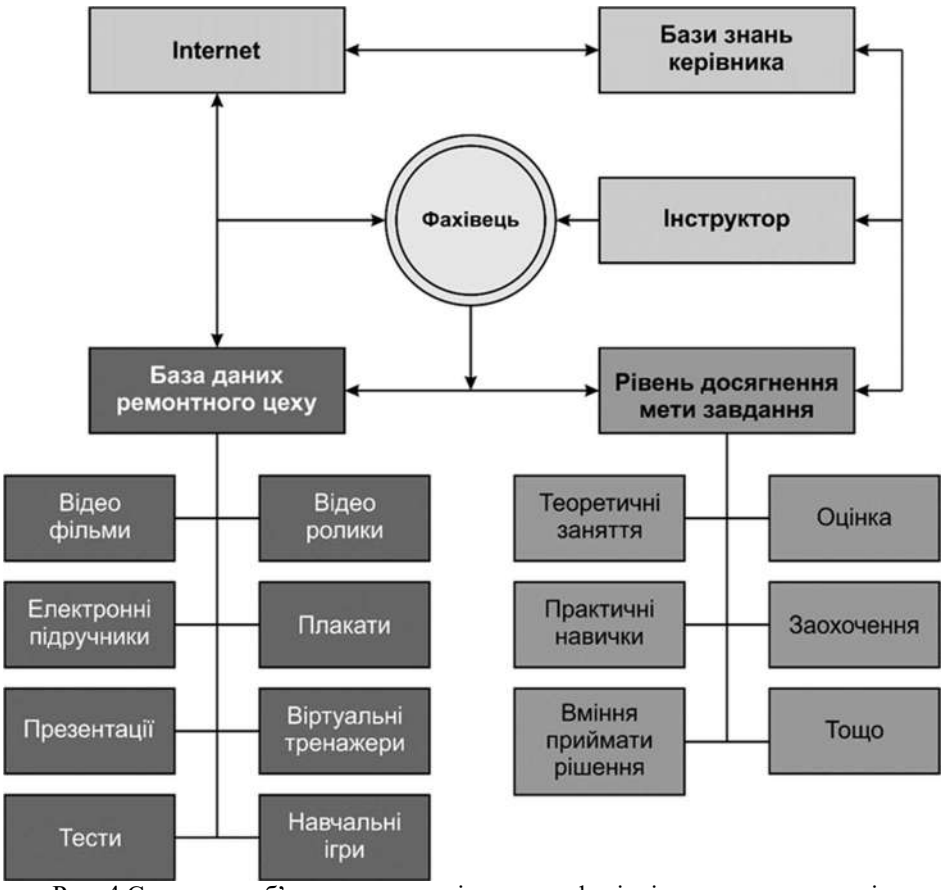



Рис. 4 Спрощена об'єктна модель підготовки фахівців ремонтних органів

Для зручного використання програмного продукту пропонується створити віртуальне меню у вигляді віртуального кубу, де грані кубу вміщують назву контенту стосовно зразків ОВТ (рис. 5а), а внутрішні «кубики» містять необхідний контент стосовно конкретного зразка (рис. 5б).

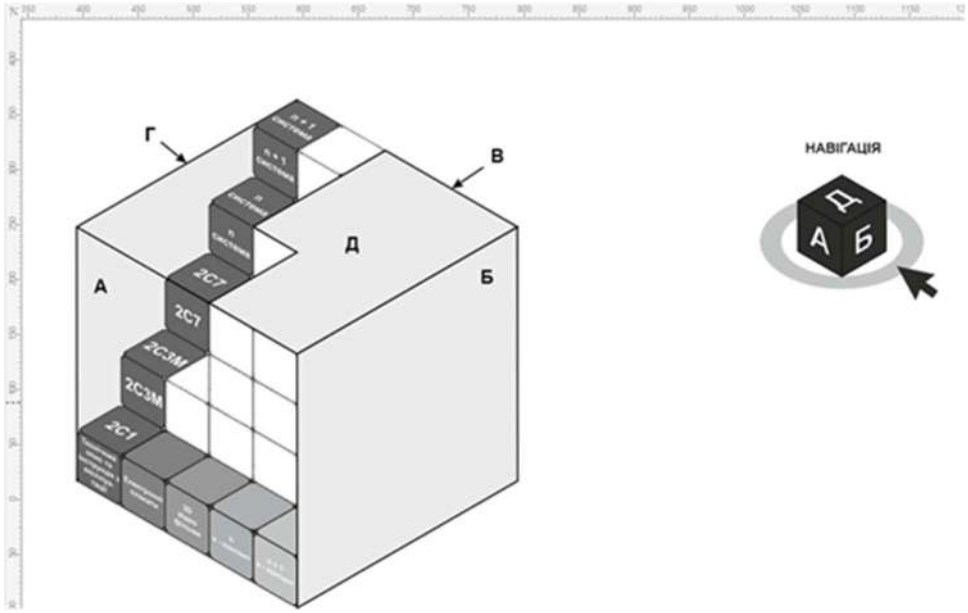



Рис. 5а. Віртуальний куб навчального контенту:
А – самохідна артилерія; Б – причіпна артилерія; В – міномети; Г – реактивні системи залпового вогню; Д – протитанкові ракетні комплекси

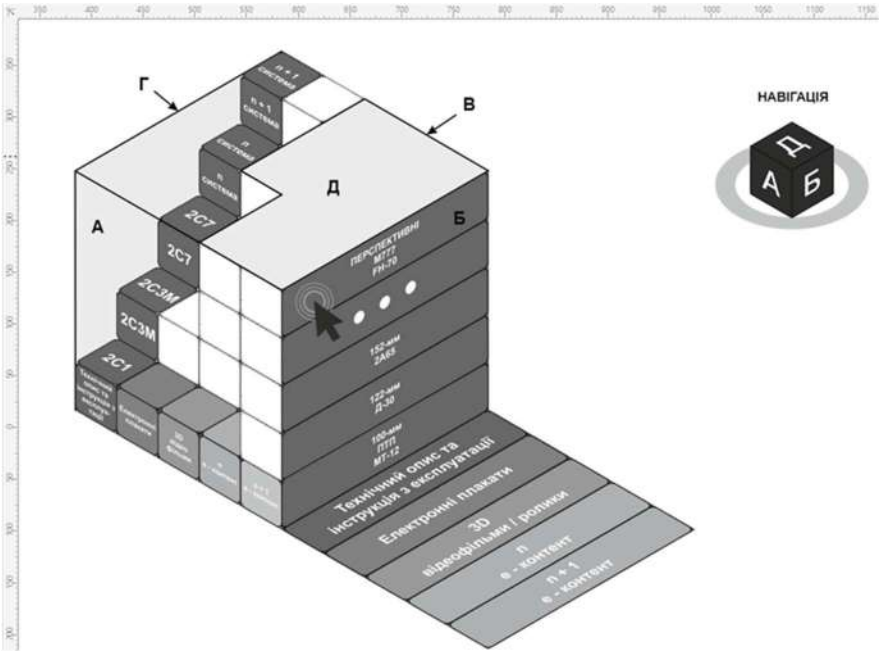



Рис. 5б. Віртуальний куб навчального контенту:
А – самохідна артилерія; Б – причіпна артилерія; В – міномети; Г – реактивні системи залпового вогню; Д – протитанкові ракетні комплекси;

Віртуальний куб являє собою інтерфейс взаємодії з цифровим контентом для навчання спеціалістів ремонтних органів. Його форма – це візуальна модель сховища даних для зручності та легкості їх використання. Навігація у віртуальному кубі відбувається як за допомогою навігаційного куба у верхньому правому кутку екрану шляхом натискання на відповідну грань або обертання його навколо своєї осі круговою стрічкою, так і обертанням навколо своєї осі безпосередньо віртуального куба. Для його руху необхідно натиснути і тримати ліву кнопку миші та обертати куб за існуючими ступенями свободи, щоб вибрати необхідну «грань з цифровим контентом». Зліва та вгорі знаходиться шкала у пікселях, що дозволяє орієнтуватися у масштабі екрану комп'ютерного пристрою користувача для роботи з віртуальним кубом. Під час наведення курсору на потрібну грань і натисканні лівої кнопки миші на потрібну грань, відкривається меню з необхідним контентом для користувача.

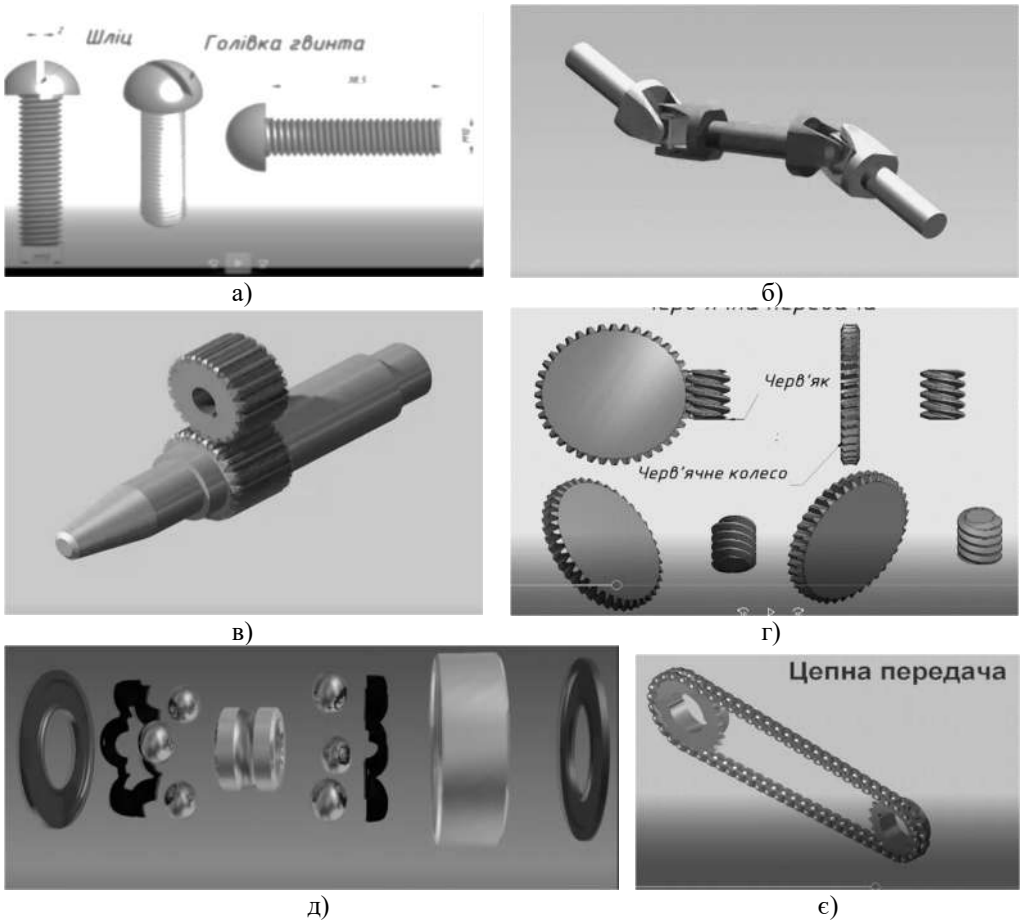
Для оптимального використання віртуального куба можна визначити такі можливі шляхи його наповнення відповідним контентом для використання в освітньому процесі: забезпечення вільного доступу до Інтернету за допомогою

бездротової мережі Wi-Fi; створення системи моніторингу функціонування інфраструктури виробничої діяльності; інтеграцію в суміжні вітчизняні та європейські телекомунікаційні мережі.

Використання сучасних інформаційних технологій, зокрема технологій 3D моделювання, у підготовці фахівців для ремонтних підрозділів створює реальні можливості зниження строків ремонтних робіт і підвищення їх якості шляхом поступової інформатизації системи підготовки фахівців.

Звідси випливає необхідність розглянути наповнення віртуального куба відповідним навчальним контентом. Досвід роботи ремонтних органів у мирний та воєнний часи свідчить, що, першочергово, куб повинен мати такий контент: технічні описи та інструкції з експлуатації зразків ОВТ; різноманітні пам'ятки; відеофільми та відеоролики з будови та експлуатації зразків ОВТ у форматі 3D з необхідною деталізацією; електронні плакати та презентації; операційні карти виконання робіт; ящики із запасними частинами, інструментами та приладдям, їх вміст; набір інструментів для виконання конкретних робіт; перелік типових несправностей та способи їх усунення; шаблони документів; оптичні прилади, акумулятори тощо.

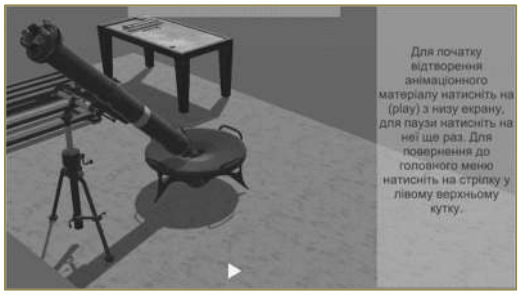
Оскільки ремонтні органи комплектуються, в тому числі особовим складом з недостатнім рівнем знань та умінь, то їх підготовка має здійснюватися за принципом – від простого до складного. Для цього розроблений спеціальний відеофільм у форматі 3D, що наводить найпростіші слюсарні інструменти, елементи різноманітних механізмів наведення гармат, їх взаємодію, порядок розбирання і збирання тощо. Як правило, показ відеофільму здійснюється кожного разу перед початком вивчення конкретної артилерійської системи. На рис. 6 надано деякі скріншоти з відеофільму «Конструктивні схеми механізмів наведення артилерійських систем».




а) б) в) г) д) є)

Рис. 6. Скріншоти механізмів наведення артилерійських гармат:
а – загальний вигляд елементів кріплення; б – карданна передача; в – циліндрична передача; г – черв'ячна передача; д – кульковий підшипник; є – ланцюгова передача

Таким чином, технології 3D передбачають розгортання і впровадження у ремонтному підрозділі інформаційних систем організації і керування процесом відновлювання ОВТ і наповнення цих систем електронним контентом (е-контент), що складається з електронних матеріалів різноманітного призначення (рис. 7).

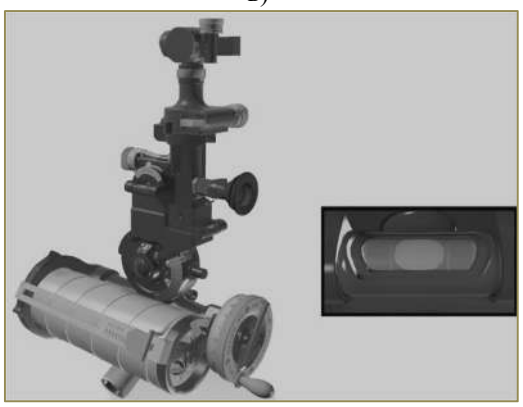



а)


б)


в)


г)



д)

є)


ж)


з)

Ствол

Щітка банника


Мастила
Циатим –205 або ГОІ – 54П

і)

Рис. 7 Скріншоти окремих складових контенту віртуального кубу:
а – загальний вигляд міномету 2Б11; б – порядок розбирання запобіжника від подвійного заряджання; в – згвинчування казенника; г – розбирання і огляд пристрою, що стріляє; д, є – заміна рівнів на прицілах С71-40 і МПМ-44М відповідно; ж – розбирання і огляд ствола; з – встановлення підйомного механізму гармати С7; і – експлуатаційні матеріали для чищення ствола

Зауважимо, що більшість відео мають пояснення послідовності розбирання та збирання механізмів, методику їх огляду на придатність до роботи, перелік необхідних інструментів, їх місце розташування та зовнішній вигляд (рис. 7а, б, в, г).

Враховуючи вищезазначене, стає очевидною проблема підготовки науково-педагогічних працівників (інструкторів) під час війни, яка полягає в тому, що вони мають стати не лише користувачами вже готових програмних продуктів, але й вміти розробляти новітні технології навчання відповідно до програм своїх дисциплін, передавати власний досвід і знання усім категоріям фахівців, які потребують підвищення професійного рівня, зокрема й призваним на військову службу під час мобілізації.

## Висновки й перспективи подальших досліджень

Наприкінці здійсненого наукового аналізу проблем, що пов'язані з підготовкою фахівців для ремонтно-відновлювальних підрозділів, констатуємо, що розроблений і запропонований методичний підхід стосовно візуалізації процесів відновлювального ремонту озброєння та військової техніки має безсумнівні переваги порівняно з традиційними методами, оскільки дозволяє візуально, з першого погляду, визначити й оцінити ймовірну несправність та спосіб її усунення. Крім того, акцентуємо увагу, що пріоритетними перевагами використання 3D технологій у відновлювальному ремонті озброєння стали:

мобільний доступ до довідкових матеріалів у будь-який час і незалежно від місця знаходження;

налаштований зворотний зв'язок з інструкторами, зокрема з фахівцями за кордоном;

можливість створення на основі 3D технологій моделей озброєння та військової техніки іноземного виробництва, що, своєю чергою, дасть можливість їхнього своєчасного і якісного обслуговування та ремонту.

Слід розуміти, що проблема подальшого удосконалення системи технічного обслуговування і ремонту в бойових умовах стає досить значущою й актуальною та потребує комплексного підходу на основі сучасних методів досліджень і впровадження їх результатів у практику військ. Подальшими перспективними напрямами наукових досліджень можуть бути питання удосконалення застосування технологій 3D моделювання та створення тривимірних моделей зразків озброєння та військової техніки закордонного виробництва.

## *Література*


**1. Дачковський В. О., Стрельбіцький М. А.** Математична модель функціонування системи відновлення озброєння та військової техніки. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2020. № 2(38). С. 87–94. **2. Шишанов М. О., Гуляєв А. В., Шевцов М. М.** Обґрунтування методу моделювання процесу функціонування відновлення озброєння та військової техніки угруповання військ *Озброєння та військова техніка*. 2017. № 1(13). С. 75–77. **3. Дачковський В. О., Коцюруба В. І.** Методика оцінювання ефективності функціонування системи відновлення озброєння та військової техніки. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2020. № 1(37). С. 5–14. **4. Старцев В. В., Гурін О. М., Просяник В. В., Коломійцев О. В.** Методики оцінювання ефективності відновлення озброєння та військової техніки повітряних сил Збройних Сил України. *Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*. 2022. № 2(12). С. 134-144. **5. Сампір О.** Удосконалена методика визначення можливостей з технічної розвідки пошкоджених зразків озброєння та військової техніки в ході ведення бойових дій. *Journal of Scientific Papers – Social Development and Security.* 2021. № 11(2). P. 141-151. **6. Сампір О.** Удосконалена методика оцінювання системи відновлення озброєння та військової техніки окремої механізованої бригади. *Journal of Scientific Papers – Social Development and Security.* 2021. Vol. 11. № 5. **7. Dachkovskyi V., Sampir O., Horbachova Y.** Methodical approach to evaluation of economic efficiency of repairing the weapons and military equipment. *VUZF review*, **2020.** Vol. 5. № 1. P. 22–30. **8. Запара Д. М., Бровко М. Б., Старцев В. В., Бортновський С. А.** Удосконалення підходів щодо прогнозування пошкоджень озброєння та військової техніки зенітних ракетних військ від впливу ударної дії засобу ураження. *Системи озброєння і військова техніка*. 2018. № 1(53). С. 20–24. **9. Запара Д. М., Бровко М. Б., Старцев В. В., Кушпета Р. Ю., Дудко М. В.** Впровадження процедури прогнозування пошкоджень ОВТ від впливу осколкової дії засобів ураження в перспективну АСУ матеріально-технічним забезпеченням. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2018. № 4(58). С. 50–56. **10. Залевський Г. С., Леках А. А., Гурін О. М., Старцев В. В., Калачова В. В.** Показники та критерії комплексної методики оцінювання ефективності виконання завдань логістичного забезпечення військових частин Повітряних Сил Збройних Сил України у збройному конфлікті. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2019. № 3. С. 45–52. **11. Старцев В. В., Третяк В. Ф., Бровко М. Б., Джігірей В. О., Коломійцев О. В.** Підходи щодо підтримки рішення на виконання заходів з відновлення озброєння та військової техніки в системі логістичного забезпечення Повітряних Сил Збройних Сил України. *Збірник наукових праць Державного науково-дослідного інституту випробувань і сертифікації озброєння та військової техніки*. 2022. № 1(11). С. 116–126. **12. Чопа Д. А., Дерев'янчук А. Й., Дерев'янчук В. А.** Інформаційні технології як засіб підвищення якості вивчення військово-технічних дисциплін. *Сучасні інформаційні технології в сфері безпеки та оборони*. 2022. № 1(43). С. 91–98.

# REMOTE VIRTUAL REPAIR LABORATORIES OF WEAPONS AND MILITARY EQUIPMENT: CURRENT REQUIREMENTS AND PERSPECTIVES

***Dmytro Chopa*** *(Candidate of technical sciences, Senior Research Fellow)*[1]
***Anatolii Derevianchuk*** *(Candidate of technical sciences, professor)*[2]
***Denys Moskalenko***[2]
***Dmytro Maksymchuk***[3]

[1]*National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine*
[2]*Sumy State University, Sumy, Ukraine*
[3]*Military academy, Odesa, Ukraine*

*The current conditions of use of the Armed Forces of Ukraine, related to the repulsion of the armed aggression of the Russian Federation, determine new requirements for the organization of education and training of military specialists of various specialties. The high intensity of hostilities makes it necessary to carry out a large volume of repair and restoration works of the weapons and military equipment. In addition, the military-technical assistance from our foreign partners makes it necessary to master the knowledge and skills of maintenance and repair of weapons and equipment of foreign production in a short period of time. Therefore, measures for accelerated and high-quality training of specialists for repair and restoration units in the absence of a traditional educational and material base require a change in views and the application of innovative approaches in the system of training specified specialists. One of such innovative approaches proposed in the article is the creation and use of remote virtual repair laboratories for the training of relevant specialists using 3D modeling technologies. The authors, on the basis of practical experience, consider the stages of creation and use of the proposed software product.*

***Key words:*** *repair and restoration works, remote virtual repair laboratories, 3D modeling technologies.*

## *References*

**1. Dachkovsky, V., Strelbytskyi, M.** (2020). Mathematical model of the functioning of the system of restoration of weapons and military equipment. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 3(38). **2. Shishanov, M., Gulyaev, A., Shevtsov, M.** (2017). Justification of the method of modeling the functioning of the process of restoring the armament and military equipment of a grouping of troops. Ozbroiennia ta viiskova tekhnika, 1(13). **3. Dachkovsky, V., Kotsyruba, V.** (2021). Methodology for evaluating the effectiveness of the system of restoring weapons and military equipment. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 1(37). **4. Startsev, V., Gurin, O., Prosyanyk, V., Kolomiytsev, O. V.** (2022). Methods of evaluating the effectiveness of the renewal of armaments and military equipment of the Air Force of the Armed Forces of Ukraine. Zbirnyk naukovykh prats Derzhavnoho naukovo-doslidnoho instytutu vyprobuvan i sertyfikatsii ozbroiennia ta viiskovoi tekhniky, 2(12). **5. Sampir, O.** (2021). An improved technique for determining the technical intelligence of damaged samples of weapons and military equipment in the course of combat operations. Journal of Scientific Papers – Social Development and Security, 11(2), 141–151. **6. Sampir, O.** (2021). Improved the methodology for evaluating the system of fire control and military equipment of the mechanized brigade. Journal of Scientific Papers – Social Development and Security‖, 11, 5. **7. Dachkovskyi, V., Sampir, O. Horbachova, Y.** (2020). Methodical approach to evaluation of economic efficiency of repairing the weapons and military equipment. VUZF review, 5, 1, 22–30. **8. Zapara, D., Brovko, M., Startsev, V., Bortnovsky, S.** (2018). Improvement of the approach to predicting the future of the fire and military equipment of anti-aircraft missiles in the form of a shock wave for the defense of the enemy. Systemy ozbroiennia i viiskova tekhnika, 1(53). **9. Zapara, D., Brovko, M., Startsev, V., Kushpet, R., Dudko, M.** (2018). Implementation of the procedure for predicting the cost of weapons and military equipment in the form of fragmentation damage in the future automated control system for material and technical security. Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl, 4(58). **10. Zalevsky, G., Lekakh, A., Gurin, O., Startsev, V., Kalachova, V.** (2019). Indications and criteria of a complex methodology for evaluating the effectiveness of vikonannya logistical security of the military parts of the Defense Forces of the Armed Forces of Ukraine in an armed conflict. Zbirnyk naukovykh prats Kharkivskoho natsionalnoho universytetu Povitrianykh Syl, 3. **11. Startsev, V., Tretyak, V., Brovko, M., Dzhigirey, V., Kolomiytsev, O.** (2022). Appropriate approach to support the decision to enter the vikonannya for the renewal of military equipment in the system of logistics security of the Defense Forces of the Defense Forces of Ukraine. Zbirnyk naukovykh prats Derzhavnoho naukovo-doslidnoho instytutu vyprobuvan i sertyfikatsii ozbroiennia ta viiskovoi tekhniky, 1(11). **12. Chopa, D., Derevyanchuk, A., Derevyanchuk, V.** (2022). Information technologies as a means of increasing the quality of studying military technical disciplines. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 1(43).

DOI:**10.33099/2311-7249/2023-46-1-124-132**

УДК 355.23(477): 378.14

***Сергій Миколайович Салкуцан*** *(кандидат військових наук, доцент.)* [1]
***Юрій Васильович Кравченко*** *(доктор технічних наук, професор)* [2]
***Андрій Михайлович Онищенко*** *(доктор технічних наук, професор)* [3]
***Максим Георгійович Тищенко*** *(кандидат технічних наук)* [2]

[1] ***Місія України при НАТО, Брюссель, Бельгія***
[2] ***Національний університет оборони України імені Івана Черняховського, Київ, Україна***
[3] ***Київський національний університет імені Тараса Шевченка, Київ, Україна***

# КОНЦЕПТУАЛЬНА МОДЕЛЬ ЄДИНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ ДИСТАНЦІЙНОГО НАВЧАННЯ ЗБРОЙНИХ СИЛ УКРАЇНИ

*В статті досліджується проблема створення та функціонування системи дистанційного навчання у процесі підготовки особового складу Збройних Сил України. Водночас узагальнено поняття дистанційного навчання, розкрито суть інформаційного простору та єдиного інформаційного простору. Останнє дозволило визначити його структурну схему та на основі теорії системного аналізу перейти до побудови концептуальної та математичної моделі єдиного інформаційного простору дистанційного навчання Збройних Сил України, а також визначити шляхи його інтелектуалізації.*

***Ключові слова:*** *дистанційне навчання; єдиний інформаційний простір; математичне моделювання; інтелектуалізація.*

## Вступ

Відповідно до політики Міністерства оборони України у сфері військової освіти, розвиток військової освіти передбачає її професіоналізацію шляхом побудови сучасної моделі професійної військової освіти, що забезпечує підготовку військових фахівців на основі їх безперервного професійного розвитку [1]. Одними з основних принципів політики є інтегрованість системи військової освіти України в європейський військово-освітній простір та безперервність і послідовність військової освіти (підготовки) упродовж військової кар'єри, що має забезпечуватися пріоритетними напрямами розвитку військової освіти шляхом впровадження технологій дистанційного навчання.

Інтеграція до європейського освітнього простору [2], а також необхідність впровадження досвіду країн-членів НАТО, у тому числі завдяки поширенню сучасних форм і методів навчання набуває ще більшої актуальності після прийняття Європейською радою 23 червня 2022 року рішення про надання Україні статусу країни-кандидата [3] та Спільного звернення Президента України Володимира Зеленського, Голови Верховної Ради України Руслана Стефанчука, Прем'єр-міністра України Дениса Шмигаля до Організації Північноатлантичного договору щодо членства України в Альянсі [4]. Україна має незмінну підтримку з боку НАТО за багатьма напрямами. Практичний аспект підтримки за рішенням Мадридського саміту – комплексний пакет допомоги, в якому домінуюча роль відведена вивченню уроків та розбудові інфраструктури військових тренувальних центрів і відновленню спроможностей системи підготовки [5; 6].

Враховуючи неминучий перехід Збройних Сил України на сучасне озброєння НАТО, який прискорився в наслідок російської агресії проти України [7] підвищується актуальність завдань підготовки, перепідготовки та підвищення кваліфікації особового складу Збройних Сил України в контексті трансформації усіх ключових аспектів підготовки, застосування, управління та забезпечення військ (сил). За таких умов зазначений процес має тривати протягом всієї кар'єри військовослужбовців, що відповідає концепції безперервної освіти, яка заснована на принципах безперервності та гнучкості [8; 9].

Враховуючи особливості професійної діяльності військовослужбовців (неможливість постійного перебування в заданій освітній установі, зміну географічного розташування, мінливість військових завдань тощо), особливої ваги в межах системи безперервної освіти, набуває дистанційне навчання, яке в інформаційному суспільстві відіграє все більш важливу роль поряд із традиційним навчанням. Очевидним є той факт, що в умовах швидкоплинних змін традиційна форма навчання не в змозі розв'язати низку проблем військової освіти та підготовки військовослужбовців ЗС України. В умовах триваючої війни та інтенсивного переходу ЗС України від пострадянської до західної парадигми підготовки, застосування та управління військ (сил) військовослужбовці повинні мати можливість вибору різних форм та способів навчання в різних сферах на різних етапах розвитку кар'єри. Дистанційна освіта повинна органічно доповнювати традиційну форму навчання, надаючи

низку переваг та доповнюючи її.

**Постановка проблеми.** На сьогодні переважна більшість освітніх систем містить обмежені стандарти та моделі даних (нерідко такі моделі відсутні взагалі), що значно ускладнює а, часто, унеможливлює інтеграцію різних ІТ-рішень або їх компонентів у сфері дистанційного навчання. За висловлюванням директорки фонду «Lumina» з питань стратегії Ембер Гаррісон Дункан: "Найбільша наша проблема – це відсутність взаємозв'язаної інфраструктури у всіх системах вищої та (або) середньої професійної освіти" [18]. Системі військової освіти також притаманна подібна проблематика оскільки переважна більшість ресурсів дистанційного навчання Збройних Сил України розміщується у незалежних інформаційних системах, які, як правило, не пов'язані між собою. Це призводить до можливих зайвих витрат часових, людських та фінансових ресурсів на створення навчальних матеріалів, які, можливо, вже існують і розміщені на певній платформі дистанційного навчання або у певній бібліотеці, але до них сторонні користувачі не мають доступу. В умовах же ведення бойових дій, час на підготовку військових фахівців стає критичним фактором. Розв'язання зазначеної проблеми дасть змогу створити основу освітньої системи військовослужбовців незалежно від віку та місця розташування особового складу.

З метою ефективного аналізу, пропонується розглядати дистанційну освіту як нову форму навчання на рівні систем. З цієї точки зору система навчання передбачає створення інформаційно-комунікативної системи, формування єдиного інформаційно-технологічного середовища її функціонування, систематизацію та структуризацію інформаційних даних та навчального контенту, формування та актуалізацію інформаційних ресурсів, постійний аналіз ринку освітніх послуг, розроблення механізму передачі слухачам інформаційних даних та начальних матеріалів, необхідних для освітньої діяльності. Такі функції повинні бути реалізовані як на рівні освітніх, так і проєктно-інноваційних технологій.

Системний підхід до вивчення проблеми дистанційного навчання у Збройних Силах України передбачає виокремлення її ключових складових, розкриття їх внутрішньої природи та, зрештою, перехід до концептуальної та математичної формалізації. Будь-яка освітня система є складною системою, в якій функціонує та взаємодіє значна кількість технічних, соціальних, гуманітарних процесів, що постійно змінюються під дією внутрішніх та зовнішніх умов. За цих обставин управління системою дистанційного навчання стає задачею, успішне розв'язання якої потребує використання наукового апарату системного аналізу, одним з ефективних методів якого є техніко-математичне моделювання.

В умовах дослідження побудови технічних систем методами математики розглядається множина з двох об'єктів: система-об'єкт та система-модель. При цьому детальне відображення повного спектру особливостей значно ускладнює математичний аналог, що може призвести до неможливості його повноцінного дослідження, а відповідно отримання необхідної інформації щодо технічної системи. Таким чином, необхідно витримати баланс між двома протилежно спрямованими задачами: максимально точним відображенням моделі-об'єкту та складністю математичної конструкції аналога. З огляду на це, моделювання доцільно провести за етапами.

Враховуючи той факт, що процес управління освітньою діяльністю належить до категорії соціальних систем, на першому етапі його бажано розглядати з позицій системного аналізу представлення об'єктів.

Після фіксації певної структури та відображення притаманних їй характеристик у математичній формі доцільно перейти до другого етапу – математичного дослідження. На цьому етапі слід абстрагуватися від змістової форми моделі та сконцентруватись на виключно математичних алгоритмах розв'язання задачі. За таких умов системність у відображенні моделі-об'єкту через математичне формулювання, як правило, призводить до використання різноманітних напрямів математичної науки як класичних (чисельні методи, теорія диференціальних рівнянь, оптимізації тощо), так і сучасних спрямованих на застосування обчислювальних алгоритмів (нечітка логіка, нейронні мережі, генетичні алгоритми, тощо).

На третьому етапі моделювання доцільно провести інтерпретацію отриманих попередньо рішень на мову досліджуваного об'єкту шляхом співставлення виявлених властивостей моделі та досліджуваної системи – верифікація отриманих результатів, а також відшукати нові, приховані властивості та взаємозв'язки. У випадку, якщо отримані результати не проходять етап верифікації, необхідними є повернення до попередніх етапів та перебудова математичної моделі [19].

Зазначений підхід дозволить створити систему дистанційного навчання здатну інтегрувати до свого складу нові зовнішні модулі або, в свою чергу, бути інтегрованою до інших технічних систем. Враховуючи складність та ієрархічність такої системи, може стати необхідною побудова низки математичних моделей різного ступеня деталізації. Останнє пов'язане з тим, що жодна абстракція реального об'єкту не в змозі відобразити весь необхідний спектр його властивостей, і це потребує відповідного аналога щодо кожної окремої його складової, можливо, з різним ступенем деталізації. Саме тому важливим завданням є побудова концептуальної моделі досліджуваної системи або процесу, відображення його головних та другорядних характеристик, якими, за певних умов, можна знехтувати. За цих обставин така процедура носить, як правило, ітераційний характер, який дозволяє покроково наблизитися до оптимальної структури вихідної концепції дослідження. Для цього необхідно сформулювати сутність проблеми, прийняті гіпотези та припущення. Існує необхідність виокремлення найсуттєвіших рис та властивостей

досліджуваного об'єкта, вивчення його структури та взаємозв'язку його елементів, попереднього формулювання гіпотези, які пояснюють поведінку та розвиток об'єкта.

У зв'язку з цим **метою** статті є виокремлення базових понять концепції побудови системи дистанційного навчання, властивостей та їхнє подальше визначення. Це дозволяє перейти до постановки наступного завдання: формалізації досліджуваної проблеми, тобто запис її у вигляді загальних, концептуальних математичних залежностей, визначення типу моделей, можливостей їх застосування в досліджуваній проблемній області, уточнення низки змінних та параметрів, форми їх зв'язку. Заразом будемо виходити з простих умов та переходити по ланках ієрархічної градації, поступово ускладнюючи модель.

Такий підхід забезпечить створення загального концепту дослідження та задасть необхідність подальшої деталізації у вивченні окремих складових на рівні окремих етапів побудови системи дистанційного навчання у Збройних Силах України.

**Аналіз останніх досліджень і публікацій.** Традиційна форма навчання змінюється за цілою низкою аспектів: форми, методи, віковий ценз, доступ до інформації, індивідуальний підхід, спрямованість на результат тощо. Ключовою рисою сьогодення є той факт, що навчання все більше виходить за межі традиційної аудиторії, що обумовлено стрімким зростанням можливостей цифрових інформаційно-комунікаційних технологій та їх широким прикладним застосуванням у галузі освітніх програм [10]. Зазначений аспект набуває ще більшої ваги в умовах триваючої війни, коли більшість об'єктів навчально-тренувальної інфраструктури ЗС України стали об'єктами ураження російських військ, що суттєво ускладнило реалізацію більшості сталих форм підготовки фахівців для ЗС України та вимагатиме пошуку шляхів підвищення стійкості системи військової освіти та підготовки в особливий період.

Зростання частки дистанційної освіти в освітньому процесі вимагає перегляду всіх складових освітнього процесу від змісту програм до критеріїв успішності засвоєння навчального контенту [11]. А головним критерієм для оцінювання успішності освітніх програм має стати їх зв'язок з потребами сектору безпеки та оборони України [12]. Успішна реалізація зазначеного тандему дозволить перейти на наступний рівень інтеграції – застосування та подальший розвиток передових наукових здобутків та створення тріади: практика – навчання – наука. У цих умовах всебічне врахування різноманітних факторів впливу на процес навчання є підґрунтям для їх врахування в дистанційній освіті.

В результаті аналізу використання технологій дистанційного навчання в ході російської агресії проти України було виявлено 4 основні фактори, які необхідно обов'язково враховувати під час подальшого удосконалення системи дистанційного навчання у Збройних Силах України, а саме:

персонал – система не працює автономно і для її функціонування необхідно мати відповідний особовий склад, який буде обслуговувати як технічну складову, так і користувачів системи. Досвід показав, що персонал може бути залучений до виконання бойових завдань, що впливатиме на стан функціонування системи (часткове/обмежене функціонування або повна зупинка) через що, більшість процесів мають бути автоматизовані;

інфраструктура – існуючі програмно-апаратні рішення, на яких розміщуються платформи дистанційного навчання та інші інформаційні ресурси здебільшого розгортаються безпосередньо у навчальних закладах. За досвідом російські війська постійно завдають ударів по не тільки військовій, а й по цивільній інфраструктурі України. Це призводить до нестабільного забезпечення електроенергією, доступу до мережі Інтернет, а також може призвести до знищення (пошкодження) інфраструктури дистанційного навчання. Тому, для забезпечення безперебійного функціонування інфраструктури дистанційного навчання необхідно розглядати використання хмарних рішень для її розгортання. Водночас, необхідно передбачати ресурси, які будуть забезпечувати доступ кінцевих користувачів до інформаційних тренувальних ресурсів з високим ступенем мобільності та автономності. Використання автономних та мобільних ресурсів живлення і засобів доступу до мережі Інтернет мають критичне значення. Також, вкрай актуальним є використання мобільних інтерактивних тренувальних комплексів, які не потребують прив'язки до конкретного місця розгортання і забезпечують набуття необхідного рівня теоретичних знань та практичних навичок військовослужбовців;

персональні дані – противник може використовувати персональну інформацію з метою отримання даних про діючих (колишніх) військовослужбовців та членів їх сімей, що може становити загрозу їх здоров'ю або життю. Рекомендується обмежено використовувати будь-яку персональну інформацію в інформаційних системах дистанційного навчання або, за необхідності її використання, забезпечувати належний рівень захисту зазначеної інформації;

доступ до матеріалів – з метою підготовки військових фахівців в Україні використовуються різноманітні інформаційні ресурси, найбільш поширеними з яких є: YouTube, LMS Moodle, месенджери та електронні бібліотеки. Враховуючи значну кількість таких ресурсів, їх розрізненість та складність вибору існує потреба створення та використання єдиного інформаційного порталу дистанційного навчання. На порталі доцільно розмістити інформацію щодо: переліку існуючих платформ дистанційного навчання, порядку отримання доступу до них, переліку доступних дистанційних курсів, електронних бібліотек тощо. Науковим центром дистанційного навчання Національного університету оборони України створено подібний портал, який доступний за

посиланням https://adl.nuou.org.ua/. В НАТО також діє подібний портал – «Joint Advanced Distributed Learning, JADL», доступний за посиланням https://jadl.act.nato.int/.

Окрім освітньої та оцінювальної функції така система може включати інституційні, управлінські, технологічні, педагогічні, етичні, інтерфейсні, ресурсні фактори [13]. Зазначена множина факторів була закладена у моделі з дослідження різних сценаріїв реалізації дистанційного навчання, врахування різноманітних його форм та менторів-кураторів. Зазначається, що навчання відбувається у більш широкому сенсі, коли його здійснюють фахівці міждисциплінарних груп з контенту, науки про навчання, технологій, обробки даних та ін. Критично важливим фактором для системи військової освіти України є широке залучення до процесу розроблення програм учасників бойових дій, експертів з питань бойового застосування родів військ та видів ЗС України, а також представників органів військового управління, до відповідальності яких належить узагальнення і впровадження досвіду бойових дій в систему військової освіти та підготовки. Окремо наголошується на залученні експертів з нових напрямів, наприклад, юзабіліті та психометрії, а також необхідності створення адміністративного центру керування навчальним процесом [14–16].

Побудова, вище наведеної системи навчання передбачає низку кроків: використання кількох теорій для обґрунтування розроблення освітніх програм на кожному рівні військової освіти; забезпечення унікальності контенту та його відповідності цілям навчання на відповідному рівні військової освіти; об'єднання специфічного і агностичного за змістом та соціально-емоційного навчання; сумісність технологій для вимірювання та об'єднання; використання науки про навчання для оптимізації системи навчання [17].

## Виклад основного матеріалу дослідження

Дистанційні освітні технології охоплюють освітні технології, реалізовані переважно із застосуванням засобів інформатизації та телекомунікації за частково або повністю опосередкованої взаємодії слухача і науково-педагогічного працівника. В межах таких технологій виділяють низку складових: технологічну, змістову та організаційну. До першої належить спектр інженерного та програмного забезпечення, що дозволяє безпосередньо реалізувати дистанційну комунікацію між лектором та слухачем. Її доповнює змістова складова, яка відображає наповнення навчальних курсів у вигляді презентацій, сайтів, порталів, тощо, а також організаційна – спрямована на застосування передових методик реалізації навчального процесу. Кожна з вказаних підсистем оперує інформаційними ресурсами та їх складовими, серед яких особливу роль відіграє інформаційний простір.

Інформація є основним джерелом трансформації в парадигмі дистанційного навчання і відграє важливу роль на всіх рівнях його організаційної структури. Можна стверджувати, що стабільність функціонування і подальшого розвитку систем дистанційного навчання залежить від інформаційних потоків внутрішнього та зовнішнього середовищ, оскільки від якості й обсягів наданої інформації буде залежати ефективність організації дистанційного навчання, особливо в умовах мінливості завдань та цілей передбачених в межах такого освітнього процесу. У цьому контексті низка дослідників виокремлюють наявність інформаційного простору як обов'язкову складову дистанційного навчання.

На сьогодні можна констатувати той факт, що єдиного загальноприйнятого поняття цієї дефініції не сформовано. Саме тому поставимо завдання узагальнити найбільш відомі існуючі визначення категорії «інформаційний простір», від суспільно-філософського трактування до спеціалізованого, з метою відпрацювання його трактування з погляду застосування цього терміну під час реалізації концепції дистанційного навчання у Збройних Силах України. Варто констатувати, що існує низка досліджень поняття терміну «інформаційний простір», що виходять з логіки трактування його складових, змісту того чи іншого наукового напряму досліджень. Крім того, ця категорія зазнавала зміни у трактуванні з плином часу, модифікувалась, доповнювалась новими ознаками, характеристиками та властивостями [20–22].

Розглянемо низку сучасних визначень поняття терміну «інформаційний простір», виходячи з різних умов та завдань дослідників цієї категорії. У спробі відпрацювання поняття інформаційного простору в межах реалізації концепції дистанційного навчання Збройних Сил України будемо надавати перевагу технічному підходу, як більш придатному для подальшої математичної формалізації. Однак, ураховуючи той факт, що об'єктами дистанційної освіти, а також особами, які приймають рішення, є люди (особовий склад Збройних Сил України), для поведінки яких притаманний певний суб'єктивізм, не варто відмовлятися від гуманітарної складової, тобто спробуємо обрати симбіоз першого та другого підходів. Отже, під поняттям інформаційного простору пропонується розуміти взаємодію різноманітних суб'єктів, які продукують або споживають інформацію на основі інформаційно-комунікаційних систем та технологій.

З точки зору змісту інформаційного простору, принципів його функціонування виділяють поняття його єдності. Згідно з поняттям єдиного інформаційного простору, введеному в [23], його характеристиками є універсальність, яка полягає у чітко регламентованих правилах організації технічної, методичної та організаційної складових. Це передбачає певні правила створення, доступу, перетворення інформаційного ресурсу, його презентування, методик викладання та забезпечує доступ будь-якому споживачеві освітніх послуг в разі виконання вимог єдиності. Таким чином, можна констатувати, що єдиний інформаційний простір – це взаємодія різноманітних суб'єктів, які

продукують або споживають інформацію на основі інформаційно-комунікаційних систем та технологій, що функціонують на основі єдиних принципів та законів.

Виходячи із завдання вивчення освітнього процесу, а саме окремої його форми – дистанційної – та розглядаючи необхідність постійної самоосвіти військовослужбовців, підвищення їх кваліфікації, та реалізації поставлених завдань на відстані від навчального закладу поняття єдиного інформаційного простору дистанційного навчання Збройних Сил України набуває певних уточнень – це взаємодія різноманітних суб'єктів, які продукують або споживають інформацію на основі інформаційно-комунікаційних систем та технологій, що функціонують на основі єдиних принципів та законів з управління освітнім процесом, розподілу прав доступу до освітніх ресурсів та засобів управління, розмежування взаємодії суб'єктів освітнього процесу.

До основних завдань єдиного інформаційного простору дистанційного навчання Збройних Сил України слід віднести:

навчання незалежно від місця перебування військовослужбовця;

зменшення витрат на навчання порівняно з традиційними освітніми програмами;

гнучкість у виборі часових меж навчання;

забезпечення можливості навчання паралельно з виконанням військових завдань;

зняття обмеження на кількість військовослужбовців, що одночасно проходять навчання;

забезпечення гнучкого графіку навчання військовослужбовців та роботи викладацького складу;

реалізацію особистісно орієнтованого підходу;

можливість ефективного контролю набутих умінь та навичок;

набуття навичок використання інформаційних технологій.

До складових єдиного інформаційного простору дистанційного навчання Збройних Сил України слід віднести інформаційно-аналітичні системи, інформаційно-технологічне середовище, засоби систематизації та структуризації інформаційних даних та матеріалів, програми формування та актуалізації інформаційних ресурсів. Об'єктами єдиного інформаційного простору будемо розглядати інформацію, її редагування та кодування з метою її уніфікації та формалізації, схему взаємодії всіх учасників освітнього середовища. Суб'єкти єдиного інформаційного простору – особовий склад Збройних Сил України.

Інфраструктуру єдиного інформаційного простору можна розглядати як ієрархічну та багаторівневу, яка на кожному рівні поєднує інформаційні ресурси, системи накопичення та передачі освітніх даних. Водночас між сусідніми ієрархічними рівнями існує взаємозв'язок із визначеними функціями передачі, аналізу та трансформації інформації. Норми та принципи функціонування єдиного інформаційного простору в системі дистанційного навчання Збройних Сил України залишаються загальноприйнятими.

Загальне визначення поняття єдиного інформаційного простору Збройних Сил України, виокремлення його властивостей та складових дозволяє перейти до вищого рівня його дослідження – математичної формалізації (моделювання). Окреслимо його найбільш загальну форму як системного об'єкту та об'єкту керування.

На будь-якому рівні побудови єдиного інформаційного простору Збройних Сил України – стратегічному, оперативному, тактичному – необхідним є розгляд таких складових: мета, керовані та некеровані фактори, множина можливих рішень, обмеження, критерії, вибір оптимального рішення. Відсутність принаймні одного з них робить побудову системи єдиного інформаційного простору неповноцінною або навіть неможливою. Розглянемо кожну зі складових більш детально.

Мета – образ кінцевого результату, досягнення якого заплановано за проведення певної діяльності. Формулювання мети визначає в якому стані бажано отримати об'єкт або систему через певний час. В реальних умовах, як правило, розглядається досягнення не однієї, а кількох цілей, особливо в умовах побудови складних систем. Під час формулювання мети слід враховувати, що їй, як правило, притаманні внутрішня суперечливість, невизначеність, двоїстість, суб'єктивізм, а також складність поєднання бажаного та реального. Мета може змінюватись з часом, зазнавати корегування залежно від зміни зовнішнього середовища, використовувати інші інструменти для досягнення кінцевого результату. Коректно визначена мета має бути конкретною (ясно та однозначно сформульованою, мати оцінку часу для її досягнення), реальною (узгодженою з реальними можливостями та обставинами), гнучкою (допускає можливість корегування під впливом змін), вимірюваною (здатною бути оціненою щодо ступеня досягнення рівня критерія).

Для реалізації управління тим чи іншим процесом необхідно, щоб об'єкт управління володів керуючими факторами, впливаючи на які можливо змінювати стан об'єкту, а суб'єкт управління мав можливість впливу на перебіг процесу побудови тієї чи іншої системи через керовані фактори. Одночасна наявність керуючих та керованих факторів означає, що діяльність або об'єкт керування є керованими. Тобто керованість – це властивість об'єкта управління змінювати свої властивості в умовах впливу на нього керуючих факторів і разом з тим – властивість суб'єкта управління здійснювати вплив на керуючі фактори (в цьому випадку вони стають керованими факторами). Всі фактори, що належать множині керуючих факторів та не є керованими, вважатимемо некерованими факторами [24].

Розглянемо співвідношення між керуючими, керованими та некерованими факторами. Множина керованих факторів $S_{cf}$ належить множині керуючих факторів $S_{CF}$ ($S_{cf} \subset S_{CF}$), а множина

некерованих факторів $S_{ucf}$ складається зі всіх тих елементів множини $S_{CF}$, які не належать множині $S_{cf}$ (множина $S_{ucf}$ є доповненням множини $S_{cf}$, тобто $S_{ucf} = S_{CF} \setminus S_{cf}$). Умова керованості означає, що перетин множин керуючих та керованих факторів не є порожнім. Відповідно некерованість має місце в тому випадку, коли множина керуючих факторів $S_{CF}$ або множина керованих факторів $S_{cf}$ для даного суб'єкта керування є порожніми або їх перетин – порожнім $S_{cf} \cap S_{CF} = \varnothing$.

Сукупність рішень $x_i$, з яких відбувається вибір, утворюють множину можливих рішень $X$. Множина можливих рішень може містити як скінченну, так і нескінченну кількість рішень. Природа альтернатив або рішень у множині можливих рішень при цьому не має принципового значення. При побудові множини можливих рішень слід враховувати, що остаточний вибір рішення відбувається саме з цієї множини і якщо в цю множину деякі з рішень не потраплять, то це може призвести до того, що остаточно буде обрано не оптимальне рішення. Для того, щоб не втратити жодного потенційного рішення необхідно розглянути структуру рішення або складові рішення. Можливе рішення та множина керуючих факторів безпосередньо пов'язані між собою – будь-яке рішення є сукупністю керуючих факторів: $x_i = \{S_{CF}\}$, $x_i \in X$. Керуючі фактори можна розділити на керовані та некеровані $S_{CF} = S_{cf} \cup S_{ucf}$, відповідно $x_i = \{S_{cf}, S_{ucf}\}$. В конкретній заданій ситуації некеровані фактори залишаться незмінними, в той час як керовані фактори є доступними суб'єкту керування і тому можуть зазнавати з його сторони впливу як шляхом безпосередньої зміни їх значень, так і шляхом вибору із множини їх значень. Тому різні рішення із множини можливих рішень відрізняються одне від одного лише значеннями керованих факторів, відповідно рішення є сукупністю всіх керованих факторів $x_i = \{S_{cf}\}$, $x_i \in X$. Різні набори значень керованих факторів визначають різні рішення. Зміна значення хоча б одного з керованих факторів призводить до нового можливого рішення.

Будь-яка діяльність проходить в певному оточуючому середовищу або в внутрішніх та зовнішніх умовах, які для даного виду діяльності є об'єктивною реальністю, і на яку суб'єкт керування впливати не може. Сукупність всіх тих факторів, які впливають на діяльність системи є об'єктивними і не залежать від суб'єкта управління називають обмеженнями. Обмеження утворюють середовище, в якому функціонує система. Всі фактори, які утворюють обмеження, можна поділити на внутрішні та зовнішні.

Зовнішні фактори складаються з елементів, які знаходяться за межами системи, поза діяльністю суб'єкта керування. Ці фактори утворюють зовнішні умови, в яких існує організація і реалізується певна діяльність. Вони можуть проявлятися у вигляді загальних тенденцій та сил, законів та розпоряджень. Внутрішні фактори знаходяться в самій системі і утворюють саме середовище, в якому протікає діяльність. До них належать ресурси, технології засоби керування тощо.

Оскільки обмеження є сукупністю всіх факторів, які з одного боку впливають на хід діяльності, а з іншого не залежать від суб'єкта управління, то такими є саме некеровані фактори. Сукупність некерованих факторів утворює множину обмежень, тобто $Y = \{S_{ucf}\}$. Визначення поміж керуючих факторів некерованих та побудова на їх основі обмежень називають структуруванням обмежень.

Слід зазначити, що межа між керованими та некерованими факторами є не завжди чітко визначеною та може зазнавати змін. Це означає, що окремі фактори, які формують обмеження, можуть стати доступними для керування та перейти в категорію рішень і, відповідно, фактори, які формують рішення, можуть стати некерованими та перейти в категорію обмежень. Обмеження також формують множину допустимих рішень в межах функціонування досліджуваної системи.

Для того щоб вибір із множини альтернатив або можливих рішень був можливим необхідно володіти певним кількісним показником. Розуміючи оцінку того чи іншого рішення з погляду ефективності досягнення поставленої мети, ведуть мову про показник ефективності. Кількісний показник, за яким порівнюють між собою різні рішення називають критерієм ефективності функціонування побудованої системи. Формулювання такого критерію є досить складною задачею, яка потребує врахування того факту, що за умов його некоректного визначення, досягнення поставленої мети може стати неможливим або призвести до невиправданих витрат та збитків. В більшості практичних задач для оцінки різних альтернатив вибору рішення використовується не один, а кілька критеріїв. В таких випадках йдеться про розв'язання багатокритеріальних проблем.

Сформована низка критеріїв дозволяє визначити механізм оцінювання реалізації досягнення побудови системи або ефективності її функціонування. У ролі такого індикатора введемо до розгляду функцію якості досягнення мети. Для окреслення її властивостей будемо вважати, що множина можливих рішень володіє властивостями транзитивності, рефлексивності, ірефлексивності, симетричності, асиметричності, антисеметричності. Диференційовані таким чином співвідношення називають пріоритетними порядками, до яких належать: порядок еквівалентності, ірефлексивний та слабкий порядок [25]. За наявності пріоритетного співвідношення з ознаками слабкого порядку його можна представити функцією якості досягнення мети $F$. Така функція для всіх елементів множини можливих рішень трансформує пріоритетні співвідношення еквівалентності та строгості у

числові співвідношення слабкості або рівності, дозволяючи визначати ефективність функціонування системи:

$$x_i \succ x_j \leftrightarrow F(x_i) > F(x_j),$$
$$x_i \approx x_j \leftrightarrow F(x_i) = F(x_j),$$
$$x_i, x_j \in X, i, j = 1,...,n .$$

Таким чином, формалізуємо наведену вище теорію у вигляді математичної моделі:

$$F(x_i) \to opt$$
$$X = \{S_{cf}, S_{ucf}\}, \quad (1)$$
$$x_i \in X ,$$
$$Y = \{S_{ucf}\}.$$

Наведена модель відображає вибір оптимальної системи побудови та функціонування єдиного інформаційного простору дистанційного навчання Збройних Сил України на множині можливих рішень (альтернатив), що складаються з керованих та некерованих факторів в умовах існуючих обмежень на множині некерованих факторів. Розглянута теорія математичного опису оцінки якості побудови та функціонування єдиного інформаційного простору дистанційного навчання Збройних Сил України та виражена у вигляді математичної моделі (1) дозволяє побудувати її аналог у вигляді блок-схеми керування (рис. 1).

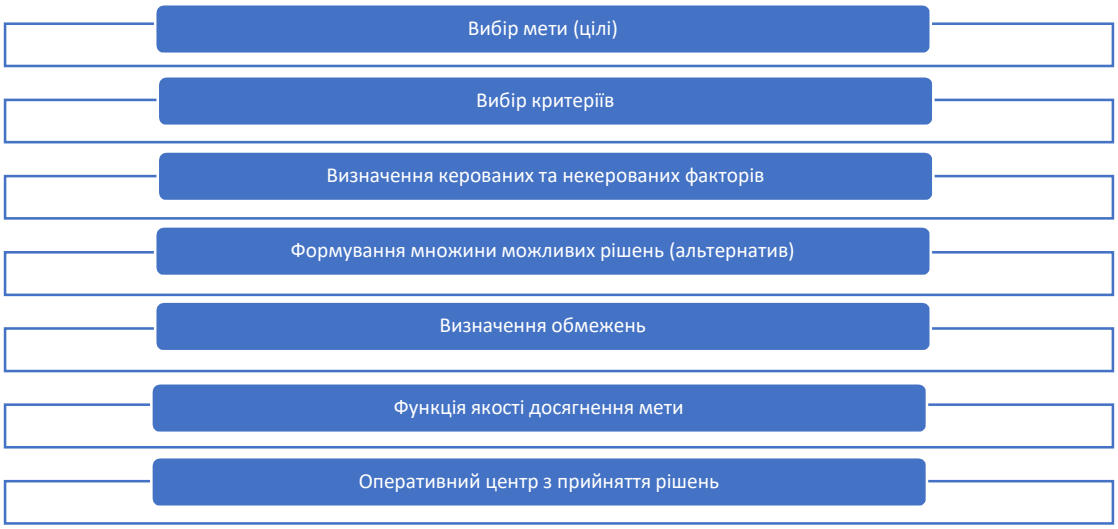



Рис. 2. Блок-схема керування єдиного інформаційного простору дистанційного навчання Збройних Сил України

Порівняно з попередньою концепцією, таку модель доповнимо блоком, який оцінює значення функції якості $F$ – оперативний центр оцінки та прийняття рішень. Саме ця одиниця несе повну відповідальність за остаточне прийняття рішень. За таких умов слід наголосити на тому, що оптимальних рішень, які визначає функція $F$ може бути декілька або, навіть, нескінченна множина. Вибір, в такому випадку, ґрунтується на окремій теорії, розгляд якої виходить за межі цієї публікації.

Враховуючи специфіку предметної області єдиного інформаційного простору дистанційного навчання Збройних Сил України, слід відзначити завдання інтелектуалізації його складових, які можуть набувати додаткових системних властивостей – адаптації, навчання та самонавчання, накопичення знань та отримання нових знань на основі існуючих. Для єдиного розуміння введемо поняття терміну «інтелектуалізація дистанційного навчання» – це розроблення, впровадження та використання у відповідних програмних продуктах алгоритмів штучного інтелекту для автоматизованого вирішення складних завдань освітнього процесу в умовах невизначеності. В наслідок цього виникає інтегративний ефект, який проявляється як розширення функціоналу на проблемну область освітніх задач, характерних для інтелектуальної діяльності суб'єкта навчання [26].

З метою реалізації інтелектуалізації складових єдиного інформаційного простору дистанційного навчання Збройних Сил України актуальним є покрокова реалізація такої схеми (концептуальної моделі):

формулювання цілей, задач, вихідних даних стосовно об'єкту та процесів дослідження, основних факторів, взаємозв'язків, формулювання вихідних гіпотез щодо закономірностей розвитку, методів та організації процедур моделювання;

вивчення зовнішнього середовища, виявлення зовнішніх впливів на розвиток об'єкту та внутрішнього управління, уточнення критеріїв розвитку та параметрів керування;

розроблення техніко-математичної моделі, визначення її структури та складових елементів, виявлення взаємозв'язків між ними, які дозволяють прослідкувати закономірності розвитку системи;

оцінювання розроблення альтернативних варіантів концепції та порівняння їх з основним базовим аналогом;

визначення достовірності, точності та обґрунтованості розробленої системи, наслідків її функціонування;

розроблення рекомендацій з управління розвитком системи з врахуванням впливу зовнішніх факторів та еволюції внутрішньої

структури;

формулювання задач із розроблення оптимізації тих чи інших параметрів системи з врахуванням аналізу отриманих результатів та нової виявленої інформації.

На сьогодні практичні роботи з впровадження інтелектуалізації єдиного інформаційного простору дистанційного навчання знаходяться на початковому етапі реалізації – теоретичному. Основним напрямом їх подальшого розвитку є розроблення конкретних схем інтелектуалізації окремих складових єдиного інформаційного освітнього простору.

## Висновки й перспективи подальших досліджень

Дистанційне навчання посідає все більш важливе значення в системі військової освіти, особливо в умовах збройної агресії, коли ціною неналежної підготовки є життя громадян та безпека держави. Володіючи низкою переваг, воно стає домінуючим інструментом в питанні безперервного навчання та підготовки особового складу Збройних Сил України. Водночас ключові складові системи дистанційного навчання у Збройних Силах України – єдиний інформаційний простір – потребують окремого дослідження на рівні математичного апарату з метою узагальнення наявних та виявлення прихованих властивостей. Наступним кроком слід розглядати процес інтелектуалізації єдиного інформаційного простору як сучасну складову кібернетичної тріади «аналіз – синтез – оптимізація».

## *Література*


**1. Політика** Міністерства оборони України у сфері військової освіти. 2021 р. URL : https://www.mil.gov.ua/content/education/politika mou osv ita.pdf (дата звернення: 09.12.2022). **2. Стратегія** розвитку вищої освіти в Україні на 2021–2031 роки. 2020 р. URL : https://mon.gov.ua/storage/app/media/ rizne/2020/09/ 25/rozvitku-vishchoi-osviti-v-ukraini-02-10-2020.pdf (дата звернення: 09.12.2022). **3. European** Council conclusions on Ukraine, the membership applications of Ukraine, the Republic of Moldova and Georgia, Western Balkans and external relations, 23 June 2022. URL : https://www.consilium.europa.eu/en/press/ press-releases/2022/06/23/european-council-conclusions-on-ukraine-the-membership-applications-of-ukraine-the-republic-of-moldova-and-georgia-western-balkans-and-external-relations-23-june-2022/ (дата звернення: 09.12.2022). **4. Спільне** звернення Президента України Володимира Зеленського, Голови Верховної Ради України Руслана Стефанчука, Прем'єр-міністра України Дениса Шмигаля до Організації Північноатлантичного договору. 2022 р. URL : https://www.president.gov.ua/ storage/j-files-storage/01/16/49/930828c389f438917f22e67e 5d64c98e_1667835181.pdf (дата звернення: 09.12.2022). **5. Madrid** Summit Declaration Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid 29 June 2022. URL : https://www.nato.int/cps/en/natohq/official_texts_196951.ht m (дата звернення: 09.12.2022). **6. 2022 NATO** Summit (Overview). URL : https://www.nato.int/cps/en/natohq/ news_196144.htm (дата звернення: 09.12.2022). **7. Перспективи** забезпечення воєнної компанії 2023 року: український погляд. Режим доступу: URL : https://www.ukrinform.ua/rubric-ato/3566162-ak-zabezpeciti-voennu-kampaniu-u-2023-roci-ukrainskij-poglad.html (дата звернення: 09.12.2022). **8. Щипанський П. В., Тимошенко Р. І., Салкуцан С. М.** Формування нової парадигми військової освіти. *Наука і оборона*. 2017. № 2. С. 37–42. **9. Mariusz S., Tyshchenko M., Tony R., Gareis S., Gawliczek P., Petek B.** Defence Education Enhancement Programme (DEEP) Strategy for Distance Learning Support, 2021. URL : https://www.nato.int/nato_static_fl2014/ assets/pdf/2021/12/pdf/211209-deep-strategy-dist-learn.pdf (дата звернення: 09.12.2022). **10. Allen I. E., Seaman J.** Online Report Card: Tracking Online Education in the United States (ERIC No. ED572777). Babson Park, MA: Babson Survey Research Group, 2016. URL : eric.ed.gov/?id=ED572777 (дата звернення: 09.12.2022). **11. Association** for Talent Development Research. Next Generation E-Learning: Skills and Strategies (Product Code 191706). Alexandria,VA: ATD Research, 2017. **12. Артамощенко В. С.** Розвиток системи військової освіти. Розроблення програмного документа Кабінету Міністрів України. *Наука і оборона*. 2021. № 4. С. 26–33. **13. Farid S., Ahmad R., Alam M.** A hierarchical model for e-learning implementation challenges using AHP. *Malaysian Journal of Computer Science.* 2015. № 28(3). С. 166–188. **14. Roscoe R. D., Branaghan R., Cooke N. J., Craig S. D.** Human systems engineering and educational technology. / In Eds. R. D. Roscoe, S. D. Craig & I. Douglas, End-user considerations in educational technology design. New York : IGI Global, 2017. P. 1–34. **15. Sohoni S., Craig S. D., Vedula K.** A blueprint for an ecosystem for supporting high quality education for engineering. Journal of Engineering Education Transformation. 2017. № 30(4). С. 58–66. **16. Cooke N. J., Hilton M. L.** Enhancing the effectiveness of team science. Washington, D.C.: National Academies Press, 2015. **17. Sae Schatz** and her colleagues have dubbed this integrated approach «Industrial Knowledge Design» and outline it in an article, see: Schatz S., Berking P., Raybourn E. M. Industrial knowledge design: an approach for designing information artefacts. *Theoretical Issues in Ergonomics Science.* 2017. № 18(6). P. 501–518. **18. Johnson-Freese J.** The reform of military education: Twenty-five years later (ADA570086). Philadelphia, PA: Foreign Policy Research Inst., 2012. URL : apps.dtic.mil/docs/citations/ADA570086 (дата звернення: 09.12.2022). **19. Serovajsky S.** Mathematical modeling. – Chapman and Hall/CRC. 1st edition, 2021. 442 p. **20. Walcutt J. J., Schatz S.** (Eds.). Modernizing Learning: Building the Future Learning Ecosystem. Washington, DC: Government Publishing Office. License: Creative Commons Attribution CC BY 4.0 IGO, 2019. 405 p. **21. Montemayor C.** The Problem of the Base and the Nature of Information. *Jornal of Consciousness Studies*. 2017. № 24. P. 91–102. **22. Ball B., Nagle F., Votsis I.** Editorial: Computationalism Meets the Philosophy of Information. *Review of Philosophy and Psychology*, 2020. P. 507–515. **23. Теорія і практика** дистанційного навчання у Збройних Силах України. Ч. 1: Основи використання технологій дистанційного навчання в освітньому процесі вищих військових навчальних закладів та військових навчальних підрозділів закладів вищої освіти : навч.-метод. посіб. / колектив авторів ; за заг. ред. А. М. Сиротенка. Київ : НУОУ ім. Івана Черняховського, 2020. 220 с. **24. Bellman R.** Classic Papers in Control Theory. *Dover Publications*. 2017. 208 p. **25. Rosen K.** Discrete Mathematics and Its Applications. Mc Graw Hill Education (UK); 8th edition, 2000. 2018 p. **26. Організація** та використання технологій дистанційного навчання у Збройних Силах України: навч.-метод. посіб. / заг. ред. С. М. Салкуцана. Київ : НУОУ, 2017. 124 с.

# CONCEPTUAL MODEL OF THE UNIFIED INFORMATION SPACE FOR DISTANCE LEARNING OF THE ARMED FORCES OF UKRAINE

***Serhii Salkutsan*** *(Candidate of Military Sciences, Associate Professor)* [1]
***Yurii Kravchenko*** *(Doctor of Technical Sciences, Professor, Lead Researcher of a Center)* [2]
***Andrii Onyshchenko*** *(Doctor of Technical Sciences, Professor, Professor of a Department)* [3]
***Maksym Tyshchenko*** *(Candidate of Technical Sciences, Senior Researcher, Chief of a Center)* [2]
[1] ***Military representative of Mission of Ukraine to NATO***
[2] ***National Defense University of Ukraine named after Ivan Chernyakhovskyi, Kyiv, Ukraine***
[3] ***Taras Shevchenko National University of Kyiv, Kyiv, Ukraine***

*The article examines the problem of creation and functioning of a distance learning system in the training of personnel of the Armed Forces of Ukraine. At the same time, the concept of distance learning is generalized, the essence of the information space and the unified information space is revealed. The latter made it possible to determine the block diagram and, on the basis of the theory of system analysis, proceed to the construction of a conceptual and mathematical model of a single information space for distance learning of the Armed Forces of Ukraine, as well as to determine the ways of its intellectualization.*

***Keywords:*** *distance learning; single information space; mathematical modeling; intellectualization.*

## *References*

**1. Politics of the Ministry of Defense** of Ukraine in the sphere of military education. (2021). Available at:: https://www.mil.gov.ua/content/education/politika mou osvita.pdf. **2. Strategy** for the development of higher education in Ukraine for 2021–2031. (2020). Available at: https://mon.gov.ua/storage/app/media/rizne/2020/09/25/rozvitku-vishchoi-osviti-v-ukraini-02-10-2020.pdf.
**3. European** Council conclusions on Ukraine, the membership applications of Ukraine, the Republic of Moldova and Georgia, Western Balkans and external relations (23 June 2022). Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/06/23/european-council-conclusions-on-ukraine-the-membership-applications-of-ukraine-the-republic-of-moldova-and-georgia-western-balkans-and-external-relations-23-june-2022/. **4. Speech** of the President of Ukraine Volodymyr Zelensky, Head of the Verkhovna Rada of Ukraine Ruslan Stefanchuk, Prime Minister of Ukraine Denis Shmyhal to the Organization of the Pivnichno-Atlantic Treaty. (2022). Available at: https://www.president.gov.ua/storage/j-files-storage/01/16/49/930828c389f438917f22e67e5d64c98e_1667835181.pdf. **5. Madrid Summit Declaration** Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Madrid. (29 June 2022). Available at: https://www.nato.int/cps/en/natohq/official_texts 196951.htm **6. 2022 NATO Summit** (Overview). (2022). Available at: https://www.nato.int/cps/en/natohq/news_196144.htm
**7. Prospects for providing a military company** in 2023: the Ukrainian view. (2023). Available at: https://www.ukrinform.ua/rubric-ato/3566162-ak-zabezpeciti-voennu-kampaniu-u-2023-roci-ukrainskij-poglad.html. **8. Shchypanskyi, P. V., Tymoshenko, R. I., Salkutsan, S. M.** (2017), Formation of a new paradigm of military education. Nauka i oborona, 2, 37–42. **9. Mariusz, S. Tyshchenko, M., Tony, R., Gareis, S., Gawliczek, P., Petek, B.** (2021). Defence Education Enhancement Programme (DEEP) Strategy for Distance Learning Support. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2021/12/pdf/211209-deep-strategy-dist-learn.pdf.
**10. Allen, I. E., Seaman, J.** (2016). Online Report Card: Tracking Online Education in the United States (ERIC No. ED572777). Babson Park, MA: Babson Survey Research Group. Available at: eric.ed.gov/?id=ED572777. **11. Association** for Talent Development Research. (2017). Next Generation E-Learning: Skills and Strategies (Product Code 191706). Alexandria,VA: ATD Research. **12. Artamoshchenko, V. S.** (2021). Development of the military education system. Development of a program document of the Cabinet of Ministers of Ukraine. Nauka i oborona, 4, 26–33. **13. Farid, S., Ahmad, R., & Alam, M.** (2015). A hierarchical model for e-learning implementation challenges using AHP. Malaysian Journal of Computer Science, 28(3), 166–188. **14. Roscoe, R. D., Branaghan, R., Cooke, N. J., & Craig, S. D.** (2017). Human systems engineering and educational technology. In R. D. Roscoe, S. D. Craig & I. Douglas (Eds.), End-user considerations in educational technology design. New York: IGI Global, 1–34. **15. Sohoni, S., Craig, S. D. & Vedula, K.** (2017). A blueprint for an ecosystem for supporting high quality education for engineering. Journal of Engineering Education Transformation, 30(4), 58–66**. 16. Cooke, N. J. & Hilton, M. L.** (2015). Enhancing the effectiveness of team science. Washington, D.C.: National Academies Press. **17. Sae Schatz and her colleagues** have dubbed this integrated approach «Industrial Knowledge Design» and outline it in an article, see: Schatz, S., Berking, P., & Raybourn, E. M. (2017). Industrial knowledge design: an approach for designing information artefacts. Theoretical Issues in Ergonomics Science, 18(6), 501–518. **18. Johnson-Freese, J.** (2012) The reform of military education: Twenty-five years later (ADA570086). Philadelphia, PA: Foreign Policy Research Inst. apps.dtic.mil/docs/citations/ADA570086. **19. Serovajsky, S.** (2021). Mathematical modeling. Chapman and Hall/CRC; 1st edition, 442. **20. Walcutt, J. J. & Schatz, S.** (Eds.). (2019). Modernizing Learning: Building the Future Learning Ecosystem. Washington, DC: Government Publishing Office. License: Creative Commons Attribution CC BY 4.0 IGO, 405. **21. Montemayor, C.** (2017). The Problem of the Base and the Nature of Information. Jornal of Consciousness Studies, 24, 91–102. **22. Ball, B., Nagle, F., Votsis, I.** (2020). Editorial: Computationalism Meets the Philosophy of Information. Review of Philosophy and Psychology, 507-515. **23. Syrotenko, A. M.** (2020). Theory and practice of distance learning in the Armed Forces of Ukraine. Part 1: Basics of using distance learning technologies in the educational process of higher military educational institutions and military educationa units of higher education institutions : educational method manual, 220. **24. Bellman, R.** (2017). Classic Papers in Control Theory. Dover Publications, 208. **25. Rosen, K.** Discrete Mathematics and Its Applications – Mc Graw Hill Education (UK); 8th edition. – 2000. – 2018 p. **26. Salkutsan, S. M.** (2017). Organization and use of distance learning technologies in the Armed Forces of Ukraine. Educational method manual, 124.

DOI:**10.33099/2311-7249/2023-46-1-133-140**

УДК: 358.1

***Олексій Миколайович Загорка*** *(доктор військових наук, професор)*
***Сергій Васильович Поліщук*** *(кандидат військових наук)*
***Ірина Олексіївна Загорка***
***Наталія Миколаївна Фреган***

***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# НЕЧІТКО-МНОЖИННИЙ ПІДХІД ДО ОЦІНЮВАННЯ РИЗИКУ НЕВИКОНАННЯ ЗАВДАНЬ УГРУПОВАННЯМ ВІЙСЬК (СИЛ) В ОБОРОНІ

*Під час планування операцій (бойових дій) органами військового управління проводиться оцінювання ефективності застосування військ (сил) в операції та визначаються очікувані втрати протидіючих сторін. Проте аналіз існуючих підходів дозволив зробити висновок, що оцінювання ефективності застосування військ під час ведення бойових дій зазвичай здійснюється за фіксованих напрямків ударів та складу сил і засобів противника, а також без урахування ризику невиконання завдань угрупованням своїх військ (сил) в операції (бойових діях). Для підвищення обґрунтованості прийнятих органами військового управління рішень під час планування операцій (бойових дій) необхідно враховувати ці чинники. У статті наведено методичний підхід для оцінювання ризику невиконання завдань угрупованням власних військ (сил) в обороні в умовах невизначеності складу сил і засобів противника та напрямків завдання його ударів. Запропоновано нечітко-множинний підхід, в якому використовуються функції приналежності трикутного типу співвідношення сил і засобів протидіючих сторін, імовірності виконання завдань противником та ступені використання противником напрямків ударів. Функція приналежності співвідношення сил і засобів сторін з використанням наведених у статті аналітичних залежностей трансформується в функцію приналежності імовірності виконання завдань противником. Під час оцінювання ризику на можливому напрямку завдання удару противником визначається центр ваги нечіткого числа функцій приналежності, добутку функцій приналежності імовірності виконання завдань і ступеня використання напрямків ударів противником. Для визначення центру ваги приведена аналітична залежність. Ризик невиконання завдань угрупованням військ (сил), що обороняється, визначається як ступінь наближення центру ваги нечіткого числа добутку цих функцій приналежності до імовірності виконання завдань противником. Визначення інтегрального ризику невиконання завдань угрупованням військ (сил) в обороні здійснюється шляхом адитивного згортання ризиків на напрямках завдання ударів з урахуванням їх важливості. Застосування розробленого підходу показано на прикладі.*

***Ключові слова****: нечітко-множинний підхід; функція приналежності; центр ваги нечіткого числа; ризик.*

## Вступ

**Постановка проблеми.** Планування органами військового управління (далі – ОВУ) операцій (бойових дій) здійснюється в умовах часткової невизначеності як способів бойових дій противника, зокрема, напрямків завдання ударів у наступу, так і бойового складу його угруповання військ (сил). Під час планування ОВУ оцінюється ефективність застосування угруповання військ (сил), яка зазвичай характеризується втратами в операції (під час ведення бойових дій) військ (сил) протидіючих сторін, що є не зовсім достатнім для прийняття обґрунтованих рішень. Для підвищення обґрунтованості прийняття рішень доцільно додатково враховувати ризик невиконання завдань угрупованням військ (сил) в операції (під час ведення бойових дій), оцінювання якого потребує використання відповідних методичних положень.

**Аналіз останніх досліджень і публікацій.** На теперішній час у багатьох наукових працях розглянуті питання оцінювання ефективності застосування угруповань військ (сил) в операціях (під час ведення бойових дій).

У працях [1; 2] для оцінювання втрат протидіючих угруповань військ (сил) залежно від початкового співвідношення бойової могутності сил і засобів сторін використовується відомий закон Осіпова-Лачестера. У праці [3] для визначення кількісно-якісного співвідношення сил і засобів протидіючих сторін обґрунтована можливість використання замість бойової могутності бойових потенціалів угруповань військ (сил).

Застосування системи диференційних рівнянь Колмогорова в моделі загальновійськового бою

для визначення імовірностей перебування протидіючих підрозділів у боєздатному стані, стані вогневої протидії противнику, небоєздатному стані наведено у працях [4; 5]. Відзначається, що агрегуючи подібні моделі, можна синтезувати моделі вищестоячих рівнів, тобто моделі загальновійськових частин, з'єднань, об'єднань. Проте, у наведених [1–5] та інших працях оцінювання ефективності застосування військ під час ведення бойових дій здійснюється за фіксованих напрямків ударів та складу сил і засобів противника, невизначеність яких доцільно враховувати під час прийняття рішень ОВУ.

Тому **метою статті** є розроблення методичного підходу до визначення ризику невиконання завдань угрупованням військ (сил) в обороні з урахуванням невизначеності напрямків завдання ударів та складу сил і засобів противника.

## Виклад основного матеріалу дослідження

Ризик невиконання завдань угрупованням військ (сил) в обороні залежить від можливостей щодо виконання завдань військами противника. За аналогією праці [6] ризик можна оцінювати через імовірність виконання завдань військами противника у наступі. Зазвичай, імовірність виконання оборонних $P_o$ і наступальних $P_н$ завдань угрупованнями військ визначається залежно від кількісно-якісного співвідношення сил і засобів протидіючих сторін, яке оцінюється з використанням їх бойових потенціалів або бойової могутності [2]. Залежності імовірностей $P_o, P_н$ від співвідношення сил і засобів $C$ отримується шляхом узагальнення результатів моделювання операцій (бойових дій). Для оперативного рівня застосування військ характер змінювання таких залежностей показано на рис. 1.

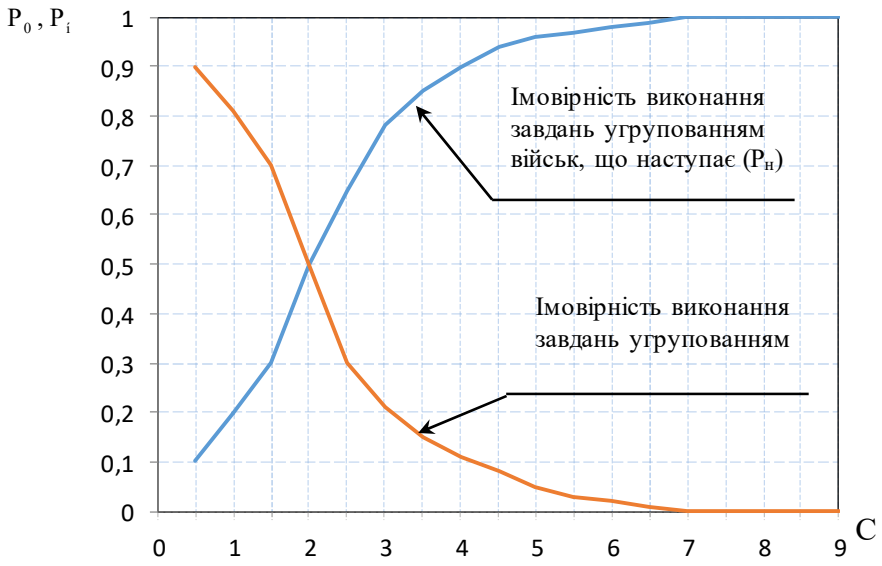



Рис. 1. Характер змінювання залежностей імовірностей виконання завдань угрупованнями військ, що обороняються і наступають від співвідношення сил та засобів протиборчих сторін

За умов співвідношення сил і засобів $C = 2$ імовірності становлять $P_o = P_н = 0{,}5$. За попередніми дослідженнями встановлено, що характер змінювання імовірностей $P_o, P_н$ від співвідношення $C$ для стратегічного і тактичного рівнів застосування військ залишається як показано на рис. 1. Але для стратегічного рівня застосування військ залежності будуть переміщатися ліворуч паралельно осі абсцис, для тактичного рівня – праворуч.

Для апроксимації змінювання імовірності $P_н$ від співвідношення сил і засобів протидіючих сторін $C$ на оперативному рівні їх застосування доцільно використати такі аналітичні залежності:

$$\begin{aligned} P_н &= a_1 e^{b_1 C} \text{ при } 0{,}5 \le C \le 2; \\ P_н &= b_2 C - a_2 \text{ при } 2 \le C \le 3; \\ P_н &= 1 - a_3 e^{-b_3 C} \text{ при } C > 3, \end{aligned} \qquad (1)$$

де $a_1, a_2, a_3, b_1, b_2, b_3$ – коефіцієнти апроксимації.

Коли напрямки завдання ударів та склад сил і засобів військ противника відомі, ризик невиконання завдань угрупованням військ в обороні визначається імовірністю $P_н$, яка розраховується за виразом (1). В умовах невизначеності напрямків завдання ударів, складу сил і засобів противника на цих напрямках для визначення ризику невиконання завдань угрупованням військ (сил) в обороні доцільно використовувати нечітко-множинний підхід.

Терми, які утворюють функції приналежності ступеня використання противником напрямків завдання ударів по військах, що обороняються, і співвідношення сил і засобів сторін на цих напрямках, визначаються експертами. Використовуються трикутні типи функцій приналежності, які більш зручні для їх формування експертами.

Для кожного напрямку завдання ударів експерти визначають трикутні нечіткі числа, які характеризують мінімальне ($C_{min}$), середнє ($C_{сер}$), максимальне ($C_{max}$) співвідношення сил і засобів сторін. За таких умов:

$$C_{сер} = \frac{C_{min} + C_{max}}{2}. \quad (2)$$

Таким чином утворюються трикутні функції приналежності $\mu(C)$ співвідношення сил і засобів сторін. Далі, за значеннями співвідношень $C_{min}, C_{сер}, C_{max}$ з використанням виразу (1) розраховуються відповідні імовірності $P_н^{min}, P_н^{сер}, P_н^{max}$ виконання завдань стороною, що наступає. Співвідношення сил і засобів протидіючих сторін С для розрахунку проміжних значень імовірності $P_н$ за заданими рівнями функції приналежності $\mu(C)$ визначаються виразами:

$$C = C_{min} + \mu(C)(C_{сер} - C_{min}) \text{ при } C_{min} < C_{сер};$$
$$C = C_{сер} + [1 - \mu(C)](C_{max} - C_{сер}) \text{ при } C_{сер} \le C_{max}. \quad (3)$$

Таким чином функція приналежності співвідношення сил і засобів протидіючих сторін $\mu(C)$ трансформується у функцію приналежності імовірності виконання завдань військами (силами) противника у наступу $\xi(P_н)$. Значення функції $\xi(P_н)$ визначає ступінь приналежності результату оцінювання імовірності $Р_i$ до діапазону її змінювання (нечіткій множині). Вигляд функції приналежності $\xi(P_i)$, визначеною за виразом (1) для $C_{min} = 1, C_{max} = 2$ і коефіцієнтів $a_1 = 0{,}0833, b_1 = 0{,}9$, наведено на рис. 2.

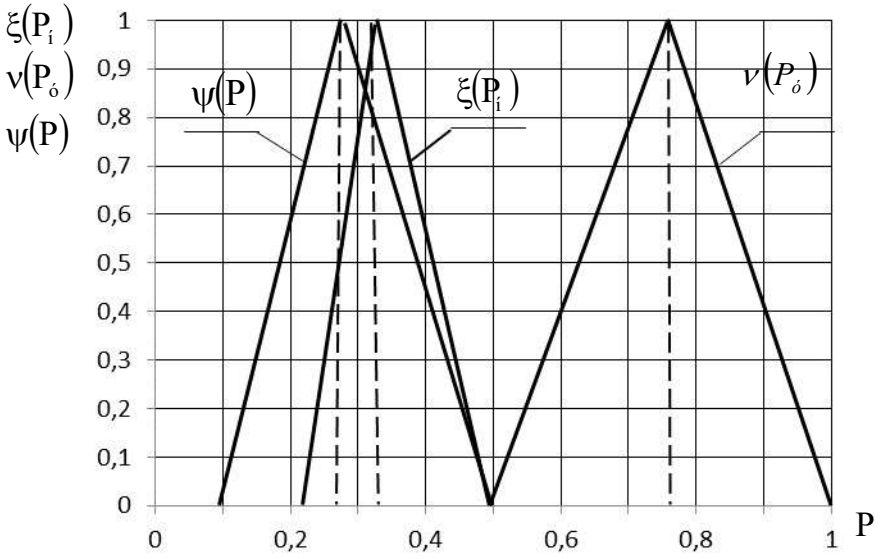



Рис. 2. Вигляд функції приналежності $\xi(P_н), \nu(P_y), \psi(P)$

Отримані імовірності виконання завдань стороною, що наступає, становлять: $P_н^{min} = 0{,}206, P_н^{сер} = 0{,}323, P_н^{max} = 0{,}500$. За нечіткого оцінювання ступеня використання противником напрямків удару розглядаються як терми п'яти лінгвістичних змінних: дуже низький (ДН); низький (Н); середній (С); високий (В); дуже високий (ДВ). Для представлення лінгвістичних змінних використовуються лінгвістичні терми. Трикутні нечіткі числа термів відповідають: ДН (0; 0; 0,25); Н (0; 0,25; 0,50); С (0,25; 0,50; 0,75); В (0,50; 0,75; 1,00); ДВ (0,75; 1,00; 1,00). Вигляд функції приналежності ступеня використання противником напрямку удару $\nu(P_y)$ для терму В показано на рис. 2.

Імовірність виконання завдань угрупованням військ (сил) в обороні визначається за виразом:

$$P_o = 1 - P_н. \quad (4)$$

За умов відомого співвідношення сил і засобів сторін, ризиком невиконання завдань угрупованням військ (сил) в обороні можна вважати імовірність виконання завдань військами противника у наступу. За невизначеності напрямків удару та складу сил і засобів військ противника необхідно під час оцінювання ризику враховувати добуток функцій приналежності $\xi(P_н)\,\nu(P_y)$. Трикутні нечіткі числа функції приналежності $\psi(P)$ добутку цих функцій

визначаються виразами:

$$P^{min} = P_н^{min}P_y^{min}; P^{cep} = P_н^{cep}P_y^{cep}; P^{max} = P_н^{max}P_y^{max}, \quad (5)$$

де $P_y^{min}, P_y^{cep}, P_y^{max}$ – трикутні нечіткі числа функції приналежності $\nu(P_y)$.

Для прикладу на рис. 2 $P^{min} = 0{,}103; P^{cep} = 0{,}242; P^{max} = 0{,}500$ .

Трикутні нечіткі числа функції приналежності $\psi(P)$ визначаються експертами для кожного $k$ - го напрямку удару противника ($k = \overline{1,K}$), що розглядаються.

У ході оцінювання ризику невиконання завдань угрупованням військ (сил) в обороні під час завдання противником удару з $k$ - го напрямку доцільно використовувати центр ваги $q_k$ нечіткого числа функції приналежності $\psi_k(P)$ [8]. Центр ваги нечіткого числа поділяє площу, яка утворюється функцією приналежності, на рівні частини. Для функції приналежності трикутного типу це дозволяє отримати квадратне рівняння:

$$2q_k^2 - 4P_k^{max}q_k + P_k^{max}\left(P_k^{min} + P_k^{cep} + P_k^{max}\right) - P_k^{min}P_k^{cep} = 0. \quad (6)$$

$$q_k = P_k^{max} - \frac{\sqrt{16P_k^{max2} - 8\left(P_k^{max}\left(P_k^{min} + P_k^{cep} + P_k^{max}\right) - P_k^{min}P_k^{cep}\right)}}{4}. \quad (7)$$

З рис. 1 та залежності (4) випливає, що імовірності виконання завдань угрупованням військ в обороні не менше заданої $P_o^{зад}$ повинна відповідати імовірність виконання завдань військами противника не більше допустимої $P_н^{доп}$. Тому ризик невиконання завдань угрупованням військ (сил) в обороні можна характеризувати ступенем наближення центра ваги нечіткого числа $q_k$ до імовірності $P_н^{доп}$. Звідси для k- го напрямку удару військ противника ризик визначається за формулою

$$R_k = \frac{q_k - P_н^{доп}}{P_н^{доп}}. \quad (8)$$

За $q_k = P_н^{доп}$ ризик $R_k = 0$. На рис. 3 наведена ризик-функція $R_k = f(q_k)$, що має додатну та від'ємну ділянки.

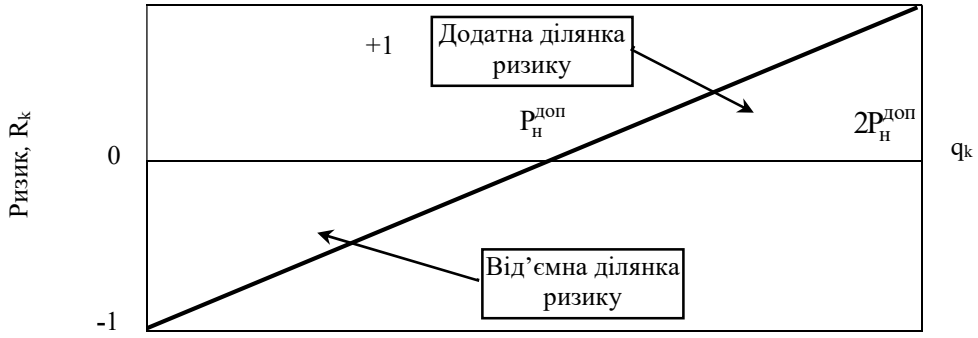



Рис. 3. Ризик-функція $R_k = f(q_k)$.

Від'ємний ризик ($q_k < P_н^{доп}$) характеризує упевненість виконання, а додатний ($q_k > P_н^{доп}$) – небезпечність невиконання завдань угрупованням військ в обороні. Для оцінювання інтегрального ризику невиконання завдань угрупованням військ (сил) в обороні необхідно визначити важливість можливих напрямків ударів військ противника. Для цього може бути використаний експертний метод ранжирування [9; 10]. За використання цього методу експерти повинні розташувати напрямки у порядку їх важливості і приписати кожному з них числа натурального ряду. Найбільш важливому напрямку надається перший ранг, а найменш важливому – останній. Коефіцієнт, який характеризує вплив застосування військ противника на $k$ - му напрямку на виконання завдань угрупованням військ (сил), визначається виразом [10]:

$$S_{kn} = 1 - \frac{r_{kn} - 1}{K}; \; k = \overline{1,K}; \; n = \overline{1,N}, \quad (9)$$

де $r_{kn}$ – ранг, наданий n - м експертом $k$ - му напрямку удару військ противника;

N – кількість експертів.

Для отримання коефіцієнтів важливості напрямків удару n - м експертом коефіцієнти $S_{kn}$ нормуються виразом:

$$\omega_{kn} = \frac{S_{kn}}{\sum_k S_{kn}}; \sum_k \omega_{kn} = 1. \quad (10)$$

Коли компетентність експертів однакова, коефіцієнти важливості напрямків удару визначаються за формулою:

$$\omega_k = \frac{1}{N}\sum_n \omega_{kn}; \sum_k \omega_k = 1. \quad (11)$$

Коли компетентність n - го експерта оцінюється певним коефіцієнтом $\xi_n, \sum_n \xi_n = 1$, то

$$\omega_k = \sum_n \xi_n \omega_{kn}. \quad (12)$$

Інтегральний ризик виконання завдань

угрупованням військ (сил) в обороні визначається за формулою

$$R = \sum_k \omega_k R_k, k = \overline{1,K}. \qquad (13)$$

Структурна схема методичного підходу до оцінювання ризику невиконання завдань угрупованням військ (сил) в обороні наведено на рис. 4.

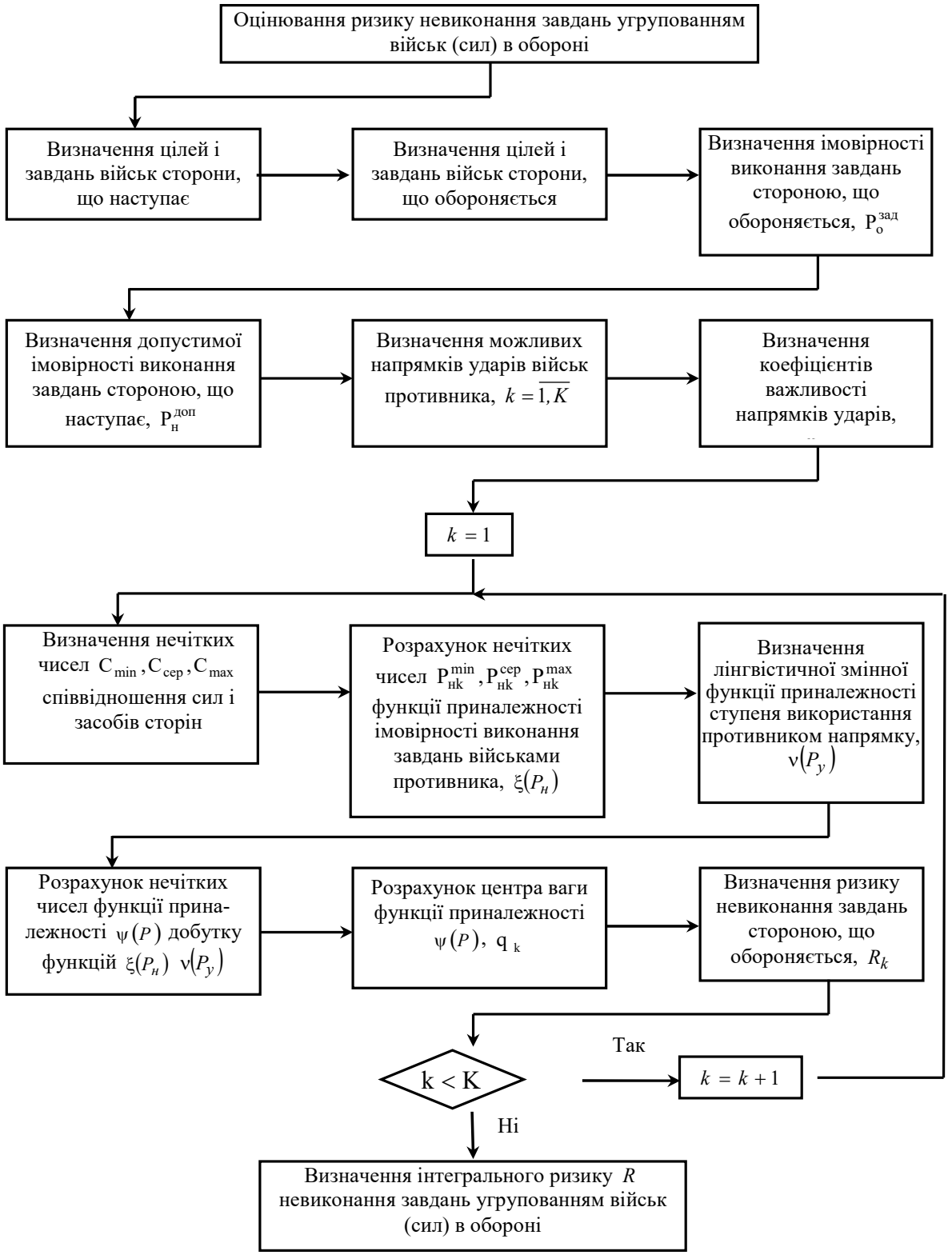



Рис. 4. Структурна схема методичного підходу до оцінювання ризику невиконання завдань угрупованням військ (сил) в обороні

Для прийняття рішень ОВУ під час планування операцій (бойових дій) необхідно мати відповідні

критерії ризику. За умов створення критеріальної шкали ризиків доцільно використовувати лінгвістичні змінні (з урахуванням їх рівнозначущості), які застосовувалися раніше під час визначення експертами функцій приналежності. Шкала критеріальних інтервалів ризиків приведена у табл. 1.

Критерії визначаються для інтегрального R і часткових $R_k$ ризиків. Коли отримується середній додатній ризик, доцільно підсилювати угруповання військ (сил). Середній від'ємний ризик характеризує наявність певного надлишку сил і засобів для виконання угрупованням військ (сил) оборонних завдань. Застосування розробленого методичного підходу розглянуто для визначення ризику невиконання завдань угрупованням військ (сил) в обороні за можливих дій військ противника з п'яти напрямків.

Таблиця 1

Критеріальні інтервали ризиків

| Ділянка ризик-функції | Характеристика ризику | Нечіткі терми | | | | |
|---|---|---|---|---|---|---|
| | | Дуже низька | Низька | Середня | Висока | Дуже висока |
| Додатна | небезпека невиконання завдань | 0 – 0,19 | 0,20 – 0,39 | 0,40 – 0,59 | 0,6, – 0,79 | ≥ 0,8, |
| Від'ємна | упевненість виконання завдань | 0 – (– 0,19) | (– 0,19) – (– 0,39) | (– 0,40) – (– 0,59) | (– 0,60) – (– 0,79) | (– 0,80) – (– 1,00) |

Розрахунки приведені для заданої імовірності $P_{зад} = 0,7$, що відповідає допустимій імовірності $P_н^{доп} = 0,3$. У табл. 2 приведені трикутні нечіткі числа функцій приналежності співвідношення сил і засобів сторін $\mu(C)$, імовірності виконання завдань стороною, що наступає $\xi(P_i)$, ступеня використання військами противника напрямків удару $\nu(P_y)$.

Таблиця 2

Трикутні нечіткі числа функцій приналежності $\mu(C), \xi(P_н), \nu(P_y)$

| Напрямок удару, k | Функції приналежності | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | $\mu(C)$ | | | $\xi(P_i)$ | | | $\nu(P_ó)$ | | |
| | $C_{mink}$ | $C_{cepk}$ | $C_{maxk}$ | $P_{нk}^{min}$ | $P_{нk}^{cep}$ | $P_{нk}^{max}$ | $P_{ók}^{min}$ | $P_{yk}^{cep}$ | $P_{yk}^{max}$ |
| 1 | 2,5 | 2,75 | 3,00 | 0,65 | 0,73 | 0,77 | 0,75 | 1,00 | 1,00 |
| 2 | 1,5 | 1,75 | 2,00 | 0,30 | 0,39 | 0,50 | 0 | 0,25 | 0,50 |
| 3 | 2,25 | 2,50 | 2,75 | 0,60 | 0,65 | 0,73 | 0,50 | 0,75 | 1,00 |
| 4 | 2,00 | 2,25 | 2,50 | 0,50 | 0,60 | 0,65 | 0,25 | 0,50 | 0,75 |
| 5 | 1,00 | 1,25 | 1,50 | 0,20 | 0,24 | 0,30 | 0 | 0 | 0,25 |

Трикутні нечіткі числа функції приналежності імовірності виконання завдань противником $P_{нk}^{min}, P_{нk}^{cep}, P_{yk}^{max}$ визначені на підставі залежності, що показана на рис. 1.

Результати розрахунків ризиків невиконання завдань угрупованням військ (сил) в обороні наведено у табл. 3.

Таблиця 3

Ризики невиконання завдань угрупованням військ (сил) в обороні

| Напрямок удару, *k* | Коефіцієнт важливості напрямку, $\omega_k$ | Трикутні числа функції приналежності, $\psi(P)$ | | | Центр ваги нечіткого числа функції приналежності, $\psi(P)$, $q_k$ | Ризик невиконання оборонних завдань на напрямку, $R_k$ | Інтегральний ризик невиконання завдань, $R_k$ |
|---|---|---|---|---|---|---|---|
| | | $P_k^{min}$ | $P_k^{cep}$ | $P_k^{max}$ | | | |
| 1 | 0,33 | 0,49 | 0,73 | 0,77 | 0,69 | 1,30 | 0,45 |
| 2 | 0,12 | 0 | 0,07 | 0,25 | 0,10 | - 0,66 | |
| 3 | 0,28 | 0,30 | 0,49 | 0,73 | 0,50 | 0,68 | |
| 4 | 0,17 | 0,12 | 0,30 | 0,49 | 0,30 | 0,01 | |
| 5 | 0,10 | 0 | 0 | 0,07 | 0,02 | - 0,93 | |

Відповідно до шкали критеріальних інтервалів (табл. 1) інтегральний ризик невиконання завдань угрупованням військ (сил) в обороні вважається за середній, що потребує його підсилення. Найбільш небезпечним є перший напрямок, який вважається і найбільш важливим. Дуже високий від'ємний ризик на п'ятому напрямку обумовлює можливість передислокації частини сил і засобів для підсилення угруповання військ (сил), що повинне відбивати удар з першого напрямку. Через те, має забезпечуватися зниження інтегрального ризику невиконання оборонних завдань угрупованням військ (сил).

Таким чином на прикладі показана доцільність урахування ОВУ ризиків невиконання оборонних завдань угрупованням військ (сил) під час планування операцій (бойових дій).

## Висновки й перспективи подальших досліджень

Вироблення рішення на застосування угруповання військ (сил) в обороні, зазвичай, здійснюється в умовах часткової невизначеності складу сил і засобів противника та напрямків завдання його ударів, що обумовлює доцільність урахування ОВУ у ході планування операцій (бойових дій) не тільки ефективності, а й ризиків невиконання завдань. Для оцінювання ризиків застосовується нечітко-множинний підхід, використовуються лінгвістичні змінні, що описуються трикутними функціями приналежності. Під час оцінювання ризику на можливому напрямку завдання удару противником визначається центр ваги нечіткого числа добутку функцій приналежності імовірності виконання завдань і ступеня використання напрямку удару противником. Ризик невиконання завдань угрупованням військ (сил), що обороняється, визначається як ступінь наближення центру ваги нечіткого числа добутку цих функцій приналежності до імовірності виконання завдань противником. Інтегрований ризик визначається як адаптивна згортка ризиків на напрямках завдання ударів противником із врахуванням їх важливості.

## *Література*

**1. Загорка О. М., Павліковський А. К., Корецький А. А., Кириченко С. О., Загорка І. О.** Теоретичні основи управління угрупованнями військ (сил) у сучасних умовах збройної боротьби: монографія / за заг. ред. І. С. Руснака. Київ : НУОУ ім. Івана Черняховського, 2020. 248 с. **2. Рябчук В. Д.** Элементы военной системологии применительно к решению проблем оперативного искусства и тактики общевойсковых объединений, соединений и частей: Военно-теоретический труд. Москва : Академия им. М.В. Фрунзе, 1995. 228 с. **3. Загорка О.М., Поліщук С.В., Загорка І.О.** Методичні положення прогнозування втрат протидіючих сторін у загальновійськовій операції (бою). *Наука і оборона*. 2020. № 1. С. 52–57. **4. Булойчик В. М., Скрипко Д. М.** Моделирование боя мотострілкового подразделения. *Наука и военная безопасность*. 2005. № 5. С. 27–29. **5. Пермяков О. Ю., Сбітнєв А. І.** Інформаційні технології і сучасна збройна боротьба. Луганськ : Знання, 2008. 204 с. **6. Кириченко І. О., Наливайко Ю. В.** Війна і математика: Елементи теорії складних бойових систем. Харків : Академія ВВ МВС України, 2012. 260 с. **7. Герасимов Б. М., Локазюк В. М., Оксіюк О. Г., Поморова О. В.** Інтелектуальні системи підтримки прийняття рішень: Навч. посібник. Київ : Вид-во Європ. ун-ту, 2007. 335 с. **8. Свешников С. В., Бочарников В. П.** Основы нечеткой технологии и примеры решения аналитических задач в государстве и бизнесе. Москва : ДМК Пресс, 2014. 408 с. **9. Бешелев С. Д., Гурвич Ф. Г.** Математико-статистические методы экспертных оценок. Москва : Статистика, 1974. 160 с. **10. Денисов А. А., Колесников Д. Н.** Теория больших систем управления: учебное пособие для вузов. Ленинград : Энергоиздат, 1982. 288 с.

## FUZZY-MULTIPLE APPROACH TO ASSESSING THE RISK OF FAILURE TO ACCOMPLISH TASKS BY GROUPS OF TROOPS (FORCES) IN DEFENSE

***Oleksii Zahorka*** ***(Doctor of Military Sciences, Professor)***
***Serhii Polishchuk*** ***(Candidate of Military Sciences)***
***Iryna Zahorka***
***Natalia Fregan***

***National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine***

*During the planning of combat operations, the military management bodies evaluate the expected effectiveness of the troop's usage in the operation and determine the expected losses of the opposing parties. However, the analysis of the existing approaches made it possible to conclude that the assessment of the expected effectiveness of the troop's usage during combat operations is usually carried out with fixed directions of strikes and the composition of the enemy's forces and means. Also they do not take into account the risk of non-fulfillment of tasks by the grouping of own troops in operations. In order to increase the validity of the decisions made by the military management bodies during the planning of operations, it is necessary to take into account the partial uncertainty of the enemy's forces and means and the expected direction of their strikes, as*

*well as the risk of failure to fulfill tasks by the grouping of own troops in the operation. The article provides a methodical approach for assessing the risk of non-fulfillment of tasks by the grouping of own troops in defense in conditions of uncertainty about the composition of the enemy's forces and means and the directions of their strikes. A fuzzy-multiple approach is proposed, which uses the affiliation functions of the triangular type of the forces and resources ratio of the opposing sides, the probability of the enemy's tasks performance, and the degree of the enemy's use of the direction of strikes. The affiliation function of the forces and resources ratio of the parties using the analytical dependencies given in the article is transformed into the affiliation function of the probability of the enemy's tasks performance. When assessing the risk on a possible direction of an enemy's strike, the center of gravity of a fuzzy number of affiliation functions, the product of the affiliation functions, the probability of completing tasks, and the degree of enemy's usage of strike directions are determined. An analytical dependence is given to determine the center of gravity. The risk of non-fulfillment of tasks by a defending group of troops is defined as the degree of approximation of the center of gravity of the fuzzy number of the product of these affiliation functions to the probability of the completing tasks by the enemy. Determination of the integral risk of non-fulfillment of tasks by the grouping of troops in defense is carried out by additively collapsing the risks in the directions of the strike, taking into account their importance. The application of the developed approach is shown on an example.*

***Keywords:*** *fuzzy set approach; membership function; center of gravity of a fuzzy number; risk.*

## *References*

**1. Zagorka, O.M., Pavlikovsky, A. K., Koretskyi, A. A., Kyrychenko, S. O., Zagorka, I. O.** (2020). Theoretical foundations of the management of groups of troops (forces) in modern conditions of armed struggle: a monograph / in general ed. I. S. Rusnak. Kiyv : NUOU named after Ivan Chernyakhovskyi, 248. **2. Ryabchuk, V. D.** (1995). Elements of military systemology applied to solving problems of operational art and tactics of combined forces, formations and units: Military-theoretical work. Moskva : Academy named after M. V. Frunze, 228. **3. Zagorka, O. M., Polishchuk. S. V., Zagorka, I. O.** (2020). Methodical provisions for forecasting the losses of opposing parties in a combined military operation (battle). Science and defense, 1, 52–57. **4. Buloychik, V. M., Skrypko, D. M.** (2005). Modeling the battle of a motorized rifle unit. Science and military security. 5. 27–29. **5. Permyakov, O. Yu., Sbitnev, A. I.** (2008). Information technologies and modern armed struggle. Luhansk : Znannia, 204. **6. Kirichenko, I. O., Nalivayko, Yu. V.** (2012). War and mathematics: Elements of the theory of complex combat systems. Kharkiv : Academy of the Armed Forces of the Ministry of Internal Affairs of Ukraine, 260. **7. Gerasimov, B. M., Lokaziuk, V. M., Oksiyuk, O. G., Pomorova, O. V.** (2007). Intelligent decision support systems: Education. manual. Kiyv : View of Europe. University, 335. **8. Sveshnikov, S. V., Bocharnikov, V. P.** (2014). Basics of fuzzy technology and examples of solving analytical problems in government and business. Moskva: DMK Press, 408. **9. Beshelev, S. D., Gurvych, F. G.** (1974). Mathematical and statistical methods of expert evaluations. Moskva : Statistics, 160. **10. Denisov, A. A., Kolesnikov, D. N.** (1982). The theory of large control systems: A textbook for universities. Leningrad : Energoizdat, 288.

DOI:**10.33099/2311-7249/2023-46-1-141-144**

УДК 355.02: 396

***Сергій В'ячеславович Заболотний***
***Віталій Олександрович Кацалап*** *(кандидат військових наук, доцент)*

***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ СИСТЕМ МОНІТОРИНГУ ІНФОРМАЦІЙНОГО ПРОСТОРУ В ІНТЕРЕСАХ ВІЙСЬК (СИЛ)

*У статті розглянуто питання обґрунтування інформаційної технології забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил). Основна увага досліджень зосереджена на побудові варіантів системи моніторингу інформаційного простору. Формалізовано інформаційну технологію забезпечення функціональної стійкості та визначено підходи щодо методів її оцінювання. Наведено актуальність та перспективність процесу представлення формалізованої інформаційної технології забезпечення функціональної стійкості для подальшої автоматизації процесу класифікації систем моніторингу інформаційного простору в інтересах військ (сил). Метою статті є обґрунтування інформаційної технології забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил). Запропоновано інформаційну технологію забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил), що може вважатися методичним підходом для оцінювання доцільних варіантів системи моніторингу інформаційного простору. Визначається, що поєднання методів оптимізації аналізу варіантів побудови систем моніторингу інформаційного простору дозволяє визначити та оцінити порядок роботи особи, яка приймає рішення на побудову відповідної системи моніторингу інформаційного простору. Це у подальшому дає можливість розробити архітектуру спеціалізованого програмного забезпечення для підвищення оперативності оцінки інформаційних ресурсів, що циркулюють у системах моніторингу інформаційного простору. Використання інформаційної технології забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил) дозволяє орієнтовно визначити складові моніторингу інформаційного простору та провести деталізацію систем, які до нього входять. Наведені результати наукового дослідження підтверджують адекватність застосування інформаційної технології для забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил).*

***Ключові слова***: *інформаційна технологія; моніторинг; інформаційний простір; оцінювання інформації; інформаційний ресурс; функціональна стійкість систем моніторингу інформаційного простору в інтересах військ (сил).*

## Вступ

Ведення сучасних операцій військами (силами) пов'язане з масованим дублюванням інформації. Тому, цілком очевидно, що основне спрямування систем моніторингу інформаційного простору є створення конкретного виду інформаційного ресурсу із національного інформаційного простору та інформаційного простору противника для формування командної інформації на пунктах управління.

**Постановка проблеми.** Побудова будь-якої системи моніторингу визначається реальною потребою, що стосується функціональної стійкості, зокрема систем моніторингу інформаційного простору. Як свідчить широкомасштабна збройна агресія рф проти України забезпечення функціональної стійкості є очевидною та актуальним питанням для військ (сил). Одночасно слід зазначити, що виважений підхід до забезпечення функціональної стійкості систем моніторингу інформаційного простору потребує обґрунтування основних складових цього процесу:

формування вимог до системи;
побудова системи з урахуванням вимог;
технічна реалізація (створення) системи;
впровадження та освоєння системи.

Зазначені складові інформаційної технології забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил), є багатоелементним та потребують комплексного моделювання. Найбільш проблемними для отримання рішення є складові формування вимог до функціональної стійкості, оскільки тут закладається функціонально-технічна сутність системи відповідно до умов дослідження. Інші складові побудови системи мають ієрархічний характер відносно вищеназваних. Тому в складі

науково-методичної бази підтримки рішень з питань забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ, найбільш відповідальною є та її частина, яка забезпечує формування вимог до системи та їх побудови. З цієї причини, подальші дослідження будуть зосереджені у напрямі наукового забезпечення реалізації зазначених складових забезпечення функціональної стійкості систем моніторингу інформаційного простору. Виходячи з потреби з'ясування існуючого рівня такого наукового забезпечення, розглянемо відомі підходи до вирішення завдань формування вимог до забезпечення функціональної стійкості інформаційних систем моніторингу інформаційного простору в інтересах військ (сил).

**Аналіз остатніх досліджень і публікацій.** З метою дослідження питань, присвячених проблемам забезпечення функціональної стійкості систем моніторингу інформаційного простору, було оглянуто і проаналізовано [1–6]. У [1; 3; 4] вимога – правило або умова, обов'язкові для виконання. Вимогами до об'єкта стають його обґрунтовані очікувані характеристики, як відображення визначальних властивостей об'єкта, що затверджені встановленим порядком і є обов'язковими до виконання об'єктом у визначених умовах застосування. В дослідженні [2; 5] затверджені вимоги, також нормативно визначено фундаментальні характеристики будь-якої системи, які необхідно використовувати під час їх побудови та розвитку. У методології [6] визначено, що завдання синтезу до різноманітних об'єктів військового призначення є постійним для органів військового управління, оскільки, по-перше, безперервна динаміка зміни умов збройної боротьби вимагає повсякденного та адекватного розвитку (удосконалення) наявних сил та засобів, а по-друге, ці органи є замовниками та фундаторами військових об'єктів. Тому, з практичної точки зору, це завдання є завжди актуальним для органів військового управління Збройних Сил України.

**Метою статті** є обґрунтування інформаційної технології забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил).

## Виклад основного матеріалу дослідження

Системи моніторингу інформаційного простору, що функціонують в інтересах військ (сил) мають свою специфіку стосовно багатоелементності їх функціонування із розгалуженою структурою, які поєднують у собі велику кількість рознесених на значній території технічних засобів розвідки. Головне завдання цих систем полягає у формування інформації на основний командний пункт (пункт управління) Збройних Сил України та створення інформаційних ресурсів із національного інформаційного простору й інформаційного простору противника з відповідним інформаційним забезпеченням бойової діяльності угруповань військ, які можуть бути різного рівня – від оперативно-тактичних до стратегічних. Тому рівень задач систем моніторингу інформаційного простору також знаходиться в цьому діапазоні. Це значить, що залежно від рівня задач, які повинна виконувати така система, до неї можуть бути висунуті системні, тобто оперативно-тактичні, оперативні, оперативно-стратегічні або навіть стратегічні вимоги (коли інформацією забезпечуються одночасні дії військ (сил) в межах усієї держави), а до її елементів – тактико-технічні вимоги.

Завдання формування вимог до інформаційних систем моніторингу інформаційного простору об'єктивно та коректно може бути вирішене органом військового управління лише на основі визначення очікуваних характеристик таких систем, що потребує застосування спеціально розробленого науково-методичного апарату та проведення кількісних розрахунків для належного обґрунтування таких характеристик.

Розглянемо існуючий рівень розроблення теми формування системних вимог в інтересах військ (сил), підкресливши при цьому, що у світовій науковій практиці поза межами України, така тема фактично не розглядалася. Враховуючи потребу застосування загального теоретичного підходу, з метою подальшого розв`язання поставленої проблеми, більш детально розкриємо базове поняття «обрис інформаційної технології забезпечення функціональної стійкості систем моніторингу інформаційного простору», які формують, узагальнюють та зберігають інформаційні ресурси в інтересах військ (сил). Крім цього, для вирішення поставленої проблеми, поряд із визначенням поняття «обрис систем моніторингу інформаційного простору», необхідно також описати його зв'язок із характеристиками систем, які, за функціональністю, використовуються для моніторингу інформаційного простору.

Оскільки раніше зазначено, що обрис інформаційних систем моніторингу інформаційного простору формується в єдиному процесі обґрунтування вимог до забезпечення функціональної стійкості, тому визначимо схему формування вимог до інформаційних систем (рис. 1).

Адекватність наведеного порядку на рис. 1, підтверджує і загальносвітова практика формування вимог будь-якого змісту інформації в складних інформаційних системах за потреби їх створення. Зокрема, в роботі [5], зазначається, що головним фактором, який перешкоджає чіткому формулюванню вимог є недостатній рівень розуміння замовником того, що він дійсно хотів би отримати від системи, яка розробляється. Тому, для розуміння цього пропонуємо замовнику бути співучасником проєктування системи та здійснювати, спільно з її розробником, коригування початкових вимог на основі поточного аналізу проміжних рішень у процесі створення системи, тобто тоді, коли проєктувальником отримуються її

певні аналоги або добре зрозумілі рішення. Цю ідею також підтримує методологія структурного аналізу та проєктування систем SSADM (Structured System Analisis and Design Method), яка з 1993 року є загальнонаціональним стандартом Великобританії і вважається однією із найбільш передових серед європейських методологій у сфері проєктування складних інформаційно-керуючих систем [6].

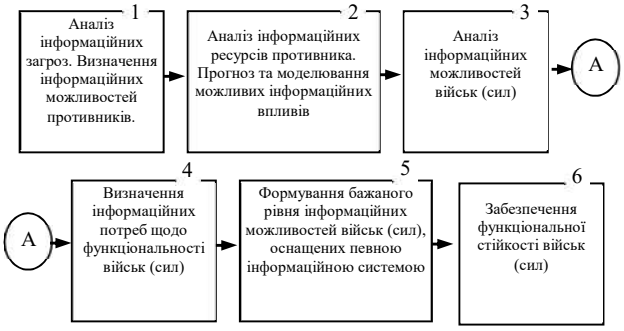



Рис. 1. Порядок формування вимог для забезпечення функціональної стійкості систем моніторингу інформаційного простору

Вищезазначене вказує на те, що знання очікуваного технічного обрису системи моніторингу інформаційного простору, і як наслідок, можливість отримання прогнозованих характеристик якості та вартості, невід'ємно поєднане з формуванням вимог до неї для очікуваних умов застосування. Сформульований головний методичний принцип, однозначно підводить до висновку, що на етапі формування вимог до систем моніторингу інформаційного простору, знаходження компромісу між вартістю системи та її майбутніми характеристиками якості, що визначають прогнозовану ефективність, може бути досягнуто лише у поєднанні з прогнозуванням технічного обрису (складу і структури) та показників ефективності систем моніторингу інформаційного простору, що еквівалентно потребі їх побудові.

Отже, під час реалізації процесу обґрунтування інформаційної технології забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил) за умови фінансових обмежень на їх побудову, визначаються їх функціональне призначення, склад та структура, показники ефективності. За таких умов, функціональними вимогами до систем слід вважати їх показники за призначенням, а нефункціональними вимогами – показники ефективності та вартості, які визначають загальну ефективність систем моніторингу інформаційного простору.

Таким чином, обґрунтування інформаційної технології забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил) можна описати як сукупність, що включає їх очікувані функціональні і нефункціональні вимоги та характеристики для очікуваних умов застосування.

## Висновки та перспективи подальших досліджень

Таким чином, наведене обґрунтування інформаційної технології забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил), на відміну від існуючих, враховує як функціональну, так і нефункціональну характеристики стійкості. Наведене поєднання дозволить обґрунтувати підходи щодо оцінювання очікуваних характеристик якості, що визначають ефективність систем моніторингу інформаційного простору, а саме:

обґрунтування переліку показників ефективності систем;

обґрунтування методичної схеми оцінювання очікуваних показників ефективності систем;

розробка моделі врахування критичних факторів (відсутність елементів інформаційної інфраструктури, які формують інформаційні ресурси).

Зазначимо також, що забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил), за умов вартісних (фінансових) обмежень, є принциповим питання для розвитку Збройних Сил України.

Розробка *прикладних моделей* для обґрунтування обрису інформаційної технології забезпечення функціональної стійкості систем моніторингу інформаційного простору в інтересах військ (сил) на основі розробленої загальної теоретичної бази буде напрямом подальших досліджень у цій сфері.

## *Література*

**1**. **Купрієнко Д. А., Боровик О. В.** Структурний синтез динамічних систем із квазілінійним і часовим розподіленням компонентів: монографія. Хмельницький : Видавництво НАДПСУ, 2015. 348 с. **2. Korobiichuk R., Hryshchuk V. Katsalap P. Snitsarenko P.** Determination and Evaluation of Negative Informational and Psychological Influence on the Military Personnel Based on the Quantitative Measure 1st International Workshop on Control. *Optimisation and Analytical Processing of Social Networks*. COAPSN 2019; Lviv; Ukraine; 16–17 May 2019. P. 66–78. **3**. **Pysarchuk O., Lagodnyi O., Mikhieiev Y.** Statistical Analysis of the Thematic Content on the Internet for Predicting the Development of Information Treats. *Traektoria Nauki = Path of Science.* 2017. Vol. 3. № 8. P. 3011–3019. DOI: 10.22178/pos.25-2. **4**. **Snitsarenko P., Vakonechnyi V., Mikhieiev Y., Sayko V., Hrytsiuk V.** The approach to automated internet monitoring system creation. *2019 IEEE International Conference on Advanced Trends in Information Theory*. December 2019. P. 257–261. URL: https://ieeexplore.ieee.org/document/9030446 DOI:10.1109/ATIT49449.2019.9030446 (дата звернення;14.12.2022). **5**. **Shixiang Zh., Heejin J., Green P. A.** How Consistent Are the Best-Known Readability Equations in Estimating the Readability of

Design Standards? IEEE Trans. Prof. Commun. 2017. №60(1). P. 97–111. URL: https://ieeexplore.ieee.org/document/7839917 (дата звернення;14.12.2022). **6. Coleman M. and Liau T. L.** A computer readability formula designed for machine scoring, Journal of Applied Psychology. 1975. Vol. 60. P. 283–284. URL: https://content.apa.org/record/1975-22007-001 (дата звернення;14.12.2022)..

## INFORMATION TECHNOLOGY FOR ENSURING FUNCTIONAL SUSTAINABILITY OF INFORMATION SPACE MONITORING SYSTEMS IN THE INTERESTS OF TROOPS (FORCES)

**Ser*hii Zabolotnyi***
***Vitaliy Katsalap*** ***(Candidate of Military Sciences, assistant professor)***

***National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine***

*The article examines the substantiation of information technology for ensuring the functional stability of information space monitoring systems in the interests of troops (forces). The main focus of research is on the construction of variants of the information space monitoring system. The information technology for ensuring functional sustainability has been formalized and the approaches to its evaluation methods have been determined. The relevance and perspective of the process of formalized presentation of information technology for ensuring functional stability for further automation of the process of classification of information space monitoring systems in the interests of troops (forces) are presented. The purpose of the article is to justify the information technology for ensuring the functional stability of information space monitoring systems in the interests of troops (forces). The proposed information technology for ensuring the functional stability of information space monitoring systems in the interests of troops (forces) is a methodical step for evaluating expedient options for the information space monitoring system. It is determined that the combination of methods of optimizing the analysis of options for building information space monitoring systems allows to determine and evaluate the work order of the person who makes the decision to build the appropriate information space monitoring system. The use of information technology for ensuring the functional stability of information space monitoring systems in the interests of troops (forces) makes it possible to tentatively determine the components of information space monitoring and to detail the systems included in it. The presented results of the scientific research confirm the usage adequacy of information technology for ensuring the functional stability of information space monitoring systems in the interests of troops (forces).*

***Keywords:*** *methodological information technology, monitoring, information space, information evaluation, information resource, functional stability of information space monitoring systems in the interests of troops (forces).*

## *References*

**1**. **Kuprienko, D. A., Borovik, O. V.** (2015). Structural synthesis of dynamic systems with quasi-linear and time distribution of components: monograph. Khmelnytskyi : NADPSU Publishing House, 348. **2**. **Korobiichuk, R. Hryshchuk, V. Katsalap, P. Snitsarenko, P.** (2019). Determination and Evaluation of Negative Informational and Psychological Influence on the Military Personnel Based on the Quantitative Measure 1st International Workshop on Control, Optimisation and Analytical Processing of Social Networks, COAPSN 2019; Lviv; Ukraine; 16–17 May 2019, 66–78. **3**. **Pysarchuk, O. Lagodnyi, O., Mikhieiev, Y.** (2017). Statistical Analysis of the Thematic Content on the Internet for Predicting the Development of Information Treats. Traektoria Nauki = Path of Science, 3, 8, 3011–3019. URL: http://pathofscience.org/index.php/ps/article/view/376. DOI: 10.22178/pos.25-2. **4**. **Snitsarenko, P., Vakonechnyi, V., Mikhieiev, Y., Sayko, V., Hrytsiuk, V.** (2019). The approach to automated internet monitoring system creation. 2019 IEEE International Conference on Advanced Trends in Information Theory. December 2019, 257–261,. https://ieeexplore.ieee.org/document/9030446 DOI:10.1109/ATIT49449.2019.9030446. **5**. **Shixiang, Zh., Heejin, J., Green, P. A.** (2017). How Consistent Are the Best-Known Readability Equations in Estimating the Readability of Design Standards? IEEE Trans. Prof. Commun, 60(1), 97–111. URL: https://ieeexplore.ieee.org/document/7839917.
**6. Coleman, M. and Liau, T. L.** (1975). A computer readability formula designed for machine scoring, Journal of Applied Psychology, 60, 283–284. URL: https://content.apa.org/record/1975-22007-001.

DOI:**10.33099/2311-7249/2023-46-1-145-150**

УДК 355.4:004.056:159.9

***Сергій Васильович Базарний***

***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

# МЕТОД ВИЯВЛЕННЯ АГЕНТІВ СОЦІАЛЬНИХ МЕРЕЖ, ЩО МАЮТЬ НАЙБІЛЬШИЙ ВПЛИВ

*У статті розроблений метод виявлення агентів соціальних мереж, що мають найбільший вплив на визначену цільову аудиторію, який поєднує дані про кількість публікацій за визначеною тематикою і кількість зв'язків агентів у соціальній мережі. Комплексний показник, що описаний у методі, характеризує потенційну кількість актів доведення інформаційних матеріалів від агента соціальної мережі, що має найбільший вплив, до інших агентів соціальної мережі, що мають з ним зв'язки. Метод складається з п'яти етапів і може бути корисним для фахівців під час аналізу впливу агентів соціальних мереж на цільові аудиторії у ході проведення психологічної операції. За допомогою пошукової системи «SOFIYA» були досліджені множини агентів соціальної мережі, що мають найбільший вплив, які розповсюджують інформаційні матеріали за двома визначеними тематиками. Також була проведена класифікація агентів соціальної мережі, що мають найбільший вплив, за видом їх мережевої активності та визначено їх ролі як постер, репостер, коментатор і той, що робить вподобання.*

***Ключові слова:*** *соціальні мережі; цільові аудиторії; психологічна операція; агенти соціальних мереж; пошукова система.*

## Вступ

За останні кілька років соціальні мережі (далі – СМ) значно змінили наш спосіб спілкування та обміну інформацією. Нині вони стали потужним інструментом впливу на громадську думку та поведінку людей. Більшість молодих людей, які потрапили у злочинне середовище, суїцидальні спільноти, різні протестні, екстремістські та терористичні рухи, залучаються до них за допомогою СМ [1]. Вплив на користувачів (агентів) СМ розглядається як психологічний вплив внаслідок розповсюдження інформаційних матеріалів (тематик), інформація про які має бути розміщена в соціальних мережах серед максимальної кількості агентів СМ та посилена численними коментарями, обговореннями і вподобаннями широкої аудиторії СМ. За цими діями стоять конкретні агенти, які виконують певні ролі. Ідентифікація ролей даних агентів дозволить виявити їх структуру та мережу. Аналіз патернів поведінки таких структур за різними інформаційними приводами (тематиками) дозволить:

виявляти закономірності, що з'являються у ході проведення інформаційних дій;

встановлювати ознаки цілеспрямованого впливу;

прогнозувати поведінку структур у процесі виникнення інформаційних акцій;

блокувати їх ключові вузли для протидії поширенню їхнього впливу.

Таким чином, з метою підтримки прийняття рішень під час протидії цілеспрямованим деструктивним впливам на користувачів СМ актуальним науковим завданням є розробка ефективних методів ідентифікації ролей агентів СМ та рівня їх впливу, а також програмного забезпечення для автоматизації даного процесу.

**Постановка проблеми.** Найбільший деструктивний вплив здійснюють агенти СМ, що мають найбільший вплив. Існуючі методики, що використовуються для їх ідентифікації, не враховують деякі суттєві характеристики, зокрема, роль агентів СМ, через те, що фахівцям доводиться обробляти значну кількість профілів і витрачати багато часу на встановлення агентів, які підлягають моніторингу чи впливу.

**Аналіз останніх досліджень і публікацій.** Дослідженнями соціальних мереж, з огляду на розробку методів виявлення агентів СМ, які мають найбільший вплив, та їх ролей у мережах, активно працюють науковці з університетів та наукових центрів США, Канади, Великобританії, Німеччини, Італії та України. Серед них можна виокремити таких вчених, як Maksym Gabielkov, який досліджує методи взаємодії та споживання інформації агентами соціальних мереж [2]. Проте автор не вирішує задачу фільтрації та персоналізації контенту, що може призвести до зменшення різноманітності інформації, що споживається агентами. Крім того, він, зазвичай, використовує дані з Twitter, що обмежує

універсальність його висновків та можливість застосування їх до інших соціальних мереж. Автор Emilio Ferrara досліджує вплив соціальних ботів на поширення низькодостовірного контенту в Twitter [3], але він не враховує можливості впливу реальних користувачів на поширення такого контенту. Також, автор не досліджує питання того, чому агенти СМ віддають перевагу контенту, який має низький рівень достовірності та не бере до уваги можливості боротьби з цим явищем з боку платформ соціальних мереж. Kristina Lerman у своїй науковій праці [4] досліджує методи автоматизованої фільтрації соціальної інформації та виявлення впливових агентів у соціальних мережах. Однак, вона не враховує можливість використання фальсифікованих акаунтів і соціальних ботів, що можуть змінювати результати аналізу та впливати на думки агентів СМ. Також не враховується можливість використання соціальних мереж для поширення небажаної інформації, такої як фейкові новини та дезінформація. Врахування цих факторів дозволить покращити результати аналізу та ефективність фільтрації соціальної інформації. Кравець В. у науковій праці [5] розкриває моделювання соціальних мереж з використанням мультиагентних технологій. Автор досліджує способи моделювання взаємодії агентів у СМ, але не розглядає застосування методів машинного навчання та аналізу тексту для виявлення агентів у соціальних мережах, що мають найбільший вплив. Вчені Іващенко О. А. та Лавріщева О. В. не враховують можливість виникнення фальшивих або некоректних зв'язків між агентами СМ [6]. Крім того, їхні методи не передбачають можливості врахування динаміки зміни впливовості агентів СМ з урахуванням часових показників. Дослідження вчених Музики О. М., Турянської О. В. присвячені моделюванню процесів психологічного впливу на агентів СМ [7]. Автори враховують такі фактори, як кількість друзів, кількість публікацій, активність агентів СМ. Проте у цих дослідженнях не розглядається зміна вищезазначених показників, а також не враховуються особливості цільових аудиторій (далі – ЦА).

**Метою статті** є розробка методу для виявлення агентів СМ, що мають найбільший вплив, з урахуванням ролей агентів СМ та визначення рівня їх впливу на ЦА з метою покращення ефективності проведення психологічних операцій.

## Виклад основного матеріалу дослідження

Досвід широкомасштабної збройної агресії рф проти України свідчить, що однією з основних умов перемоги над агресором є завоювання переваги в інформаційному просторі. Інформаційний простір та інформаційні ресурси, які його наповнюють, сьогодні є важливим інструментом, що впливає на ведення бойових дій. Для здійснення впливу на емоційний стан, мотивацію, раціональне мислення ЦА противника, і з метою зміни моделей їх поведінки у спосіб, що сприятиме застосуванню військ (сил) Збройних Сил України, проводяться психологічні операції (далі – ПсО).

В межах ПсО здійснюються психологічні акції, під час яких розробляються інформаційні матеріали, причому найбільш ефективними з них є ті, що спрямовані на висвітлення суперечностей між офіційною точкою зору військово-політичного керівництва держави та поглядами і настроями ЦА противника. [8] В умовах широкомасштабної збройної агресії російської федерації проти України, влада рф обмежила доступ своїх громадян до частини інформаційних ресурсів (СМ «Фейсбук», «Інстаграм», європейських та світових засобів масової інформації (далі – ЗМІ) та ін.), і більшість ЦА рф отримують інформацію лише з державних ЗМІ.

Прикладом кінцевої ЦА можуть бути громадяни рф, які підлягають мобілізації для направлення до району проведення так званої «СВО», причому психологічний вплив на ці ЦА доцільно здійснювати через проміжні ЦА, якими є представники російської діаспори, які проживають за кордоном рф, а також через громадян рф, які виїхали після вересня 2022 року, уникаючи мобілізації.

Для проведення аналізу інформаційного простору за визначеною тематикою була застосована запропонована пошукова система (далі – ПС) «SOFIYA» [9], що написана скриптовою мовою програмування «Personal Home Page Tools» (далі – «PHP») та створена для генерації HTML-сторінок вебсервера. Ця мова є одна з найпоширеніших та являється проєктом відкритого програмного забезпечення, що використовуються у сфері веброзробок та підтримується переважною більшістю хостинг-провайдерів.

Запропонована ПС поділяється на дві складові:

index/php – скрипт пошукового запиту, який безпосередньо здійснює пошук, а саме надсилає пошукові запити;

request.php – скрипт для відображення отриманої інформації, а саме який формує у вигляді таблиці з кількістю рядків, що складають 100 одиниць по 50 слів кожної електронної адреси (сайту).

Пошук здійснюється методом контент-аналізу СМ, за визначеними search terms-пошуковими термінами (ключовими словами, що можна змінювати відповідно до поставленого завдання, або ситуації, що склалася) на інтернет-порталах противника. Відповідно використання ПС дозволяє встановити наступне:

хто є першоджерелом поширення інформації;

в який спосіб розповсюджується інформація у СМ;

агенти СМ, які сприяють розповсюдженню інформації;

агентів СМ, які мають найбільшу кількість друзів, підписників і можуть забезпечити ефективний психологічний вплив на визначену ЦА.

За допомогою ПС «SOFIYA» були виявлені агенти СМ та їх ролі, що опублікували матеріали в СМ «ВКонтакте» за тематикою "Непростое решение Суровикина" (далі – тематика 1) і "частичная мобилизация в россии" (далі – тематика 2), а саме проведення мобілізації в рф протягом 2022 року, що містять дані про кількість постів, репостів і коментарів, що опубліковані цими агентами СМ за визначними тематиками були проаналізовані методом контент-аналізу. Були виявлені ролі агентів СМ (автори, перепостери, коментатори постів), що стосуються вищезазначених тематик.

Для аналізу зв'язків агентів СМ з визначеної ЦА були зібрані дані про їх друзів і друзів їх друзів. Такий підхід обрано через те, що кількість зв'язків безпосередньо залежить від того, з ким саме пов'язаний агент СМ. За однакової кількості друзів на першому коліні, кількість друзів на другому коліні може відрізнятися на декілька порядків. Однак, подальше додавання колін в графі не є доцільним, оскільки це призводить до нівелювання різниці у кількості зв'язків.

Необхідно також враховувати обсяг обчислювальних ресурсів, потрібних для збору інформації, у процесі побудови графів та обчислення метрик центральності. З кожним додатковим коліном обчислювальна складність збільшується на декілька порядків, тому дослідження обмежимо 2-х колінним графом для економії обчислювальної можливості ПЕОМ.

Для кожної досліджуваної тематики визначимо рейтинг активності агентів СМ за кількістю матеріалів, які вони опублікували.

Аналіз даних публікаційної активності агентів СМ показав, що найбільш активні агенти не завжди мають велику кількість зв'язків, в той час як агенти з великою кількістю зв'язків, як правило, мають невисокий рівень активності.

Для обчислення рівня впливу агентів СМ розрахуємо множення кількості публікацій агента СМ на кількість його зв'язків у цій СМ, що дозволить оцінити потенційну кількість актів доведення інформації від кожного агента СМ до інших агентів. Знайдений комплексний показник характеризує потенційний рівень впливу (далі – РВ) агента СМ.

Метод виявлення агентів СМ, що мають найбільший вплив, має п'ять етапів:

1. Розрахуємо кількість зв'язків вузла СМ $p_k$ з іншими вузлами графа СМ за формулою:

$$C\left(p_k\right)=\sum_{k}^{n} a\left(p_i, p_k\right), \qquad (0)$$

де: $n$ – кількість вузлів у СМ;

$a\left(p_i, p_k\right)=1$ – якщо вузли $p_i$ та $p_k$ пов'язані між собою;

$a\left(p_i, p_k\right)=0$ – якщо вузли $p_i$ та $p_k$ не пов'язані між собою.

2. Розрахуємо кількість інформаційних матеріалів $m_k$ (рівень публікаційної активності), які були опубліковані агентом $k$ за виразом:

$$m_k = g_1 x_k + g_2 y_k + g_3 z_k + g_4 v_k, \qquad (2)$$

де: $x_k$ – кількість публікацій (постів), що опубліковані агентом $k$;

$y_k$ – кількість репостів, зроблених агентом $k$;

$z_k$ – кількість коментарів, опублікованих агентом $k$;

$v_k$ – кількість вподобань, зроблених агентом $k$;

$g_1$ – ваговий коефіцієнт важливості постів, що опубліковані агентом $k$;

$g_2$ – ваговий коефіцієнт важливості репостів, зроблених агентом $k$;

$g_3$ – ваговий коефіцієнт важливості коментарів, опублікованих агентом $k$;

$g_4$ – ваговий коефіцієнт, що враховує важливість кількості вподобань, зроблених агентом $k$.

Експертним методом визначено вагові коефіцієнти публікацій, репостів, коментарів та вподобань за силою психологічного впливу як: $g_1=1$; $g_2=0{,}3$; $g_3=0{,}1$; $g_4=0{,}01$ [10]. Але залежно від ЦА та умов проведення ПсО вагові коефіцієнти можуть бути змінені.

3. Розрахуємо РВ ($l_k$) агента СМ $k$ за виразом:

$$l_k = C\left(p_k\right) m_k. \qquad (3)$$

Комплексний показник РВ, що наведений вище, має зрозумілий сенс, але не можна стверджувати, що кожний пост, репост або коментар отримає агент СМ з ЦА. Чим вище значення РВ у агента СМ, тим більший ПсВ він має на визначену ЦА.

4. Розрахунок нормалізованого РВ агенту СМ.

Аналіз кількості зв'язків агентів СМ та кількості їх публікацій за двома визначеними тематиками показав, що ці величини змінюються у різних діапазонах. Кількість зв'язків може досягати десятків мільйонів ($10^7$), тоді як публікаційна активність обмежується сотнею публікацій ($10^2$), тобто різниця діапазонів досягає п'яти порядків. Для урахування різних діапазонів зміни вищезазначених показників, нормалізуємо кількість зв'язків і кількість публікацій за їх максимальними значеннями, для чого обчислимо нормалізований РВ за формулою:

$$l_n = \frac{C\left(p_k\right)}{p_{max}\, m_{max}} \frac{m_k}{m_{max}}. \qquad (4)$$

5. Знаходження множини агентів СМ, що мають найбільший – вплив.

Для знаходження множини агентів СМ, що мають найбільший вплив, використовуємо спосіб "половинної маси": знайдемо множину агентів СМ, сума РВ яких складає 50% сумарного РВ всіх агентів СМ, що розповсюджують визначену тематику. Для цього проведемо ранжирування агентів СМ за рівнем їх впливу.

Розраховуємо сумарний РВ $L$ всіх агентів СМ, що розповсюджують визначену тематику за формулою:

$$L = \sum_{n=1}^{N} l_n \,, \qquad (5)$$

де $N$ – загальна кількість агентів СМ.

Далі послідовно за рейтингом сумуємо РВ агентів СМ, починаючи з лідера рейтингу та порівнюємо із загальною сумою РВ усіх агентів СМ. Обрахунок зупиняємо, коли сума РВ досягає 50% від загальної суми РВ, що розрахована за формулою (5). Таким чином, знаходимо множину агентів СМ, що мають найбільший вплив.

У результаті аналізу інформаційних матеріалів за допомогою використання ПС «SOFIYA» розробленим методом виявлення агентів СМ, що мають найбільший вплив, знайдено:

за першою тематикою – 472 агентів СМ, що мають найбільший вплив (серед 4480 агентів СМ, що розповсюджують інформаційні матеріали за тематикою 1);

за другою тематикою – 345 агентів СМ, що мають найбільший вплив (серед 3310 агентів СМ, що розповсюджують інформаційні матеріали за тематикою 2).

Для підвищення наочності отриманих результатів зручно використати діаграми Венна (діаграми Ейлера-Венна), що візуально показують відношення декількох підмножин (шляхом об'єднання, перетину, різниці) між декількома (зазвичай, трьома) однієї множини [11].

На рисунку 1 показана діаграма Венна, яка була використана для аналізу 82 агентів СМ, що мають найбільший вплив та публікують пости одночасно за двома тематиками: "Непростое решение Суровикина" – 472 найбільш впливових агентів СМ та "частичная мобилизация в россии" - 345 найбільш впливових агентів СМ.

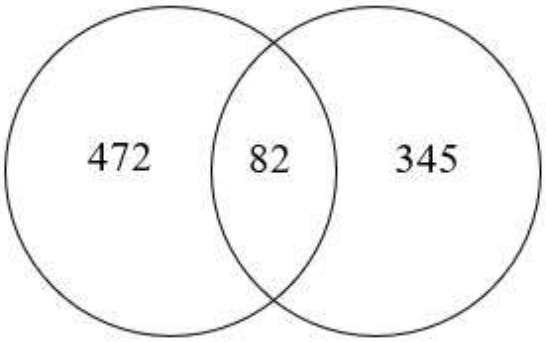



Рис. 1. Діаграма Венна, що відображає множини агентів СМ, які мають найбільший вплив та публікують пости за двома тематиками

Аналіз отриманих множин агентів СМ, що мають найбільший вплив, дозволяє провести класифікацію агентів за видом мережевої активності у СМ. У переважної більшості випадків агенти СМ проявляють мережеву активність однакового типу: або тільки публікують інформаційні матеріали, або переважно репостять їх, або коментують, або тільки роблять вподобання. Тому проведемо класифікацію агентів СМ залежно від виду їх переважної мережевої активності та визначимо їх ролі як: Постер, Репостер, Коментатор та той, що робить Вподобання, якщо переважний вид активності складає не менше 80 % від сумарної його активності.

Тоді:

якщо $x_k \geq 0{,}8m_k$ – роль агенту визначається як Постер,

якщо $y_k \geq 0{,}8m_k$ – роль агенту визначається як Репостер,

якщо $z_k \geq 0{,}8m_k$ – роль агенту визначається як Коментатор,

якщо $v_k \geq 0{,}8m_k$ – роль агенту визначається як той, що робить Вподобання.

Якщо жодна з вищезазначених нерівностей не виконується, то агенту СМ присвоюється статус Універсал, тобто агент, що не має чітко вираженої ролі мережевої активності.

Для класифікації агентів СМ за першою тематикою, що мають найбільший вплив, за аналізом статистичних даних ПС «SOFIYA», вищенаведеним способом було розраховано кількість агентів за ролями їх переважної мережевої активності. Результати розрахунків наведені на рисунку 2.

З рисунку 2 можна зробити висновок, що Постери серед агентів СМ, які мають найбільший вплив, складають приблизно тільки десяту частину загальної чисельності агентів СМ, що

досліджуються. Але це найбільш креативна частина агентів СМ, що мають найбільший вплив. Ця категорія агентів СМ відіграє ключову роль під час генерації інформаційних матеріалів і вимагає найбільшої уваги під час прогнозування розповсюдження інформаційних матеріалів у процесі планування ПсО.

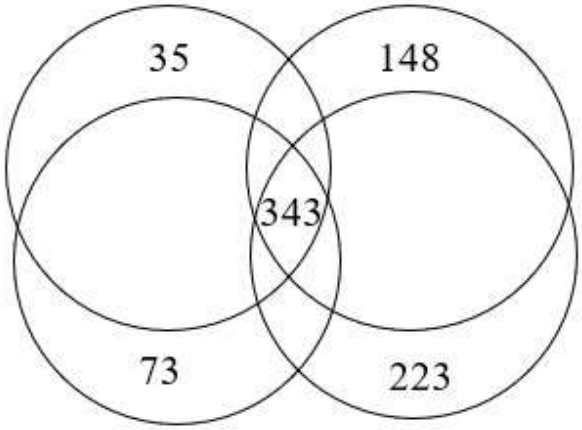



Рис. 2. Діаграма Венна, що відображає кількість агентів за ролями їх переважної мережевої активності

## Висновки та перспективи подальших досліджень

Таким чином, вперше розроблено метод виявлення агентів СМ, що мають найбільший вплив, який заснований на обчисленні потенційного рівня їх впливу на визначені ЦА та містить показники рівня публікаційної активності у СМ і кількості мережевих зв'язків агентів у СМ. Зазначений метод дає змогу підвищити ефективність проведення ПсО за рахунок збільшення ефекту від розповсюдження інформаційних матеріалів агентами СМ, що мають найбільший вплив.

За допомогою ПС «SOFIYA» були проаналізовані агенти СМ «Вконтакте», що мають найбільший вплив, які мають публікаційну активність за двома тематиками: "Непростое решение Суровикина" та "частичная мобилизация в россии".

Напрямом подальших досліджень може бути дослідження кореляції між рівнем впливу агентів, що мають найбільший вплив, та зміною поведінки їх друзів у вигляді репостів, коментарів, тих, хто робить вподобання і переглядів інформаційних матеріалів.

## *Література*

**1. The Guardian**:"How social media is helping gangs to recruit young people". URL:https://www.theguardian.com/media/2018/apr/02/social-media-violence-young-people-gangs-say-experts

**2. Gabielkov M.** "Social Clicks: What and Who Gets Read on Twitter?" URL: https://inria.hal.science/hal-01281190/document

**3. Ferrara E.** " Bots increase exposure to negative and inflammatory content in online social systems " URL: https://www.pnas.org/doi/abs/10.1073/pnas.1803470115

**4. Lerman K.** URL:https://www.researchgate.net/publication/2216262_Social_Browsing_Information_Filtering_in_Social_Media

**5. Кравець В.** "Моделювання соціальних мереж на основі агенентної парадигми".

**6. Іващенко О.А., Лавріщева О.В.** Методи виявлення впливових користувачів у соціальних мережах на основі теорії графів.

**7. Музика О.М., Турянська О.В.** Аналіз впливу користувачів у соціальних мережах на основі гібридної моделі рекомендацій та інформації про активність

**8.Кацалап В.О., Ю.В. Цурко** Планування інформаційних операцій за стандартами НАТО: навч. посіб. НУОУ ім. Івана Черняховського. С. 19–20.

**9. Базарний С.В**. Розробка пошукової системи для виявлення активних користувачів соціальних мереж. Стратегічні комунікації у сфері забезпечення Національної Безпеки та оборони:проблеми, досвід, перспективи Матер. III Міжнарод. наук.-практ. конф., м. Київ, 31 жовтня 2022 р. / НУОУ, 2022. С. 65–66.

**10. Березовський В.** Особливості аналізу впливу користувачів у соціальних мережах з використанням методу PageRank.

**11.** Навчальний посібник з дисципліни «Дискретна математика» Частина1 для студентів спеціальностей 126 «Інформаційні системи та технології» та 121 «Інженерія програмного забезпечення» / Гавриленко О.В., Клименко О.М., Рибачук Л.В. – Київ: КПІ, 2020. – 75 с.

**12. Доктрина НАТО AJP-3.10** "Allied Joint Doctrine for Information Operations", December 2015 (Chapter 1).

**13. Прібилєв Ю.Б., Базарний С.В**. Спосіб визначення місцезнаходження користувачів соціальних мереж. Забезпечення кібероборони держави. Зб. матер. III науково-практичного вебінару, м. Київ, 29 вересня 2022 р. НУОУ, 2022. С. 150–160.

**14. Базарний С.В.** Розроблення комплексного методу виявлення найбільш впливових користувачів соціальних мереж в сучасних умовах. Стратегія кіберстійкості: управління ризиками та безперервність бізнесу. Матер. Всеукр. наук.-практ. конф., м. Київ, 23 лютого 2023 р. ДУТ, 2023. С. 69–72.

.

# METHOD FOR IDENTIFYING SOCIAL NETWORK AGENTS WITH THE GREATEST INFLUENCE

*Serhii Vasyliovych Bazarnyi*

*National Defence University of Ukraine named after Ivan Cherniakhovsky, Kyiv, Ukraine*

*The article presents a method for identifying social network agents that have the greatest impact on a given target audience. The method combines data on the number of publications on a specific topic and the number of connections between agents in the social network. The comprehensive indicator described in the method characterizes the potential number of acts of disseminating information from the social network agent with the greatest influence to other agents in the social network who have connections with them. The method consists of five stages and can be useful for professionals in analyzing the impact of social network agents on target audiences during psychological operations. Using the search system «SOFIYA», sets of social network agents that have the greatest impact were investigated, and who disseminate informational materials on two specified topics. Additionally, social network agents with the greatest impact were classified according to the type of their network activity, and their roles as posters, re-posters, commenters, and likers were determined.*

***Key Keywords:*** *social networks; target audiences; psychological operations; social network agents; search system.*

## *References*

**1**. **The Guardian**: "How social media is helping gangs to recruit young people." Article on the website about how social media is helping gangs recruit young people. URL: https://www.theguardian.com/society/2019/mar/22/how-social-media-is-helping-gangs-to-recruit-young-people

**2**. **Maksym Gabielkov** "Social Clicks: What and Who Gets Read on Twitter?" URL: https://dl.acm.org/doi/10.1145/2740908.2742763

**3**. **Emilio Ferrara** "The spread of low-credibility content by social bots" URL: https://science.sciencemag.org/content/359/6380/1146

**4**. **Kristina Lerman** "Social Information Filtering: Algorithms for Automating "Word of Mouth"" - article in the ACM Communications journal: URL: https://dl.acm.org/doi/10.1145/358916.358995

**5**. **Kravets V.** "Modeling Social Networks Based on the Agent Paradigm" URL: https://ieeexplore.ieee.org/document/7234271

**6**. **Ivashchenko O.A.**, **Lavrishcheva O.V.** Methods for detecting influential users in social networks based on graph theory. URL: https://www.researchgate.net/publication/315904045_Metodi_viyavlennya_vplivovikh_koristuvachiv_u_sotsialnikh_merezhakh_na_osnovi_teorii_grafiv

**7**. **Music O.M.**, **Turyanska O.V.** Analysis of social media users' influence based on a hybrid model of recommendations and activity information. URL: https://www.researchgate.net/publication/324618469_Analiz_vplivu_koristuvachiv_u_sotsialnikh_merezhakh_na_osnovi_gibridnoyi_modeli_rekomendatsiy_ta_informatsiyi_pro_aktivnist

**8**. **Katsalap V.O.** Planning of information operations according to NATO standards: a textbook. / V.O.Katsalap, Yu.V.Tsurko: NUOU named after Ivan Chernyakhovsky, p.19-20.

**9**. **Bazarnyi S.V.** Development of a search system for detecting active users of social networks. Proceedings of the III International Scientific and Practical Conference, October 31, 2022, Kyiv. – K.: NUOU, 2022, p. 65-66.

**10**. Berezovskyi V. Features of analyzing the influence of users in social networks using the PageRank method. URL: http://nbuv.gov.ua/UJRN/ictlt_2017_3_17

**11**. "Math is Fun": URL: https://www.mathsisfun.com/sets/venndiagrams.html.

**12**. NATO Doctrine AJP-3.10 "Allied Joint Doctrine for Information Operations", December 2015 (Chapter 1).

**13**. Pribilyev Yu.B., Bazarnyi S.V. Method of determining the location of social media users. Collection of materials of the III scientific and practical webinar, September 29, 2022, Kyiv. – K.: NUOU, 2022, p. 150-160.

**14**. Bazarnyi S. Development of a comprehensive method for identifying the most influential users of social networks in modern conditions. Materials of the All-Ukrainian Scientific and Practical Conference, Kyiv. – DUT, February 23, 2023, p. 69-72.

# *Шановні колеги!*

*Запрошуємо до участі в науковому журналі*
***“Сучасні інформаційні технології у сфері безпеки та оборони”***,
Видавець: Національний університет оборони України імені Івана Черняховського.
Наказом Міністерства освіти і науки України №409 від 17.03.2020 р. та №886 від 02.07.2020 р.
журнал включено до Переліку наукових фахових видань України категорії “Б” в галузях
“технічні науки” та “військові науки”, спеціальності – 122, 124, 253, 255
Наклад – 100 примірників, відкрите видання.

***Основні тематичні напрями журналу:***

1. Військова кібернетика та системний аналіз.
2. Протиборство у кібернетичному просторі.
3. Військово-космічні та геоінформаційні технології.
4. Інтелектуальні інформаційні технології та робототехніка у сфері безпеки та оборони.
5. Інформаційно-аналітична діяльність у сфері безпеки та оборони.
6. Розвиток теорії та практики створення інформаційно-телекомунікаційних систем.
7. Стратегічні комунікації та когнітивні системи спеціального призначення
8. Інтерактивні моделі розвитку науково-освітнього простору;
9. Високотехнологічні аспекти воєнного мистецтва
10. Історичний дискурс розвитку високих оборонних технологій

## Схема оформлення статей

**DOI** (*Arial*, *кегль – **11** пт.*)

⟵ *1 пустий рядок – **6** пт.*

**УДК** (*Arial*, *кегль – **11** пт.*)

⟵ *1 пустий рядок – **10** пт.*

*[1]**Анатолій Анатолійович Іванов** **(д-р техн. наук, професор)***
*[2]**Іван Іванович Петров** **(канд. техн. наук, доцент, доцент кафедри)***

⟵ *(кегль – **11** та **8** пт.)*

⟵ *1 пустий рядок – **6** пт.*

*[1]**Університет…, Київ, Україна***
*[2]**Інститут…, Київ, Україна***

⟵ *(кегль – **11** пт.)*

⟵ *1 пустий рядок – **10** пт.*

**НАЗВА СТАТТІ** (*Arial, кегль – **14** пт.; накреслення – “напівжирне”, по правому краю)*

⟵ *1 пустий рядок – **10** пт.*

*Анотація друкується мовою тексту статті (в даному випадку – українською). Зміст анотації має стисло і достатньо інформативно підсумовувати основні ідеї та отримані результати дослідження. Анотацію рекомендовано подавати, орієнтуючись на умови міжнародно визнаного формату «IMRAD», за такими структурними елементами: мета (завдання) статті; методи дослідження; елементи наукової новизни; результати дослідження; практична значущість. Розмір анотації повинен становити не менше 250 слів. Зверніть увагу на те, що дані про авторів, назва, ключові слова та анотація будуть використані як метадані для опису Вашої статті, тому вони повинні максимально чітко описувати її зміст. Для більш якісного пошуку даного контенту в мережі, будь-ласка, уникайте занадто узагальнених та складних формулювань, використовуйте тільки загальновідомі абревіатури.* ***(Обсяг анотації – не менше 250 слів.)***

***Ключові слова:*** *поняття1; поняття 2; поняття3 – до 8. Рекомендовано подавати від 3-х до 8-ми ключових слів та словосполучень* (*кегль – **10** пт.*)

## Вимоги до набору

**Формат аркуша:** А4 (21 × 29,7 см).

**Параметри сторінки** (відступи від краю): зліва – 3 см.; справа – 2 см.; зверху – 2 см.; знизу – 2 см.

**Шрифт статті** – *Times New Roman*; накреслення – пряме; кегль – 10 пт.; міжрядковий інтервал – одинарний.

**Текст статті** розташовується у два стовпчики однакової ширини – 7,75 см.; відстань між стовпчиками – 0,5 см.; відступ першого рядка абзацу – 0,5 см.; вирівнювання – за шириною.

**Підзаголовок** – кегль – 12 пт.; накреслення – напівжирне; відступів немає; вирівнювання – центроване.

*Не використовуйте для форматування тексту пропуски, табуляцію тощо. Не встановлюйте ручне перенесення слів, не використовуйте колонтитули. Між значенням величини та одиницею її вимірювання ставте нерозривний пропуск (Ctrl + Shift + пропуск).*

***УВАГА! Остання сторінка статті заповнюється не менше 3/4, рекомендована парна кількість аркушів.***

***Кількість авторів – не більше трьох.***

**Набір формул:** редактор формул *MS Equation*.

**Забороняється** використовувати для набору формул графічні об'єкти, кадри й таблиці.

В меню “*Размер* → *Определить*” ввести такі розміри:
Обычный – 10 пт.; Крупный индекс – 8 пт.;
Мелкий индекс – 7 пт.; Крупный символ – 15 пт.;
Мелкий символ – 9 пт.

Стиль формул – “прямий”, тобто в меню “*Стиль* → *Определить*” поля “Формат символов” – пусті.

Табличний заголовок (10 пт.) – **обов’язковий**.

Рисунки **обов’язково** супроводжуються центрованими підрисунковими підписами (кегль – 10).

**Не допускаються** кольорові та фонові рисунки.

Допускається розташування великих рисунків, формул та таблиць в одну колонку (до 16 см.).

Список літератури виділяється підзаголовком “***Література***”та оформлюється згідно з міждержавним стандартом ДСТУ 8302:2015 ”(кегль – 9 пт.).

## Структура рукопису

Відповідно до постанови ВАК України від 15.01.2003 № 7-05/1 текст статті повинен мати таку структуру: ***постановка проблеми*** *у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями*; ***аналіз останніх досліджень і публікацій***, *на які спирається автор*; ***формулювання мети статті*** (*постановка завдання*); ***виклад основного матеріалу*** *дослідження з повним обґрунтуванням отриманих наукових результатів*; ***висновки*** *з наукової роботи і перспективи подальших досліджень даного напряму*.

Текст статті розбивається на відповідні розділи з підзаголовками, які виділені напівжирним шрифтом.

Робочі мови – українська, англійська.

На останньому аркуші статті після списку літератури наводяться: назва статті, прізвище, ім'я, по батькові, науковий ступінь та вчене звання автора (співавторів), назва організації, у якій працює автор (співавтори), анотація та ключові слова українською, російською та англійською мовами (крім основної мови статті) за нижченаведеним зразком (10 кегль (8 для наукового ступеня, звання, посади), міжрядковий інтервал – 1,0, вирівнювання – по центру).

**ARTICLE TITLE**

[1]***Anatolii Ivanov*** ***(Doctor of technical sciences, professor)***
[2]***Ivan Petrov*** ***(Candidate of technical Sciences, associate professor)***

[1]***University…, Kyiv, Ukraine***
[2]***Institute…, Kyiv, Ukraine***

*Translation of the abstract and keywords*

Після цього наводиться список літератури англійською мовою, що оформлюється за міжнародним бібліографічним стандартом «Harvard» за зразком (9 кегль):

## *References*

**1. Hryshchuk, R. V. and Danik, Y. G.,** (2016). *Fundamentals of cyber security*: a monograph. Zhytomyr: ZHNAEU. **2. Kucherenko, N. P.,** (2016). Treasury business: in 6 volumes. Kyiv : Pravo,. T. 3 : Kontrol' u systemi Derzhavnoho kaznachejstva. **3. Pavlyk, I. M.,** (2007). Intellectual property rights. *Velykyj entsyklopedychnyj iurydychnyj slovnyk* / za red. Yu. S. Shemshuchenka. 2-he vyd., pererob. i dop. Kyiv : Yuryd. dumka, 683. **4. Hrytsiuk, Y. I.,** (2016). Cyber Intervention and Cybersecurity in Ukraine: Problems and Prospects for Overcoming Them. *Naukovyj visnyk NLTU Ukrainy*. 26, 8. **5. Vakulenko, O. V., Nikolaienko, B. A.,** (2019). *Broadband radio relay station SRS-5000 (radio relay station R-402): a study guide*. Kyiv : ISZZI KPI im. Ihoria Sikors'koho, [online]. Available at: https://ela.kpi.ua/bitstream/123456789/50387/1/SRSh-5000.pdf [Accessed : 15 February 2023]. **6. Krzystofowicz, R., Long, D.,** (1990). Fusion of Detection Probabilities and Comparison of Multisensor Systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. 20(3), 665–677. DOI: 10.1109/21.57281. **7. *Sony SRS-RA5000 audio system*** [online], (2023). *E-katalog*. Available at: https://core.ac.uk/download/pdf/80561473.pdf [Accessed : 14 December 2022]. **8. Levchuk, S. A.,** (2002). *Green's matrices of equations and systems of elliptic type for the study of static deformation of composite bodies*. PhD. 01.02.04. Zaporiz'kyj derzh. un-t. **9. Petruk, L. A.,** (2004). *Study of static deformation of composite bodies*. Avtoref. dys…. Doctor of sciences. 01.02.04. NU «L'vivs'ka politekhnika». **10. Tsekhmistrov, I. I., Perets', I. P.,** (2016). About the budget. In: *Doslidzhennia problem v Ukraini ochyma molodykh vchenykh*: *materialy Mizhnar. nauk.-prakt. konf. Zaporizhzhia, Ukraina, 3-4 bereznia 2016.* Zaporizhzhia: NU «Zaporiz'ka politekhnika». **11. *Broadband radio relay station SRS,*** (2019). Vynakhidnyk: A. O. Varuschak. 13 chervnia. Podanyj: 3 hrudnia 2018. Ukraina. Pat. 142. **12. Zakon Ukrainy**, (2014). *About education* [online], № 1556-VII, 1 July. Available at: http://zakon2.rada.gov.ua/laws/show/1556-18. [Accessed 15 November 2022]. **13. Derzhspozhyvstandart Ukrainy,** (2005). *Water quality. Glossary of terms. Part 1* DSTU ISO 6107-1:2004. Kyiv: Vyd. ofits.

**Корисні посилання для здійснення транслітерації:**

**http://translit.kh.ua/?passport –** автоматична транслітерація з української мови
**http://translate.meta.ua/ua/translit/** – автоматична транслітерація з російської мови

**На окремому аркуші наводяться відомості про авторів**.

**Автор***:* Прізвище, ім'я та по-батькові; посада; вчена ступінь та вчене звання; адреса електронної поштової скриньки; контактний телефон; ORCID ID в форматі: http://orcid.org/0000-0001-9037-787X

## Подання матеріалів

Обсяг рукопису – від 4 до 20 аркушів українською або англійською мовами.

Для публікації необхідно надіслати статтю в електронній формі **doc**.

Подані матеріали автору не повертаються.

Матеріали просимо подавати через сайт журналу (sit.nuou.org.ua) або на e-mail: sitnuou@ukr.net.

З питань оплати звертатись до редакції (sitnuou@ukr.net).

Редколегія залишає за собою право відмови у публікації статей, що не відповідають проблематиці журналу, умовам оформлення матеріалів та за результатами незалежного рецензування.

Засновник і видавець Національний університет оборони України імені Івана Черняховського.
Св-во КВ № 20490-10290ПР. Адреса редакції: 03049, м. Київ, Повітрофлотський пр-т, 28. Тел. (044) 271-07-31.
Підписано до друку 30.05.2023. Формат 60×84 ⅛. Ум. друк. а. 19. Тираж 100 прим.
Надруковано у друкарні Національного університету оборони України імені Івана Черняховського.