

**Збірник наукових праць  
Центру воєнно-стратегічних досліджень  
Національного університету оборони України  
імені Івана Черняхівського**

**№ 1(71), 2021**

УДК 355:623 (08)

ISSN 2304-2699 (Print)  
ISSN 2304-2745 (Online)

**Збірник наукових праць Центру воєнно-стратегічних досліджень  
Національного університету оборони України  
імені Івана Черняховського. – 2021. – № 1(71).**

Створений у 1997 році, внесений до *переліку наукових фахових видань України в галузі технічних та військових наук* (Наказ МОН України від 02.07.2020 № 886), входить до Переліку наукових фахових видань України (категорія “Б”) за спеціальностями:

- 122 – Комп’ютерні науки та інформаційні технології;
- 253 – Військове управління (за видами збройних сил)

**Журнал індексується у наукометричній базі Index Copernicus Journals Master List.  
Видання індексується: Google Scholar, CiteFactor, WorldCat.**

**Програмні цілі збірника:** інформування науково-дослідних організацій Міністерства оборони України, інших міністерств і відомств, потенційних замовників науково-технічної продукції Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського та публікація результатів здобувачів наукового ступеня (свідцтво про державну реєстрацію друкованого засобу масової інформації від 28.11.2013 КВ № 20446-10246 ПР).

Рекомендовано до друку рішенням Вченої ради НУО України імені Івана Черняховського (протокол № 3 від 29.03.2021)

**Головний редактор:** ЗАГОРКА Олексій Миколайович, доктор військових наук, професор  
**Редакційна колегія:**

- БОГДАНОВИЧ Володимир Юрійович, доктор технічних наук, професор;
- БИЧЕНКОВ Василь Васильович, доктор технічних наук, ст. наук. співробітник;
- БОЧАРНИКОВ Віктор Павлович, доктор технічних наук, професор;
- ВЯЛКОВА Віра Іванівна, кандидат технічних наук;
- ГАВЛІЧЕК Петро, кандидат технічних наук, професор (Польща);
- КОРЕЦЬКИЙ Андрій Анатолійович, кандидат військових наук, ст. наук. співробітник;
- КОСЕВЦОВ В’ячеслав Олександрович, доктор військових наук, професор;
- КОТЛЯРЕНКО Олександр Петрович, кандидат юридичних наук;
- ЛИСЕНКО Олександр Іванович, доктор технічних наук, професор;
- МАРКО Іван Юрійович, доктор економічних наук, професор;
- МОСОВ Сергій Петрович, доктор військових наук, професор;
- НІЛЛІСОН Ніклас, PhD (Military), assistant professor (Швеція);
- ОПЕНЬКО Павло Вікторович, кандидат технічних наук;
- ПАВЛІКОВСЬКИЙ Анатолій Казимирович, кандидат військових наук, доцент;
- РИБИДАЙЛО Анатолій Анатолійович, кандидат технічних наук, ст. наук. співроб. (відп. редактор);
- САГАНЮК Федір Васильович, кандидат юридичних наук, доцент;
- САФРОНОВ Олександр Васильович, доктор технічних наук, професор;
- СЕМОН Богдан Йосипович, доктор технічних наук, професор;
- СНІЦАРЕНКО Петро Миколайович, доктор технічних наук, ст. наук. співробітник;
- СИРОТЕНКО Анатолій Миколайович, доктор військових наук, старший дослідник;
- ТЕЛЕЛИМ Василь Максимович, доктор військових наук, професор;
- ТИМОШЕНКО Радіон Іванович, доктор військових наук, ст. наук. співробітник;
- ТКАЧ Іван Миколайович, доктор економічних наук, доцент;
- ФАТТЕРЛІ Росс, PhD (War Studies) adjunct professor (Канада);
- ШЕВЧЕНКО Віктор Леонідович, доктор технічних наук, професор;
- ШОПІНА Ірина Миколаївна, доктор юридичних наук, професор;
- ЩИПАНСЬКИЙ Павло Володимирович, кандидат військових наук, професор

**Адреса редакції:** вул. Авіаконструктора Антонова, 2/32, корп. 14, Київ, 03186  
Центр воєнно-стратегічних досліджень  
Національного університету оборони України імені Івана Черняховського  
Тел./факс: (044) 271-09-08; (044) 271-07-74

Редакція може не поділяти думку авторів.

Автори відповідають за достовірність поданих матеріалів.

Посилання на збірник у разі використання його матеріалів попереджує плагіат.

© ЦВСД НУО України імені Івана Черняховського, 2021

**CONTENT**

<b>MILITARY STRATEGY</b>	
<b>A. Zahorka, DsM, professor; V. Boyko, PhD (Economic), senior research; I. Zahorka</b> Substantiation of the combat composition of a group of troops to reflection aggression	<b>6</b>
<b>MILITARY AND INFORMATION SECURITY OF THE STATE</b>	
<b>S. Kyrychenko, PhD (Military)</b> The role of private military companies in military conflicts: history and modernity	<b>12</b>
<b>A. Lepihov; A. Hrapach</b> Project activities in the sphere of ensuring national resilience: essence, content, structure	<b>18</b>
<b>D. Fedyanovich, PhD (Military), senior researcher;</b> <b>S. Vozniak, PhD (Technical), senior researcher; V. Dobrogursky</b> Recommendations for countering influence agents and resistance movements acting in the interests of the state initiating hybrid aggression	<b>27</b>
<b>INTERNATIONAL COOPERATION IN THE MILITARY SPHERE</b>	
<b>M. Pavlunko, PhD (Military); O. Posmituh, PhD (Military), assistant professor;</b> <b>V. Sergienko, PhD (Technical), assistant professor; O. Bohatov, PhD (Technical), assistant professor</b> Analysis of the combat use of the armed forces of the Russian Federation during the strategic command and staff exercises of the “West” series	<b>33</b>
<b>N. Andriianova, PhD (Political); N. Shpura, PhD (Military), senior researcher; V. Fedoriienko</b> Modern military conflict resolution using military force	<b>41</b>
<b>L. Golopatuk, PhD (Military)</b> Prospects and scenarios for NATO's development in the global system of international relations	<b>46</b>
<b>DEFENSE PLANNING</b>	
<b>P. Shchipansky, PhD (Military), professor;</b> <b>F. Sahaniuk, PhD (Jurisprudence), assistant professor; Y. Mydrak</b> Defense management: approaches to managing defense planning processes	<b>52</b>
<b>A. Hrinenko, PhD (Military), assistant professor</b> Issues of improving the efficiency of management of the mobilization training of the defense sector of the national economy of Ukraine	<b>59</b>
<b>A. Bratko, PhD (Military), associate professor</b> Improving defense planning in the State Border Guard Service of Ukraine	<b>67</b>
<b>CONSTRUCTION AND ECONOMIC RATIONALE FOR THE DEVELOPMENT OF THE ARMED FORCES</b>	
<b>S. Yakimyak, PhD (Military), assistant professor; E. Vdovitsky</b> Analysis of factors that may affect on the effectiveness of use the Navy duties during the protection of the economic activities of the state at sea in the context of hybrid enemy actions	<b>75</b>
<b>LEADERS OF TROOPS (FORCES) OF DEFENSE</b>	
<b>M. Lobko, PhD (Military), assistant professor; A. Fuchko; V. Copystyra</b> Institutional model of the Defense System of Ukraine	<b>82</b>
<b>INFORMATIZATION OF THE ARMED FORCES</b>	
<b>V. Galagan, PhD (Military), assistant professor</b> Proposals for development and implementation of an analytical module for monitoring the process of procurement of goods and services for the needs of the Armed Forces of Ukraine	<b>87</b>
<b>G. Rudenska</b> Ways to improve testing of special software of the defense resource management information system at the operational stage	<b>93</b>
<b>S. Bondarchuk</b> The justification of approach concerning of data preparation for initial loading for testing Defense Resource Management Information Systems	<b>99</b>
<b>V. Beliachenko; S. Bobrov, PhD (Technical), assistant professor; M. Utyushev; A. Muliavka</b> The main differences and features of structural and object-oriented approaches into designing of military information systems	<b>106</b>
<b>O. Androshchuk, PhD (Psychology)</b> Analysis of the application of global approaches to the creation of information infrastructure of the Ministry of Defense of Ukraine	<b>116</b>
<b>A. Litovchenko</b> Analysis of information management processes for information systems in the field of defense resource management	<b>123</b>
<b>ENSURING THE ACTIVITIES OF THE ARMED FORCES</b>	
<b>V. Semenenko, PhD (Technical), senior researcher;</b> <b>V. Shidlyukh; I. Sivoha;</b> The culture of Strategic Communication as the basis for targeting	<b>128</b>
<b>S. Frolov, PhD (Historical);</b> <b>I. Krylov</b> Classification of thematic groups of naval terms	<b>134</b>
<b>O. Hudyma, PhD (Technical), senior researcher</b> Analysis of the scientific and methodological apparatus of formation of organizational and functional structures of the strategic level	<b>139</b>
<b>INFORMATION ABOUT THE AUTHORS</b>	<b>146</b>

## ЗМІСТ

### ВОЄННА СТРАТЕГІЯ

<b>Загорка О. М., д-р військ. наук, професор;</b>	<b>6</b>
<b>Бойко В. О., канд. екон. наук, ст. наук. співроб.;</b>	
<b>Загорка І. О.</b>	
Обґрунтування бойового складу угруповання військ для відбиття агресії	

### ВОЄННА ТА ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

<b>Кириченко С. О., канд. військ. наук</b>	<b>12</b>
Роль приватних військових компаній у воєнних конфліктах	
<b>Лепіхов А. В.;</b>	<b>18</b>
<b>Храпач Г. С.</b>	
Проектна діяльність у сфері забезпечення національної стійкості: сутність, зміст, структура	
<b>Федянович Д. Л., канд. військ. наук, ст. наук. співроб.;</b>	<b>27</b>
<b>Возняк С. М., канд. техн. наук, ст. наук. співроб.;</b>	
<b>Доброгурський В. І.</b>	
Рекомендації щодо протидії агентам впливу та рухам опору, які діють в інтересах держави – ініціатора гібридної агресії	

### МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У ВОЄННІЙ СФЕРІ

<b>Павлунько М. Я., канд. військ. наук;</b>	<b>33</b>
<b>Посмітюх О. І., канд. військ. наук, доцент;</b>	
<b>Сергієнко В. Д., канд. техн. наук, доцент;</b>	
<b>Богатов О. І., канд. техн. наук, доцент</b>	
Аналіз бойового застосування збройних сил Російської Федерації під час стратегічних командно-штабних навчань серії “Захід”	
<b>Андріянова Н. М., канд. політ. наук;</b>	<b>41</b>
<b>Шпура М. І., канд. військ. наук, ст. наук. співроб.;</b>	
<b>Федорієнко В. А.</b>	
Застосування воєнної сили для врегулювання сучасних воєнних конфліктів	
<b>Голопатюк Л. С., канд. військ. наук</b>	<b>46</b>
Перспективи та сценарії розвитку НАТО в глобальній системі міжнародних відносин	

### ОБОРОННЕ ПЛАНУВАННЯ

<b>Щипанський П. В., канд. військ. наук, професор;</b>	<b>52</b>
<b>Саганюк Ф. В., канд. юрид. наук, доцент;</b>	
<b>Мудрак Ю. М.</b>	
Оборонний менеджмент: підходи до управління процесами оборонного планування	
<b>Грінченко О. І., канд. військ. наук, доцент</b>	<b>59</b>
Питання підвищення ефективності управління мобілізаційною підготовкою оборонного сектору національної економіки України	
<b>Братко А. В., канд. військ. наук, доцент</b>	<b>67</b>
Удосконалення оборонного планування у Державній прикордонній службі України	

### БУДІВНИЦТВО ТА ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ РОЗВИТКУ ЗБРОЙНИХ СИЛ

<b>Яким'як С. В., канд. військ. наук, доцент;</b>	<b>75</b>
<b>Вдовицький Є. А.</b>	
Аналіз чинників, які впливають на виконання завдань Військово-Морськими	

Силами під час захисту економічної діяльності держави на морі в умовах гібридних дій противника

### **КЕРІВНИЦТВО ВІЙСЬКАМИ (СИЛАМИ) ОБОРОНИ**

**Лобко М. М., канд. військ. наук, доцент;** **82**

**Фучко А. Й.;**

**Копистира В. М.**

Інституційна модель системи оборони України

### **ІНФОРМАТИЗАЦІЯ ЗБРОЙНИХ СИЛ**

**Галаган В. І., канд. військ. наук, доцент** **87**

Пропозиції щодо розроблення та впровадження аналітичного модуля контролю за процесом закупівель товарів, робіт та послуг для потреб Збройних Сил України

**Руденська Г. В.** **93**

Шляхи удосконалення тестування спеціального програмного забезпечення інформаційної системи управління оборонними ресурсами на етапі експлуатації

**Бондарчук С. В.** **99**

Обґрунтування підходу щодо підготовки даних до первинного завантаження для проведення тестування інформаційних систем управління оборонними ресурсами

**Беляченко В. В.; Бобров С. В., канд. техн. наук, доцент;** **106**

**Утюшев М. К.; Мулявка А. С.**

Основні відмінності та особливості структурного та об'єктно-орієнтованого підходів до проектування інформаційних систем військового призначення

**Андрощук О. В., канд. психол. наук** **116**

Аналіз застосування світових підходів для створення інформаційної інфраструктури Міністерства оборони України

**Литовченко Г. Д.** **123**

Аналіз процесів управління інформаційним забезпеченням інформаційних систем у сфері управління оборонними ресурсами

### **ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ЗБРОЙНИХ СИЛ**

**Семененко В. М., канд. техн. наук, ст. наук. співроб.;** **128**

**Шидлюх В. В.;**

**Сівоха І. М.**

Культура стратегічних комунікацій як основа таргетингу

**Фролов С. М., канд. іст. наук;** **134**

**Крилов І. О.**

Класифікація тематичних груп військово-морських термінів

**Гудима О. П., канд. техн. наук, ст. наук. співроб.** **139**

Аналіз науково-методичного апарату формування організаційно-функціональних структур систем стратегічного рівня

**Відомості про авторів** **146**

УДК 355.42 DOI: <https://doi.org/10.33099/2304-2745/2021-1-71/6-11>

Загорка О. М., д-р військ. наук, професор (0000-0003-1131-0904)  
Бойко В. О., канд. екон. наук, ст. наук. співроб. (0000-0002-3264-7111)  
Загорка І. О. (0000-0002-0693-1434)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

## Обґрунтування бойового складу угруповання військ для відбиття агресії

**Резюме.** На підставі двоетапного застосування методу таксономії розроблено методику, що дає змогу більш повно врахувати можливі способи бойових дій військ противника і своїх військ, та забезпечити збалансованість родів військ під час визначення бойового складу угруповання військ для відбиття агресії.

**Ключові слова:** угруповання військ; бойовий склад; збалансованість; способи бойових дій; метод таксономії; планування експерименту.

**Постановка проблеми.** Визначення бойового складу угруповання військ є одним з важливих завдань, яке має виконуватися органами військового управління (ОВУ) під час створення угруповання військ для відбиття агресії та планування розвитку (реформування) збройних сил на визначений період. Вирішення цієї проблеми набуває особливої актуальності через воєнно-політичну обстановку, яка складається навколо України, та у зв'язку з подіями останніх років на Сході країни. Це потребує перегляду підходів до забезпечення воєнної безпеки держави.

На теперішній час у Збройних Силах (ЗС) України проводяться заходи щодо підвищення їх боєздатності, створюються нові військові формування, удосконалюються організаційно-штатні структури військових формувань. В умовах наявності загроз у воєнній сфері та суттєвих ресурсних обмежень проблема визначення раціонального бойового складу угруповання військ для відбиття агресії має як наукову, так і практичну значущість.

**Аналіз останніх досліджень і публікацій.** Методичні положення обґрунтування складу ЗС наведені у працях [1, 2].

У праці [1] тільки фрагментарно розглянуто методичний підхід до обґрунтування бойового складу угруповання військ для відбиття агресії. Бойовий склад угруповання військ у праці [2] пропонується визначати з використанням однокритеріального методу оцінювання, що не дає змоги визначати його збалансований бойовий склад за видами ЗС і родами військ

[3]. У праці [4] розглянути методичні положення визначення доцільного способу бойових дій угруповання військ в операції (застосовуються методи теорії ігор) та його раціонального бойового складу (застосовується метод таксономії). Однак ці методичні положення не можуть повною мірою забезпечити визначення збалансованого бойового складу угруповання військ з урахуванням можливих способів бойових дій військ противника.

**Мета статті** полягає в удосконаленні методичних положень обґрунтування бойового складу угруповання військ для відбиття агресії.

**Виклад основного матеріалу.** Відповідно до принципів системного підходу угруповання військ розглядається як складна організаційно-технічна система, яка поділяється на підсистеми (рис. 1).

Ударна підсистема є основою угруповання військ, оскільки її склад (бойові сили і засоби) визначає спроможність відбиття агресії. Саме методичні положення визначення бойового складу ударної підсистеми угруповання військ розглядаються надалі.

Склад інших підсистем угруповання військ може визначатися нормативно з урахуванням попереднього досвіду створення угруповань військ.

Ударну підсистему угруповання військ утворюють бойові сили і засоби, які відповідають родам військ видів ЗС. Підрозділи цих родів військ уважаються параметрами ударної підсистеми угруповання військ.

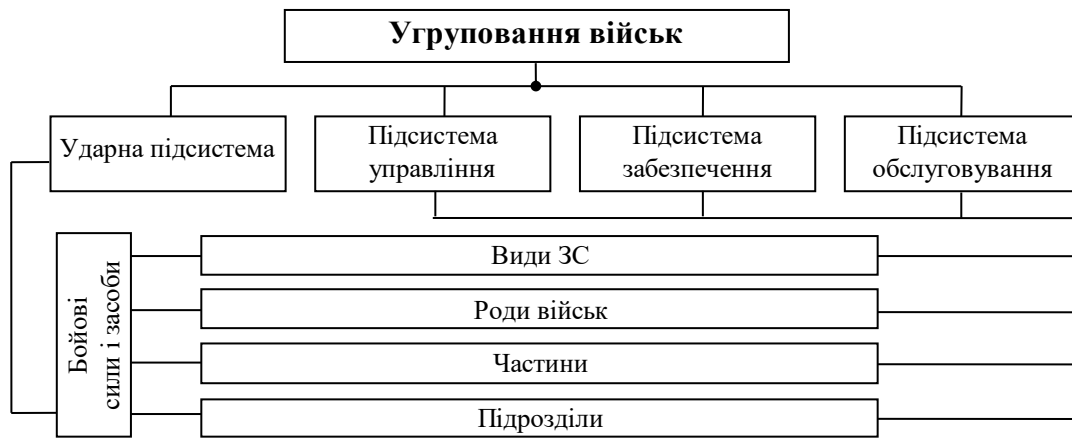


Рис. 1. Структура угруповання військ як складна організаційно-технічна система

Відповідно до методичних положень, що викладені у працях [1-4], для обґрунтування бойового складу угруповання військ формується множина варіантів цього складу та з них обирається найкращий. Такий підхід доцільно застосовувати і під час удосконалення методичних положень обґрунтування бойового складу угруповання військ для відбиття агресії.

Для досягнення мети дослідження необхідно:

розробити структурну схему методики обґрунтування бойового складу угруповання військ для відбиття агресії;

визначити порядок урахування можливих способів бойових дій угруповань військ противника і своїх військ в операції (під час ведення бойових дій);

уточнити порядок формування варіантів бойового складу угруповання військ;

удосконалити методичні положення визначення раціонального бойового складу угруповання військ для відбиття агресії.

Структурна схема методики обґрунтування бойового складу угруповання військ для відбиття агресії наведена на рис. 2.

У методиці, насамперед, визначаються завдання угруповання військ, можливі способи бойових дій військ противника і наших військ у воєнному конфлікті. У процесі визначення способів бойових дій військ противника ураховується мета розв'язання воєнного конфлікту, склад угруповання військ противника і форма його застосування. Для протидії противнику призначається базовий (початковий) склад угруповання наших військ і визначаються адекватні форма і способи бойових дій в операції (під час ведення бойових дій).

Найбільш представницькими показниками оцінювання ефективності застосування військ є втрати сторін в операції (під час ведення бойових дій), тому вимоги до ефективності застосування угруповання військ пропонується задавати критерієм, який визначається співвідношенням

$$W_{\text{потр}} = \frac{\delta_{\text{пр потр}}}{\delta_{\text{нев доп}}}; \delta_{\text{нев доп}} > 0, \quad (1)$$

де  $\delta_{\text{пр потр}}$  – математичне сподівання величини відносних втрат, яких потрібно завдати військам противника;

$\delta_{\text{нев доп}}$  – математичне сподівання величини відносних втрат, які допускаються для угруповання наших військ.

У методиці визначення раціонального бойового складу угруповання військ здійснюється на підставі порівняння його варіантів. Така задача належить до задач багатокритеріального аналізу [4]. Під час її розв'язання доцільно ураховувати такі показники:

математичне сподівання величини відносних втрат, яких завдають противнику наші війська в операції (під час ведення бойових дій);

математичне сподівання величини відносних втрат, яких завдає противник нашим військам;

внески родів військ (параметри ударної підсистеми) у загальні втрати військ противника;

математичні сподівання величин відносних втрат родів наших військ;

вартість озброєння угруповання наших військ;

вартість озброєння родів військ.

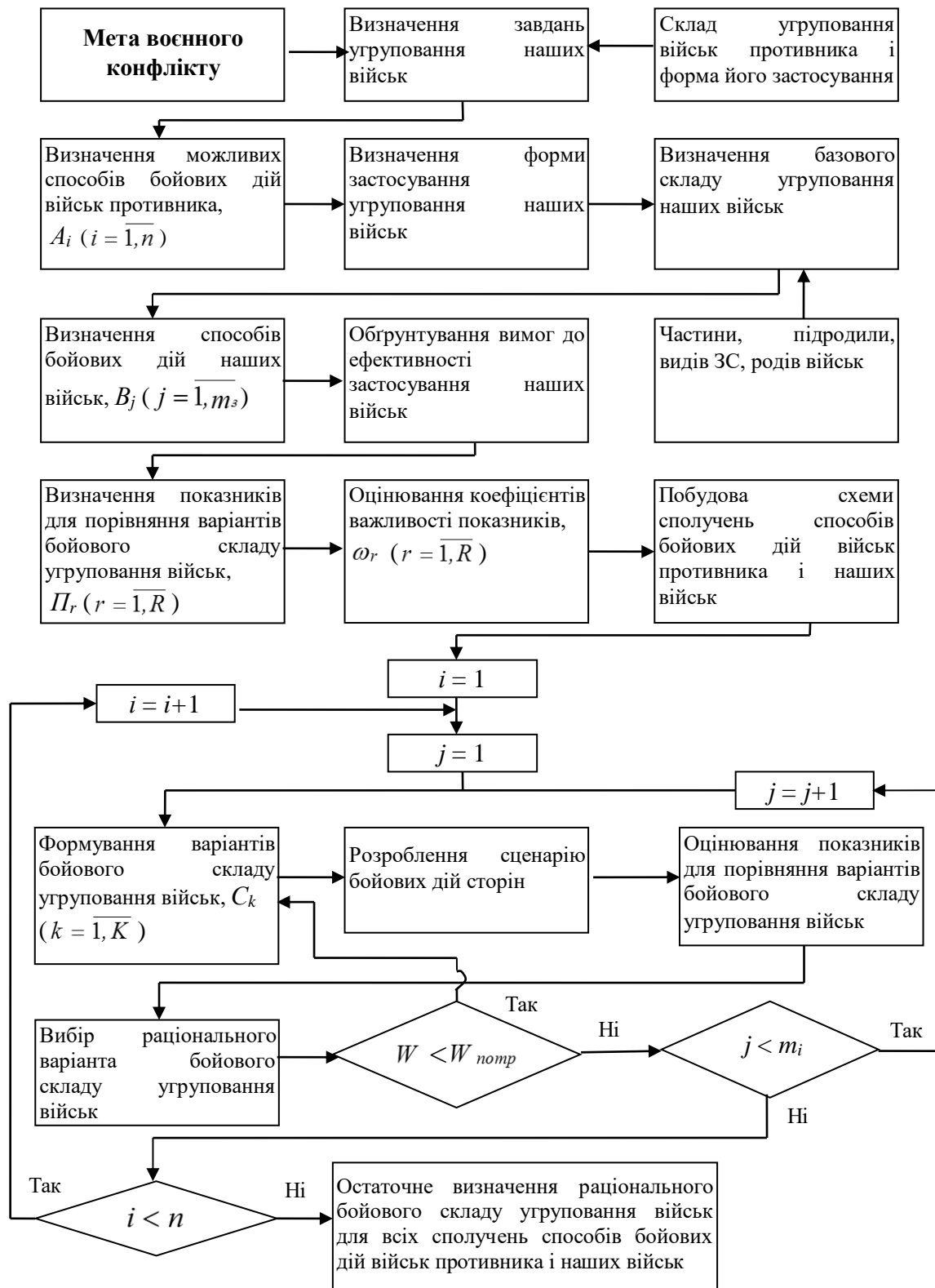


Рис. 2. Структурна схема методики обґрунтування бойового складу уgrupовання військ для відбиття агресії

Для оцінювання важливості показників можна використовувати експертний метод ранжирування [5, 6], який часто застосовується і не потребує подальших пояснень.

Визначення бойового складу уgrupовання військ здійснюється для можливих способів бойових дій військ

противника і наших військ. Кожному способу бойових дій військ противника протиставляється декілька способів бойових дій наших військ.

Схема сполучень способів бойових дій військ противника і наших військ наведена на рис. 3.



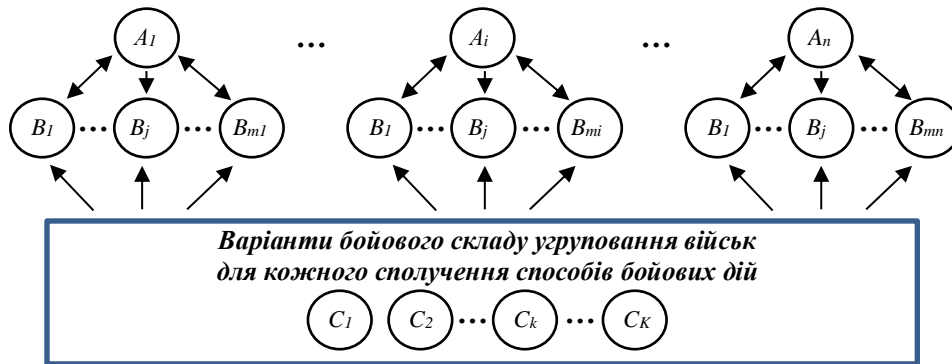


Рис. 3. Схема сполучень способів бойових дій військ противника і наших військ

На відміну від методики, викладеної у праці [4], у якій бойовий склад угруповання військ визначається для найбільш імовірних способів бойових дій сторін, пропонується під час розв'язання цієї задачі враховувати всі способи бойових дій військ противника і наших військ як показано на рис. 3.

Відповідно до схеми методики (див. рис. 2) формування варіантів бойового складу угруповання військ здійснюється для кожного сполучення способів бойових дій військ противника і наших військ.

Для цього застосовується метод планування експерименту [7]. План експерименту складається за допомогою варіювання параметрів ударної підсистеми. До таких параметрів можуть, наприклад, належати [4]: склад механізованих, танкових, аеромобільних військ, ракетних військ і артилерії, зенітних ракетних військ, тактичної авіації. Склад решти родів військ може залишатися незмінним. Рівні варіювання параметрів ударної підсистеми встановлюються з урахуванням обмежень на склад родів військ. Варіювання параметрів здійснюється відносно їх початкового значення. За одиниці варіювання параметрів бойового складу угруповання військ доцільно прийняти: батальйон, дивізіон, батарея, ескадрилья.

У праці [8] рекомендується при кількості параметрів, що варіюються до чотирьох, використовувати повний факторний експеримент, а більше чотирьох – дрібне факторне планування. Звичайно варіювання параметрів під час розв'язання подібних задач здійснюється на трьох рівнях. Готові плани експериментів наведені у праці [9]. Для трьох параметрів план обчислювального експерименту містить 10, для чотирьох – 15, для п'яти – 21, для шести – 28, для семи – 37 спроб (варіантів).

Відповідно до розробленого сценарію для кожного варіанта бойового складу угруповання військ оцінюються показники, за

якими здійснюється їх порівняння (вибір раціонального варіанта).

Задача визначення раціонального бойового складу угруповання військ за сутністю є задачею синтезу ударної підсистеми. Відповідно до праці [10] під раціональним розуміється збалансований склад параметрів (родів військ) угруповання військ, який забезпечує потрібний рівень ефективності його застосування за мінімальних витратах (втрат) сил і засобів. Збалансованість бойового складу угруповання військ – це взаємна відповідність якісного та кількісного складу родів військ для виконання усього діапазону завдань, що покладаються на угруповання військ в операції (під час ведення бойових дій).

У методиці під час розв'язання задачі визначення раціонального бойового складу угруповання військ для кожного сполучення способів бойових дій військ противника і наших військ, як і у працях [3, 4], використовується метод таксономії [11].

Під час порівняння варіантів бойового складу угруповання військ використовується таксономічна відстань, яка визначається за правилами аналітичної геометрії. Усі показники поділяються на стимулятори і дестимулятори. У нашому випадку показники, збільшення яких сприяє ефективності виконання завдань угрупованням військ (втрати противника) вважаються стимуляторами, а навпаки – дестимуляторами (втрати своїх військ), зокрема вартість озброєння. Варіанти порівнюються з еталонним варіантом, якому відповідають максимальні значення показників-стимуляторів і мінімальні значення показників-дестимуляторів.

Вихідними даними для застосування методу таксономії є матриця значень показників

$$\|x_{rk}\|, (r = \overline{1, R}, k = \overline{1, K}),$$

наведено у Табл. 1.

Таблиця 1

**Значення показників для порівняння варіантів бойового складу угруповання військ**

Показник	Варіант бойового складу					
	$C_1$	$C_2$	...	$C_k$	...	$C_K$
$\Pi_1$	$x_{11}$	$x_{12}$	...	$x_{1k}$	...	$x_{1K}$
$\Pi_2$	$x_{21}$	$x_{22}$	...	$x_{2k}$	...	$x_{2K}$
$\Pi_r$	$x_{r1}$	$x_{r2}$	...	$x_{rk}$	...	$x_{rK}$
$\Pi_R$	$x_{R1}$	$x_{R2}$	...	$x_{Rk}$	...	$x_{RK}$

Оскільки елементи матриці можуть мати різні одиниці вимірювання, вони приводяться до стандартизованого вигляду за формулою

$$z_{rk} = w_r \cdot \frac{x_{rk} - \bar{x}_r}{\sigma_r},$$

де  $\bar{x}_r$ ,  $\sigma_r$  – математичне сподівання і середнє квадратичне відхилення  $r$ -го показника відповідно;

$w_r$  – коефіцієнт важливості  $r$ -го показника.

Для еталонного бойового складу угруповання військ  $z_{10}, z_{20}, \dots, z_{r0}, \dots, z_{R0}$  показники визначаються таким чином:

$$\bar{\gamma}_0 = \frac{1}{K} \sum_k \gamma_{k0}; \alpha_0 = \left[ \frac{1}{K} (\gamma_{k0} - \bar{\gamma}_0)^2 \right]^{1/2}; \gamma_0 = \bar{\gamma}_0 + 2\alpha_0; \beta_k = 1 - \frac{\gamma_{k0}}{\gamma_0}.$$

Для кожного сполучення способів бойових дій військ противника і наших військ раціональним вважається варіант бойового складу угруповання військ, якому відповідає максимальне значення таксономічного показника  $\beta_k$ .

Відповідно до методики (див. рис. 2), коли ефективність застосування угруповання військ обраного складу  $W$  менше потрібної  $W_{номр}$ , корегуються варіанти бойового складу і розрахунки повторюються.

Раціональні варіанти бойового складу угруповання військ визначаються для  $L$  сполучень способів бойових дій військ противника і наших військ

$$L = \sum_i m_i, i = \overline{1, n}.$$

Кожному раціональному варіанту бойового складу угруповання військ відповідають певні значення його параметрів (кількість підрозділів родів військ)  $a_{sl}$ ,  $s = \overline{1, S}$ ,  $l = \overline{1, L}$ , де  $S$  – кількість параметрів ударної підсистеми, що досліджується.

Якщо визначені максимальні значення параметрів  $\max_l a_{sl}$ , то такий бойовий склад

$$z_{r0} = \left\{ \begin{array}{l} \max_r z_{rk}, r \in S \\ \min_r z_{rk}, r \in D_s \end{array} \right\},$$

де  $S, D_s$  – сукупність показників-стимуляторів і показників-дестимуляторів відповідно.

Таксономічні відстані обчислюються за формулою

$$\gamma_{k0} = \left[ \sum_r (z_{rk} - z_{r0})^2 \right]^{1/2}; k = \overline{1, K}; r = \overline{1, R}.$$

Таксономічний показник  $\beta_k$  розраховується таким чином:

угруповання військ може забезпечити виконання завдань при будь-якому сполученні способів бойових дій військ противника і наших військ. Однак такий бойовий склад є зайво збільшеним і не може бути збалансованим.

Параметри бойового складу угруповання військ (ударної підсистеми) також можуть визначатися як середнє значення  $a_s^* = \frac{1}{L} \sum_l a_{sl}$ , що також не забезпечує збалансованість родів військ.

Водночас під час визначення раціонального бойового складу угруповання військ для кожного сполучення способів бойових дій військ противника і своїх військ було оцінено відповідні показники. Це дає змогу для визначення збалансованого бойового складу угруповання військ також використати метод таксономії. У цьому випадку кількість варіантів бойового складу угруповання військ дорівнює  $L$ . Таким чином у методиці, що розроблена, для визначення збалансованого бойового складу угруповання військ застосовано двоетапне використання методу таксономії.

**Висновок.** Угрупування військ під час удосконалення методичних положень

обґрунтування його бойового складу розглядається як складна організаційно-технічна система, основним структурним елементом якої є ударна підсистема. Саме для визначення збалансованого складу бойових сил і засобів ударної підсистеми призначена розроблена методика. У методиці, на відміну від існуючих підходів для визначення збалансованого бойового складу угруповання військ для відбиття агресії, застосовано двоетапне використання методу таксономії.

Розроблені методичні положення надалі доцільно використати під час створення спеціального математичного програмного забезпечення ОВУ.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Тимошенко Р. І., Загорка О. М. Загальні методологічні положення військово-економічного обґрунтування складу Збройних Сил України на сучасному етапі їх реформування. *Наука і оборона*. 2014. № 1. С. 43–48.
2. Основы теории и методологии планирования строительства вооруженных сил Российской Федерации : военно-теоретический труд / под общ. ред. А. В. Квашнина. Москва : Воентехиздат, 2002. 232 с.
3. Методичний підхід до визначення бойового складу Збройних Сил воєнного і мирного часу / О. М. Загорка, В. С. Фролов, В. М. Можаровський, І. О. Загорка // Збірник наукових праць Центру військово-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ, 2019. № 1 (65). С. 6–11.
4. Можаровський В. М., Загорка О. М. Основні положення методики визначення варіанта (способу) бойових дій та складу угруповання військ (сил) для відбиття агресії. *Наука і оборона*. 2011. № 1. С. 3–6.
5. Бешелев С. Д., Гурвич Ф. Г. Экспертные оценки. Москва : Наука, 1973. 160 с.
6. Денисов А. А., Колесников Д. Н. Теория больших систем управления : уч. пособ. для вузов. Ленинград : Энергоиздат, 1982. 288 с.
7. Барабашук В. И., Креденцер Б. П., Мирошниченко В. И. Планирование эксперимента в технике / под общ. ред. Б. П. Креденцера. Киев : Техника, 1989. 200 с.
8. Ашмарин И. П., Васильев Н. Н., Амбросов В. А. Быстрые методы статистической обработки и планирование экспериментов. Ленинград : Ленингр. университет, 1974. 76 с.
9. Таблицы планов эксперимента для факторных и полиномиальных моделей / В. З. Бродский и др. Москва : Металлургия, 1982. 350 с.
10. Загорка О. М., Мосов С. П., Сбітнев А. І., Стужук П. І. Елементи дослідження складних систем військового призначення : навч. посіб. Київ : НАОУ, 2005. 100 с.
11. Плюта В. Сравнительный многомерный анализ в эконометрическом моделировании. Москва : Финансы и статистика, 1989. 176 с.

Стаття надійшла до редакційної колегії 21.03.2021

### **Substantiation of the combat composition of a group of troops to reflection aggression**

#### **Annotation**

A major task which decides the organs of military management during creation of grouping of troops for the reflection of aggression is determination of her rational composition. The methods of ground of combat composition of grouping of troops, which is based on the use of method of taxonomy, is offered in the article.

The grouping of troops is examined as a difficult organizationally technical system, its basis is a strike subsystem which contains combatant forces and facilities of branches of troops of types of Armed Forces. Exactly for determination of her composition methods are intended.

Determination of combat composition of strike subsystem is carried out for the possible methods of combat actions of troops of opponent and troops. Thus every method of combat actions of troops of opponent a few methods of combat actions of our troops are matched against. For every method of combat actions of our troops with the use of method of planning of experiments the variants of combat composition of strike subsystem of grouping of our troops are formed.

The rational variant of combat composition of strike subsystem is determined for every method of combat actions of grouping of our troops with the use of method of taxonomy on indexes, which characterize efficiency of his application and cost of armament. At a decision, tasks are taken into account only variants of combat composition of strike subsystem, at which efficiency of application of grouping of troops is provided not below than necessary.

In second times the method of taxonomy is used for the choice of the best (balanced) variant of combat composition from rational variants which were certain for every method of combat actions of grouping of troops. A two-stage use of method of taxonomy allows most reasonably determining combat composition of grouping of troops taking into account the possible methods of combat actions of troops of opponent.

The organs of military management can use this methodology during determination of combat composition of grouping of troops for the reflection of aggression.

**Keywords:** grouping of troops; combat composition; balance; methods of combat actions; method of taxonomy; planning of experiment.

Кириченко С. О., канд. військ. наук

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

## Роль приватних військових компаній у воєнних конфліктах

**Резюме:** Розглянуто сутність приватних військових компаній, їх класифікацію за видами діяльності, роль у сучасних воєнних конфліктах, зокрема на території України.

**Ключові слова:** приватна військова компанія; воєнні конфлікти; бойові дії; найманці; збройні сили.

**Постановка проблеми.** Окремі аспекти створення та діяльності приватних військових компаній, користування їх послугами різними державами та міжнародними організаціями на сьогодні мають істотне значення для організації та забезпечення оборони держави.

Не є виключенням у цій проблемі значущість Російської Федерації, яка використовує підрозділи приватної військової компанії “Вагнер” як дієвий інструмент гібридної агресії проти України.

Ретроспективний аналіз діяльності приватних військових компаній, їх класифікація і роль у сучасних воєнних конфліктах є актуальним і для забезпечення воєнної безпеки України, що потребує ґрунтовнішого дослідження та врахування на сучасному етапі захисту й оборони держави.

**Аналіз останніх досліджень і публікацій.** У роботах [1–5] розглянуті історичні аспекти створення перших приватних військових компаній у США та Європі.

Низка інших публікацій [6–18] присвячена дослідженню регіонів, де західні держави та міжнародні організації користувались послугами приватних військових компаній (ПВК), а також аналізу діяльності російської ПВК “Вагнер”, зокрема на території України,

**Мета статті.** Дослідити тенденції розвитку ПВК, їх можливості для застосування в сучасних воєнних конфліктах та їх переваги і недоліки порівняно з регулярними військами, стан правового врегулювання їх діяльності для можливого врахування в Україні під час військового будівництва та у безпековій і оборонній сферах.

**Виклад основного матеріалу.** Здавня володарі перших держав дійшли висновку, що територіальні та майнові конфлікти із сусідами можна вирішувати за допомогою воєнної сили спеціально найнятих для цього людей. Наймані армії завжди мали велику

вагу в історії, однак згодом з’ясувалося, що за своїми можливостями і моральною стійкістю вони поступаються регулярним військам.

Незважаючи на це, з 70-х років минулого століття у воєнних конфліктах, міжнародних миротворчих операціях і в процесі забезпечення повсякденної діяльності збройних сил почали активно використовуватися послуги приватних воєнних компаній (Private Military Companies) [1]. Вони офіційно зареєстровані, мають необхідні ліцензії та статuti, розгалужені бізнес-структури, новітнє озброєння тощо. Їхніми послугами користується навіть ООН, міжнародні гуманітарні організації та уряди деяких демократичних країн.

На сьогодні існують різні тлумачення терміну “приватна воєнна компанія”. Наприклад, у документах ООН застосовується термін “приватні воєнні та охоронні компанії” (ПВОК), під якими розуміють “приватні підприємницькі суб’єкти, які надають воєнні та/або охоронні послуги, незважаючи на те, як вони себе характеризують” [1]. Воєнні й охоронні послуги включають, зокрема, збройну охорону і захист людей та об’єктів, наприклад, транспортних колон, споруд та інших місць; техобслуговування й експлуатацію бойових комплексів; утримання під вартою ув’язнених; консультування або підготовку місцевих військовослужбовців і охоронців.

Фахівці Женецького Центру демократичного контролю за збройними силами трактують ПВК як “комерційні структури, що пропонують спеціалізовані послуги, які пов’язані з участю у війнах і збройних конфліктах, включаючи бойові операції, стратегічне планування, збір розвідувальної інформації, оперативну підтримку і логістику, підготовку, постачання, обслуговування” [2].

Американські політологи вважають, що приватні воєнні компанії є не що інше, як орієнтовані на прибуток організації, які

надають професійні послуги, пов'язані з веденням війни. Це корпоративні організації, які торгують воєнним мистецтвом, включаючи рекомендації щодо тактики ведення бойових дій, стратегічного планування, збір розвідувальних даних, навчання військ і технічну допомогу [3].

Аналізуючи наведене, можна виокремити певні ознаки ПВК.

*Перша.* Наявність статусу приватної комерційної організації, основною метою якої є одержання прибутку.

*Друга.* Переважна більшість визначених статутом такої компанії напрямів її діяльності (або всі) стосується надання воєнних послуг. До них належать послуги з таких питань як створення, реформування та розвиток сил безпеки і оборони; планування та підготовки їх до застосування; розвідка та контррозвідка; навчання особового складу; застосування, обслуговування та експлуатації озброєння і військової техніки; матеріально-технічне забезпечення сил безпеки і оборони; гуманітарне розмінування; збройна охорона об'єктів, захист дипломатичного персоналу, окремих осіб і транспортних перевезень тощо.

*Третя.* Об'єктами ПВК для надання послуг можуть бути національні та іноземні юридичні або фізичні особи.

*Четверта.* ПВК надають послуги переважно за межами своїх держав. Вони можуть функціонувати в умовах мирного часу та в період воєнного конфлікту, а також безпосередньо в зоні такого конфлікту.

За результатами аналізу характеру послуг, які можуть надаватися ПВК, відповідних документів міжнародних організацій і публікацій [4, 5] найбільш прийнятною є наведена нижче типологія таких компаній.

*Компанії бойового забезпечення* (military provider companies), які надають послуги з підтримання бойових дій сил безпеки і оборони (за термінологією НАТО – тактичну підтримку), включно з безпосередньою участю в бойових операціях. Утім, остання зі згаданих послуг сучасними ПВК не надається, принаймні офіційно.

*Воєнні консалтингові компанії* (military consulting companies) спеціалізуються на наданні послуг з планування, створення, реформування й розвитку сил безпеки і оборони, зокрема, органів розвідки й контррозвідки, їхньої бойової та спеціальної підготовки тощо.

*Воєнні логістичні компанії* (military support companies) – сфера їхньої діяльності

охоплює: обслуговування й експлуатацію складних систем озброєння, військової техніки та комп'ютерних систем; матеріально-технічне забезпечення військ; будівництво військових об'єктів.

До ПВК відносять і *приватні охоронні компанії* (private security companies), які працюють в умовах воєнного конфлікту або в зоні підвищеного ризику, зокрема на території країн з нестабільною обстановкою. Хоча зазвичай вони здійснюють захист об'єктів і фізичних осіб, а не бойові дії, однак у районах воєнного конфлікту чітке розмежування між цими видами діяльності відсутнє. Наприклад, під час захисту аеродромів, нафтопроводів та інших об'єктів інфраструктури охоронні компанії можуть проводити бойові операції проти незаконних військових формувань, терористів тощо.

Окрему групу складають ПВК, які спеціалізуються на розвідувальній та контррозвідувальній діяльності. Їх мережа є практично закритою. За різними Інтернет-джерелами, з державними розвідувальними органами співпрацюють, зокрема, американські компанії “Strategic Forecasting Inc”, “Booz Allen Hamilton”, британські – “Aegis” і “Hakluyt & Company” [6].

Останніми роками ПВК почали активно залучатися до боротьби з піратством, забезпечуючи супроводження та збройний захист суден, ведення переговорів з нападниками тощо. Нині тільки в Аденській затоці та у районі Африканського Рогу діють понад двадцять таких ПВК. Річні витрати судноплавних компаній на їх найм становлять близько 100 млн дол. США [6].

Практика використання приватних силових (воєнізованих) організацій у збройних конфліктах, залучення на контрактній основі військових фахівців, радників та інструкторів для підготовки поліцейських і збройних сил має багатовікову історію.

Перша в сучасному розумінні приватна військова компанія “Watchguard International” була створена в 1967 р. у Великобританії. Її творцем став нащадок шотландського аристократичного роду, офіцер британської армії, підполковник сер Арчибальд Девід Стірлінг. Починав він свою службу у Північній Африці під час Другої світової війни. У 1941 р., будучи лейтенантом, Стірлінг став творцем легендарного спецназу Великобританії – Спеціальної авіадесантної служби (Special Air Service, SAS) – одного з кращих спеціальних підрозділів у світі.

Основним напрямом діяльності ПВК Watchguard International стала підготовка різних силових організацій у країнах Близького Сходу і Африки [7].

Збільшення чисельності контрактників було в середині 1970-х. Один з перших масштабних контрактів у новітній історії був укладений у 1974 р., коли приватна військова компанія “Vinnell Corp”, яка належала американському військово-промислового концерну “Northrop Grumman”, уклала з урядом США контракти більш ніж на півмільярда доларів. Її співробітники мусили зайнятися підготовкою Національної гвардії Саудівської Аравії і захистом нафтових родовищ у цій країні [8].

Кількість приватних військових компаній невпинно зростає. Їх послугами користувалися не тільки уряди різних держав, а й великий бізнес. Цією проблемою зацікавилися навіть в ООН. У 1979 р. була прийнята спеціальна резолюція з цього приводу і організований комітет, до складу якого увійшли представники 35 держав. Проте нормативно-правових документів з цієї проблеми прийнято не було [9].

Під час холодної війни приватні військові компанії були створені в США, Великобританії, Ізраїлі та ПАР. Їх діяльність проходила під патронажем відповідних держав. Надалі, кількість ПВК стала збільшуватися [10].

Після закінчення холодної війни ситуація істотно змінилася. У США були різко скорочені витрати на оборону, закриті багато проєктів, зменшилася чисельність американських збройних сил. Саме в цей момент у військового керівництва США з'явилася ідея більш активно залучати наймані компанії. Спочатку вони займалися забезпеченням збройних сил (логістика, ремонт техніки, постачання), але потім ПВК стали залучати для виконання серйозніших завдань.

Під час війни в Іраку в 1991 р. кількість найманців із різних ПВК становила 1 % від загального числа американських військовослужбовців, яка знаходилась у Перській затоці.

У 1999 р. командування армії США прийняло нормативно-правовий документ, який встановив порядок взаємодії військовослужбовців США та співробітників приватних охоронних і військових компаній у зоні бойових дій – FM 100-21.

З початку 2000-х спостерігається зростання зацікавленості до послуг ПВК з

боку великих міжнародних корпорацій, бізнес яких пов'язаний з присутністю в точках нестабільності. Відмічено випадки використання приватних військових компаній міжнародними організаціями, як приклад, “DynCorp”, яка стала підрядником ООН [11].

У квітні 2001 р. була створена організація “Peace Operations Association” (POA), яка координує діяльність приватних військових і охоронних компаній на міжнародному рівні. Після початку війни в Іраку була створена асоціація західних приватних військових і охоронних компаній “Private Security Company Association of Iraq” (PSCAI), яка координує їх діяльність в Іраку. До складу асоціації увійшли 40 військових і охоронних компаній [11].

У 2004 р. керівник тимчасової адміністрації в Іраку Пол Бремер підписав наказ (Coalition Provisional Authority Order 17), відповідно до якого контрактники США, зокрема співробітники військових і охоронних компаній, отримували недоторканність. Вони не могли бути притягнуті до відповідальності за скоєні злочини на території Іраку відповідно до законодавства Іраку.

На сьогодні в світі офіційно зареєстровано 450 приватних військових компаній, перелік їх послуг дуже широкий. Найвідомішими західними ПВК є: Academi (це колишня Blackwater), G4S (Великобританія), Kellog, Brown and Root (США), Groupe-ЕНС (Франція), Erinys (США), DynCorp (США), FDG Corp (США), MPRi (США), Aegis Defence Services (Великобританія) [12].

Натхненником створення приватних військових компаній в Росії був Ебен Барлоу, колишній генерал-лейтенант південно-африканських сил безпеки і засновник першої в світі легальної приватної армії Executive Outcomes, яка виконує широкий спектр послуг – від захисту глав держав і охорони до військового втручання. У [13] зазначається, що Барлоу прибув до Росії в 2010 р. як учасник Петербурзького міжнародного економічного форуму. Крім офіційного виступу, він провів закриту презентацію концепції ПВК перед представниками Генерального штабу, де тоді вже розглядали ідею формування приватної армії з відставних військових і контрактників для секретних завдань. Структуру вирішено було зробити нелегальною через складнощі з контролем за обігом зброї. Набір контрактників почався тільки у 2013 р. Перші завдання найманці стали виконувати в Криму під час його анексії

та на південному Сході України і Донбасі. Одночасно продовжувались активні їх тренування на базі ГРУ на півдні Росії. До більш масштабних дій російські ПВК Вагнера перейшли вже в Сирії після початку там російської військової кампанії.

Приватна військова компанія Вагнера/група Вагнера – неофіційна військова організація, яка не входить до регулярних збройних сил Росії і не має юридичного статусу на її території. Військові підрозділи ПВК Вагнера налічували в різний час від 1350 до 2000 осіб. За даними німецької газети Bild у бундесвері загальна чисельність їх найманців сягає 2500 чоловік. Усього, за підрахунками видання, через ПВК Вагнера з 2014 р. завербовано від семи до десяти тисяч контрактників. У минулому році витрати на забезпечення діяльності цього угруповання склали майже два мільярди рублів РФ [13].

Перші свідчення про діяльність ПВК Вагнера на території України (на Донбасі) зафіксовані українськими спецслужбами в травні 2014 р. [14]. РФ використовує тут ПВК Вагнера як елемент гібридної війни Росії проти України. Під вивіскою приватної компанії зібрано інтернаціональні найманці, але основою цієї структури є російські військовослужбовці, які виконують накази російського командування. Вони проходять підготовку на базі 10-ї окремої бригади спецпризначення ГРУ Росії. Бійці компанії і їх командири, на чолі з “Вагнером”, отримують відомчі нагороди, підписані особисто Президентом Росії. Важке озброєння і техніку вони отримують безпосередньо з баз зберігання МО РФ. Від кадрових військовослужбовців Збройних сил РФ їх відділяє тільки формулювання в контракті та розмір грошового забезпечення, а також те, що офіційній Москві від них легше відмовитися [14].

Російський МЗС визнав присутність приватних військових компаній Росії і в Судані та факт зміцнення фахівцями Міноборони армії Центральноафриканської республіки хоча ці факти керівництво Кремля неодноразово заперечувало.

Офіційно відомо, що Росія “на безоплатній основі” поставила для потреб центральноафриканської армії партію стрілецької зброї та боєприпасів, а також відрядила 5 військових і 170 російських цивільних інструкторів для підготовки військовослужбовців ПАР [15].

Російська “група Вагнера” також бере активну участь й у конфлікті в Лівії. Росія

продовжує поставляти туди техніку та зброю в порушення ембарго Радбезу ООН. Зокрема, у вересні 2019 р. група Conflict Intelligence Team (СІТ), яка спеціалізується на розслідуваннях втручання Росії у військові конфлікти, виявила, що російська приватна військова компанія “Вагнер” бере активну участь у громадянській війні в Лівії на боці Лівійської національної армії маршала Халіфи Хафтара, який намагається повалити міжнародно визнаний Уряд національної згоди [16].

Глава МВС, створеного за підтримки ООН уряду національної згоди (УНЗ) Лівії, Фатхі Башага звинуватив бійців російської ПВК Вагнера у застосуванні хімічної зброї (нервово-паралітичного газу) на території Лівії [17].

Вагнерівці РФ нещодавно були виявлені й у Білорусі, зокрема під Мінськом, де були затримані 32 їхніх бойовики, а ще одного затримали на півдні Білорусі [16, 17].

*Позитивні сторони* використання ПВК: не викликає у населення такого незадоволення, як застосування регулярних збройних сил;

вони можуть становити певну протизвагу місцевим збройним силам у державах зі слабкими політичними інституціями;

здатні до швидкого розгортання;

втрати особового складу ПВК, зазвичай, не враховуються в офіційних звітах урядів;

мають більш гнучке оперативне управління;

відсутність у них бюрократії;

більш високий професіоналізм порівняно з регулярними військами (проте порівняно з контрактними військами – він сумнівний).

*Негативні сторони:*

відсутність ідейної та ідеологічної мотивації особового складу;

умови контрактів ПВК не передбачають усі можливі варіанти розвитку ситуації, що зменшує гнучкість їх дій в бойовій обстановці;

відсутність єдиного плану заходів та єдиного оперативного центру управління військами і ПВК;

відсутність обміну або неповні дані оперативного характеру.

Правовий статус приватних військових компаній недостатньо внормований. Державо-наймач не несе відповідальності за протиправні дії приватних військових компаній, якщо вони діяли за її вказівками, інструкціями або вона здійснювала над ними ефективний контроль. До того ж під інструкціями і вказівками можуть вважатися

такі цілі та положення контракту, виконання яких неможливо іншим способом, крім як протиправним.

Нині діяльність приватних військових компаній набирає істотного розмаху по всьому світу. Зі збільшенням збройних конфліктів у світі збільшується і кількість ПВК. З початку 2000-х виявлено різкий сплеск зацікавленості до послуг ПВК з боку великих міжнародних корпорацій, компаній, бізнес яких пов'язаний з присутністю в “гарячих точках” Середнього і Близького Сходу та в Африці.

Як зазначено у [20], станом на 2006 р. обсяг ринку послуг приватних військових компаній становив до 20 млрд дол. США. У 2017 р. він становив від 100 до 400 млрд дол. США. Сучасні ПВК – це справжні армії чисельністю до 70 тисяч чоловік, оснащених новітньою технікою, в тому числі важким озброєнням (бойовими вертольотами, БТР, БМП і танками), які відкрито позиціонують себе на ринку послуг безпеки і продають свої акції на фондовій біржі.

Послугами ПВК активно користуються державні та неурядові організації, збройні формування, комерційні компанії, ООН і навіть Міжнародний комітет Червоного Хреста.

За даними інституту Брукінгса США, оборот світового ринку приватних військових послуг, монополізованого американськими, британськими і південноафриканськими компаніями, перевищує сьогодні 180 млрд дол.

ПВК на сьогодні мають не тільки якісне бойове і тилове забезпечення угруповань військ, а й контроль захопленої території, даючи змогу не залучати на ці цілі сили регулярної армії. Адже ПВК на відміну від регулярних армій фактично знаходяться поза межами цивільного контролю. Їм можна доручити найганебнішу роботу від повалення законних урядів до усунення негодних політиків і громадських діячів. До того ж, у разі розголосу місії найманців нового типу, держава, яка відрядила їх воювати, завжди може не визнавати такого злочину.

Саме такі ознаки нині притаманні російським ПВК, які продовжують стрімко розвиватися. Тепер їх майже не відрізнити від більшості регулярних армій. У них є штурмові підрозділи, розвідка та артилерія; вони мають на озброєнні ПЗРК і бронетехніку та бойові танки [20].

## Висновки

1. В умовах глобалізації роль приватних військових організацій у майбутніх війнах і збройних конфліктах зростає.

2. На відміну від традиційних інститутів армії і поліції, дії яких регламентуються як міжнародним, так і національним законодавством, законодавчих норм для ПВК на сьогодні не визначено. Женевські конвенції не є перешкодою для них навіть під час їх використання у відкритих бойових діях.

3. Дослідження показує, що ПВК, допоки вони не стали частиною збройних сил сторін конфлікту і не беруть безпосередню участь у військових діях, мають розглядатися як цивільні особи і підпадати під захист Міжнародного гуманітарного права (МГП).

У разі їх участі у збройних конфліктах вони мають дотримуватися МГП, а за порушення його норм можуть притягуватися до встановленої чинним законодавством і МГП відповідальності.

## Напрями подальших досліджень.

Надалі на основі використання результатів цього дослідження доцільно провести аналіз можливих способів як військових, так і невійськових, а також механізми протидії агресії РФ за участю приватних військових компаній, ґрунтовніше дослідити у цих цілях діяльність в Україні “Добробатів” та інших волонтерських організацій, які сприяли і сприяють активній боротьбі проти російської агресії.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Документ Монтрё о соответствующих международно-правовых обязательствах и передовых практических методах государств, касающихся функционирования частных военных и охранных компаний в период вооруженного конфликта. URL: <http://www.icrc.org/rus/resources/documents/misc/ih11montreau.htm> (дата звернення: 23.04.2020).
2. DCAF Backgrounder. Приватні військові компанії. Женевський Центр демократичного контролю за збройними силами. URL: [http://www.dcaf.ch/content/download/34962/52514/file/bg\\_private-military-companies\\_ukr.pdf](http://www.dcaf.ch/content/download/34962/52514/file/bg_private-military-companies_ukr.pdf) (дата звернення: 23.04.2020).
3. Singer Peter. Corporate Warriors. The Rise of the Privatized Military Industry and Its Ramification for International Security. *International Security*. Vol. 26. № 3 (Winter 2001/02). P. 186.
4. Уэсселер Р. Война как услуга / пер. с нем. Г. Сахацкого. Москва: Столица-Принт, 2007.
5. Валецкий О. Частные военные компании, их создание, развитие и опыт работы в Ираке и других регионах мира. URL:



- <http://www.vrazvedka.ru/main/analytical/valeckiy.html> (дата звернення: 23.04.2020).
6. Небольшая статистика по морским ЧВК. URL: <http://ir-ingr.livejournal.com/883373.html> (дата звернення: 15.05.2020).
  7. Ю. Мукин. Использование гражданских контрактников и частных вооружённых формирований в современных конфликтах. *Зарубежное военное обозрение*. 2008. № 6 (735). С. 26 – 31.
  8. В. Солдатов. Обсуждается проблема наёмников. *Известия*. 1987. № 21 (21828).
  9. Капитан 1 ранга А. Логунов. Зарубежные негосударственные субъекты военно-политических отношений в XXI веке. *Зарубежное военное обозрение*. 2006. № 3 (708).
  10. Горovenko В., Тютюнник В. Приватні військові компанії: міжнародний досвід і можливі шляхи його реалізації в Україні. URL: <https://www.ukrmilitary.com/2015/11/private-military-companies.html> (дата звернення: 15.05.2020).
  11. Michael Hirsh. The Age of Irresponsibility. How Bush has created a moral vacuum in Iraq in which Americans can kill for free. *Newsweek*. 2007. 20 сентября.
  12. История создания российских ЧВК. *The Bell*. 2019. 29 січня.
  13. Танкісти ПВК “Вагнера” на службі Росії від Донбасу до Сирії. URL: <https://uk.wikipedia.org/wiki/ПВК-Вагнера> (дата звернення: 15.05.2020).
  14. Гольц А. Почему в России решили не легализовывать ЧВК. URL: <https://openmedia.io/news/pochemu-v-rossii-reshili-ne-legalizovyvat-chvk> (дата звернення: 22.05.2020).
  15. Розвідка США: російська “група Вагнера” бере активну участь у конфлікті в Лівії. *Info@lb.ua*, 23.04.2020.
  16. Лівія звинуватила ПВК Вагнера у застосуванні хімічної зброї. *Info@lb.ua*, 23.04.2020.
  17. ЧВК Вагнера: все, что о ней известно. *Deutsche Welle*, 2020.
  18. Белоусов О. М., Григорьев И. В. Частные военные компании, история образования и перспективы развития. *Ростовский научный журнал*. 2018. № 11. С. 57–65.
  19. Дмитро Веденєєв. Армія тіньової світобудови. Чи потрібні Україні приватні військові компанії?. URL: [https://defence-ua.com/army\\_and\\_war/armija\\_tinovoji\\_svitobudovi\\_chi\\_potribni\\_ukrajini\\_privatni\\_vijskovi\\_kampaniji-331.html](https://defence-ua.com/army_and_war/armija_tinovoji_svitobudovi_chi_potribni_ukrajini_privatni_vijskovi_kampaniji-331.html) (дата звернення: 22.05.2020).
  20. ПВК-Лихоманка: Російські приватні армії. URL: <http://informnapalm.rocks/pmc-rush-ua> (дата звернення: 22.05.2020).

Стаття надійшла до редакційної колегії 09.12.2020

## The role of private military companies in military conflicts: history and modernity

### Annotation

Numerous publications reveal some aspects of the creation and operation of private military companies (PMC), the use of their services by various states and international organizations. It is also noted that recently the number and equipment of these companies has increased significantly, the role in military conflicts in different regions of the world is becoming crucial in some places. A retrospective analysis of the activities of PMC, their classification and role in modern military conflicts is an urgent task in terms of ensuring the military security of Ukraine.

In the context of further globalization of the world economy, the role of PMC in future wars and armed conflicts will increase. Unlike traditional military and police institutions, which are governed by both international and national law, there is currently no legal framework for PMC activities at the international and national (excluding the United States and South Africa) levels. The Geneva Conventions are not an obstacle for western PMC, even when these organizations use their contractors in open battles.

As long as PMC personnel are not part of the armed forces of the parties to the conflict and are not directly involved in hostilities, they should be treated as civilians and enjoy the protection of International Humanitarian Law (IHL). In the case of direct participation in an armed conflict, the contractors lose the right to protection and may be attacked, and when captured they do not have the status of prisoners of war, but are provided with the full range of protection under the Fourth Geneva Convention.

Involvement of private commercial structures in the provision and, often, combat operations, as well as the emergence of their own armies in large international corporations, the close intertwining in the conflict zone of interests of state and non-state actors significantly changes the image of modern war military construction.

**Keywords:** private military company; military conflicts; combat actions; mercenaries; armed forces.

Лепіхов А. В.<sup>1</sup>

(0000-0003-0745-8113)

Храпач Г. С.<sup>2</sup>

(0000-0002-1089-1535)

<sup>1</sup> – Національний інститут стратегічних досліджень, Київ;

<sup>2</sup> – Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

## Проектна діяльність у сфері забезпечення національної стійкості: сутність, зміст, структура

**Резюме.** Метою статті є визначення сутності, змісту та структури проектної діяльності у сфері забезпечення національної стійкості. Для вирішення завдань дослідження використовувалися проблемно-структурний, програмно-середовищний та компаративний методи. Зміст соціального проектування системи забезпечення національної стійкості передбачає визначення місії, цілей, функцій і завдань, а також розроблення механізмів забезпечення національної стійкості. У статті визначено структуру проектної діяльності у сфері забезпечення національної стійкості України в умовах динамічного безпекового середовища, яка містить п'ять етапів.

**Ключові слова:** гібридні загрози; гібридна війна; національна безпека; національна стійкість; система національної безпеки; система забезпечення національної стійкості.

**Постановка проблеми.** Згідно з п. 47 Стратегії національної безпеки України від 14.09.2020 “Україна запровадить національну систему стійкості для забезпечення високого рівня готовності суспільства і держави до реагування на широкий спектр загроз...” [1]. У п. 4, розділу I цієї стратегії поняття “стійкість” визначається як здатність суспільства та держави швидко адаптуватися до змін безпекового середовища і підтримувати стале функціонування, зокрема, шляхом мінімізації зовнішніх і внутрішніх уразливостей. У Річній національній програмі під егідою Комісії Україна – НАТО на 2020 рік визначено мету впровадження “національної системи стійкості”, а Ціль 1.6.4 цього документа [2] потребує її створення до кінця 2025 р. Це завдання передбачатиме вжиття комплексних заходів щодо розвитку стійкості як до традиційних загроз (природних, техногенних, біологічних, екологічних, соціальних, воєнних), так і до безпрецедентних, зокрема, гібридних загроз. До того ж, за результатами аналізу наукових досліджень вітчизняних науковців доцільно констатувати, що словосполучення “національна система стійкості” використовується у цих та інших нормативно-правових документах України у значенні “система забезпечення національної стійкості”, яка являє собою організаційний і нормативно-правовий механізм, який упорядковує діяльність суб'єктів системи у рамках визначеної моделі та національних інтересів [24].

Отже вимоги зазначених нормативно-правових документів визначають зв'язок загальної проблеми вивчення феномену “національної стійкості” з найбільш важливими науковими та практичними завданнями дослідження проблем теорії та практики розбудови системи національної безпеки України на сучасному етапі державного будівництва, а також адаптації досвіду держав – членів ЄС та НАТО щодо забезпечення національної стійкості для потреб Української держави.

**Аналіз останніх досліджень і публікацій.** Явище “гібридні загрози” досліджували як вітчизняні науковці [3–11], так й іноземні дослідники [12–14]. Крім того, українськими науковцями досліджувалися характерні риси і особливості розбудови системи національної безпеки та системи забезпечення національної безпеки адаптивного і креативного типу (остання є найбільш прийнятною для протидії гібридним загрозам) [15, 16]; концептуальні підходи до розбудови системи забезпечення національної стійкості до широкого спектру загроз [17–25]. Аналіз результатів указаних наукових досліджень дає змогу констатувати, що одними з ключових завдань розбудови системи національної стійкості України є:

1) вивчення трендів світового розвитку, розвитку зовнішнього та внутрішнього безпекового середовища конкретної держави, які мають ґрунтуватися на фундаментальних наукових знаннях щодо закономірностей розвитку глобалізованого світу, із застосуванням перспективних методів

стратегічного аналізу та довгострокового прогнозування, поміж інших, таких як “сканування горизонту подій”;

2) розроблення та запровадження у вітчизняну практику забезпечення національної безпеки методики комплексної оцінки загроз, зокрема, оцінки широкого спектру традиційних і нетрадиційних загроз, які у сукупності можуть мати ознаки гібридності – такі методики широко застосовуються у державах - членах НАТО;

3) вивчення та оцінювання можливостей застосування в Україні позитивного досвіду держав – членів НАТО щодо розвитку спроможностей і забезпечення готовності сектору безпеки і оборони до кризових та надзвичайних ситуацій (моніторинг, аналіз і прогнозування змін безпекового середовища, оцінювання ризиків і загроз, виявлення вразливостей, оцінювання наявних спроможностей, планування, розвиток спроможностей і готовності, профілактика, реагування, відновлення).

Незважаючи на значну кількість робіт, у яких досліджуються проблеми розбудови системи національної безпеки України на сучасному етапі державного будівництва маємо констатувати, що на сьогодні ще обмаль наукових праць у яких би розглядалися проблеми теорії і практики проектування та конструювання системи забезпечення національної стійкості України на основі дотримання одного з принципів організації систем безпеки – врахування зовнішніх процесів для кореляції та адаптації внутрішньосистемних властивостей і зв'язків системи безпеки.

Саме тому **мета статті** полягає у визначенні сутності, змісту та структури проектної діяльності у сфері забезпечення національної стійкості.

Для вирішення завдань дослідження використовувалися: проблемно-структурний метод, який ґрунтується на принципах проблематизації, структуризації і дивергенції; програмно-середовищний метод, який ґрунтується на принципах програмування, визначального впливу середовища, і конвергенції; метод порівняльного аналізу для вивчення першоджерел з проблематики дослідження, а також для узагальнення зарубіжного досвіду забезпечення національної стійкості.

**Виклад основного матеріалу.** На підставі аналізу результатів наукових досліджень [26–31] встановлено, що складовими проектної діяльності у сфері

забезпечення національної стійкості є проектування та конструювання системи забезпечення національної стійкості. До того ж з'ясовано, що сутність соціального проектування системи забезпечення національної стійкості полягає у проектній діяльності із конструювання ідеальної моделі вказаної системи. Зміст соціального проектування системи забезпечення національної стійкості передбачає визначення місії, цілей, функцій і завдань вказаної системи, а також розроблення механізмів забезпечення національної стійкості. Сутність соціального конструювання системи забезпечення національної стійкості, як завершального етапу процесу проектування, полягає у впровадженні проекту в соціальну матерію відповідно до вимог місії та завдань вказаної системи. Зміст соціального конструювання передбачає: політико-правове, структурно-функціональне, просторове, часове, організаційне, операційно-діяльнісне конструювання.

Поцінуючи напрацювання Ю. Сурміна [27] запропоновано структуру соціального проектування системи забезпечення національної стійкості, яка містить такі етапи:

**1 етап.** Усвідомлення і формулювання практичної проблемної ситуації у сфері забезпечення національної стійкості в умовах динамічного та агресивного безпекового середовища, що характеризується широким спектром загроз, зокрема реалізацією гібридних загроз.

Варто зазначити, що у концепції “NATO’s Bi-Strategic Command Capstone Concept” (2010) [20], поняття “гібридні загрози” визначено як загрози, які створені супротивниками, здатними одночасно адаптовано використовувати традиційні та нетрадиційні засоби для досягнення власних цілей. У спільній концепції протидії гібридним загрозам Європейського Союзу від 06.04.2016 поняття “гібридні загрози” визначено як поєднання примусової та підривної діяльності, традиційних і нетрадиційних методів (тобто дипломатичних, військових, економічних, технологічних), які можуть бути скоординовано використані державними або недержавними суб'єктами для досягнення конкретних цілей, залишаючись на рівні нижче порогу формально оголошеної війни [21].

Аналіз наведених концепцій НАТО і ЄС [32, 33], а також досліджень вітчизняних науковців [3–14, 19–21] свідчить про те, що

джерелами гібридних загроз можуть бути окремі держави, транснаціональні корпорації (ТНК), а силовим інструментарієм – структури міжнародного тероризму і транснаціональної організованої злочинності, приватні воєнні компанії та інші іррегулярні та парамілітарні формування. Гібридні загрози являють собою спектр загроз, які штучно створюються їх ініціатором в рамках заздалегідь розробленого задуму та зорієнтовані на обраний об'єкт впливу (конкретну державу і суспільство). Ініціатори гібридних загроз із числа суб'єктів міжнародних відносин (держави, ТНК та ін.) здатні створювати центри координації та управління гібридними загрозами. До того ж, як правило, вони офіційно не визнають своєї прямої причетності до джерел гібридних загроз, але комплексно застосовують невійськові засоби і заходи тиску: політичні, дипломатичні, економічні, інформаційні, психологічні тощо. Гібридні загрози можуть комплексно являти собою різноманітну інтерпретацію сукупних проявів, зокрема: сценаріїв асиметричних конфліктів низької інтенсивності; терористичних актів; організованих злочинних дій; кібератак; диверсій та інших форм розвідувально-підривної діяльності; вбивств, неконтрольованої масової нелегальної міграції; дестабілізації суспільно-політичної ситуації в країні, які призводять до масових соціальних заворушень насильницького характеру; створення небезпек для критичної інфраструктури держави. Під час реалізації гібридних загроз можуть застосовуватися різноманітні засоби і способи досягнення цілей, а також поєднуватися як збройні, так і невійськові форми та методи насилля. Зокрема, не виключено ймовірність застосування небезпечних біологічних, хімічних, радіологічних і ядерних матеріалів. Заходи можуть проводитись із застосуванням технологій: політичної дестабілізації суспільства екстремістськими, сепаратистськими та терористичними організаціями; прихованим втручанням у політичні вибори; створення ситуації економічної нестабільності; регіональної дезінтеграції держави [6]. Як правило, процес дестабілізації супроводжується інформаційно-психологічними операціями та пропагандистськими кампаніями [3].

Основними цілями реалізації гібридних загроз є: створення передумов для десоверенізації держави – об'єкта гібридних загроз; створення тиску на владу такої країни шляхом реалізації розширеного спектру

взаємопов'язаних загроз у різних сферах національної безпеки; підриву стійкості і позицій держави та її влади у середині країни та на міжнародній арені; послаблення опору уряду таких держав у переговорних процесах і їх примусу до поступок [3, 6, 11].

Гібридним загрозам характерна комплексність, взаємодоповненість, висока ступінь асиметричності та непередбачуваності. Вони утворюють більш складну та багатовимірну загрозу. Синергетичність їх прояву та націленість на створення ситуації дезорієнтації та дезадаптації суб'єктів забезпечення національної безпеки можуть спричинити катастрофічні наслідки для безпеки людини, суспільства, держави.

Процес реалізації гібридних загроз може стати первинним етапом перед початком гібридних війн. У вітчизняному науковому дискурсі визначено такі змістовні виміри гібридної війни, як: воєнні дії, що здійснюються через поєднання мілітарних, квазімілітарних, дипломатичних, інформаційних, економічних та інших засобів для досягнення державою-агресором своїх стратегічних політичних цілей у війні [3]; використання воєнних і невоєнних інструментів в інтегрованій кампанії, спрямованій на досягнення раптовості, захоплення ініціативи та отримання психологічних переваг для використання у дипломатичних діях; форма збройних конфліктів, яким характерно комплексне застосування військової сили у поєднанні з невійськовими технологіями ведення війни, зокрема, застосування інформаційних, електронних, кібернетичних операцій у поєднанні з діями збройних сил, спеціальних служб та економічним тиском [10].

Так, явища “гібридні загрози” та “гібридні війни” мають одну спільну характерну рису – наявність високого ступеня асиметричності, невизначеності та раптовості. За таких умов динамічного та агресивного безпекового середовища, система національної безпеки може мати такі стани:

стабільно стійкий, за якого система національної безпеки протягом тривалого часу функціонує в безпековому середовищі, зберігаючи свою цілісність;

нестабільно стійкий, за якого стійкість системи національної безпеки до впливів безпекового середовища спостерігається на невеликих проміжках часу;

стабільно нестійкий, за якого упродовж тривалого часу безпекове середовище впливає

на внутрішній стан системи національної безпеки, яка постійно змінюється, втрачає цілісність, стає хаотичною, й насамкінець руйнується;

нестабільно нестійкий, за якого нестійкість системи національної безпеки до впливу безпекового середовища спостерігається на невеликих проміжках часу.

Є сенс зауважити, що відповідно до теорій модернізації, трансформації і катастроф, стійкість будь-якої соціальної системи зумовлена дією двох тенденцій: одна з яких відтворює і зберігає “старі” системні якості, а друга забезпечує пошук нового, прогресивного, щоб адаптувати соціальні структури до нових історичних умов. До того ж стабільність соціальних систем співвідноситься з оперативними та тактичними параметрами соціальної динаміки, а стійкість – зі стратегічними [30, с. 49].

На думку В. Кириленка [29] та В. Абрамова [28] система національної безпеки повинна мати низку характерних рис:

вона має бути керована, спостережувана та ідентифікована;

за її створення можливе існування дестабілізуючих елементів підсистем, наприклад, підсистеми забезпечення національної безпеки, саме тому мають бути відрегульовані заходи для забезпечення стійкості системи національної безпеки в цілому;

необхідне виокремлення рівнів національної безпеки за принципом їхньої відносної самостійності, оскільки кожен рівень являє собою локальну підсистему, поєднану з іншими структурними елементами (підпорядкованість рівнів);

контроль за функціонуванням усіх її елементів.

Отже, найважливішими рисами системи національної безпеки є суспільний розвиток і національна стійкість.

Вітчизняний дослідник В. Кириленко під поняттям “стійкість” пропонує розуміти “здатність суспільства і в критичних умовах задовольняти свої інтереси, можливість відновлювати становище” [29].

Вітчизняна дослідниця О. Резнікова визначає поняття “національна стійкість” як “здатність держави і суспільства ефективно протидіяти загрозам будь-якого походження і характеру, адаптуватись до змін безпекового середовища, підтримувати стаке функціонування до, під час і після кризи, швидко відновлюватися до бажаної рівноваги” [24]. О. Резнікова надає визначення терміну

“Національна система стійкості” як “комплексний механізм взаємодії органів державної влади і місцевого самоврядування, підприємств, установ, організацій, громадянського суспільства, а також цілеспрямованих дій, методів, чинників і механізмів, які гарантують збереження безпеки і безперервності функціонування основних сфер життєдіяльності суспільства і держави до, під час і після кризи” [24]. Сутність системи забезпечення національної стійкості як складової системи національної безпеки, вона розкриває як “сукупність взаємодіючих суб’єктів, цілеспрямованих дій, методів, чинників і механізмів, які гарантують збереження безпеки і безперервності функціонування національних систем до, під час і після кризи завдяки адаптації до дії загроз і швидких змін безпекового середовища” [17].

**2 етап.** Збирання інформації, а також вивчення накопиченого досвіду перетворення дійсності, розроблення та впровадження у державно-управлінську практику забезпечення національної стійкості аналогічних проєктів.

Аналіз результатів наукових досліджень О. Резнікової дає змогу констатувати, що забезпечення національної стійкості до широкого спектру ризиків і загроз є практикою, яка запроваджена у передових державах – членах ЄС та НАТО у сфері забезпечення національної безпеки [18, 23].

**3 етап.** Обґрунтування можливості та доцільності проєкту, формулювання його задуму і розроблення концепції.

Наразі позитивний досвід держав – членів НАТО щодо забезпечення національної стійкості визнається вищими політичним керівництвом України як один із основних напрямів зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення національної безпеки [1]. Європейська та євроатлантична інтеграція України обумовлює доцільність упровадження стандартів НАТО у вітчизняну практику забезпечення національної стійкості. Вбачається, що у контексті гібридних загроз, система забезпечення національної стійкості має забезпечувати розвиток спроможностей та готовності сектору безпеки і оборони до надзвичайних ситуацій та інших кризових подій, наслідки від яких можуть мати багатокаскадний ефект.

Є сенс зауважити, що на етапі формулювання задуму проєкту та створення концепції проєктування системи національної

стійкості варто враховувати в рамках системно-діяльнісного підходу [31]:

базові цінності суспільства – добробут, безпека, справедливість та національні цінності, ідеали культури національної безпеки, стратегічної, воєнної та організаційної культури суспільства;

національні інтереси та цілі у сфері національної безпеки і суспільного розвитку;

цивілізаційний і геополітичний коди держави;

інтегральний показник національної могутності держави;

панівний тип комунікації в суспільстві та тип політичного режиму;

діалектичний взаємозв'язок між економікою, політикою та війною, суспільним розвитком і безпекою, культурою та ідеологією національної безпеки;

наукові закони геоекономіки, геополітики, війни;

закономірності геополітичного протистояння, збройної та інформаційної боротьби;

закономірності розгортання криз соціоприродних і соціальних систем;

сучасні тренди розвитку світової цивілізації;

глобальні трансформації у різних сферах суспільного життя, й зокрема, у сфері політики та економіки, міжнародної і національної безпеки;

зміни організаційно-функціональних форм державного управління;

результати порівняльного аналізу світового досвіду розбудови систем міжнародної та регіональної безпеки, зарубіжного досвіду розбудови систем національної безпеки та систем забезпечення національної стійкості;

результати пошукового та нормативного прогнозування у сфері міжнародної та національної безпеки, зокрема сучасні тренди розвитку загроз.

Класифікацію вказаних загроз за критеріями: об'єкт безпеки; джерело загрози та інше наведено у табл. 1.

Таблиця 1

**Багатокритеріальні класи загроз**

<b>Класи</b>	<b>Критерії загроз</b>
<b>Клас А</b>	Загрози з високим ступенем непередбачуваності через їх міжсекторальний і міжгалузевий характер та синергію прояву наслідків
<b>Клас Б</b>	Загрози, які супроводжуються із застосуванням воєнної сили у поєднанні з невійськовими технологіями проведення війни: демонстрація воєнної сили; реалізація сценаріїв асиметричних конфліктів низької інтенсивності; диверсії; застосування технологій політичної дестабілізації суспільства екстремістськими, сепаратистськими та терористичними організаціям; приховане втручання у політичні вибори; розповсюдженням екстремістських ідеологій тощо
<b>Клас В</b>	Загрози зовнішньополітичній безпеці держави, які взаємодоповнюють одна одну: геополітичний, геоекономічний та воєнно-політичний тиск на державу; порушення критично важливих процесів у забезпеченні міжнародної і регіональної безпеки на шкоду держави; внесення конфронтації між союзними державами; запровадження політичних, фінансових, торгівельно-економічних та інших санкцій проти держави та ін.
<b>Клас Г</b>	Загрози міжнародній безпеці, які комплексно та штучно зорієнтовані на шкоду державі-мішені: міжнародний тероризм, кібертероризм, транснаціональна організована злочинність, масова нелегальна міграція, піратство, міжнародна наркоторгівля та ін.
<b>Клас Д</b>	Загрози внутрішньообезпеченого характеру, які через деструктивний зовнішній вплив комплексно створюють небезпеки для функціонування держави: у сферах державного і воєнного управління, боротьби із корупцією, організаційно-правового регулювання, безперебійності функціонування антикризового управління, сектору безпеки і оборони, політичної системи, економіки, енергетики, критичної інфраструктури життєдіяльності держави і населення та в інших сферах країни
<b>Клас Е</b>	Загрози інформаційного характеру, які пов'язані із проведенням інформаційно-психологічних операцій, кібератак, поширенням дезінформації та ворожої пропаганди, а також зорієнтованих на руйнацію ментально-ціннісних та політико-ідеологічних основ суспільства
<b>Клас Є</b>	Загрози, які згруповані за пріоритетом державного реагування на них та їх наслідки
<b>Клас Ж</b>	Загрози, які згруповані за ступенем важливості і терміновості нарощування спроможностей для посилення національної стійкості
<b>Клас З</b>	Загрози, які згруповані за методичними особливостями розроблення державної політики щодо реагування на гібридні загрози та ін.
<b>Клас...</b>	.....

**4 етап.** Формування завдання щодо проектування системи забезпечення національної стійкості та визначення вимог до проекту.

Для проектування системи забезпечення національної стійкості використовуються

проблемно-структурний та програмно-середовищний методи.

Проектування системи забезпечення національної стійкості структурно включає в себе структурно-функціональне моделювання процесу забезпечення національної стійкості,

просторове, часове, оперативно-діяльнісне, інституційне, організаційне проектування вказаної системи. Соціальне проектування системи забезпечення національної стійкості передбачає визначення місії, функцій і завдань вказаної систем, а також механізмів забезпечення національної стійкості. При цьому в рамках інституціонального підходу необхідно враховувати закономірності розвитку триад “культура – інститути – економіка”, “економіка – політика – війна”, “війна – зброя – насильство”, “насильство – інститути – організації”, “організація – ресурси – час”. Це дає змогу проектувальникам виявити перспективні моделі системи забезпечення національної стійкості, що узгоджується зі станом і перспективами геополітичного, суспільно-політичного і соціально-економічного розвитку Української держави [31].

**5 етап.** Соціальне конструювання системи забезпечення національної стійкості, як завершальний етап проектної діяльності, передбачає впровадження проекту в державно-управлінську практику відповідно до вимог щодо виконання завдань системи національної безпеки, а саме:

1) *політико-правове конструювання:*

удосконалення національного законодавства щодо розвитку готовності сектору безпеки і оборони до реагування на гібридні загрози;

активна участь держави у процесах удосконалення міжнародного права у сфері протидії гібридним загрозам;

законодавче забезпечення процесів стратегічного планування в державі з урахуванням принципів сталого розвитку, безпеки і стійкості;

розвиток єдиної нормативно-правової бази у сфері планування та реагування на кризові ситуації та загрози для скоординованих дій державних органів;

2) *структурно-функціональне конструювання* – створення нових та удосконалення вже існуючих елементів, структур, підсистем, механізмів забезпечення національної стійкості та встановлення зв'язків між ними:

розвиток єдиної системи стратегічного планування та її методологічної основи, яка комплексно об'єднуватиме безпекову сферу та сфери сталого і регіонального розвитку держави і суспільства;

створення державного координуючого органу у сфері забезпечення національної

стійкості (національного координатора) та структури його допоміжних органів;

розвиток національної мережі уповноважених державних органів і наукових установ з питань стратегічного аналізу і прогнозування, стратегічного планування;

розвиток ефективної взаємодії державних органів (як сектору безпеки і оборони, так і інших), громад, бізнесу і населення у запобіганні й реагуванні на загрози та подоланні наслідків їх реалізації, а також координації такої діяльності;

удосконалення державних систем боротьби з тероризмом, цивільного захисту, територіальної оборони та захисту державних кордонів;

3) *просторове та часове конструювання* – розміщення створення нових елементів, структур, підсистем, механізмів забезпечення національної стійкості у своєму типу соціального простору та соціальному часі:

забезпечення створення необхідних резервів і розвитку спроможностей держави щодо реагування на загрози національній безпеці у різних сферах;

4) *організаційне конструювання* – формування алгоритмів функціонування системи національної безпеки та системи забезпечення національної стійкості, а також підготовки фахівців у сфері національної безпеки:

запровадження повного циклу забезпечення національної стійкості (моніторинг, аналіз і прогнозування, оцінювання загроз, виявлення вразливостей, забезпечення готовності, планування, профілактика, реагування, відновлення) та ефективного функціонування єдиного комплексного механізму координації цієї діяльності;

удосконалення кризового менеджменту; забезпечення розподілу відповідальності та повноважень державних органів за визначеними напрямками забезпечення національної стійкості;

забезпечення безперервності основних процесів у державі (урядування, надання критично важливих для суспільства послуг, бізнес-процесів тощо);

підвищення рівня ефективної протидії загрозам для критичної інфраструктури країни, її захист від можливих диверсій, терористичних актів і кібератак, а також забезпечення достатнього рівня пожежної і техногенної безпеки;

активізація розвідувальної діяльності, спрямованої на викриття можливих планів, намірів та ходу підготовки потенційних супротивників до війни проти держави із застосуванням нових форм її проведення;

розвиток надійних і постійно діючих двосторонніх каналів комунікацій держави з населенням;

проведення підготовки (теоретичної, практичної) усіх наявних сил і населення на національному, регіональному та місцевому рівнях держави до реагування на гібридні та інші загрози та превентивної мінімізації або нейтралізації можливих негативних наслідків надзвичайних ситуацій;

5) *операційно-діяльнісне конструювання* – розроблення правил і принципів діяльності у сфері забезпечення національної стійкості: запровадження єдиних стандартів та рекомендацій (інструкцій) з питань забезпечення національної стійкості.

**Висновки.** З огляду на наведене підсумуємо:

1. З'ясовано, що сутність соціального проектування системи забезпечення національної стійкості полягає у проектуванні ідеальної моделі вказаної системи. Зміст соціального проектування системи забезпечення національної стійкості передбачає визначення місії, цілей, функцій і завдань вказаної системи, а також розроблення механізмів забезпечення національної стійкості. Сутність соціального конструювання системи забезпечення національної стійкості, як етапу процесу проектування, полягає у впровадженні проекту в соціальну матерію відповідно до вимог місії та завдань вказаної системи. Зміст соціального конструювання передбачає: політико-правове, структурно-функціональне, просторове, часове, організаційне, операційно-діяльнісне конструювання.

2. Визначено, що структура проектно-діяльності у сфері забезпечення національної стійкості України в умовах динамічного безпекового середовища містить п'ять етапів:

усвідомлення і формулювання практичної проблемної ситуації у сфері забезпечення національної стійкості в умовах динамічного та агресивного безпекового середовища, що характеризується реалізацією гібридних загроз;

збирання інформації, а також вивчення накопиченого досвіду перетворення дійсності, розроблення та впровадження у державно-управлінську практику забезпечення національної стійкості аналогічних проєктів;

обґрунтування можливості й доцільності проєкту, формулювання його задуму та розроблення концепції;

формування завдання щодо проектування системи забезпечення національної стійкості та визначення вимог до проєкту;

соціальне конструювання системи забезпечення національної стійкості, як завершальний етап проектно-діяльності, що передбачає впровадження проєкту в державно-управлінську практику відповідно до вимог щодо виконання завдань системи національної безпеки.

Перспективним **напрямом подальших досліджень** вбачається розроблення методики соціального проектування системи забезпечення національної стійкості.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про Стратегію національної безпеки України : Указ Президента України від 14.09.2020 р. №392/2020. URL: <https://zakon.rada.gov.ua/laws/show/n0005525-20#Text> (дата звернення: 08.12.2020).
2. Про Річну національну програму під егідою Комісії Україна-НАТО на 2020 рік : Указ Президента України від 26.05.2020 р. №203/2020. URL: <https://www.president.gov.ua/documents/2032020-33861> (дата звернення: 08.12.2020).
3. Горбулін В. П. Світова гібридна війна: український фронт : монографія / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 496 с.
4. Ситник Г. П. Вплив глобалізації на воєнну сферу та принципові особливості сучасних воєнних конфліктів. URL: <http://nationalecurity.org.ua/2016/07/06/vpliv-globalizaciina-voehnnu-sferu-ta-principovi-osobli-vosti-suchasnikhvoehnnikh-konfliktiv/> (дата звернення: 10.12.2020).
5. Горovenko В. К. Боротьба в економічній сфері як складова гібридної війни. URL: <https://niss.gov.ua/sites/default/files/2019-07/Економічна%20боротьба.pdf> (дата звернення: 10.12.2020).
6. Шевченко М. М., Соколов В. А., Давиденко О. Г., Курганевич В. І., Масовець В. П. Сучасні тенденції міждержавного протистояння та стратегії державного реагування на загрози територіальній цілісності України. *Державне управління: удосконалення та розвиток*. 2017. № 9. URL: [http://nbuv.gov.ua/UJRN/Duug\\_2017\\_9\\_5](http://nbuv.gov.ua/UJRN/Duug_2017_9_5) (дата звернення: 04.12.2020).
7. Почепцов Г. Г. Из истории понятия гибридной войны в США и России (2015) URL: <http://www.academia.edu/17801641> (дата звернення: 04.12.2020).
8. Мартинюк В. Гібридні загрози Україні та суспільна безпека. Досвід ЄС і східного партнерства (2018) URL: <https://geostrategy.org.ua/ua/analitika/item/1401->



- hibrydni-zagrozy-i-syspilna-bezpeka (дата звернення: 09.12.2020).
9. Воротнок М. О. Особливості міжнародних конфліктів постбіполярного періоду. *Стратегічна панорама*. 2009. Вип. 4. URL: <http://www.niisp.org.ua/default3.php> (дата звернення: 09.12.2020).
  10. Воєнні аспекти протидії “гібридній” агресії: досвід України : монографія / колектив авторів ; за заг. ред. А. М. Сиротенка. Київ : НУОУ ім. Івана Черняхівського, 2020. 176 с.
  11. Смолянчук В. Ф. Десуверенізація сучасних держав як наслідок глобалізації (22.04.2015). URL: <http://nationalsecurity.org.ua/2015/04/22/desuvereni-zaciya-suchasnikh-derzhav-yak-naslidok-globalizacii> (дата звернення: 04.12.2020).
  12. Арзуманян Р. В. Стратегия иррегулярной войны: теория и практика применения. URL: <http://csef.ru/ru/oborona-i-bezopasnost/504/arzumanyanrv-strategiya-irregulyarnoj-vojniy-teoriya-i-praktikaprimeneniya-60941> (дата звернення: 10.12.2020).
  13. Хофман Ф. Гибридные угрозы (21.10.2013). URL: <http://navoine.info/hybriddange.html> (дата звернення: 10.12.2020).
  14. Лютвак Э. Государственный переворот : практ. пособ. 2012. URL: <https://mybook.ru/author/edvardlyuttvak/gosudarstvennyj-perevorot-prakticheskoe-posobie/read/> (дата звернення: 10.12.2020).
  15. Семенченко А. І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України : монографія. Київ : НАДУ, 2008. 428 с.
  16. Шевченко М. М., Зозуля О. С. Системи забезпечення національної безпеки адаптивного та креативного типів: порівняльний аналіз. *Інвестиції: практика та досвід*. 2015. № 16. С. 125–129.
  17. Резнікова О. О. Розбудова національної стійкості: концептуальні підходи, передові світові практики. 2019. URL: [https://niss.gov.ua/sites/default/files/2019-11/roa\\_presentation\\_niss\\_v01.pdf](https://niss.gov.ua/sites/default/files/2019-11/roa_presentation_niss_v01.pdf) (дата звернення: 10.12.2020).
  18. Резнікова О. О., Войтовський К. С., Лепіхов А. В. Організація системи забезпечення національної стійкості на регіональному і місцевому рівнях : аналіт. доповідь / за заг. ред. О. О. Резнікової. Київ : НІСД, 2021. 112 с. URL: <https://niss.gov.ua/publikacii/analitichni-dopovidi/organizaciya-sistemi-zabezpechennya-nacionalnoi-stiykosti-na> (дата звернення: 10.12.2020).
  19. Майбутнє безпекове середовище 2030: стратегічне передбачення (попередній опис) : монографія / В. В. Скібіцький та ін. Київ, 2020. 51 с.
  20. Zhytnyk O. M. Quo vadis das Phänomen des Krieges? Der Frieden ohne den Krieg oder der Krieg ohne das Frieden. *East European Scientific Journal*. 2018. № 4 (32). P. 26–31.
  21. Шевченко М. М. Феноменологія воєнно-політичного конфлікту. *Virtus*. 2018. № 26. С. 38–42.
  22. Кириленко В. І., Шевченко М. М. Методологія побудови та використання комплементарної моделі національної економічної безпеки. *Науковий вісник Дипломатичної академії України*. 2015. Вип. 22. Частина III. С. 40–50.
  23. Резнікова О. О., Войтовський К. С., Лепіхов А. В. Національні системи оцінювання ризиків і загроз: кращі світові практики, нові можливості для України : аналіт. доп. / за заг. ред. О. О. Резнікової. Київ : НІСД, 2020. URL: <https://niss.gov.ua/publikacii/analitichni-dopovidi/nacionalni-sistemi-ocinki-riziki-v-i-zagrozk-raschi-svitovi-praktiki> (дата звернення: 12.12.2020).
  24. Резнікова О., Войтовський К. Проблема термінологічної невизначеності у сфері розбудови національної стійкості. URL: <https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/problema-terminologichnoi-neviznachenosti-u-sferi-rozbudovi> (дата звернення: 12.12.2020).
  25. Лепіхов А. В. Причини та характер сучасних міжнародних конфліктів. *Досвід застосування збройних сил у війнах і воєнних конфліктах ХХ – початку ХХІ ст.: тенденції та закономірності* : зб. наук. праць. Київ, 2016. Вип. 5. С. 157–163.
  26. Кримський С. Б. Запити філософських смислів. Київ : ПАРАПАН, 2003. 240 с.
  27. Сурмин Ю. П. Социальное проектирование в кризисном обществе: методологический аспект. *Вісник Національної академії державного управління при Президенті України*. Київ, 2014. № 3. С. 5–17.
  28. Абрамов В. І. Духовність суспільства: методологія системного вивчення : монографія. Київ : КНЕУ, 2004. 236 с.
  29. Кириленко В. І. Інвестиційна складова економічної безпеки : монографія. Київ : КНЕУ, 2005. 232 с.
  30. Михальченко М. І. Україна як нова історична реальність: запасний гравець Європи : монографія. Дрогобич : Відродження, 2004. 488 с.
  31. Шевченко М. М. Соціально-філософська концепція науково-освітнього забезпечення публічного управління у сфері національної безпеки України. *Гілея* : наук. вісн. Київ, 2018. Вип. 134. С. 320–325.
  32. BI-SC Inputfor a New NATO Capstone Conceptfor The Military Contributionto Countering Hybrid Enclosure 1 to 1500/PPCAM/FCR/10-270038 and 5000 FXX/0100/TT-0651/SER: NU0040, dated 25 August 2010. URL: [https://www.act.nato.int/images/stories/events/2010/20100826\\_bi-sc\\_cht.pdf](https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf) (дата звернення: 12.12.2020).
  33. Joint Framework oncounteringhybridthreats a EuropeanUnionresponse. JOIN/2016/018 final. eur-lex.europa.eu. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018> (дата звернення: 12.12.2020).

Стаття надійшла до редакційної колегії 06.01.2021

## **Project activities in the sphere of ensuring national resilience: essence, content, structure**

### **Annotation**

According to paragraph 47 of the National Security Strategy of Ukraine dated 14.09.2020: “Ukraine will introduce a national system of resilience to ensure a high level of readiness of society and the state to respond to a wide range of threats...”. This task will involve taking comprehensive measures to develop resilience to both traditional threats (natural, technogenic, biological, environmental, social, military) and unprecedented, including hybrid threats.

This circumstance determines the connection of the general problem of studying the phenomenon of “national stability” with the most important scientific and practical tasks of studying the problems of theory and practice of building Ukraine's national security system at the present stage of state building, and adapting the experience of EU and NATO national stability for the needs of the Ukrainian state.

It is determined that the structure of project activities in the sphere of ensuring the national stability of Ukraine in a dynamic security environment contains five stages:

- awareness and formulation of the practical problem situation in the sphere of ensuring national stability in a dynamic and aggressive security environment;
- gathering information, as well as studying the experience gained in the transformation of reality, development and implementation in public administration practice of ensuring the national sustainability of similar projects;
- substantiation of possibility and expediency of the project, formulation of its plan and development of the concept;
- formation of the task of designing a system for ensuring national stability and determining the requirements for the project;
- social construction of the system of national stability, as the final stage of project activities, which involves the implementation of the project in public administration practice in accordance with the requirements for the tasks of the national security system.

**Key words:** hybrid threats; hybrid warfare; National security; national resilience; national security system; system of ensuring national stability.

Федянович Д. Л., канд. військ. наук, ст. наук. співроб. (0000-0002-9896-8655)  
 Возняк С. М., канд. техн. наук, ст. наук. співроб. (0000-0002-9015-813X)  
 Доброгурський В. І. (0000-0002-5263-6102)

Національний університет оборони України імені Івана Черняхівського, Київ

## Рекомендації щодо протидії агентам впливу та рухам опору, які діють в інтересах держави – ініціатора гібридної агресії

**Резюме.** Запропоновано рекомендації щодо протидії агентам впливу та рухам опору, які діють в інтересах держави-агресора. Визначено основні сфери національної безпеки та об'єкти впливу, на які спрямована дія агентів впливу. Розкрито роль агентів впливу у дестабілізації суспільно-політичної обстановки. Запропоновано методи боротьби з агентами впливу, які доцільно застосовувати на прихованій фазі гібридної агресії. Наведено напрями удосконалення асиметричної протидії гібридним загрозам завдяки вирішенню проблемних питань протидії агентам впливу та рухам опору.

**Ключові слова:** агенти впливу; асиметрична протидія; гібридна агресія; рух опору; спеціальна операція; методи протидії; способи протидії агентам впливу.

**Постановка проблеми.** Досвід України у протидії гібридній агресії показав, що держава – ініціатор гібридної агресії використовує всі можливі інструменти та механізми для досягнення стратегічної цілі деструктивного впливу на відповідні сфери національної безпеки держави, проти якої вона здійснює агресію. До того ж залучаються всі можливі ресурси, зокрема ресурси агентів впливу (“п’ята колона”), які разом з опозиційними силами та рухом опору спроможні забезпечити сприяння реалізації планів держави-агресора, особливо на початку (у прихованій фазі) зародження воєнного конфлікту. Незважаючи на широке використання понять “агент впливу” та “рух опору”, спроби їхнього суто практичного (юридично значущого) застосування викликають значну кількість проблем. У сучасних умовах сферами діяльності “агентів впливу” та “рухів опору” є політична, економічна, інформаційна та частково військова. Організаційні форми їх діяльності в умовах демократичного суспільства та статуси “агентів впливу” роблять практично неможливим створення ефективної системи протидії, яка б урахувала всі можливі варіанти їх деструктивної діяльності, що і підтверджує актуальність теми.

**Аналіз останніх досліджень і публікацій.** У сучасних дослідженнях та публікаціях [1–10] приділяється достатньо уваги проблемам протидії гібридній агресії. Насамперед це пов’язано із ситуацією на Сході України, де відносини між суспільством та політичним керівництвом держави піддавалося певним впливам з боку осіб, які

на той час мали вплив на всі сфери життєдіяльності суспільства у Донецькій та Луганській областях і використовували це здебільшого у власних цілях. Водночас питанням нейтралізації, так званих, агентів впливу та рухів опору, які діють в інтересах держави-агресора приділяється недостатньо уваги. Системних досліджень з цього питання у відкритих джерелах не виявлено.

**Мета статті** – обґрунтування рекомендацій щодо протидії агентам впливу та рухам опору, що діють в інтересах держави – ініціатора гібридної агресії.

**Виклад основного матеріалу.** За оцінками експертів російські геополітичні амбіції є надзвичайно витратними, що обмежує можливості внутрішнього розвитку цієї країни. Це стимулює пошуки РФ можливостей обміну обтяжливих геополітичних активів на менш витратні, але більш для неї важливі, наприклад, встановлення контролю над Україною та іншими сусідніми країнами пострадянського простору. Російське керівництво й надалі докладатиме зусиль щодо схилення ключових провідних країн до компромісів завдяки привабливому для РФ вирішенню проблеми окупованих українських територій і надання їй права вето на характер і темпи європейської і євроатлантичної інтеграції України [10]. Більшість з цих завдань на сьогодні намагаються покласти на агентів впливу (АВ) через використання протестного потенціалу опозиційних сил і створення рухів опору у нашій державі.

Під агентами впливу розуміються особи, які ведуть розповсюдження ідей будь-

якої організації у середовищі, яке не належить до цієї організації. У політичній сфері агенти впливу зазвичай просувають інтереси іноземних держав або політичних партій. Такі особи є каналом поширення пропаганди, впроваджують ворожі наративи та меседжі в інформаційному просторі, забезпечують видимість суспільної підтримки чи осуду певних політико-управлінських рішень. У більш радикальних випадках вони можуть використовуватися для дестабілізації політичної системи держави, порушення суспільної злагоди та роздмухування конфліктних тем тощо. За даними [8] часто діяльність таких агентів впливу може майже не відрізнятися від їхньої повсякденної професійної діяльності, проте, реалізується в певному ракурсі. Наприклад, зменшення фінансування певних напрямів наукової чи військової сфери, ініціювання скорочень у структурах, що можуть становити небезпеку для іншої держави, під приводом “реформ” чи “оптимізації”. Під поняттям *рух опору* (РО) розуміються організовані зусилля частини населення країни, що спрямовані на опір легітимній владі та підрив громадського порядку і стабільності, які зумовлюються рішучими діями для досягнення успіху, зокрема радикальними методами.

Основними сферами впливу агентів впливу та рухів опору є економічна, політична й інформаційна сфери національної безпеки. Основними завданнями їх діяльності, особливо на початковій фазі розв’язання державою-агресором збройного конфлікту є створення соціально-політичної нестабільності у державі, дискредитація воєнно-політичного керівництва держави, введення в оману населення країни (через медійний простір) стосовно реалізації державної та воєнної політики. Це потребує не тільки оцінювання та прогнозування негативних наслідків їх діяльності для визначальних сфер національної безпеки, а й вироблення дієвих заходів протидії.

Запобігання несанкціонованим акціям, що організовуються АВ, зокрема за сприянням рухів опору має здійснюватися законними та легітимними методами, а організатори акцій нести юридичну відповідальність. В умовах дестабілізації соціально-політичної ситуації важливо проведення профілактичної та роз’яснювальної роботи серед населення країни з використанням усіх можливих ресурсів. Відомі методи протидії можна розділити на *дві групи* – профілактичні та

оперативні. Ці методи застосовуються одночасно та мають спільну мету протидії агентам впливу та діяльності рухів опору, яка спрямована на дестабілізацію обстановки в державі.

*Профілактичні методи*, як свідчить досвід, є достатньо ефективним механізмом із запобігання загрози дестабілізації внутрішньої соціально-політичної обстановки на початковому етапі розвитку збройного конфлікту змістом якого є створення протестного та масового руху опору державній владі. *Оперативні методи* використовуються як відповідь на дестабілізуючі та агресивні акції рухів опору під проводом АВ. На відміну від профілактичних заходів, що спрямовуються на запобігання загрози ще до її зародження, оперативні методи запроваджуються вже після виявлення деструктивних впливів, які здійснюють рухи опору та організовуються агентами впливу (в окремих випадках за участі опозиційних лідерів). Запровадження оперативних методів потребує оцінювання ступеня загрози з боку АВ і РО та аналізу наявних ресурсів для нейтралізації (запобігання) їх деструктивної діяльності.

На прихованій фазі гібридної агресії найбільш ефективними методами протидії можуть бути методи, які використовують агенти впливу та рухи опору, але спрямовані суб’єктами сектору безпеки і оборони проти них самих. До таких методів доцільно віднести [11]:

персоніфікацію дій опозиційних сил та агентів впливу, тобто виказання конкретних осіб, які своїми діями призводять до масових безпорядків і матеріальних збитків державній власності та, що важливо, власності громадян;

деморалізація та делегітимізація учасників руху опору, лідерів опозиції та агентів впливу за допомогою критики в інформаційному просторі відомими особами країни, які мають авторитет у суспільстві;

оповіщення суспільства про відкриття адміністративних і кримінальних проваджень стосовно відомих агентів впливу, заколотників, активних учасників масових акцій протестів, діяльність яких може бути пов’язана з дестабілізацією суспільно-політичної обстановки;

заперечення інформації, що транслюється опозиційними ЗМІ, дискредитація їх в очах учасників протестів і лідерів рухів опору;

використання психологічних прийомів і технологій на масових опозиційних заходах,

упровадження в маси спеціалістів відповідної кваліфікації для протидії діяльності різного роду провокаторів;

розгін несанкціонованих масових заходів і відкрита демонстрація сили державних органів влади;

активний моніторинг соціальних мереж АВ і відомих лідерів РО, а також відслідковування і заборона координації та організації руху опору, блокування каналів передавання інформації та їх сторінок у соціальних мережах;

заборона активних медіаканалів антидержавних, які мають деструктивний вплив на суспільно-політичну, економічну та інформаційну сфери національної безпеки держави тощо.

За даними [12, 13] дієвим способом протидії деструктивним чинникам впливу на суспільно-політичну обстановку в країні, яка впроваджується агентами впливу за допомогою створених ними рухів опору та упередженою опозицією, є спосіб в основу якого покладено моніторинг державою підконтрольних АВ ЗМІ та ідентифікація інформації, яка може бути використана для введення суспільства в оману та просування інтересів держави-агресора (особливо в інформаційній, політичній та економічній сферах).

Важливість своєчасної та ефективної протидії деструктивним факторам, які реалізують агенти впливу та опозиційні сили обумовлена, насамперед тим, що саме успішність їх дій є каталізатором нарощування протестного руху та плацдармом для реалізації наступного етапу дій у рамках стратегії гібридної агресії, який отримав у фахівців РФ назву Стратегія “Троянського коня” [14]. Цей етап полягає в активізації угруповання сил спеціальних операцій (ССО) противника, що може бути завчасно приховано створене на території держави проти якої розв’язано агресію. У разі успішних дій агентів впливу та опозиції з дестабілізації соціально-політичної обстановки, ССО противника розпочинають активні дії при одночасному нарощуванні чисельності протестантів під виглядом добровольців та мирних мігрантів. Цілями дій угруповання ССО на цьому етапі гібридної агресії є дезорганізація державного та військового управління, створення перешкод економічній діяльності, взяття під контроль сил опозиції та збір інформації. Важливим є завдання з ліквідації найбільш небезпечних, з огляду на організацію протидії агресору,

державних діячів або їх підкуп та виведення з ладу найбільш важливих об’єктів критичної інфраструктури держави [10] під маскуванням масових заворушень мирних громадян.

З появою на території держави – жертви агресії незаконних збройних формувань (НЗФ) та іноземних найманців завдання угруповання ССО розширюються, а саме завдання управління бойовиками, контроль за діями іноземних збройних формувань, координація дій агентів впливу; зачистка фактів і доказів участі у дестабілізації обстановки в країні; ліквідація агентів впливу, що не виконали завдання або діяли всупереч планам. Після переходу агресора до відкритої підтримки НЗФ регулярними силами угруповання ССО виконують завдання з інформаційного забезпечення їх дій. Лише з початком прямої агресії (вторгнення на територію противника регулярних збройних формувань) стратегія Троянського коня на думку аналітиків завершується.

Питання пошуку та протидії агентам впливу (передусім російським) загострилося з початком бойових дій у 2014 році. Водночас досі актуальною проблемою є формування достатньої нормативно-правової бази для притягнення таких осіб до відповідальності, механізмів їх чіткої ідентифікації та недопущення використання поняття “агент впливу” для обмеження свободи слова та думки. Іноземні держави (передусім з демократичними політичними системами) так само шукали і шукають механізми протидії. У статті як рекомендація пропонується удосконалення асиметричної протидії державі – агресору, що переважає у військовому та економічному відношенні в частині протидії агентам впливу. Відомо з [6], що асиметричні дії притаманні конфліктній ситуації, у якій заходами економічного, дипломатичного, інформаційного та безпосередньо воєнного характеру більш слабкий противник проводить асиметричну стратегію (тактику) ведення збройної боротьби, відповідно до наявних у нього обмежених ресурсів, для нівелювання воєннотехнологічних переваг сильної сторони. Однак законодавство країни проти якої здійснюється агресія не завжди може швидко адаптуватися під реальну ситуацію, що потребує пошуку асиметричних дій [4]. Основні напрями удосконалення асиметричної протидії (АП) агентам впливу наведено на рис. 1.

Важливою умовою ефективності проведення заходів асиметричної протидії є точне визначення найбільш уразливих і

слабких місць противника, вплив на які дасть максимальний ефект за мінімальних затрат власних сил і ресурсів. Основним бажаним результатом асиметричної протидії має стати відмова противника від активних воєнних дій, тобто деескалація загрози воєнного або гібридного характеру до прийнятного (допустимого) рівня [6].

До критичних груп осіб, які мають бути у полі постійного відслідковування діяльності з боку відповідних державних безпекових структур і мають відповідні офіційні можливості для здійснення впливу: журналісти; експерти (урядові та неурядові,

зокрема керівники НДУ); політичні діячі; популярні блогери; державні службовці (від середньої ланки і вище); науковці; радники (при державних органах або окремих посадових особах); творчі працівники (актори, митці та інші); релігійні діячі [8]. Крім указаних груп, окрему складність щодо ідентифікації агентів впливу становлять особи, які перебувають біля “статусних” суб’єктів і можуть впливати на них: чоловіки/дружини, співмешканки/співмешканці, родичі та інші особи.



**Рис. 1. Напрями удосконалення асиметричної протидії державі-агресору, яка переважає у військовому та економічному відношенні в частині протидії агентам впливу у системі кадрових органів**

Своєчасне виявлення деструктивної діяльності агентів впливу, лідерів рухів опору державній владі та їх ефективна нейтралізація в умовах організації асиметричної протидії державі-агресору (за результатами проведених розрахунків) підвищує ймовірність прийняття противником рішення на відмову від застосування військової сили на 10 % та зменшує час і ресурси на організацію асиметричної протидії [6].

За розрахунками своєчасна нейтралізація агентів впливу та рухів опору зменшує на 15-20 % використання ресурсів на організацію та здійснення асиметричної протидії державі-агресору, що проводиться, як правило у формі спеціальної операції [6].

Складність виявлення та нейтралізації агентів впливу підтверджує той факт, що за даними [8], наприклад, у США робота своєрідних “колективних агентів впливу” або спроба створення квазімережі агентів впливу (з-поміж осіб, наближених до чинного президента США) в межах поточного розслідування щодо втручання у виборчу кампанію 2016 р. кваліфікується американським слідством за іншими статтями кримінального права.

Важливим ресурсом у боротьбі з

агентами впливу є громадські організації, діяльність яких спрямована на зміцнення державних інституцій та забезпечення державного суверенітету. Для забезпечення участі громадськості у виявленні підривної інформаційної діяльності, здійснюваної, зокрема, агентами впливу та протидії дезінформації суспільства доцільно створити певну структуру. Наприклад, це може бути Комісія з протидії дезінформації та підривній інформаційній діяльності. З урахуванням світового досвіду та зважаючи на особливості показників довіри громадян до ключових інституцій, задіяних у захисті національних інтересів, можна сформулювати вимоги до моделі цієї структури:

основна робота має бути реалізована представниками громадянського суспільства, здійснюватися прозоро та за чіткими критеріями;

структура має бути належним чином інституалізована державою для надання відповідного юридичного статусу її діяльності;

важливо, щоб держава (її представники) не мали повного контролю за тим, як структура функціонує, але за допомогою певних механізмів задавали формат її роботи.

Станом на сьогодні вирішення будьяких складних питань в інформаційній сфері (зокрема, контроль за контентом) є ключовим світовим трендом і всебічно підтримується міжнародним співтовариством, зокрема міжнародними організаціями та національними урядами, що забезпечить опосередковану підтримку цієї ініціативи на зовнішній арені.

### Висновки

1. Запобігання несанкціонованим акціям, що організуються опозиційними силами за допомогою агентів впливу має здійснюватися законними та легітимними методами, а організатори акцій нести юридичну відповідальність.

2. Доцільним є закріплення в українському законодавстві поняття “агент впливу” та введення відповідальності не лише за діяльність цих осіб на території України, а й за співпрацю з ними.

3. Потребує удосконалення нормативно-правова база щодо притягнення агентів впливу до відповідальності з визначенням механізмів їх чіткої ідентифікації та недопущення використання поняття “агент впливу” для обмеження свободи слова та думки.

4. Рекомендацією є удосконалення системи протидії гібридним загрозам завдяки вирішенню проблемних питань протидії агентам впливу в умовах асиметричної протидії гібридній агресії РФ.

5. Серед основних середньострокових загроз політичній стабільності варто вказати використання Росією агентів впливу серед політичних партій, громадських і релігійних організацій для провокування громадянського протистояння й політичної кризи.

6. На прихованій фазі гібридної агресії методами протидії доцільно вважати методи, які використовують агенти впливу та рухи опору, але спрямовані суб’єктами сектору безпеки і оборони проти них самих.

**Напрями подальших досліджень** полягають в удосконаленні існуючих методів протидії агентам впливу та рухам опору на території, яка стала жертвою агресії, пошуку нових механізмів протидії деструктивним впливам з боку недружніх держав.

### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Михайло Гончар, Володимир Горбач, Сергій Савченко. Осінь гібридного наступу. Операція “Через народовладдя до федералізації”. URL: <https://zn.ua/ukr/internal/osin-hybridnoho-nastupu->

operatsija-cherez-naodovlad-dja-do-federalizatsiji.html (дата звернення: 09.02.2021).

2. Моделі і ціна врегулювання конфлікту на Донбасі: міжнародний досвід та українські реалії / В. Філіпчук, А. Октисюк, В. Поворозник, Є. Ярошенко // Міжнародний центр перспективних досліджень (МЦПД). 2016. С. 11–18. URL: <http://icps.com.ua/assets/uploads/images/images/eu/donetsk.pdf> (дата звернення: 09.02.2021).

3. Доброгурський В. І., Дублян О. В. Рекомендації щодо визначення завдань складовим інтегрованого потенціалу асиметричної протидії в інтересах здійснення контролю території збройного конфлікту. *Актуальні проблеми застосування національної гвардії України для здійснення контролю території збройного конфлікту неміжнародного характеру* : зб. тез доп. наук.-практ. семінару. (Харків, 27 лист. 2020 р.). Харків, 2020. С. 9–13.

4. Воєнні аспекти протидії “гібридній” агресії: досвід України : монографія / колектив авторів ; за заг. ред. А. М. Сиротенка. Київ : НУОУ ім. Івана Черняхівського, 2020. 176 с.

5. Леонов В. В., Ворочич Б. О. Парадокс асиметрії в сучасних міжнародних збройних конфліктах. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. 2016. № 1 (56). С. 29–34.

6. Богданович В. Ю., Сиротенко А. М., Дублян О. В. Концепція асиметричної протидії ворожій державі для нейтралізації її впливу на визначальні сфери національної безпеки України. *Наука і техніка Повітряних Сил Збройних Сил України*. Харків, 2020. № 3 (40). С. 7–11.

7. Комплексна модель процесу протидії гібридній агресії / В. Ю. Богданович, А. М. Сиротенко, О. В. Дублян, О. В. Передрій, В. П. Малінко. *Вісник воєнної розвідки*. Київ, 2020. № 61. С. 93–98.

8. Про внутрішнє та зовнішнє становище України в 2018 році : Аналітична доповідь до Щорічного Послання Президента України до Верховної Ради України. Київ : НІСД, 2018. 688 с. URL: [https://niss.gov.ua/sites/default/files/2019-02/Analit\\_Dopovid\\_Poslannia\\_2018.pdf](https://niss.gov.ua/sites/default/files/2019-02/Analit_Dopovid_Poslannia_2018.pdf) (дата звернення: 12.02.2021).

9. Світова гібридна війна: український фронт : колект. монографія / за заг. ред. В. П. Горбуліна. Київ : НІСД, 2017. 494 с.

10. Деякі питання об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109. URL: <https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text> (дата звернення: 06.02.2021).

11. Юсупова-Фарзалиева Д. М. Информационно-коммуникативные технологии как основа “цветных революций” в современных политиях : автореф. дисс. ... канд. полит. наук. Пятигорск, 2012. 24 с. URL: <https://www.dissercat.com/content/informatsionno-kommunikativnye->

- tekhnologii-kak-osnova-tsvetnykh-revolutsii-v-sovremennykh-p (дата звернення: 06.02.2021).
12. Пономарева Е. Г. Секреты “цветных революций”. Современные технологии смены политических режимов. *Свободная мысль*. 2012. № 1–2. С. 43–59.
13. Меркурьев В. В., Агапов П. В. Противодействие технологиям “цветных революций” в системе мер по предупреждению преступлений против основ конституционного строя и безопасности государства. *Всероссийский криминологический журнал*. 2014. № 2. С. 63–71.
14. Сивков Константин “Троянский конь” агрессия нового типа. *Военно-промышленный курьер*. 2020. 8–14 сентября. (№ 34 (847)) URL: <http://www.vpk-news.ru> (дата звернення: 12.02.2021).

Стаття надійшла до редакційної колегії 09.03.2021

## **Recommendations for countering influence agents and resistance movements acting in the interests of the state initiating hybrid aggression**

### **Annotation**

The experience of Ukraine in countering hybrid aggression has shown that the state initiating hybrid aggression uses all possible tools and mechanisms to achieve the strategic goals of destructive influence on the relevant spheres of national security of the state against which it is carrying out the aggression.

In modern conditions, the spheres of activity of “influence agents” and “resistance movements” are political, economic, informational and partly military. The issues of neutralizing the so-called influence agents and resistance movements that act in the interests of the aggressor state are not given enough attention, its specificity. No systemic studies on this issue have been found in open sources.

The purpose of the article is to substantiate recommendations on counteracting influence agents and resistance movements acting in the interests of the state-initiator of hybrid aggression.

It is advisable to consolidate the concept of “influence agent” in Ukrainian legislation and introduce responsibility not only for the activities of these persons on the territory of Ukraine, but also for cooperation with them.

The regulatory and legal framework for bringing “influence agents” to justice with the definition of mechanisms for their clear identification and prevention of the use of the concept of “influence agent” to restrict freedom of speech and thought needs to be improved.

The recommendation is to improve the system of counteraction to hybrid threats by solving problematic issues of counteraction to influence agents in the conditions of asymmetric counteraction to hybrid aggression of the Russian Federation.

In the latent phase of hybrid aggression, it is advisable to consider methods used by influence agents and resistance movements, but directed by the subjects of the security and defense sector against themselves.

**Keywords:** influence agents; asymmetric counteraction; hybrid aggression; resistance movement; special operation; methods of counteraction; ways to counteract the agents of influence.



Павлуцько М. Я., канд. військ. наук	(0000-0001-8255-6245)
Посмітюх О. І., канд. військ. наук, доцент	(0000-0002-4467-9532)
Сергієнко В. Д., канд. техн. наук, доцент	(0000-0001-6388-1763)
Богатов О. І., канд. техн. наук, доцент	(0000-0001-7342-7556)

Інститут забезпечення військ (сил) та інформаційних технологій Національного університету оборони України імені Івана Черняхівського, Київ

## Аналіз бойового застосування збройних сил Російської Федерації під час стратегічних командно-штабних навчань серії “Захід”

**Резюме.** У статті розглянуто стратегічні командно-штабні навчання серії “Захід”, які є основним елементом воєнно-політичної діяльності Союзної держави Білорусі та Російської Федерації у воєнно-політичній сфері, а також підсумковим етапом бойової підготовки Регіонального угруповання військ їх збройних сил. Проаналізовано форми і способи застосування видів і родів військ збройних сил Російської Федерації.

**Ключові слова:** військові навчання; військові операції; оперативна та бойова підготовка; “холодна війна”; прогноз; безпека.

**Постановка проблеми.** Проведення масштабних військових операцій є одним з основних інструментів з реалізації зовнішньої політики Російської Федерації (РФ). Воєнна доктрина РФ, яка була прийнята в грудні 2014 р. та доопрацьована на основі положень нової Стратегії національної безпеки РФ від 2015 р., а також у проєкті нової Воєнної доктрини, презентованої 2 березня 2019 р. на засіданні Академії військових наук у Москві начальником генштабу збройних сил (ЗС) Російської Федерації, трактуються основні завдання ЗС РФ. Під час проведення стратегічних командно-штабних навчань були апробовані форми і способи застосування видів і родів ЗС РФ у розрізі виконання основних завдань нових доктринальних документів, що потребує аналізу і вивчення.

**Аналіз останніх досліджень і публікацій.** На теперішній час у Воєнній доктрині РФ 2014 р. [1] та положеннях нової Стратегії національної безпеки РФ [2] від 2015 р. визначаються основні завдання ЗС РФ, вирішення яких відпрацьовуються під час стратегічного командно-штабного навчання (СКШН) серії “Захід”. СКШН є основним елементом воєнно-політичної діяльності РФ у воєнно-політичній сфері та підсумковим етапом бойової підготовки Регіонального угруповання військ їх збройних сил. Можливості щодо використання ЗС РФ в різного роду масштабних військових операцій проти її противників розглянуто у публікаціях, а саме у:

[3] проаналізовані завдання бойового застосування ЗС РФ на основних стратегічних (операційних) напрямках;

[4] відмічено, що вперше під час проведення СКШН серії “Захід-1999” були задіяні МВС, МНС та інші силові структури оперативно підпорядковані одній особі, одному відомству і діяли під одним керівництвом;

[5] висвітлено основне завдання СКШН – безпосередня підготовка збройних сил РФ і Білорусі до забезпечення стратегічної стабільності в Східноєвропейському регіоні та надані президентом РФ першочергові завдання щодо розбудови ЗС РФ;

[6] оцінено оперативну сумісність збройних сил РФ та Білорусі;

[7] перевірено злагодженість дій всіх органів військового управління, всіх підрозділів – від окремого взводу до армії, оперативна сумісність штабів різних рівнів, а також перспективних систем управління військами та зброєю.

Під час СКШН серії “Захід” РФ демонструє силу перед США і НАТО в Європі та відпрацьовує сценарій підготовки до широкомасштабної війни з ними на Європейському ТВД із зосередженням основних зусиль на Балтійському регіоні. Отже, аналіз застосування ЗС Російської Федерації під час проведення СКШН серії “Захід” є актуальним.

**Мета статті.** Під час аналізу положень СКШН серії “Захід”, виділити спрямованість заходів оперативної і бойової підготовки ЗС РФ і готовності їх до різного роду можливих масштабних військових операцій проти імовірних противників РФ.

На основі аналізу СКШН серії “Захід” виділити характерні особливості завдань,

принципів та форм і способів застосування видів і родів військ ЗС РФ.

**Виклад основного матеріалу.** Так, уперше після розпаду СРСР, навчання “Захід-1999” було проведено з 21 по 26 червня 1999 р. в п’яти військових округах – Ленінградському, Московському, Північнокавказькому, Приволзькому, Уральському, які на той час отримали статус оперативно-стратегічних напрямків, як відповідь РФ на військову операцію США та НАТО “Союзницька сила” проти Союзної Республіки Югославія (мала на меті примушення керівництва Сербії до припинення геноциду албанського населення Косово). Крім того, через демонстрацію готовності до військового протистояння із США та НАТО Росія попереджувала їх про неприпустимість втручання у її дії в Чечні (у 1999 р. РФ була розпочата друга компанія за відновлення контролю над Чеченською Республікою) [3, 4].

Після відносного налагодження відносин між РФ та США і НАТО на початку 2000-х РФ тимчасово призупинила проведення таких СКШН, однак не відмовилась від них. Наступні навчання “Захід-2009” було проведено на тлі наступного ускладнення російсько-американських та російсько-європейських відносин після нападу РФ на Грузію в серпні 2008 р. Таким чином РФ знову попереджувала США та НАТО про неприпустимість втручання у її дії на пострадянському просторі. Завдання навчань – безпосередня підготовка ЗС РФ і Білорусі до забезпечення стратегічної стабільності в Східноєвропейському регіоні [3, 5].

Такий самий показовий характер мало СКШН “Захід-2013”, під час якого було відпрацьовано значний комплекс дій з підготовки РФ до збройної агресії проти України та стримування США і НАТО. Крім того було проведено оцінювання оперативної сумісності збройних сил РФ та Білорусі [3, 6].

Активний етап СКШН “Захід-2017” був проведений 14-20 вересня 2017 р. на білоруській та російській територіях під керівництвом начальників генеральних штабів РФ і Республіки Білорусь (РБ). До того ж, на відміну від минулих років, коли навчання серії “Захід” мали відверто демонстративний

характер, у 2017 р. керівництво РФ істотно зменшило реальні масштаби СКШН та приховало його дійсний характер. Причиною цього стали критично негативні наслідки санкцій США та ЄС проти РФ та загроза їх подальшого посилення у відповідь на черговий прояв “Москвою” агресивності її зовнішнього курсу.

Так, на офіційному рівні СКШН “Захід-2017” була названа лише частина широкого комплексу навчань ЗС РФ, які проводились на єдиному оперативному фоні у період з середини серпня до середини жовтня 2017 р. До того ж був зроблений наголос на суто “оборонному” характері СКШН, його “контртерористичній” спрямованості та “ненаправленості проти будь-яких інших країн”.

Сценарій СКШН включав такі основні складові [3, 7]:

застосування Регіонального угруповання військ РФ і Білорусі для придушення масових соціальних заворушень (фактично “кольорової” революції) на білоруській території, які були організовані західними країнами для зміни влади в країні;

проведення збройними силами РФ і Білорусі наступальної операції для встановлення контролю над країнами Балтії. Зважаючи на досвід “гібридних” війн РФ проти України та інших пострадянських країн демократичного та європейського вибору, умови для нападу на Литву, Латвію та Естонію можуть бути створені за допомогою провокування внутрішніх конфліктів на їх території з подальшим втручанням у них під приводом захисту російськомовного населення;

забезпечення оборони території РФ на всіх інших напрямках силами Південного, Центрального та Східного військових округів, а також інших видів та родів військ, дислокованих на їх території;

нанесення ядерних ударів по США та інших країнах НАТО у разі стратегічного програву РФ.

СКШН “Захід-2017” проводилось за декількома етапами [3, 7].

Перший (підготовчий) етап розпочинався з попередньої підготовки – з лютого по серпень 2017 р., під час якої проводилося планування навчання та здійснювались окремі заходи з відпрацювання його основних питань.

Так, фактичною “репетицією” СКШН “Захід-2017” стала комплексна перевірка ЗС РФ за зимовий період навчання в березні-квітні 2017 р. У межах перевірки була проведена низка навчань і тренувань військ Регіонального угруповання збройних сил РФ і Білорусі, а також Західного військового округу (ВО) ЗС РФ. До того ж відпрацьовувались елементи організації та проведення наступальної операції на Північно-Західному (Балтійському) напрямку.

Крім того, у липні 2017 р. було проведено командно-штабне навчання (КШН) з управління авіацією та військами ППО ЗС РФ на Західному стратегічному напрямку із залученням оперативних груп від Збройних сил Республіки Білорусь.

Безпосередня підготовка – з середини серпня 2017 р. до початку навчання, під час якої здійснювались [3, 7]:

перевірка готовності федеральних органів виконавчої влади та підприємств оборонно-промислового комплексу до дій в умовах воєнного часу;

проведення мобілізації. Загалом із запасу було призвано майже 100 тис. резервістів. З огляду на це Міністерством оборони РФ був оприлюднений законопроект щодо внесення змін до федеральних законів “Про оборону” та “Про військову повинність і військову службу”. Законопроект був підготовлений як акт воєнного часу. Згідно з документом президент РФ отримував право надавати наказ про призов громадян на військову службу по мобілізації та у воєнний час виходячи з фактичних потреб збройних сил та інших силових структур (з урахуванням поповнення втрат та особового складу нових з’єднань і частин);

налагодження взаємодії між штабами різних рівнів збройних сил РФ і Білорусі для організації та проведення СКШН. Зокрема, такі заходи включали створення спільних оперативних груп, встановлення каналів зв’язку, а також узгодження дій учасників навчання;

розгортання системи логістичного забезпечення навчання та організація транспортних перевезень.

У межах виконання наведених завдань напередодні СКШН було проведено низку окремих і спільних спеціальних навчань з органами військового управління, з’єднаннями та військовими частинами і організаціями тилового, технічного

(матеріально-технічного) забезпечення збройних сил обох країн.

Навчання мали на меті удосконалення оперативної сумісності органів військового управління під час переведення військ у вищі ступені бойової готовності, а також відпрацювання питань матеріально-технічного, інженерного, морально-психологічного, медичного, топографічного та гідрометеорологічного забезпечення військ.

Крім того, відпрацьовувались питання організації зв’язку, радіаційного, хімічного та біологічного захисту, розгортання дорожньо-транспортної інфраструктури, технічного прикриття об’єктів і визначених ділянок автошляхів, евакуації, ремонту та відновлення несправної техніки та озброєння, розгортання польового магістрального трубопроводу, а також ділянок масової заправки техніки.

Другий етап СКШН “Захід-2017” розпочинався з розгортання міжвидового Регіонального угруповання збройних сил РФ і Білорусі на білоруській та російській територіях.

Перекидання російських військ до району проведення навчання на території Білорусі здійснювалось комбінованим шляхом: залізничним, повітряним та автомобільним транспортом, зокрема своїм ходом.

Крім передислокації військ під час СКШН особлива увага приділялась розгортанню системи управління воєнного часу Західного та частково Південного ВО ЗС РФ та ЗС Республіки Білорусь, зокрема польові рухомі командні пункти армій та підпорядкованих їм з’єднань і частин. До того ж застосовувалась Єдина система управління тактичної ланки, яка використовується російськими окупаційними військами на сході України.

Під час третього етапу СКШН “Захід-2017” проводились антитерористична, оборонна та наступальна операції.

Згідно з офіційною версією навчання, яка була оголошена командуванням ЗС РФ, на першій фазі цього етапу навчання 14-16 вересня 2017 р. на полігонах “Борисовский” та “Осиповичский” силами Регіонального угруповання ЗС РФ і Білорусі вирішувались завдання: знищення ворожих диверсійних груп, ізоляції районів дій незаконних збройних формувань, відбиття повітряного нападу противника, а також

нанесення повітряних і ракетно-артилерійських ударів по силах і об'єктах його інфраструктури [3, 7].

Такі ж завдання у складі Регіонального угруповання військ (сил) на Західному напрямку виконували інші підрозділи Західного ВО, Балтійського флоту, повітряно-космічних сил (ПКС), повітрянодесантних військ (ПДВ) та військ спеціального призначення на полігонах “Лужский”, “Струги Красные” у Ленінградській області та “Правдинский” у Калінінградській області РФ [3, 7].

Крім того, у Ленінградській області було проведено окреме навчання з відпрацювання питань прикриття Центрального промислового району РФ від повітряного нападу противника.

На тлі вирішення зазначених завдань у штабах відповідних рівнів здійснювались заходи з планування стратегічної операції (при офіційно заявленому проведенні “антитерористичної” операції) у районах відповідальності, а також нарощування Регіонального угруповання військ (сил) завдяки прибуттю до Білорусі російських військ.

На другій фазі третього етапу навчання з 17 по 20 вересня 2017 р. на полігонах у РФ і Білорусі та в акваторії Балтійського моря військами (силами) Регіонального угруповання ЗС РФ та РБ і російських збройних сил був проведений розіграш практичних дій з ведення маневреної оборони, переходу до наступальних дій та завершення розгрому противника. Основні зі згаданих заходів відпрацьовувались 18 вересня на полігоні “Лужский” та 20 вересня на полігоні “Борисовский” [3, 7].

Згідно з легендою, групи терористів, які прорвалися до Білорусі, об'єдналися в декілька загонів та розпочали підготовку до проведення терактів і диверсій.

У такій ситуації Регіональному угрупованню військ РФ і Білорусі було поставлене завдання щодо знищення бойовиків, а також відновлення територіальної цілісності Республіки Білорусь та наведення конституційного ладу на її території.

У межах виконання цього завдання були проведені операції з блокування спроб загонів терористів просунути в глибину території Білорусі, а також оточення та ліквідації їх

формувань. Найбільш масштабний характер мали заходи бригадного рівня на полігоні “Борисовский” за участю підрозділів 6 отбр та ПДВ ЗС РФ, а також мотострілецьких, танкових, зенітних та спеціальних підрозділів ЗС Білорусі.

На інших полігонах навчальні питання відпрацьовувались на рівні батальйонних тактичних груп (БТГ).

Як на першій, так і на другій фазі навчань, завдання вогневого ураження умовного противника вирішувалися силами [3, 7]:

ракетно-артилерійських підрозділів Західного ВО. Здійснювались умовні пуски оперативно-тактичних ракет “Искандер-М” і тактичних ракет “Точка-У”, а також проводилися бойові стрільби з буксируваних гаубиць “Мста-Б” і реактивних систем залпового вогню “Град”. Стрільба велася по повнорозмірних мішенях, які імітували бойову техніку та фортифікаційні споруди умовного противника, прямою та напівпрямою наводкою на різних дальностях. До того ж застосовувались розвідувально-вогневі контури у складі БпЛА, засобів артилерійської розвідки “Аистенок”, а також комплексу розвідки, управління та зв'язку “Стрелец”;

фронтових бомбардувальників Су-34 та літаків дальньої (стратегічної) авіації Ту-22М3. Під час розіграшу епізоду фронтова авіація Західного ВО застосовувала авіаційні бомби вагою 250 кг із використанням новітньої обчислювальної підсистеми “Гефест”, яка суттєво підвищує точність бомбометання. Польоти проводилися двома ланками по чотири літаки в кожній. Загалом залучалось понад 10 літаків;

корабельних угруповань Балтійського флоту ВМС РФ. Корабельні ракетні стрільби проводились у складній радіоелектронній обстановці із застосуванням засобів РЕБ. Завдання із забезпечення безпеки виконували понад 10 кораблів та суден забезпечення БФ.

Під час навчань із застосуванням засобів АСУ та зв'язку 6-го покоління (зокрема супутникових і тропосферних радіостанцій, цифрових радіорелейних станцій Р-419МП “Андромеда-Д” та уніфікованих радіостанцій Р-166-05) відпрацьовувалися питання координації дій Південного та Західного ВО на рівні Міноборони РФ, а також управління

військами від об'єднань до з'єднань, частин і підрозділів, включаючи БТГ.

Також на тлі СКШН “Захід-2017” проводились заходи оперативної та бойової підготовки у Стратегічних ядерних силах ЗС РФ [3, 7].

З початку і до кінця вересня 2017 в ракетних військах стратегічного призначення (РВСП) проходили комплексні навчання за участю одинадцяти ракетних полків у двадцяти регіонах країни.

Відпрацьовувались питання [3, 7]:

переведення частин РВСП у підвищенні ступені бойової готовності;

виходу рухомих ракетних комплексів “Тополь”, “Тополь-М” та “Ярс” на маршрути бойового патрулювання у денний та нічний час;

освоєння нових маршрутів бойового патрулювання та бойових позицій;

обладнання польових складів інженерних боєприпасів, ракетно-артилерійського озброєння, палива та мастильних матеріалів, продовольства та спорядження;

протидії ударам високоточної зброї та диверсійним групам противника;

радіаційного та хімічного захисту.

Основними цілями навчань стало оцінювання реального стану справ та рівня бойової готовності ракетних частин і з'єднань, а також якості роботи керівного складу щодо організації виконання поставлених завдань на 2017 навчальний рік. Комісія командування РВСП проінспектувала стан бойової підготовки та перевірила злагоженість дій військовослужбовців під час виконання завдань.

У цей період також було здійснено три навчально-бойові пуски міжконтинентальних балістичних ракет (МБР), зокрема [3, 7]:

12 вересня – випробувальний пуск з космодрому Плесецьк (Архангельська обл.) твердопаливної МБР “Ярс” шахтного базування, оснащений бойовою частиною, що розділяється;

20 вересня – випробувальний пуск з космодрому Плесецьк МБР “Ярс” мобільного базування;

26 вересня – випробувальний пуск МБР РС-12М “Тополь-М”.

Водночас шість літаків дальньої (стратегічної) авіації ПКС ЗС РФ Ту-95МС та Ту-22МЗ здійснювали політ у повітряному

просторі над Баренцовим, Балтійським і Норвезьким морями у супроводі, на окремих ділянках, винищувачів F-16 ВПС Бельгії, F-18 ВПС Фінляндії, F-15 та F-16 ВПС США та JAS 39 ВПС Швеції.

Під час СКШН, як стратегічна складова ВМС ЗС РФ, ракетний підводний крейсер стратегічного призначення “Дмитрий Донской” Північного флоту РФ здійснив електронний пуск МБР морського базування.

Паралельно із СКШН “Захід-2017” на початку вересня, а саме з 5 по 10 вересня у Південному військовому окрузі (ПдВО) проходили КШН усіх трьох загальновійськових армій округу та окремих видів військ.

Особливістю КШН стало його проведення на тлі навчань НАТО “Agile Spirit 2017” на території Грузії.

Брало участь у КШН близько 2 тис. військовослужбовців та 200 од. військової техніки. Згідно з офіційним повідомленням командування ПдВО, сценарій навчання передбачав відпрацювання питань прикриття державного кордону РФ у районах перевалів через Великий Кавказький хребет (на російсько-грузинському кордоні), а також виявлення та ліквідації розвідувально-диверсійних груп противника у гірській та рівнинній місцевостях. До того ж урахувався досвід війн у Чечні та російсько-грузинського конфлікту в 2008 році [3, 7].

Крім того, вирішувались завдання посилення угруповання збройних формувань самопроголошених республік на Кавказі та російських військ на окупованих територіях України.

У межах навчань ПдВО було відпрацьовано також комплекс заходів оперативної та бойової підготовки угруповання російських військ на території окупованого Криму.

15 вересня 2017 р. на полігоні Опук у районі Феодосії було проведено батальйонне тактичне навчання за участю мотострілецьких, танкових та артилерійських підрозділів зі складу 810-ї окремої бригади морської піхоти та 126-ї бригади берегової оборони 22-го корпусу берегових військ Чорноморського флоту РФ. Відпрацьовувались дії військ в умовах застосування противником хімічної зброї та засобів РЕБ. Під час навчання розвідувальні

підрозділи застосовували комплекси БПЛА “Орлан-10”, які передавали інформацію щодо місцезнаходження умовного противника на пункти управління мінометних батарей “Сани” та гаубичних батарей “Мста-Б”.

Загалом під час КШН було проведено понад 100 тактичних навчань і стрільб, а з полігону на території Криму було здійснено пуск крилатої ракети.

У Західному ВО 12 вересня під час навчань 6-ї армії військово-повітряних сил та протиповітряної оборони (ВПС та ППО) ПКС ЗС РФ відпрацьовувались завдання щодо завоювання переваги у повітрі, над сушею та над морем, зокрема в районах Ленінградської, Курської, Тверської, Калінінградської областей. Загалом залучались понад 100 літаків і вертольотів, включаючи винищувачі МіГ-29СМТ, МіГ-31БМ, Су-27 та Су-30СМ. Під час навчання проводились навчальні повітряні бої та здійснювалися пуски керованих ракет.

З 12 по 29 вересня 2017 р. у Центральному ВО здійснювався комплекс заходів оперативної та бойової підготовки. Так, уперше під час навчань військ РЕБ відпрацьовувались питання виявлення та подавлення систем зв'язку та управління стратегічного угруповання військ умовного противника, яке перебувало на дальності до 4 тис. км від Уралу в районах Атлантики та Індійського океану (баз, корабельних груп та авіації ЗС США). Крім того, за допомогою комплексу управління частинами (підрозділами), засобами РЕБ РФ вирішувались завдання захисту критично важливих об'єктів від масованого ракетно-авіаційного удару умовного противника, а також дезорганізації управління диверсійно-розвідувальних груп, зокрема блокування їх засобів мобільного зв'язку.

25 вересня під час навчань ракетних військ і артилерії Центрального ВО на полігоні під Челябінськом за участю понад 1 тис. військовослужбовців та 150 од. бойової і спеціальної техніки відпрацьовувались питання ураження цілей на дальність до 18 км із застосуванням розвідувальних комплексів “Стрелец” та БПЛА “Орлан-10”. Усього було виконано близько 40 вогневих завдань.

У цей період у Східному ВО було проведено оцінювання здатності органів військового управління та з'єднань округу до виконання завдань за призначенням.

Комплексні заходи оперативної та бойової підготовки під час СКШН “Захід-2017” також здійснювались на Чорноморському і Північному флотах.

6 вересня 2017 р. на Чорноморському флоті під час проведення КШН відпрацьовувались питання управління корабельними групами Кримської та Новоросійської військово-морських баз Чорноморського флоту РФ.

На Північному флоті (ПФ) у навчанні брали участь бойові кораблі, які здійснили перехід до архіпелагу Новосибірських островів, а також підрозділи тактичної групи флоту з місцем постійного базування на острові Котельний.

З 15 по 22 вересня проводились навчання різнорідних сил флоту в Баренцовому морі за участю понад 20 бойових кораблів та 10 атомних і дизельних підводних човнів. Водночас відпрацьовувались питання відбиття масованої повітряної атаки (було збито 6 крилатих ракет), а також нанесення артилерійських і ракетних ударів по кораблях і берегових цілях противника.

У період проведення СКШН “Захід-2017” здійснювались військові навчання на територіях самопроголошених республік колишнього СРСР.

20 вересня 2017 р. мотострілецький батальйон зі складу Оперативної групи російських військ у Придністров'ї та артилерійського підрозділу збройних формувань самопроголошеної Придністровської Молдавської Республіки відпрацьовували питання оборонних і наступальних дій військ за підтримки артилерії.

В Абхазії 25 вересня 2017 р. за участю підрозділів 7-ї військової бази Південного ВО ЗС РФ відпрацьовувались дії БТГ з бойовими стрільбами.

Крім того, було проведено серію військових навчань ЗС РФ та її партнерів, у тому числі:

у серпні-вересні проводилось спільне навчання ВМС РФ та Китаю “Морська взаємодія-2017”. Проводилось у два етапи у Балтійському та Японському морях. Відпрацьовувались питання спільних дій під час проведення рятувальних операцій [3, 8];

28 серпня – середина вересня – спільне навчання ЗС РФ та Монголії “Селенга-2017”. Проводилось на полігоні “Зуунбаян” у пустелі Гобі на монгольській території. Відпрацьовувались питання ліквідації

незаконних збройних формувань у складних природних умовах [3, 9].

6-17 вересня – спільне навчання підрозділів повітряно-десантних військ РФ та парашутно-десантних військ Єгипту “Захисник дружби-2017”. Навчання проводилось на полігоні “Раевское” у Краснодарському краї РФ. Відпрацьовувались питання захоплення та утримання перевалів з висадкою повітряних десантів із літаків Іл-76 [3, 10];

26 вересня – 4 жовтня – спільне навчання гірських підрозділів ЗС РФ та Пакистану “Дружба-2017”. Проводилось на території Карачаєво-Черкесії у високогірному районі Кавказького хребта на висоті 2,3 тис. метрів над рівнем моря. Відпрацьовувались питання взаємодії під час виконання навчально-бойових завдань у гірських умовах, зокрема знищення незаконних збройних формувань [3, 11].

**Висновки.** Головною метою СКШН “Захід-2017” була демонстрація сили перед США і НАТО у Європі та відпрацювання сценарію підготовки до широкомасштабної війни з ними на Європейському ТВД на основі нових доктринальних документів. Вирішувались завдання організації та проведення антитерористичної, наступальних і оборонних операцій.

Аналіз характеру та спрямованості заходів оперативної та бойової підготовки ЗС РФ підтверджує, що СКШН серії “Захід” були підсумковим етапом бойової підготовки Регіонального угруповання військ збройних сил РФ і Білорусі.

Під час підготовчого етапу значна увага приділена:

готовності федеральних органів виконавчої влади та підприємств оборонно-промислового комплексу до дій в умовах воєнного часу;

організації забезпечення оперативного розгортання. Проведені спеціальні навчання з органами військового управління, з'єднаннями та військовими частинами і організаціями тилового, технічного, інженерного, морально-психологічного, медичного, топографічного та гідрометеорологічного забезпечення військ, під час яких відпрацьовувались питання організації зв'язку, радіаційного, хімічного та біологічного захисту, розгортання дорожньо-транспортної інфраструктури, технічного прикриття об'єктів і визначених ділянок автошляхів, евакуації, ремонту та відновлення

несправної техніки та озброєння, розгортання польового магістрального трубопроводу, а також ділянок масової заправки техніки.

Висування, під час розгортання міжвидового угруповання збройних сил на білоруській та російській територіях, здійснювалось комбінованим шляхом з використанням залізничного, повітряного, автомобільного транспортом та своїм ходом.

Система управління була розгорнута на польових рухомих командних пунктах армій та підпорядкованих їм з'єднань і частин. До того ж застосовувалась Єдина система управління тактичної ланки із застосуванням засобів АСУ та зв'язку 6-го покоління (зокрема супутникових і тропосферних радіостанцій, цифрових радіорелейних станцій Р-419МП “Андромеда-Д” та уніфікованих радіостанцій Р-166-05).

Під час третього етапу СКШН міжвидовим угрупованням збройних сил відпрацьовані дії в антитерористичній, оборонній та наступальній операціях.

Під час антитерористичної операції вирішувались завдання: знищення диверсійних груп, ізоляції районів дій незаконних збройних формувань, відбиття повітряного нападу противника, а також нанесення повітряних та ракетно-артилерійських ударів по силах і об'єктах його інфраструктури. Крім того виконано завдання з нарощування угруповання військ.

Оточення та ліквідації загонів терористів здійснювалося батальйонними тактичними групами, а також танковою бригадою у взаємодії з десантними та спеціальними підрозділами.

Оборонна та наступальна операції відпрацьовані під час КШН трьох загальновійськових армій ПдВО.

Вогневе ураження умовного противника під час навчань вирішувалися силами:

ракетно-артилерійських підрозділів;

фронтних бомбардувальників Су-34 та літаків дальньої (стратегічної) авіації Ту-22М3;

корабельних угруповань флоту ВМС РФ.

Для виконання завдання завоювання переваги у повітрі, над сушею та над морем залучались понад 100 літаків і вертольотів, включаючи винищувачі МІГ-29СМТ, МІГ-31БМ, Су-27 та Су-30СМ.

Уперше війська РЕБ відпрацьовували питання виявлення та подавлення систем зв'язку та управління стратегічного угруповання

військ умовного противника, яке перебувало на дальності до 4 тис. км.

Продемонстрована готовність застосування Стратегічних ядерних сил ЗС РФ. Здійснені пуски та удари з рухомих ракетних комплексів, ракетних комплексів шахтного базування, літаків дальньої (стратегічної) авіації та ракетного підводного крейсера стратегічного призначення.

Проведені заходи оперативної та бойової підготовки угруповання російських військ на території окупованого Криму, самопроголошеної Придністровської Молдавської Республіки та Абхазії.

СКШН “Захід-2017” показали здатність і готовність ЗС РФ вирішувати завдання національних інтересів і інтересів партнерів на Західному напрямку. Проте з порівняння сучасних військових потенціалів РФ та США і НАТО, на сьогодні командуванням ЗС РФ поки розглядаються обмежені варіанти конфліктів і війн із Заходом у межах окремих регіонів.

Матеріали статті будуть корисні під час розроблення КШВГ, КШН, тактичних та тактико-спеціальних навчань. **Надалі** є необхідність провести аналіз бойового застосування ЗС РФ за досвідом СКШН серії “Кавказ”, “Центр”, “Схід” як основних елементів воєнно-політичної діяльності РФ у воєнно-політичній сфері та підсумковими етапами бойової підготовки її збройних сил –

одного з основних інструментів РФ з реалізації її зовнішньої, а за певних обставин, і внутрішньої політики.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Воєнна доктрина РФ. 2014. URL: <https://militaryarms.ru> (дата звернення: 23.04.2020).
2. Стратегія національної безпеки РФ. 2015. URL: <https://rg.ru>nac-bezopasnost-sate-doc> (дата звернення: 23.04.2020).
3. Завдання бойового застосування Збройних сил РФ на основних стратегічних (операційних) напрямках. URL: <https://www.bintel.com.ua> (дата звернення: 15.05.2020).
4. ЗАПАД-99. URL: <https://www.pravda.ru> (дата звернення: 15.05.2020).
5. Оперативно-стратегические учения “Запад-2009”. URL: <https://kremlin.ru> (дата звернення: 15.05.2020).
6. Стратегические военные учения “Запад-2013”. URL: <https://kremlin.ru> (дата звернення: 15.05.2020).
7. Учения “Запад-2013”: проверка нервной системы российской армии. URL: <https://tass.ru> (дата звернення: 22.05.2020).
8. Российско-китайские учения “Морское взаимодействие”. URL: <http://tass.ru> (дата звернення: 22.05.2020).
9. Российско-монгольские учения “Селенга” URL: <http://tass.ru>, <http://syria.mil.ru> (дата звернення: 22.05.2020).
10. “Захисник дружби-2017”. URL: <http://eadaily.com>, <http://function.mil.ru/> (дата звернення: 22.05.2020).
11. Пакистан и Россия начали совместные контртеррористические учения “Дружба-2017”. URL: <http://www.golos-ameriki.ru> (дата звернення: 22.05.2020).

Стаття надійшла до редакційної колегії 25.12.2020

### **Analysis of the combat use of the armed forces of the Russian Federation during the strategic command and staff exercises of the “West” series**

#### **Annotation**

Carrying out large-scale military operations is one of the main tools for implementing Russia's foreign policy. During the strategic command and staff exercises (SCSE), the forms and methods of using the types and branches of the RF Armed Forces in terms of basic tasks and new doctrinal documents were tested, which requires analysis and study.

The purpose of the article is to analyze the provisions of the SCSE “West” series, to highlight the direction of operational and combat training of the RF armed forces and their readiness for various large-scale military operations against possible enemies of the Russian Federation. Based on the analysis of the SCSE “West” series to identify the characteristics of the tasks, principles and forms and methods of application of types and branches of the armed forces of the Russian Federation.

The main goal of the SCSE “West-2017” was to demonstrate strength to the United States and NATO in Europe and to work out a scenario of preparation for a large-scale war with them at the European battlefield on the basis of new doctrinal documents. The tasks of organizing and conducting anti-terrorist, offensive and defense operations were solved.

The SCSE “West-2017” showed the ability and readiness of the RF armed forces to address national interests and the interests of partners in the western direction. However, comparing the current military capabilities of Russia and the United States and NATO, the Russian armed forces command is currently considering limited options for conflicts and wars with the West within individual regions.

The materials of the article will be useful during the development of command and staff war games, command and staff training, tactical and tactical-special exercises. In the future, there is a need to analyze the combat use of the Russian armed forces in the experience of strategic command and staff trainings of the series “Caucasus”, “Center”, “East”, as the main elements of military and political activities in the military-political sphere and the final stages of combat training - one of the main tools of the Russian Federation for the implementation of its foreign and, under certain circumstances, domestic policy.

**Keywords:** military exercises; military operations; operational and combat training; the Cold War; forecast; security.



Андріянова Н. М., канд. політ. наук (0000-0002-7115-2445)  
 Шпура М. І., канд. військ. наук, ст. наук. співроб. (0000-0002-3350-6003)  
 Федорієнко В. А. (0000-0002-0921-3390)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

## Застосування воєнної сили для врегулювання сучасних воєнних конфліктів

**Резюме.** Стаття присвячена дослідженню особливостей застосування воєнної сили під час урегулювання сучасних воєнних конфліктів в умовах гібридних загроз. Проаналізовано причини використання воєнної сили та міжнародні норми її використання.

**Ключові слова:** воєнна сила; сучасний воєнний конфлікт; воєнні інструменти врегулювання сучасних воєнних конфліктів; ООН.

**Постановка проблеми.** У ХХІ столітті відбулись різкі зміни у безпековому середовищі, з'явилися нові виклики і загрози гібридного характеру, які потребують нових шляхів вирішення. Однак як і 100 років тому самим радикальним і ефективним шляхом залишається використання воєнної сили. Проте в науковій літературі, і в політичних реаліях застосування воєнної сили вважається найбільш складним і суперечливим рішенням. Для України проблема пошуку шляхів вирішення сучасних конфліктів є нагальною, адже з 2014 р. триває збройний конфлікт на Сході України, який забрав життя у понад 13 тис. осіб і потребує негайного, радикального вирішення.

**Аналіз основних досліджень і публікацій.** Питанню застосування воєнної сили під час урегулювання сучасних воєнних конфліктів приділяється достатньо уваги як вітчизняними, так і зарубіжними авторами. Уваги заслуговують роботи Ф. Фукуяма [1], Г. Перепелиці [2] як відомих дослідників у сфері сучасної конфліктології. Багато статей з цієї проблематики є у сучасних українських авторів, таких як Б. Парахонський і Г. Яворська [3], яким належить змістовна концептуальна робота присвячена проблемі війни і миру крізь призму сучасних загроз гібридного характеру, у якій автори аналізують деструктивний вплив на українську політичну, економічну та соціальну реальність. На увагу заслуговує і робота О. Загребельного [4], у якій автор переважно досліджує значення воєнної сили під час вирішення сучасних воєнних конфліктів, чинники і умови за яких вона застосовується. А. Пелих [5] досліджує концепцію застосування воєнної сили в системі державної політики національної

безпеки США. Я. Григоренко та Д. Черненко [6] досліджують поняття “воєнна сила” як категорію міжнародних відносин. Проте проблема використання воєнної сили під час врегулювання сучасних воєнних конфліктів ще не знайшла свого повного відображення у сучасній науковій літературі, особливо враховуючи проблему гібридизації воєнних конфліктів сучасності та потребує детального дослідження для пошуку ефективних рішень урегулювання сучасних воєнних конфліктів.

**Метою статті** є проведення аналізу умов застосування воєнної сили під час урегулювання сучасних воєнних конфліктів в умовах гібридних загроз, міжнародні норми її використання.

**Виклад основного матеріалу.** Сучасні дослідники засоби врегулювання міжнародних конфліктів розподіляють на дві основні групи невоєнні та воєнні. Воєнні засоби врегулювання сучасних воєнних конфліктів у сучасній політичній думці та конфліктології ще прийнято називати “воєнною силою” або “насильницькими” інструментами вирішення конфліктів. Сучасний воєнний конфлікт відповідно до основ конфліктології у своєму розвитку проходить три стадії: зародження, практичних дій (ескалації), врегулювання. Під врегулюванням сучасних воєнних конфліктів розуміється форма вирішення суперечностей конфліктуючих сторін, що має закінчуватись підписанням документів, які матимуть правову силу. Тобто це комплекс заходів, які здійснюються для завершення конфлікту, вичерпання його змісту.

У сучасному суспільстві виникають суперечки щодо пріоритетності значення використання воєнної сили як інструменту вирішення конфліктів. Фр. Фукуяма у своїх роботах віддавав використанню воєнної сили

саме пріоритетне місце, називаючи її основним методом підтримки світового порядку [1], хоча в своїх останніх роботах дещо змінив свою думку. Ще в 1920 – 1930 рр. американський експерт із міжнародного права Дж. Сміт також виділяє використанню воєнної сили пріоритетне значення, і зазначає: “За відсутності будь-якого загального й неупередженого органу управління, який міг би інтерпретувати міжнародні правила поведінки та оцінювати стан міжнародних відносин, кожна держава цілком природно прагне не лише розширити свій силовий потенціал у зовнішньому світі, а й попередити, якщо це можливо, будь-яке потенційне розширення впливу іншої держави, що є суперником. Інстинкт самозбереження у світі, що складається з абсолютно незалежних держав, змушує кожну з них прагнути володіти силою, щоб захистити себе від небезпеки піддатись агресії ззовні” [6, 8].

На сьогодні з появою нових гібридних конфліктів відбувається переоцінювання ролі та значення використання воєнної сили під час вирішення воєнних конфліктів, як влучно пишуть Б. Парахонський, Г. Яворська у “сучасних війнах відбувається зміщення центру тяжіння з фізичного силового складника, який переважає у традиційних війнах, на ментальний та інформаційний” [3, с. 20]. Тобто використання воєнної сили під час врегулювання сучасних воєнних конфліктів уже не несе пріоритетне значення.

На думку А. Арбатова, нині саме значення воєнної сили у врегулюванні сучасних воєнних конфліктів, дещо змінилось “...воєнна сила залишається інструментом політики, проте в умовах глобалізації, зростаючої економічної і гуманітарно-інформаційної взаємозалежності країн її роль дещо зменшилась порівняно з іншими факторами сили та національної безпеки. До останніх належать фінансово-економічний потенціал і диверсифіковані зовнішньоекономічні зв'язки, інноваційна динаміка індустрії та прогрес інформаційних технологій, інвестиційна активність за кордоном, місце в міжнародних економічних, фінансових і політичних організаціях та інститутах. Однак останнім часом воєнна сила стала частіше застосовуватися як інструмент прямого чи опосередкованого (через політичний тиск) впливу. До того ж ефективний воєнний потенціал – це не традиційні армії та флоти, а сила іншої якості, насамперед інформаційного й мережево-центричного типу. Її визначають фінансово-

економічні можливості держав, інноваційна динаміка їх індустрії, прогрес інформаційних технологій, якість міжнародних союзів” [7].

Воєнна сила є, звичайно, значною, і війна в Україні, Афганістані, Сирії, Лівії, Ємені це доводить. Людство ще не готове перейти повністю на невоєнні інструменти вирішення конфліктів і відмовитись від застосування воєнної сили. Нажаль, як доводить історія, на сьогодні найдієвішим та, водночас, найрадикальнішим інструментом врегулювання збройних конфліктів залишається використання воєнної сили.

Функціями воєнної сили визначено [9, с. 47]:

досягнення перемоги у війні;  
створення вигідного з позицій політичної еліти співвідношення сил у глобальному та регіональному або двосторонньому масштабі завдяки створенню сукупної воєнної сили, утвореної у воєнно-політичних союзах, системі колективної оборони;

політичного тиску на іншу державу, групу країн, систему міждержавних відносин;  
забезпечення національної безпеки і оборони держави (однакова для всіх країн незалежно від їх миролюбності);

підтримання політичної і воєнної стабільності;

покарання агресора як інструмент спільних акцій проти нього.

На відміну від минулих часів, головна функція – ведення війн заради повної перемоги – обмежена, адже в реаліях сьогодення, з появою гібридних конфліктів таке значення перемоги як “підписання миру” нівелюється [3], оскільки не можливо здобути перемогу у війні, яка не була проголошена.

Імовірність виникнення конфліктів у сучасному соціумі висока, оскільки на воєнно-політичній арені діють чимало політичних учасників, які не відмовляються застосовувати силу. З огляду на це уряди багатьох провідних держав і надалі будуть змушені витратити необхідні в інших сферах громадського життя матеріальні ресурси на вдосконалення воєнної сили як гаранта свого безпечного існування і стійкого розвитку [9, с. 47].

Використання воєнної сили в підтриманні миру пов'язане зі значними матеріальними витратами, людськими жертвами, що не збігається з гуманітарними ідеалами людства, а отже, постійно потребує виправдання своєї миротворчої місії, освячення її вищими найавторитетнішими міжнародними організаціями. Переваги і вади

воєнного елементу породжують два протилежних погляди на його роль і на роль невоєнного елементу у врегулюванні воєнних конфліктів [10, с. 236].

Особливістю врегулювання сучасних воєнних конфліктів є те, що в усуненні протиріч між конфліктуєчими сторонами може брати участь третя сторона, це виконують найчастіше міжнародні або регіональні безпекові організації. Організація Об'єднаних Націй є значущою у врегулюванні сучасних воєнних конфліктів і підтримання міжнародного порядку, адже метою ООН є підтримання та зміцнення миру й міжнародної безпеки.

Слід підкреслити, що Статутом ООН заборонено застосування воєнної сили у відносинах між державами, визнавши тим самим незаконним її використання як засобу здійснення зовнішньої політики й міжнародних суперечок. Загалом заборонивши застосування воєнної сили, Статут ООН визначив виключні випадки, у яких вона може використовуватися. По-перше, державою під час здійснення права на самооборону. По-друге, за рішенням Ради Безпеки ООН проти держави, що здійснила агресію, що порушила мир або створює загрозу миру (ст. 39 Статуту).

Застосовуючи воєнну силу проти держави-агресора, держава, яка порушила мир або створює загрозу миру, ООН практично веде воєнні операції проти такої держави. За таких умов суб'єкт миротворчих операцій фактично перетворюється на прямого учасника міжнародного збройного конфлікту [12].

До основних воєнних засобів урегулювання сучасних воєнних конфліктів сучасні дослідники зазвичай відносять: демонстрацію воєнної сили, рішучість її застосування, превентивне розміщення військових контингентів. Після того, як всі превентивні заходи виявляються вичерпаними, і він перейшов у форму збройного протиборства, настає час для використання арсеналу миротворчості для припинення бойових дій і досягнення перемир'я.

У доповіді 6-го Генерального секретаря ООН Бутроса Галі "Порядок денний для миру" миротворчість визначено як "дії, спрямовані на те, щоб схилити ворогуючі сторони до угоди, насамперед за допомогою таких мирних засобів, які передбачені в Главі VII Статуту ООН" [13, с. 3]. Окремо виділяється підтримка миру як забезпечення присутності ООН у даному конкретному районі, що, як правило, пов'язане з

розгортанням військового, поліцейського або цивільного персоналу ООН [13, с. 13]. Наступним етапом у процесі формування підтримки миру в межах ООН стала доповідь, зроблена Б. Галі з нагоди 50-річчя Організації Об'єднаних Націй.

Цей документ увійшов в історію під назвою "Доповнення до Порядку денного для миру". У ньому найбільш важливими інструментами з підтримання миру й безпеки оголошені превентивна дипломатія, миротворчість, підтримання миру, будівництво миру, роззброєння, санкції і примус до миру [14, с. 95]. До того ж зазначається, що перші три види діяльності можуть проводитися тільки за згодою сторін, залучених у конфлікт. Санкції та примус до миру вже не потребують згоди безпосередніх учасників колізії [14, с. 95]. І якраз з кінця 40-х років минулого століття, особливо в останні десятиліття, має велику вагу використання воєнної сили для врегулювання сучасних воєнних конфліктів. Миротворчі операції, здійснення яких передбачає використання збройних сил, тісно пов'язані з гострою і важливою проблемою – допустимості застосування воєнної сили у відносинах між державами. Сучасне міжнародне право встановлює обов'язкові для всіх держав загальнозвизнані принципи й норми щодо використання збройних сил під час міждержавних і внутрішньодержавних збройних конфліктів.

Як визначають сучасні дослідники, сьогодні існує два основних типи операцій ООН з погляду їх правової легітимізації. *Перший* – операції з підтримання миру (peacekeeping), які проводяться на основі принципів, закріплених у розділі VI Статуту ООН. Цей тип миротворчих операцій потребує документованої згоди легітимного керівництва сторін конфлікту на втручання з боку міжнародного співтовариства. У подібному випадку операція може бути проведена в тому числі регіональними міждержавними організаціями, права яких закріплені в главі VIII Статуту ООН, у взаємодії з ООН або самостійно; до того ж мандат з боку РБ ООН є бажаним, але його може і не бути. *Другий* – операції зі встановлення миру (peace enforcement), проводяться на основі закріплених у розділі VII Статуту ООН принципів силового втручання міжнародного співтовариства в особі ООН в конфлікти або внутрішні справи держав, зокрема всупереч волі легітимної влади держави, на території якої відбувається

конфлікт. Подібні операції отримали назву “політичні місії ООН” і, як правило, містять елементи примусових силових дій [15, с. 33].

Такі операції передбачають переважно примусові заходи щодо вирішення воєнних конфліктів, такі як санкції чи блокади. Рада Безпеки може дозволити використання воєнної сили в крайньому випадку.

Операції зі встановлення миру відрізняються від операції з підтримання миру тим, що для їх проведення не потрібна згода воюючих сторін. Розділ VII Статуту ООН забезпечує правову основу для таких дій. ООН, як правило, сама не бере участь у забезпеченні миру.

Рада Безпеки може санкціонувати дії щодо встановлення миру без згоди сторін конфлікту в гуманітарних цілях, для захисту цивільного населення або якщо конфлікт являє загрозу міжнародному миру та безпеці.

ООН може проводити операції з встановлення миру спільно з міжнародними і регіональними безпековими організаціями згідно з главою VIII Статуту ООН. Організація Північноатлантичного договору (НАТО), Європейський Союз (ЄС), Організація з безпеки та співробітництва у Європі (ОБСЄ) та Африканський Союз (АС) проводять все більшу кількість міжнародних миротворчих операцій із підтримання миру і безпеки але лише з дозволу Ради Безпеки ООН. Таке партнерство означає, що міжнародне співтовариство швидше та ефективніше реагує на воєнні загрози [16].

Використання воєнної сили під час врегулювання сучасних воєнних конфліктів відповідає характерним особливостями сучасних воєнних конфліктів [17]:

застосування різних форм і способів бойових дій, зокрема використання нетрадиційних та раніше невідомих, ведення збройної боротьби на суші, у повітрі та космосі, на морі з одночасним застосуванням засобів повітряно-космічного нападу;

поєднання воєнних дій за правилами воєнної науки з партизанськими та терористичними діями;

широке використання кримінальних формувань;

швидкоплинність воєнних дій;

вибірковість об'єктів, що підлягають ураженню;

підвищення ролі дистанційних боїв із застосуванням високоточних (керованих та некерованих) засобів ураження;

нанесення точкових ударів по ключових об'єктах, критичних для економіки та інфраструктури;

поєднання воєнного і потужного політико-дипломатичного, економічного, інформаційного, кібернетичного, психологічного, гуманітарного та іншого впливу на противника тощо.

**Висновки.** В Україні з 2014 р. триває збройний конфлікт, для припинення якого задіяні переважно несилові інструменти врегулювання сучасних збройних конфліктів. Звісно, не можна сказати, що вони не дають жодного результату, адже політико-дипломатичні заходи, такі як Нормандський переговорний формат та тристороння контактна група є важливими у врегулюванні конфлікту. Тим не менш, збройний конфлікт на Сході України вже триває понад 6 років і потребує більш радикального його вирішення, такого як використання воєнної сили. Однак одразу стає зрозумілим, що Україна не здатна сама протистояти країні з другим ядерним потенціалом в світі. Зважаючи на всю складність ситуації та об'єктивно оцінюючи можливості України протистояти агресії Російської Федерації самотужки радикальне врегулювання збройного конфлікту можливе лише за умов проведення міжнародної миротворчої операції з підтримання миру і безпеки під приводом міжнародних безпекових організацій.

Воєнна сила є невід'ємним інструментом вирішення сучасних збройних конфліктів, який довів свою ефективність. Статутом ООН заборонено застосування воєнної сили у відносинах між державами, визнавши тим самим незаконним її використання як засобу здійснення зовнішньої політики й міжнародних суперечок, але наявні виключні випадки, у яких вона може використовуватися. По-перше, державою під час здійснення права на самооборону. По-друге, за рішенням Ради Безпеки ООН проти держави, яка здійснила агресію, порушила мир або створює загрозу миру, тому необхідність проведення міжнародної миротворчої операції з підтримання миру і безпеки під егідою ООН є виправданим, законним і необхідним для врегулювання конфлікту на Донбасі.

Перспективним **напрямом подальших досліджень** є подальший комплексний аналіз використання воєнних інструментів врегулювання сучасних воєнних конфліктів та аналіз можливостей проведення міжнародних миротворчих операцій з підтримання миру і

безпеки для вирішення сучасних збройних конфліктів гібридного характеру.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Fukuyama F. The End of History and the Last Man. New York, Oxford, Free Press, 1992. 418 p.
2. Перепелица Г. Военно-политический конфликт: сущность, прогнозирование, урегулирования : дис. д-ра полит. наук. Київ, 1994. 290 с.
3. Парахонський Б. О., Яворська Г. М. Онтологія війни і миру: безпека, стратегія, смисл : монографія. Київ : НІСД, 2019. 560 с.
4. Загребельний О. Силові способи врегулювання воєнно-політичних конфліктів. *Політологічний вісник*. 2014. Вип. 72. С. 397-408. URL: [http://www.irbis-nbu.gov.ua/cgi-bin/irbis\\_nbu/cgiirbis\\_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE\\_FILE\\_DOWNLOAD=1&Image\\_file\\_name=PDF/Pv\\_2014\\_72\\_38.pdf](http://www.irbis-nbu.gov.ua/cgi-bin/irbis_nbu/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Pv_2014_72_38.pdf) (дата звернення: 10.02.2021).
5. Пелих А. Концепції застосування військової сили в системі державної політики національної безпеки США. *Державне управління: теорія та практика*. 2013. № 2. С. 62–68. URL: [http://nbuv.gov.ua/UJRN/Dutp\\_2013\\_2\\_9](http://nbuv.gov.ua/UJRN/Dutp_2013_2_9) (дата звернення: 10.02.2021).
6. Григоренко Я., Черненко Д. Военна сила сучасної держави як категорія міжнародних відносин: поняття та шляхи вдосконалення. *Підприємництво, господарство і право*. 2017. № 3. С. 299–301. URL: <http://prp-journal.kiev.ua/archive/2017/3/68.pdf> (дата звернення: 10.02.2021).
7. Арбатов А. Угрозы реальные и мнимые: военная сила в мировой политике начала XXI в. 2013. URL: <http://globalaffairs.ru/number/ugrozy-realnye-immimye-15863> (дата звернення: 12.12.2020).
8. Smith J. The Growth and Decadence of Constitutional Government. New York : Henry Holt and Company. 476 с.
9. Пунда В., Козинець І. П., Клименко В. С. Міжнародні відносини та зовнішня політика України : підр. Київ : НУОУ ім. Івана Черняхівського, 2020. 328 с.
10. Бернадський Б.В. Міжнародні конфлікти : курс лекцій. Київ : Персонал, 2012. 366 с.
11. Шпура М. І., Кульчицький О. С., Комолаєва Т. М. Аналіз підходів, механізмів і способів, що використовує НАТО та інші міжнародні організації з безпеки для врегулювання сучасних воєнних конфліктів. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2019. № 3 (67). С. 28–35.
12. The Decline in Global Violence: Evidence, Explanation and Contestation. Human Security Research Group Report. Simon Fraser University. Vancouver, Human Security Press, 2013. 118 p.
13. Гали Б. Повестка дня для мира. ООН. Нью-Йорк, 1992. 127 с.
14. Supplement to An Agenda for Peace. Position Paper of the Secretary – General on the Occasion of the Fiftieth Anniversary of the United Nations. SIPRI Yearbook, Oxford University Press. P. 91–100; UN documents A 50/60 (S/1995/1). 3 Jan. 1995.
15. Івашенко А. М., Возняк С. М. Аналіз можливих форм і способів проведення миротворчої операції ООН на Сході України. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2018. № 2 (63). С. 32–38.
16. Військовий спостерігач ООН : навч. посіб. Т. 1. Київ : НУОУ ім. Івана Черняхівського, 2017. 400 с.
17. Горбулін В. П. Забезпечення оборони та безпеки України: актуальні проблеми і шляхи їх вирішення. *Вісник Національної академії наук України*. Київ, 2019. № 9. С. 3–18. URL: <http://dspace.nbu.gov.ua/handle/123456789/160443> (дата звернення: 12.12.2020).

Стаття надійшла до редакційної колегії 19.02.2021

**Modern military conflict resolution using military force**

**Annotation**

The article, based on fundamental works in the field of conflict studies, articles of modern researchers, international legal documents, attempted to analyze the role and importance of the use of military force in resolving modern military conflicts, causes and international norms of its use.

Today, with the appearance of new hybrid conflicts, there is a reassessment of the role and importance of the use of military force in resolving modern military conflicts. Nevertheless, the war in Ukraine, Afghanistan, Syria, Libya, and Yemen has proved that humanity is not yet ready to switch completely to non-military conflict resolution tools and to abandon the use of military force.

Unfortunately, as history shows, the most effective and, at the same time, the most radical tool for resolving armed conflicts today is the use of military forces and means. The article defines that the military power of the state is an integrated quantity that embodies the power not only of its armed forces, but also of the military economy, science, morale of the people and soldiers of the armed forces and is used as a cardinal measure of conflict resolution.

Military force remains an integral tool in deterring modern military conflicts, one of the main means of achieving foreign policy goals. But, at the same time, the use of military force and means in general does not solve the problem of resolving the current military conflict. At best, it only creates the preconditions for this purpose. Great importance in consolidating peace in resolving the current military conflict is given to non-military measures.

**Keywords:** military force; modern military conflict; military instruments for modern military conflict resolution; UN.

Голопатюк Л. С., канд. військ. наук

(0000-0003-4153-532X)

Головне управління військового співробітництва і верифікації Збройних Сил України, Київ

## Перспективи та сценарії розвитку НАТО в глобальній системі міжнародних відносин

**Резюме.** Стаття присвячена дослідженню можливих сценаріїв розвитку НАТО в глобальній перспективі для продовження дискусії щодо майбутнього місця Організації Північноатлантичного договору в глобальній системі міжнародних відносин.

**Ключові слова:** сценарії розвитку; стратегічні напрями діяльності; НАТО; “євроцентричне НАТО”; “глобальне НАТО”; “гнучке НАТО”.

**Постановка проблеми.** Змінюється світовий порядок, з’являються нові виклики і загрози, що впливає і на розвиток НАТО. Які перспективи розвитку Альянсу через наслідки пандемії та появу воєнних конфліктів гібридного характеру? Відповідь на це питання надзвичайно важлива для України, зважаючи на впевнену заяву нашої країни про своє бажання вступити в НАТО.

**Аналіз основних досліджень і публікацій.** Питанням визначення перспектив Альянсу і можливих сценаріїв розвитку НАТО в глобальній перспективі приділяється багато уваги у працях як зарубіжних, так і вітчизняних авторів та інституцій [1–5]. Однак переважна більшість дослідників не наважується прогнозувати майбутнє НАТО за конкретними сценаріями.

**Метою цієї публікації** є визначення можливих сценаріїв розвитку НАТО в глобальній перспективі міжнародних відносин та прогнозування наслідків для України.

**Виклад основного матеріалу.** Для України в її прагненні щодо набуття членства в Альянсі, дуже важливим є з високою долею вірогідності передбачити воєнно-політичний розвиток НАТО та, з урахуванням таких прогнозів, сформулювати напрями своєї політики, включаючи питання військової співпраці щодо Організації Північноатлантичного договору.

У статті наведено три сценарії розвитку НАТО на середньо- та довгострокову перспективу, а саме: “євроцентричне НАТО”, “глобальне НАТО”, “гнучке НАТО”. Вірогідність та, у підсумку, успішність реалізації одного із зазначених сценаріїв, залежить від низки стратегічних факторів, серед яких основними є:

по-перше, готовність політичного та військового (на стратегічному рівні) керівництва у державах – членах Альянсу до реалізації одного із зазначених сценаріїв,

включаючи готовність до ресурсного забезпечення виконання відповідних запланованих заходів;

по-друге, глобальні безпекові тренди і тенденції в світі, включаючи як країни, які знаходяться в безпосередній близькості до кордонів держав – членів Альянсу, так і потенційно нестабільні регіони планети, включаючи Близький Схід, район Південно-Китайського моря, Арктику тощо;

по-третє, позиція основних учасників геополітичної шахівниці міжнародних відносин до реалізації одного із зазначених сценаріїв. До того ж такими учасниками можуть бути окремі країни (насамперед Китай і Росія), міжнародні та регіональні організації (ООН, ОБСЄ, ЄС тощо), а також інші індивіди й неформальні об’єднання.

Під час реалізації того або іншого сценарію, Альянс, у будь-якому разі, має оперативну, виражено, а найголовніше, успішно вирішуватиме низку важливих завдань [6], а саме:

досягнення та підтримка нового (прийнятного) балансу сил в Європі (з урахуванням намагань Росії бути більш впливовою на континенті). До того ж вирішення цього завдання є умовою, необхідною для успішного вирішення двох наступних;

стабілізація безпекової ситуації на півдні Європи, включаючи питання неконтрольованої міграції та підвищення рівня злочинності;

адаптація НАТО до вирішення широкого кола питань – від вирішення регіональних (локальних) завдань до прийняття рішень в умовах глобального безпекового оточення.

Зі свого боку, реалізація одного із зазначених сценаріїв в межах подальшого розвитку Організації Північноатлантичного договору матиме також значний вплив на

загальну безпекову ситуацію в світі у майбутньому.

Водночас, зазначені сценарії можуть бути реалізованими в повному обсязі тільки за умови поступового (не кризового) розвитку безпекової ситуації в світі та відсутності для НАТО нагальної необхідності в негайному реагуванні та застосуванні широкого спектру сил і засобів як військового, так і іншого характерів.

**Сценарій перший** “євроцентричне НАТО”. Такий варіант розвитку подій змушує Брюссель знайти точки спільної взаємодії з Москвою в короткостроковій та середньостроковій перспективі. Тим більше, орієнтованість європейських держав – членів Альянсу на вирішення внутрішніх проблем рано чи пізно призведе до необхідності зняття економічних санкцій з РФ та відновлення повномасштабної співпраці на двосторонній основі.

Відсутність нагальної необхідності продовження збільшення витрат на оборону буде досить позитивно сприйнято в столицях саме європейських держав – членів НАТО. Більш того, такий підхід дасть змогу зосередитися на вирішенні регіональних проблем європейського континенту, насамперед – боротьбі з неконтрольованою міграцією на Середземному морі.

Водночас, слід визнати, що на сьогодні політичне керівництво потужних країн Європи не готове сприймати такий варіант розвитку подій, як найбільш доцільний. Проте з урахуванням триваючої пандемії та пов’язаних з цим наслідків, передусім економічних, ситуація може змінитися протягом року-двох.

Щодо глобального контексту, то ситуація, під час якої Європа насамперед буде зосереджена на вирішенні внутрішніх проблемних питань, не додасть стабільності та передбачуваності світу в цілому. Це стосується також і операцій, до яких залучена Організація Північноатлантичного договору – в Іраку та Афганістані.

Крім того, ситуація із “самоізоляцією” Європи не сприятиме вирішенню локальних збройних конфліктів у світі, не зміцнюватиме світову систему контролю за розповсюдженням зброї масового ураження, а також послабить зусилля світової спільноти у протистоянні як класичним, так і новим викликам та загрозам, насамперед – боротьбі з тероризмом.

Щодо реагування ключових учасників глобальної системи міжнародних відносин, то

самоусунення Європи від участі у світовій політиці матиме неабиякий вплив на поведінку/позиції як США, так і Китаю з Російською Федерацією.

Для Вашингтону такі дії своїх союзників по НАТО з європейського континенту будуть прямим підтвердженням чисельних тез колишнього президента Д. Трампа про відсутність політичної волі в Європі для гарантування власної оборони.

Головне, що може турбувати США у разі зосередження НАТО на порядку денному європейського континенту – це потенційне зміцнення Альянсу між Росією й Піднебесною в середньостроковій перспективі.

Відтак, Пекін і Москва дуже позитивно поставляться до прибирання зі світової шахівниці європейської фігури. По-перше, це знову ж таки підтвердить кремлівську тезу про кризу неоліберального підходу до вибудови світового порядку, а по-друге – відсутність європейських амбіцій в інших регіонах світу надає Китаю і Росії унікальні можливості для нарощування свого впливу.

Такий вплив можна буде спостерігати саме в тих регіонах, які Європа вважає на сьогодні пріоритетними – Середземномор’я, Африка та Близький Схід. У цьому контексті також не є нереальним прогноз об’єднання зусиль обох країн на просування проєктів, які становлять спільний інтерес.

У підсумку, такий сценарій, на жаль не призведе до підвищення рівня стабільності та безпеки в світі. Зосередження Альянсу на справах Європи також не сприятиме вибудові системи глобального безпекового балансу, а отже – у довгостроковій перспективі потребуватиме перегляду.

**Сценарій другий** “глобальне НАТО”. Цей варіант розвитку подій примусить політичне керівництво Альянсу вирішити питання подальших відносин з Російською Федерацією в довгостроковій перспективі.

Слід визнати, що на сьогодні політичний консенсус у столицях держав – членів НАТО щодо розширення ролі Альянсу в глобальному контексті, відсутній. Це пов’язане як з розумінням необхідності збільшення витрат не тільки на власну (колективну) оборону, так і з необхідністю ресурсного забезпечення вирішення глобальних проблем. Також такий сценарій виглядає не досить привабливим з погляду різних пріоритетів потужних країн НАТО [1].

Водночас, зі стратегічної точки зору, світ тільки виграє від залучення Організації Північноатлантичного договору до вирішення

глобальних завдань. Передусім це стосуватиметься успішного проведення операцій в Іраку та Афганістані, залучення НАТО до досягнення балансу між Вашингтоном і Брюсселем з одного боку та Москвою і Пекіном – з іншого.

Такий варіант розвитку подій – розширення спектру операцій за участі Альянсу, дасть змогу з оптимізмом говорити про можливість вирішення локальних конфліктів, насамперед в Африці та на Близькому Сході.

Збільшення впливу та розширення географії залучення НАТО, скоріше за все, буде неоднозначно сприйнято як Російською Федерацією, так і Китаєм. У Кремлі добре розуміють, що впровадження “глобального НАТО” потребуватиме подальшої активізації Альянсом політики відкритих дверей, а також залучення до програм й ініціатив Брюсселю інших потужних країн світу – Японії, Південної Кореї, Австралії та, навіть, Саудівської Аравії.

Для Пекіну такий сценарій розвитку подій теж не обіцяє нічого позитивного. Зазначений стан справ, коли НАТО залучатиметься до вирішення глобальних питань, збільшить кількість потенційних районів перетинання інтересів Брюсселю та Пекіну, а також змусить останній переглянути свою політику “м’якої експансії” в сторону більшої виваженості та обережності.

У Вашингтоні очевидно без особливого ентузіазму віднесуться до ідеї реалізації “глобального НАТО”. Це пов’язане як з необхідністю бути готовим до фінансування нових проєктів та ініціатив (прийнятих Брюсселем), так і з традиційною для деяких політичних (партійних) сил пріоритетністю вирішення внутрішньоамериканських проблем.

Як результат, система міжнародних відносин з наявністю “глобального НАТО” може бути досить стійкою, а безпекова ситуація – досить стабільною. Водночас, така стабільність та передбачуваність може бути досягнута в довгостроковій перспективі, а також тільки за умови готовності політичного керівництва всіх держав – членів Альянсу до здійснення необхідних внесків не тільки на власну оборону, а і на вирішення, за допомогою НАТО, проблемних питань світового порядку денного.

**Сценарій третій “гнучке НАТО”.** Сутність сценарію полягає в адаптації НАТО до протидії новим ризикам, викликам і загрозам, з урахуванням наявних і

потенційних інтересів всіх впливових учасників глобальної системи міжнародних відносин. Такий варіант розвитку подій передбачає продовження розпочатого на саміті НАТО в Уельсі в 2014 році [7] процесу трансформації Альянсу, обумовленого швидкими змінами в геополітичному безпековому оточенні.

Слід підкреслити, що зміни відбуваються не тільки на стратегічному та оперативному рівнях. Разом зі змінами в командній структурі Альянсу, передбачається (і здійснюється) перегляд ведення бойових дій на тактичному рівні з урахуванням останніх конфліктів в Афганістані, Сирії, Ємені, Сомалі, зокрема і досвіду, набутого Збройними Силами України під час протидії російській агресії [11].

Такі підходи говорять про принципову готовність політиків у столицях держав – членів НАТО до перегляду поточної ролі та місця цієї організації в світі з урахуванням нових безпекових умов. Також такий гнучкий підхід дасть змогу учасникам НАТО як відстоювати власні інтереси під час прийняття рішень в Альянсі, так і зберігати власну політику з приводу регулювання фінансування колективної оборони.

У глобальному контексті сценарій “гнучкого НАТО” буде, скоріше за все, виграшним для стабілізації безпекової ситуації в кризових регіонах світу. Виважений підхід Брюсселя до вирішення проблемних питань у світі дасть змогу уникнути (або зменшити вірогідність) “конфлікту інтересів” серед впливових учасників системи міжнародних відносин.

“Гнучке НАТО”, скоріше за все, позитивно (у крайньому разі – нейтрально) буде сприйнято в Китаї та Російській Федерації. Це буде пов’язане з проведенням Брюсселем гнучкої та виваженої політики, яка певним чином враховуватиме інтереси Пекіна та Москви. Досить ймовірно, при “гнучкому НАТО”, політика відкритих дверей, скоріше за все, буде тимчасово призупинена, що цілком відповідає інтересам політичного керівництва Російської Федерації [8].

Для Вашингтона “гнучке НАТО” означатиме постійну адаптацію, яка, зі свого боку, сприятиме оперативному вирішенню проблемних питань у сфері безпеки. Крім того, трансформація Альянсу потребуватиме від інших країн НАТО відповідного збільшення витрат на власну (колективну) оборону, а також високу вірогідність закупівлі



озброєння та військової техніки у американських виробників [9].

У разі реалізації цього сценарію, світова система міжнародних відносин отримас більшу стабільність, а події в безпековому контексті набудуть більшої передбачуваності у короткостроковій та середньостроковій перспективі.

Проте основними умовами досягнення такого стану справ є як принципова зміна

алгоритму прийняття рішень в НАТО, так і готовність впливових країн Альянсу до фінансування окремих ініціатив, спрямованих на вирішення проблем у глобальному контексті [10].

Спробуємо визначити, які “за” та “проти” вірогідності їх втілення мають описані вище сценарії (табл. 1).

Таблиця 1

**Порівняльний аналіз “за” та “проти” наведених можливих сценаріїв розвитку НАТО**

<b>Варіанти сценаріїв</b>	<b>“За”</b>	<b>“Проти”</b>
<b>“євроцентричне НАТО”</b>	наявність суттєвих внутрішніх проблем у державах – членах НАТО, насамперед європейських, які потребуватимуть оперативного вирішення; встановлення ефективної взаємодії між НАТО та ЄС і, таким чином, зниження профілю Альянсу на політичних радарх країн – його членів; висока ймовірність підтримки такого сценарію з боку США	неготовність більшості європейських держав – членів НАТО до збільшення ресурсного забезпечення своєї безпеки та оборони; позиція політичного керівництва Канади і Великої Британії, а також позиція нової адміністрації США, яка полягає в необхідності збереження (та посилення) трансатлантичних зв’язків; збереження необхідності залучення сил та засобів збройних сил держав – членів НАТО до операцій під проводом Альянсу (тобто зосередитись на власних внутрішніх проблемах можливості може і не бути); об’єктивна залежність рівня військових оперативних спроможностей Альянсу від добровільних внесків з боку США; існування низки інших глобальних і регіональних проблем у галузі безпеки та оборони (включаючи організовану злочинність, розповсюдження зброї масового ураження та неконтрольованої міграції), які потребуватимуть втручання для їх вирішення
<b>“глобальне НАТО”</b>	наявність високого рівня залежності держав – членів НАТО від розвитку безпекової ситуації в глобальному контексті (на кшталт “якщо ти не займаєшся вирішенням глобальних проблем, настане час, коли глобальні проблеми займуться тобою”), а також відносно позитивний досвід залучення Альянсу до вирішення глобальних питань, які потребують значних ресурсів; суб’єктивне бажання низки держав – членів НАТО (зокрема з так званими “експансіоністськими” поглядами) забезпечити просування своїх інтересів у світі (особливо в умовах зростаючої конкурентності між державами світу)	неготовність більшості європейських держав – членів НАТО до збільшення внесків у колективну безпеку і оборону та у вирішення глобальних питань; неготовність інших впливових країн світу (насамперед Китаю і Росії) до сприйняття Альянсу, який бере на себе вирішення глобальних проблем; наявність певних розбіжностей у завданнях та цілях держав – членів НАТО під час вирішення безпекових проблем та необхідності протистояти класичним і новим викликам і загрозам (наприклад, розбіжності між Анкарою та Вашингтоном під час вирішення збройного конфлікту в Сирії, Анкарою та Францією, Італією і Грецією щодо врегулювання ситуації в Лівії, на Кіпрі та Східному регіоні Середземного моря); залежність Альянсу від доброї волі Вашингтону щодо виділення військового ресурсу, спрямованого на нарощування оперативних спроможностей НАТО в глобальному контексті
<b>“гнучке НАТО”</b>	неготовність інших впливових учасників світової шахівниці міжнародної системи безпеки до сприйняття Альянсу як єдиної міжнародної організації, яка несе відповідальність за світовий порядок	необхідність ретельного опрацювання механізму адаптації НАТО до протидії новим ризикам, викликам і загрозам, з урахуванням наявних і потенційних інтересів усіх впливових учасників

	<p>(адаповане НАТО, досить ймовірно не викликати відторгнення); необхідність поступового (а не раптового) збільшення з боку держав – членів НАТО витрат на колективну оборону та безпеку, а також можливість Вашингтону іноді залишатися в тіні від несення основного тягаря здійснення ресурсного забезпечення питань, у вирішенні яких зацікавлений Альянс; наявність значного досвіду адаптації Альянсу до умов глобального безпекового середовища, які швидко змінюються (особливо після незаконної окупації Криму Російською Федерацією в березні 2014 р.); існування доволі ефективних структур НАТО, які безпосередньо несуть відповідальність за реалізацію питань трансформації й адаптації в середньостроковій та довгостроковій перспективі; можливість реалізації широкого комплексу короткострокових сценаріїв саме гнучким Альянсом з огляду на збереження непередбачуваності майбутньої ситуації в галузі глобальної безпеки, а також швидкоплинності її змін; можливість оперативного формування ситуативних коаліцій і альянсів (що сприятиме зменшенню часу на прийняття рішень) для вирішення проблемних питань як регіонального, так і глобального характеру (так звана політика “розв’язаних рук”)</p>	<p>глобальної системи міжнародних відносин; необхідність напрацювання комплексного пакету планів дій на випадок виникнення кризової ситуації широкого спектру сценаріїв</p>
--	---	---

**Висновки.** Найбільш не вигідним для України, включаючи військові аспекти взаємодії з Альянсом, є сценарій “глобального НАТО”. У разі розвитку подій за зазначеним сценарієм, питання України та її безпеки стають другорядними на тлі необхідності вирішення Альянсом більш важливих завдань глобального характеру. Хоча, наявний формат співпраці між Україною та НАТО як і спектр залучення Збройних Сил України до наявних проєктів, програм, а також ініціатив буде збережено. Проте значного прориву в співробітництві між Києвом і Брюсселем сплановано та здійснено не буде.

Водночас, найбільш вірогідним на довгострокову перспективу, є сценарій розвитку подій, у процесі якого НАТО реалізовуватиме гнучку політику, намагаючись адаптуватись до змінного, невизначеного та непередбачуваного глобального безпекового оточення. Саме за цим сценарієм в Альянсі нині здійснюється опрацювання проєкту дуже важливого документа – Концепції ведення бойових дій НАТО (NWCC – NATO Warfare Capstone Concept). Також значна увага приділяється й розвитку системи командування та управління (C2 – Command and Control), зокрема

прийняття на озброєння та розміщення на авіабазі Сігонелла (Італія) стратегічних БПЛА американського виробництва Global Hawk RQ-4D.

У планах Альянсу також заміна до 2035 р. літаків системи дальнього радіолокаційного спостереження та раннього виявлення системи AWACS. У разі реалізації такого сценарію, українській стороні доцільно уважно слідкувати за новими безпековими проєктами й практичними ініціативами Альянсу для оперативного залучення до них.

Такий прагматичний підхід буде доцільним також і з урахуванням бажання військових НАТО вивчити та врахувати досвід Збройних Сил України, набутий ними під час протидії агресії на Сході України.

Крім того, саме реалізація сценарію під назвою “гнучке НАТО”, у короткостроковій та середньостроковій перспективі спонукає Брюссель (а також Вашингтон і Лондон) до пошуку союзників, зокрема з числа країн-учасниць програми Альянсу “Партнерство заради миру”.

**Перспективним напрямом подальших досліджень**, зважаючи на прагнення України щодо набуття членства в Альянсі, є аналіз розвитку НАТО і напрямів його політики для

підготовки пропозицій і рекомендацій щодо військової співпраці України з Організацією Північноатлантичного договору.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. NATO 20/2020. Twenty Bold Ideas to Reimagine the Alliance After 2020 US Election. Atlantic Council. October 2020. URL: <https://www.atlanticcouncil.org/nato20-2020/> (дата звернення: 02.02.2021).
2. Sten Rynning. NATO's Futures: the Atlantic Alliance between Power and Purpose. NDC Research Paper. No 2, March 2019. 53 p.
3. Шпігельєр С., Кортвег Р. Військові питання. Як може виглядати НАТО в майбутньому. НАТО ревію. URL: <https://www.nato.int/docu/review/2006/issue2/ukrainian/military.html> (дата звернення: 25.01.2021).
4. NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General. NATO HQ. 25 November, 2020. 67 p. URL: [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf) (дата звернення: 01.03.2021).
5. Андриянова Н. М., Голопатюк Л. С., Коваленко Г. А., Шпура М. І. Майбутнє Північноатлантичного Альянсу в умовах невизначеності та складному геополітичному оточенні. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2020. № 2 (69). С. 35–39.
6. 2020 Strategic Foresight Report. Charting the Course Towards a more Resilient Europe, August 2020. URL: <http://globaltrends.thedialogue.org/publication/2020-strategic-foresight-report-charting-the-course-towards-a-more-resilient-europe/> (дата звернення: 02.02.2021).
7. Декларація Уельського саміту, видана главами держав та урядів, які брали участь у засіданні Північноатлантичної ради в Уельсі, 05 Sep. 2014. URL: [https://www.nato.int/cps/uk/natohq/official\\_texts\\_112964.htm?selectedLocale=uk](https://www.nato.int/cps/uk/natohq/official_texts_112964.htm?selectedLocale=uk) (дата звернення 02.02.2021).
8. Промова міністра закордонних справ України Дмитра Кулеби в рамках Конференції керівників закордонних дипломатичних установ 2020. URL: <https://mfa.gov.ua/news/promova-ministra-zakordonnih-sprav-ukrayini-dmitra-kulebi-v-ramkah-konferenciyi-kerivnikiv-zakordonnih-diplomaticnih-ustanov-2020> (дата звернення: 02.02.2021).
9. On is the driver of warfare development : станом на 26 груд. 2020 р. URL: [https://www.act.nato.int/application/files/4515/7661/3881/trifold\\_20191209](https://www.act.nato.int/application/files/4515/7661/3881/trifold_20191209).
10. William J. Burns. Reimagining Transatlantic Relations. URL: <https://carnegieendowment.org/2020/10/06/introduction-pub-82864> (дата звернення: 02.02.2021).
11. Озброєння, роззброєння та міжнародна безпека : Щорічник СППРІ 2019 / редкол. укр. вид. : О. Мельник (керівник проєкту) та ін. ; пер. з англ. ; підг. спільно Стокгольм. міжнар. ін-т дослідження миру та Укр. центр. екон. і політ. досліджень ім. О. Разумкова. Київ : Заповіт, 2019. 579 с.

Стаття надійшла до редакційної колегії 19.02.2021

**Prospects and scenarios for NATO's development in the global system of international relations**

Against the background of the events of the last decade in the security sphere, the scenario has already become clear, which envisages the return of NATO to a more serious approach to decisive steps in addressing issues of collective defense and security.

The abandonment of such a prospect, given the already deployed units of the Allied forces in Eastern Europe, especially Poland, Romania and the Baltic States, will lead to the idea (if not certainty) of the inferiority of the measures taken, and a statement that NATO is not ready for global action.

For Ukraine in its aspirations for membership in the Alliance, it is very important to predict with high probability the military-political development of NATO and, taking into account such forecasts, to formulate directions of its policy, including issues of military cooperation with the North Atlantic Treaty Organization.

This article is a continuation of the discussion proposed by the authors of the article "The future of the North Atlantic Alliance in a context of uncertainty and complex geopolitical environment" which analyzes the long-term vision of the North Atlantic Treaty Organization. In fact, this article is an attempt to predict the directions of the Alliance's policy, the international security, and the military-political situation in general, in accordance with the proposed scenarios. The probability and, ultimately, the success of one of these scenarios depend on a number of strategic factors.

In this article, the author tried to identify and analyze the most plausible scenarios for NATO's development, namely: "eurocentric NATO", "global NATO", "flexible NATO". Here each of the given scenarios is analyzed; all its positive and negative sides and consequences are defined. Also important is the significance of each of the scenarios for Ukrainian policy. The author singles out the "flexible NATO" scenario as the most favorable for more thorough cooperation and providing Ukraine with the necessary support.

**Keywords:** development scenarios; strategic directions of activity; NATO; "eurocentric NATO"; "global NATO"; "flexible NATO".

УДК 355.45.02 DOI: <https://doi.org/10.33099/2304-2745/2021-1-71/52-58>

Щипанський П. В., канд. військ. наук, професор<sup>1</sup> (0000-0002-0854-733X)  
Саганюк Ф. В., канд. юрид. наук., доцент<sup>2</sup> (0000-0002-9516-0562)  
Мудрак Ю. М.<sup>2</sup> (0000-0002-1159-5746)

<sup>1</sup> – Національний університет оборони України імені Івана Черняховського, Київ;

<sup>2</sup> – Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

## **Оборонний менеджмент: підходи до управління процесами оборонного планування**

**Резюме.** Розглянуті можливі підходи до управління процесами оборонного планування.

**Ключові слова:** Збройні Сили України; модель; оборонний менеджмент; оборонне планування; сили оборони; спроможності.

**Постановка проблеми.** Державна політика у воєнній сфері, сферах оборони і військового будівництва нині спрямовується на створення сучасних, мобільних і боєздатних сил оборони, які користуватимуться повагою в суспільстві та в іноземних партнерів і міжнародних організацій, а також спільно з іншими інституціями держави забезпечуватимуть всеохоплюючу оборону України, захист її суверенітету, територіальної цілісності та недоторканності.

Базовими документами у цих сферах, окрім Стратегії національної безпеки України, Стратегії воєнної безпеки України та Стратегічного оборонного бюлетеня України, розроблених за результатами оборонного огляду фахівцями Департаменту воєнної політики та стратегічного планування Міністерства оборони України, Генерального штабу Збройних Сил України, інших військових структур, зокрема і Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, є низка методологічних і методичних керівних документів, серед яких: Доктрина з оборонного планування у Збройних Силах України, затверджена Головнокомандувачем Збройних Сил України 13.11.2020; Порядок організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони, затверджений наказом Міністерства оборони України від 22.12.2020 № 484; Положення про особливості організації освітнього процесу у вищих військових навчальних закладах Міністерства оборони України та військових навчальних підрозділах вищих навчальних закладів

України, затверджене наказом Міністерства оборони України від 20.07.2015 № 346 та ін.

У цих нормативно-правових актах зазначено, що оборонне планування в Україні здійснюється з метою забезпечення обороноздатності держави шляхом визначення пріоритетів і напрямів розвитку сил оборони.

Водночас у цих документах обґрунтовані й основні ймовірні ризики у сфері воєнної безпеки і оборони, серед яких:

ухвалення стратегічно помилкових рішень у воєнній сфері, сфері оборони і військового будівництва на підставі неякісного аналізу реальних і потенційних воєнних загроз національній безпеці;

неефективний розподіл видатків на оборону України та витрачання державних ресурсів на утримання безперспективного озброєння, військової та спеціальної техніки;

недостатня спроможність забезпечити відсіч і стримування збройної агресії з боку Російської Федерації традиційними формами і способами збройної боротьби;

недостатній рівень взаємодії та неузгодженість заходів, які здійснюються силами оборони, іншими складовими сектору безпеки і оборони;

недостатні спроможності Збройних Сил України та інших складових сил оборони щодо охорони повітряного простору та протиповітряного прикриття важливих державних і військових об'єктів, недостатні військово-морські спроможності, зокрема щодо охорони підводного простору в межах територіального моря України, берегової оборони та захисту національних інтересів України в Азовському і Чорному морях;

нездатність провести весь комплекс заходів стратегічного розгортання у короткі строки в разі ескалації воєнного конфлікту або

повномасштабної збройної агресії Російської Федерації проти України тощо.

Одним із пріоритетів і завдань вирішення вказаних проблем сучасності Стратегією воєнної безпеки України визначений ефективний менеджмент у сфері оборони, заснований на засадах демократичного цивільного контролю, інших євроатлантичних принципах і стандартах, інноваційних рішеннях і сучасних практиках, програмно-проектному управлінні оборонними ресурсами, а також на удосконалених процесах визначення та задоволення сучасних потреб оборони України [1].

Важливим завданням наукової діяльності у цій сфері є формування сучасного наукового кадрового потенціалу, здатного забезпечити розвиток наукового прогресу у військовій галузі. Належне виконання цього завдання забезпечують система підготовки науково-педагогічних і наукових кадрів.

У наукових публікаціях [2–14] обґрунтовано різні моделі та необхідність підвищення в умовах сьогодення ефективності оборонного менеджменту з управління процесами оборонного планування, передусім забезпечувального характеру, для досягнення визначених стратегічних цілей оборонної реформи та наближення цих процесів до стандартів, прийнятих в арміях держав – членів НАТО.

**Аналіз останніх досліджень і публікацій.** У літературі розкриті різні моделі менеджменту підходи до управління процесами оборонного планування. Зокрема, у [2–4] йдеться про моделі менеджменту як форми управління практичними діями для досягнення бажаного результату. В інших публікаціях розглядаються теоретичні та прикладні моделі, що дає змогу оцінити параметри функціонування конкретного об'єкта і сформулювати відповідні рекомендації для прийняття практичних рішень. У [5–9] йдеться про імплементаційну практику та інші управлінські процеси.

Автори [10] виклали підходи до можливої імплементації норм чинного Закону України “Про національну безпеку України”, пов’язані з формуванням сучасної системи оборонного планування та розвитку сектору безпеки і оборони, розробленням довго- та середньострокових документів стратегічного та оборонного планування розвитку військ (сил) на основі спроможності за базовими складовими DOTMLPFI, яка широко застосовується в арміях держав – членів НАТО. Серед них наказом Міністерства оборони України від 22.12.2020 № 484 визначені доктринальна база, організація, підготовка, ресурсне забезпечення, якість управління та освіта, персонал, військова інфраструктура, взаємосумісність, які у сукупності є визначальними для утворення та досягнення спроможності в цілому (рис. 1).



Рис. 1. Базові складові спроможності (DOTMLPFI)

В оборонному менеджменті під час управління процесами оборонного планування основним є досягнення визначених стратегічних цілей на найближчу та віддалену перспективи через всебічне нормативно-

правове, організаційне, методичне, ресурсне та інше необхідне забезпечення ефективності всіх управлінських процесів [13].

Управляти такою діяльністю, як стверджував французький дослідник Анрі

Файоль, – це прогнозувати, планувати, організувати, командувати, координувати і контролювати її [3].

Отже, з аналізу наведених та інших публікацій цього напрямку дослідження можна дійти висновку про необхідність пошуку ефективних підходів до формування сучасної моделі управління процесами оборонного планування, що й обумовлює мету цієї статті.

**Метою статті** є пошук ефективних підходів до формування сучасної моделі управління процесами оборонного планування, наближення їх до сучасних потреб Збройних Сил, а також принципів і стандартів, прийнятих в арміях розвинутих держав – членів НАТО.

#### **Викладення основного матеріалу.**

Загальна методологія оборонного менеджменту в процесі оборонного планування в Міністерстві оборони України та Збройних Силах України нині визначена згаданим вище наказом Міністерства оборони України, згідно з яким на структурні підрозділи Міністерства оборони України в межах їх компетенції покладаються такі основні завдання:

аналіз воєнно-політичної обстановки та визначення рівня загроз національній безпеці України у воєнній сфері;

підготовка пропозицій до основних документів щодо формування та реалізації державної політики з питань національної безпеки і оборони;

визначення пріоритетів, основних напрямів розвитку Збройних Сил України та інших складових сил оборони;

розроблення Стратегії воєнної безпеки України і Стратегічного оборонного бюлетеня України;

участь у розробленні та моніторинг виконання програм і планів діяльності Кабінету Міністрів України;

організація розроблення проєктів державних цільових програм, моніторинг їх виконання;

організація досліджень з питань оборонного планування;

участь у підготовці пропозицій до прогнозів видатків з державного бюджету на сили оборони;

формування бюджетного запиту Міністерства оборони України;

формування основних показників Міністерства оборони України як державного замовника для здійснення оборонних закупівель;

контроль за ефективним витрачанням коштів і матеріальних цінностей;

підготовка звітних матеріалів про використання коштів, виділених на потреби оборони;

інформаційне забезпечення оборонного планування.

Зважаючи на наказ Міністерства оборони України від 22.12.2020 № 484, процес оборонного планування, включає:

планування спроможностей;

програмування розвитку спроможностей;

бюджетування та управління ресурсами; виконання програм і планів.

Імплементуючи положення зазначених концептуальних документів, загальний алгоритм оборонного менеджменту, а саме з управління процесами оборонного планування, можна представити схематично (рис. 2).

Планування спроможностей на довгострокову перспективу полягає у визначенні основних напрямів реалізації воєнної політики, стратегічних цілей розвитку та очікуваних результатів їх досягнення з урахуванням актуальних викликів і загроз національній безпеці України у воєнній сфері.

Під час планування спроможностей:

1) проводять аналіз майбутнього безпекового середовища;

2) розробляють імовірні сценарії виникнення та розвитку ситуацій воєнного характеру і варіантів застосування Збройних Сил України та інших складових сил оборони;

3) розробляють об'єднану оперативну концепцію;

4) визначають вимоги до спроможностей сил оборони (переліки завдань, необхідних, наявних, критичних та надлишкових спроможностей);

5) формують перспективну модель сил оборони з урахуванням прогнозу ресурсного забезпечення сил оборони.

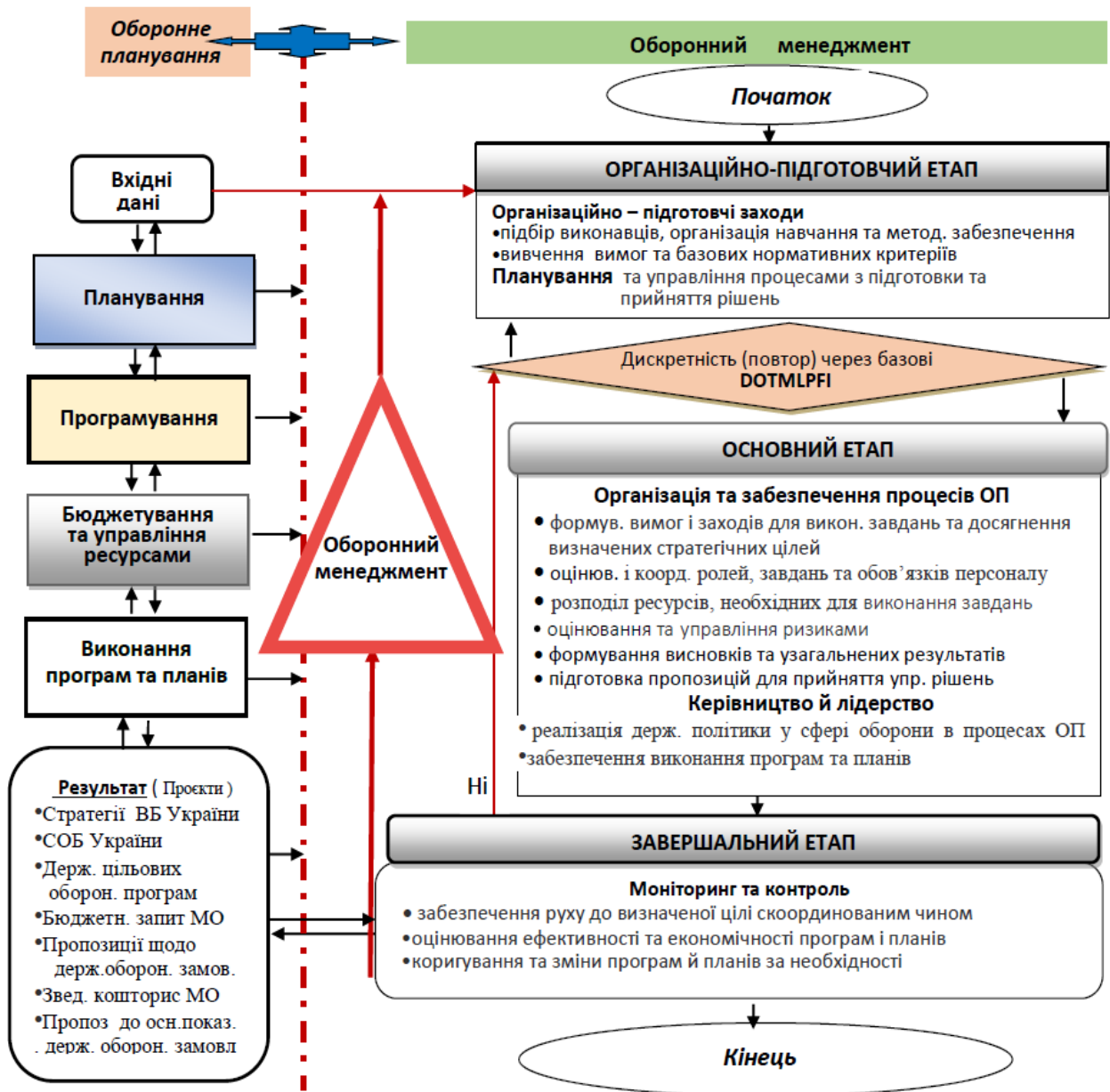


Рис. 2. Варіант алгоритму управління процесами оборонного планування

*Програмування розвитку спроможностей* на середньострокову перспективу полягає у деталізації завдань і заходів, спрямованих на досягнення цілей та очікуваних результатів розвитку складових сил оборони і передбачає розроблення:

державних цільових програм, спрямованих на розв'язання проблем забезпечення оборони держави та розвиток складових сил оборони, зокрема їх оснащення сучасним озброєнням і військовою технікою, створення необхідних запасів матеріально-технічних засобів, реалізацію інших заходів з посилення обороноздатності держави (далі – державні цільові оборонні програми);

комплексів програм (проектів), спрямованих на створення нових, розвиток існуючих і позбавлення від надлишкових

спроможностей Міністерства оборони України, Збройних Сил України та інших складових сил оборони.

Державні цільові програми складових сил оборони розробляються відповідно до Закону України від 18.03.2004 № 1621-IV (зі змінами та доповненнями) з урахуванням: завдань і пріоритетів, визначених Стратегічним оборонним бюлетенем України; викликів і загроз воєнного характеру, що впливають на рівень воєнної безпеки і оборони;

імовірних сценаріїв виникнення та розвитку ситуацій воєнного характеру; параметрів перспективної моделі, структури та чисельності складових сил оборони і потреби для їх досягнення;

обсягів прогнозованого ресурсного забезпечення складових сил оборони;

порядку досягнення необхідних спроможностей складових сил оборони за всіма їх базовими складовими із застосуванням матеріальних і нематеріальних рішень на всіх етапах життєвого циклу спроможності.

Комплекс програм (проектів) розвитку спроможностей складових сил оборони передбачає розроблення їх за методологією програмно-проектного менеджменту.

Бюджетування та управління ресурсами спрямовується на забезпечення виконання завдань з реалізації державної політики у сфері оборони на короткострокову перспективу з урахуванням процедур і термінів бюджетного процесу [13]. Цей процес передбачає розроблення:

орієнтовних планів та планів утримання і розвитку складових сил оборони;

планів утримання та розвитку видів, окремих родів військ (сил);

основних показників закупівель товарів, робіт і послуг оборонного призначення за закритим форматом (на трирічний період);

підготовку бюджетних запитів і формування кошторисів Міноборони та інших складових сил оборони.

Процес бюджетування та управління ресурсами здійснюється з урахуванням військово-політичних вказівок, які розробляються у місячний строк після затвердження Державного бюджету України та затверджуються наказом Міністерства оборони України (органів державної влади) до сфери управління (координації) яких віднесені відповідні складові сил оборони.

Визначення необхідного ресурсного забезпечення складових сил оборони включає [13]:

формування орієнтовної потреби в персоналі, інвестиціях на озброєння, військову і спеціальну техніку та системи вітчизняного й іноземного виробництва, інфраструктуру; експлуатаційних витратах для набуття силами оборони необхідних спроможностей;

формулювання вимог до вітчизняного оборонно-промислового комплексу щодо можливостей розроблення (модернізації) і виробництва основних зразків озброєння та військової техніки, з огляду на ймовірні сценарії, завдання за ними, необхідні спроможностей для виконання цих завдань та відповідний склад сил;

прогноз набуття спроможностей складових сил оборони залежно від обсягів

фінансування, можливостей вітчизняного оборонно-промислового комплексу та закупівлі озброєння й військової техніки іноземного виробництва.

За кожним варіантом розрахунків визначення та розподілу потреб в основних зразках виробів озброєння та військової техніки розраховується показник рівня виконання завдань за сценаріями (очікуваний рівень досягнення спроможностей), необхідна частка витрат на розвиток озброєння та військової техніки від загальної суми видатків, прогноз співвідношення щодо закупівлі техніки вітчизняного та іноземного виробництва, очікуваний рівень оновлення основних зразків виробів озброєння та військової техніки на кінець планового періоду.

Проведені розрахунки ресурсних потреб і визначені альтернативи досягнення мінімально-необхідного рівня виконання завдань з оборони держави використовуються під час формування перспективної моделі Збройних Сил України та інших складових сил оборони.

Розроблення проекту військово-політичних вказівок здійснює структурний підрозділ апарату Міністерства оборони України, на який покладено функції визначення засад воєнної політики та стратегічного планування (відповідний структурний підрозділ органу державної влади, до сфери управління (координації) якого належать інші складові сил оборони).

Управління процесом виконання (реалізації) цілей, завдань і планових заходів розвитку спроможностей Збройних Сил України та інших складових сил оборони здійснюється колегіальним органом Міністерства оборони України (інших складових сил оборони), який утворюється з метою:

визначення пріоритетів розвитку Збройних Сил України та інших складових сил оборони;

розроблення проектів концепцій, стратегій і програмних документів розвитку Збройних Сил України та інших складових сил оборони;

управління змінами під час реалізації програм (проектів) розвитку спроможностей Збройних Сил України та інших складових сил оборони.

Процес виконання програм і планів включає:

управління програмами (проектами) розвитку спроможностей;



проведення оцінювань спроможностей;  
моніторинг і контроль виконання заходів оборонного планування;  
управління ризиками;  
звітування про виконання програм і планів.

Методологічно, за змістовною ознакою, менеджмент з управління процесами класифікують як нормативний, стратегічний, оперативний [4]. *Нормативний менеджмент* спрямовується на створення доктринальних (нормативно-правових) основ реалізації місії певної діяльності та визначеної цілі за відповідними стандартами для формування загальної моделі й стратегії дій.

*Стратегічний менеджмент* охоплює розроблення такої стратегії для всіх складових та підрозділів організації, розподіл завдань щодо реалізації вибраної стратегії за часом. Він формує потенціал успіху й забезпечує загальний контроль за цим процесом.

*Оперативний менеджмент* розробляє методи реалізації прийнятої моделі та стратегії в конкретних умовах, тактичною адаптацією та оперативним реагуванням на умови, що змінюються.

Законом України “Про національну безпеку України” (п. 12 ст. 1) оборонне планування визнано складовою частиною системи державного стратегічного планування, що здійснюється з метою забезпечення обороноздатності держави шляхом визначення пріоритетів і напрямів розвитку сил оборони, їх спроможностей, озброєння та військової техніки, інфраструктури, підготовки військ (сил), а також розроблення відповідних концепцій, програм і планів з урахуванням реальних і потенційних загроз у воєнній сфері та фінансово-економічних можливостей держави. Виявляється, що ці правові засади мають бути імплементовані у зазначеній моделі. Указана проблема ще дискутується.

На думку авторів наукових публікацій [9–14], найбільш актуальними та складними у контексті імплементатії на перспективу є норми Закону України “Про національну безпеку України”, пов’язані з формуванням сучасної системи планування у сферах національної безпеки і оборони, розвитком сектору безпеки і оборони, розробленням та затвердженням за результатами оборонного огляду низки важливих довго- та середньострокових документів оборонного планування.

**Висновки.** З огляду на сучасну воєнно-стратегічну ситуацію, способи та методи ведення РФ агресивної гібридної війни проти України, оборонне планування розвитку та застосування Збройних Сил України на сучасному етапі потребує істотного вдосконалення, посилення оборонного менеджменту, зокрема управління його процесами, приведення їх до сучасних потреб та світового досвіду, передусім до принципів і стандартів, прийнятих в арміях держав – членів НАТО.

Для цього, як визначено Стратегією воєнної безпеки України, у сфері оборони, зокрема в процесі оборонного планування, необхідно здійснювати ефективний менеджмент, заснований на засадах демократичного цивільного контролю, інших євроатлантичних принципах і стандартах, інноваційних рішеннях та сучасних практиках, програмно-проектному управлінні оборонними ресурсами, а також на удосконалених процесах визначення та задоволення потреб оборони України.

Кінцевим результатом процесу такого оборонного планування є раціональні управлінські рішення у формі концепцій, стратегій, програм і планів щодо реалізації державної політики з питань національної безпеки і оборони у воєнній сфері, сферах оборони і військового будівництва, які, зважаючи на фінансово-економічні можливості держави, забезпечують досягнення рівня обороноздатності держави, необхідного для протидії наявним та можливим майбутнім викликам і загрозам воєнного характеру.

Відповідальність за моніторинг і контроль виконання цих стратегічних положень з оборонного планування та оборонного менеджменту в Міноборони та Збройних Силах покладається на керівників структурних підрозділів Міноборони та Генерального штабу, командувань видів, окремих родів військ (сил) та інших органів військового управління за напрямками діяльності, відповідальних за функціональні групи спроможностей, а в інших складових сил оборони – на відповідних керівників.

**Напрямок подальших досліджень.** Для якісної підготовки та ефективного оборонного менеджменту з управління процесами оборонного планування доцільно наблизити ці процеси до принципів і стандартів, прийнятих в арміях держав – членів НАТО.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року “Про Стратегію воєнної безпеки України” : Указ Президента України від 25.03.2021 р. № 121/2021.
2. Ачкасов А. С., Воронков О. О. Конспект лекцій з курсу “Економіко-математичне моделювання”. Харків : ХНАМГ, 2011. 204 с.
3. История менеджмента : уч. пособ. / под ред. Д. В. Валового. Москва : ИНФРА, 1997. С. 218–220.
4. Рудьєв В. А., Гуткевич С. О. Менеджмент : навч. посіб. Київ : Центр учбової літератури, 2011. 312 с.
5. Клименко О. Базові засади імплементації міжнародних нормативних документів у діяльності наукових бібліотек України: термінологічний аспект. URL: <http://nbuviap.gov.ua/index.php?option=com> (дата звернення: 04.01.2021).
6. Руснак І. С., Петренко А. Г., Яковенко А. В., Романюк І. М., Кохно В. Д. Оборонне планування на основі спроможностей: особливості та перспективи впровадження. *Наука і оборона*. 2017. № 2. С. 3–10.
7. Петренко А. Г. Що до впровадження оборонного менеджменту та управління змінами в Міністерстві оборони України. *Наука і оборона*. 2019. № 2. С. 3–8.
8. Романченко І. С., Богданович В. Ю., Денежкін М. М. Теоретико-методологічні засади побудови системи управління ефективністю планування та виконання програм розвитку Збройних Сил України. *Наука і оборона*. 2015. № 3–4. С. 50–55.
9. Тютюнник В. П., Лобко М. М. План оборони України: проблеми та рекомендації щодо визначення структури цього нового документа. Виклики та ризики. *Безпековий огляд Центру дослідження армії, конверсії та роззброєння* : аналіт. бюлет. 2019. № 19 (130). С. 10–21.
10. Щипанський П. В., Вдовін О. Г. Мобілізаційний резерв як фактор збільшення можливостей національної економіки задовольнити потреби Збройних Сил України. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2019. № 2 (66). С. 22–28.
11. Горovenko В. План оборони України: у зоні особливої уваги. *Defense express*. 2019. 24 жовтня.
12. Тютюнник В. П., Горovenko В. К. Як імплементувати Закон України “Про національну безпеку України”. *Defense Express*. 2018. 6 вересня.
13. Порядок організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони : затв. наказом Міністерства оборони України від 22.12.2020 р. № 484.
14. Оборонна реформа: системний підхід до оборонного менеджменту : монографія / А. Павліковський, В. Фролов, Ф. Саганюк, Ю. Мудрак та ін. ; за заг. ред. д-ра військ. наук А. Сиротенка. Київ : НУОУ, 2020. 276 с.

Стаття надійшла до редакційної колегії 01.02.2021

**Defense management: approaches to managing defense planning processes**

**Annotation**

State policy in the military sphere, defense and military construction is now aimed at creating modern mobile and combat-ready defense forces that will be respected in society and by foreign partners and international organizations, together with other state institutions will ensure comprehensive defense of Ukraine, protection of its sovereignty and territory integrity and inviolability.

Numerous scientific publications substantiate various models and the need to increase the effectiveness of defense management in the current environment of managing defense planning processes, especially security, in order to achieve certain strategic goals of defense reform and bring these processes closer to standards adopted in NATO armies.

*The purpose of the article* is to find effective approaches to the formation of a model for managing defense planning processes, bringing them closer to modern needs and the principles and standards adopted in the armies of developed NATO member states.

Defense planning is carried out in order to ensure the state's defense capabilities by determining the priorities and directions of development of defense forces, their capabilities, armaments and military equipment, infrastructure, training of troops (forces), as well as developing appropriate concepts, programs and plans taking into account real and potential threats in military sphere and financial and economic capabilities of the state. It is carried out using the capability-based planning method, which aims to develop them in the long term.

The defense planning process includes: capability planning; capacity development programming; budgeting and resource management; implementation of programs and plans.

In order to qualitatively prepare and implement effective defense management for the management of defense planning processes, it is expedient to improve the methodology of this work in practice, to bring these processes closer to the principles and standards adopted in the armies of NATO member states.

**Keywords:** Armed Forces of Ukraine; model; defense management; defense planning; defense forces; capabilities.

## Питання підвищення ефективності управління мобілізаційною підготовкою оборонного сектору національної економіки України

**Резюме.** У статті розглянуто сучасний стан управління мобілізаційною підготовкою національної економіки. Розглянуто роль керівництва центральних органів виконавчої влади, органів державної влади, інших державних органів та їх відповідальність за впровадження заходів мобілізаційної підготовки держави. Визначено можливі шляхи підвищення якості функціонування системи управління мобілізаційною підготовкою і мобілізацією національної економіки.

**Ключові слова:** мобілізаційна підготовка оборонного сектору національної економіки України; система управління; ресурсне забезпечення.

**Постановка проблеми.** Система державного управління мобілізаційною підготовкою є складовою частиною загальної системи управління державою, яка спрямовує свою діяльність також і на мобілізаційну підготовку оборонного сектору національної економіки України та ресурсне забезпечення заходів, що проводяться. Усі органи державної і недержавної влади напружено працюють для забезпечення зазначеного майже тридцять років. Нажаль ефективність цієї роботи важко признати задовільною. Прикладом цього є стан справ в авіаційній галузі, кораблебудуванні, танкобудуванні тощо.

У статті пропонується розглянути проблемні питання розподілу повноважень у системі управління мобілізаційною підготовкою національної економіки, можливості впливу на стан справ, що дасть змогу надалі визначити шляхи їх вирішення.

**Аналіз останніх досліджень і публікацій.** У вітчизняних публікаціях [2–4] багато уваги приділяється удосконаленню системи управління мобілізаційної підготовки оборонного сектору національної економіки України, але не достатньо повно і конкретно визначені функції органів управління і обов'язки їх керівників щодо розвитку та підтримання мобілізаційного потенціалу як складової національної економіки.

У публікаціях [5, 8–11] наведені матеріали досвіду управління мобілізаційною підготовкою, які стосуються широкого спектру питань планування заходів мобілізаційної підготовки економіки, однак не розкритий механізм трансформації досвіду провідних країн світу щодо питань фінансування заходів мобілізаційної підготовки економіки держави.

**Метою статті** є визначення шляхів підвищення ефективності управління мобілізаційною підготовкою оборонного сектору національної економіки України та

ролі центральних органів виконавчої влади, органів державної влади, інших державних органів відповідальних за впровадження заходів мобілізаційної підготовки в державі.

**Виклад основного матеріалу.** Оборонний сектор національної економіки (ОСНЕ) – специфічна частина економіки держави, до якої належать охоплені єдиним керівництвом сукупність центральних органів виконавчої влади, інших державних і недержавних органів управління, органів місцевого самоврядування, науково-дослідних, дослідно-конструкторських закладів, підприємств галузей національної економіки різних форм власності, на яких задіяні трудові ресурси відповідної кваліфікації, та які вирішують завдання розроблення, виробництва, модернізації і утилізації продукції військового призначення, матеріального забезпечення та надання послуг в інтересах оборони, забезпечують функціонування економіки в цілому та життєдіяльність населення.

Отже, мобілізаційні спроможності ОСНЕ можна визначити як властивості специфічної частини економіки держави, які забезпечують розгортання військового (мобілізаційного) виробництва у визначених потребах, зміну економічних пропорцій в інтересах всебічного збільшення виробництва військової продукції, перебудову роботи певної кількості органів управління державою та виробництвом, переведення роботи інформаційного простору, трудових ресурсів, промисловості, транспорту, зв'язку, енергетики, будівництва, сільського господарства, системи медичного, ветеринарного, санітарно-епідемічного забезпечення, видобутку природних ресурсів, формування системи життєзабезпечення населення в інтересах задоволення потреб особливого періоду, забезпечення живучості та стійкості господарчого механізму держави, зміни діяльності наукових і дослідно-

конструкторських закладів для задоволення потреб оборони тощо [3].

Мобілізаційна підготовка – комплекс організаційних, політичних, економічних, фінансових, соціальних, правових та інших заходів, які здійснюються в мирний час з метою підготовки національної економіки, органів державної влади, інших державних органів, органів місцевого самоврядування, Збройних Сил України, інших утворених відповідно до законів України військових формувань, а також правоохоронних органів спеціального призначення, Державної служби спеціального зв'язку та захисту інформації України та Державної спеціальної служби транспорту (далі – Збройні Сили України, інші військові формування), сил цивільного захисту, підприємств, установ і організацій до своєчасного й організованого проведення мобілізації та задоволення потреб оборони держави і захисту її території від можливої агресії, забезпечення життєдіяльності населення в особливий період [1].

Система управління мобілізаційною підготовкою – складова частина загальної системи управління державою, яка спрямовує діяльність органів державної влади, інших державних органів, органів місцевого самоврядування, єдиної державної системи цивільного захисту на підготовку систем управління, засобів зв'язку, інформаційного забезпечення, а також фінансових і матеріально-технічних ресурсів, підприємств, установ і організацій до проведення мобілізації [1].

Діяльність у сфері мобілізаційної підготовки держави регламентують: Закони України – 15; Укази Президента України – 10; Постанови Кабінету Міністрів України – 34; Розпорядження Кабінету Міністрів України – 7; накази Міністра розвитку економіки, торгівлі і сільського господарства України – 12.

Загальне керівництво у сфері мобілізаційної підготовки і мобілізації національної економіки здійснюється Президентом України. Організаційне керівництво мобілізаційною підготовкою і мобілізацією в Україні здійснюється Кабінетом Міністрів України. Координація

діяльності органів виконавчої влади з питань мобілізаційної підготовки та мобілізації покладається на Раду національної безпеки і оборони України [1, 2].

Проте в апаратних структурах на сьогодні не функціонують потужні мобілізаційні органи для підготовки рішень, обґрунтування показників ресурсів, які потрібні, вирішення завдань організації взаємодії та контролю виконання заходів.

Координація планування, методологічне забезпечення розроблення проєктів мобілізаційних планів та довгострокових і річних програм мобілізаційної підготовки в органах виконавчої влади, інших державних органах покладається на Міністерство розвитку економіки, торгівлі та сільського господарства України, але в його структурі також відсутній спроможний мобілізаційний орган.

Мобілізаційну підготовку оборонного сектору національної економіки, як це і передбачає діюча нормативно-правова база держави, доцільно розглядати за чотирма основними напрямками, а саме:

мобілізаційну підготовку до функціонування системи управління державою в особливий період;

мобілізаційну підготовку до мобілізаційного розгортання Збройних Сил України, інших військових формувань, Оперативно-рятувальної служби цивільного захисту;

мобілізаційну підготовку до функціонування національної економіки в особливий період;

мобілізаційну підготовку до функціонування системи забезпечення життєдіяльності населення в особливий період.

Перелік наведених напрямів мобілізаційної підготовки, складність завдань дають право стверджувати, що на стратегічному рівні державного управління з існуючими структурами управління та кадровим потенціалом можливо здійснювати тільки загальне керівництво відповідними процесами, а з урахуванням текучості керівних кадрів і це завдання виконувати вкрай проблематично. Це і є перше невирішене питання мобілізаційної підготовки національної економіки держави щодо підготовки до функціонування в особливий період.

Для підвищення ефективності мобілізаційної підготовки національної економіки держави пропонується розглянути

роль керівників центральних органів державної влади, інших державних органів за основними напрямками щодо готовності економіки до функціонування в особливий період.

На сьогодні повноваження з питань мобілізаційної підготовки щодо функціонування системи управління державою в особливий період визначено Положенням про Офіс Президента України, затвердженого Указом Президента України від 25 червня 2019 року № 436/2019.

Основними завданнями Офісу є організаційне, правове, консультативне, інформаційне, експертно-аналітичне та інші забезпечення, здійснення Президентом України визначених Конституцією України повноважень. Проте питання організації мобілізаційної підготовки щодо функціонування системи управління державою в особливий період в завданнях Офісу не визначено.

Ст. 8 Закону України “Про Раду національної безпеки і оборони України” встановлює, що на Апарат Ради національної безпеки і оборони України покладається інформаційно-аналітичне та організаційне забезпечення діяльності Ради національної безпеки і оборони України, у якій питання організації мобілізаційної підготовки до функціонування системи управління державою в особливий період також не визначені.

Ст. 5 Закону України “Про Кабінет Міністрів України” визначає повноваження у сфері національної безпеки та обороноздатності: “...здійснює керівництво єдиною системою цивільного захисту України, мобілізаційною підготовкою національної економіки та переведенням її на режим роботи в умовах надзвичайного чи воєнного стану”.

Так, відповідно до діючої правової бази, не визначено в державі єдиного центрального органу виконавчої влади, а особливо його повноваження та відповідальність у питаннях мобілізаційної підготовки щодо функціонування системи управління державою в особливий період. Зважаючи на те, що Конституція України визначає Кабінет Міністрів України вищим органом у системі органів виконавчої влади, він і має бути відповідальним за зазначене без делегування повноважень іншим.

Розглянемо питання щодо мобілізаційної підготовки національної

економіки до функціонування в особливий період.

Відповідно до законодавства держави, Кабінет Міністрів України:

визначає порядок управління національною економікою України та заходи із забезпечення її функціонування в особливий період;

погоджує довготермінові та річні програми мобілізаційної підготовки державних органів, Автономної Республіки Крим, областей, міст Києва та Севастополя;

визначає порядок укладання договорів (контрактів) на виконання підприємствами, установами і організаціями мобілізаційних завдань (замовлень), зокрема на поставку матеріально-технічних ресурсів, виконання робіт і надання послуг, зокрема щодо поставки готової продукції, забезпечення виконання зазначених завдань (замовлень) матеріально-технічними ресурсами, а також щодо їх фінансування;

Міністерство розвитку економіки, торгівлі та сільського господарства (далі – Мінекономіки України) у зазначеній сфері:

координує планування, методологічне забезпечення розроблення проєктів мобілізаційних планів та довготермінових і річних програм мобілізаційної підготовки в органах виконавчої влади, інших державних органах;

бере участь у розробленні проєктів державних програм економічного і соціального розвитку України для врахування мобілізаційних потреб держави;

координує роботу щодо: підготовки пропозицій до проєктів державних програм економічного і соціального розвитку України в частині мобілізаційної підготовки; створення, розвитку, утримання, передачі, ліквідації і реалізації мобілізаційних потужностей; створення мобілізаційного резерву матеріально-технічних і сировинних ресурсів;

контролює виконання довготермінових і річних програм мобілізаційної підготовки національної економіки.

Безпосереднє керівництво щодо реалізації заходів з мобілізаційної підготовки і мобілізації національної економіки здійснюється керівниками центральних органів виконавчої влади, інших державних органів, місцевих органів виконавчої влади та виконавчих органів сільських, селищних, міських рад. Тобто струнка логічна система [1], але: по-перше, у зазначених органів управління **фінансових** ресурсів на

мобілізаційну підготовку немає; по-друге, не виправдано часто застосовуються слова “бере участь, координує, визначає”, недостатньо слова – “організовує, відповідає, вирішує питання фінансування”.

До того ж не сприяють вирішенню завдань мобілізаційної підготовки оборонного сектору національної економіки існуючи на погляд автора проблемні питання щодо формування державного бюджету. Кошториси бюджетів за рівнями управління не передбачають можливостей цільової фінансової підтримки органами виконавчої влади виробника (підприємства-виконавця мобілізаційного завдання). Наприклад, в умовах обмежених фінансових ресурсів, проблематичне централізоване придбання технологій, обладнання, сировини тощо.

Існують проблемні питання фінансування бюджетними коштами мобілізаційної підготовки підприємств різної форми власності. Можливо було б вирішувати питання через кредитування банками, але проведення заходів мобілізаційної підготовки підприємств не надає прибутку. Як розрахуватись за кредити? Продукція, надані послуги та сплата за них з'являться в особливий період.

Вирішення питань мобілізаційної підготовки національної економіки у складі діючої економіки ускладняється незавершеністю галузевого структурування за багатьма напрямками, наприклад: танкобудування, суднобудування, автомобілебудування тощо. Відсутність повноцінного структурування за галузями не сприяє розробленню планів управління на особливий період, довготермінових мобілізаційних та інших програм розвитку збиральних та агрегатних підприємств, організації повноцінного фінансування заходів, що плануються. Мала ймовірність, що окреме підприємство в змозі добитися його цільового державного бюджетного фінансування заходів мобілізаційної підготовки.

Отже в існуючій структурі національної економіки мобілізаційну підготовку підприємств має організувати центральний орган виконавчої влади, в інтересах якого працюватиме зазначене підприємство. Він же має укладати договори (контракти) на виконання підприємствами, установами і організаціями мобілізаційних завдань (замовлень), фінансувати заходи мобілізаційної підготовки підприємства, контролювати

ефективність витрачання ресурсів, перевіряти мобілізаційну готовність.

Існують питання щодо організації мобілізаційної підготовки до функціонування системи забезпечення життєдіяльності населення в особливий період. У державі не визначено центральний орган виконавчої влади, на який покладається відповідальність за організацію, підготовку нормативно-правової бази, методичне та наукове забезпечення вирішення зазначеного питання. Конкретно не встановлена відповідальність, особистий організаційний, ресурсний внесок, повноваження за місцевими, районними, територіальними та державним рівнем управління. Справа в тому, що питання організації та забезпечення життєдіяльності населення в особливий період не належать до локальної території і мають міжгалузевий характер. Наприклад, транспортне забезпечення для пошуку роботи, проїзду до міста працевлаштування тощо. Енергетичне (електроенергією) забезпечення організовано в державі від району і вище. Медичне забезпечення за видами послуг ґрунтується за видами послуг на багаторівневої системі. Дуже просте, на перший погляд, але дуже складне у виконанні питання забезпечення населення паливом для опалення власного житла. У державі у більшості місцевостей відсутні ліса та копальні вугілля. Існуюча система газопостачання вкрай не стійка. Тобто потрібне організаційне начало на рівні центральних органів виконавчої влади. Торговельне забезпечення за мінімальною необхідною номенклатурою товарів для населення не можливо вирішити повноваженнями органів місцевого самоврядування тощо. З огляду на складність завдань, багаторівневість органів прийняття рішень, міжгалузевий характер виконання завдань відповідальним за організацію мобілізаційної підготовки до функціонування системи забезпечення життєдіяльності населення в особливий період має бути Кабінет Міністрів України.

Підготовка до мобілізаційного розгортання Збройних Сил України, інших військових формувань, Оперативно-рятувальної служби цивільного захисту організується органами управління відповідних військових формувань і правоохоронних органів.

Міністерство оборони України є головним органом у системі центральних органів виконавчої влади, яке забезпечує формування та реалізує державну політику з

питань національної безпеки у війсьній сфері, сферах оборони і військового будівництва у мирний час та особливий період. До повноважень Міністерства оборони України належать організація військово-технічної політики у сфері оборони, здійснення в установленому порядку координації діяльності державних органів та органів місцевого самоврядування щодо підготовки держави до оборони.

Генеральний штаб Збройних Сил України (ГШ ЗС України) визначає потреби в ресурсах. Міністерство оборони України разом з органами управління інших військових формувань, іншими центральними органами виконавчої влади під керівництвом Мінекономіки України готують проект мобілізаційного плану національної економіки України на особливий період.

Кабінет Міністрів України визначає і затверджує основні показники мобілізаційного плану національної економіки та мобілізаційні завдання (замовлення) центральним і місцевим органам виконавчої влади, іншим державним органам тощо. Нажаль на цьому повноваження та можливості впливу з боку Міністерства оборони України, ГШ ЗС України на проведення заходів матеріального забезпечення, надання послуг мобілізаційними ресурсами національної економіки закінчуються.

Уже тривалий час не працюють підприємства реального сектору економіки танкобудування, літакобудування, суднобудування тощо. Хоча продукція зазначених підприємств вкрай необхідна державі. Наприклад, ДП “Завод імені В. О. Малишева” за певних умов виробляв сотні танків на рік, за останні роки сучасні бойові машини у достатньої кількості не виробляє, а ПАТ “АвтоКрАЗ” основний постачальник у війська (сили) автомобільної техніки – банкрут через недостатнє завантаження замовленнями та скрутним фінансовим становищем. І таких прикладів багато. Імпортозаміщення майже не проводиться, робочі місця у потрібній кількості не створюються, фахівців готують недостатньо.

Проблеми, що виникли, це наслідки відсутності необхідних *фінансових* ресурсів у державі (табл. 1, 2). Наведені в таблицях показники витрат на оборону не сприяють завантаженню в потрібних обсягах промисловість України в межах державного оборонного замовлення. Держави, які за показниками валового внутрішнього продукту за оцінкою Міжнародного валютного фонду розташовані поруч з Україною взагалі не мають ВПК, мобілізаційних потужностей для забезпечення потреб оборони.

Таблиця 1

Витрати на оборону міністерств оборони деяких держав за 1999 – 2022 роки, млн дол. [6]

Рік	Чехія	Угорщина	Польща	Румунія	Росія	Україна	Німеччина
1999	1205,93	702,94	3226,56	955,34	6469,04	620,81	31185,04
2000	1157,29	715,86	3146,11	935,57	9228,20	696,40	26924,87
2001	1182,52	845,06	3630,65	985,66	11683,15	741,71	26231,68
2002	1494,39	1079,16	3776,17	1056,14	13943,83	872,39	28056,59
2003	1885,71	1401,56	4150,26	1250,33	16973,74	1104,81	33529,45
2004	2042,09	1532,61	4778,63	1530,18	20955,41	1322,22	36353,48
2005	2439,54	1596,09	5896,41	1975,98	27336,98	1680,11	36397,87
2006	2449,96	1410,07	6619,41	2251,49	34517,78	2085,90	36434,56
2007	2707,68	1776,46	8589,14	2607,69	43534,99	2860,87	41116,12
2008	2918,70	1867,88	9349,42	3000,41	56183,79	3360,26	46459,88
2009	2718,56	1475,82	7903,81	2225,15	51532,12	2320,41	46119,78
2010	2497,90	1350,82	8790,17	2086,22	58720,23	2587,45	44852,96
2011	2474,31	1472,07	9455,42	2379,87	70237,52	2502,30	46765,51
2012	2220,61	1322,28	8986,84	2102,89	81469,40	2835,91	44470,34
2013	2148,78	1280,05	9275,71	2452,51	88352,90	2895,00	44865,69
2014	2022,88	1209,80	10345,15	2691,47	84696,50	2997,18	44216,06
2015	1779,89	1132,48	10212,79	2580,59	66418,33	2959,58	37020,07
2016	1954,94	1288,68	9164,19	2644,16	69245,31	2943,81	39724,91
2017	2077,72	1463,01	9870,68	3622,07	66527,30	3246,79	42365,77
2018	2710,02	1791,55	12040,67	4359,02	61387,55	4169,71	46511,57
2019	2910,25	1904,37	11902,53	4944,96	65102,57	5228,93	49276,76
2020*	2995,47	1964,44	12336,33	5144,44	68034,25	5459,34	50181,35
2021*	3080,69	2024,51	12770,13	5343,92	70965,93	5689,75	51085,94
2022*	3165,91	2084,58	13203,93	5543,40	73897,61	5920,16	51990,53

Джерело: www.svspsb.net; \* – прогнозні дані.

Таблиця 2

**Валовий внутрішній продукт деяких держав світу за 2018 рік, млрд дол. США (данні МВФ) [7]**

Держава	Показник ВВП(млрд дол. США)
Ефіопія	80,3
Марокко	118,3
Еквадор	107,5
Україна	124,6
Угорщина	155,7
Казахстан	170,5
Катар	192,5

З огляду на критичність позицій для поступового ресурсного забезпечення вирішення завдань оборони ГШ ЗС України пропонується визначати потребу невідкладного задоволення: першочергову, другочергову і т. ін. В умовах обмеженості ресурсів можна і потрібно поступово при відповідній політичній волі та економічній доцільності спочатку створити можливості щодо задоволення невідкладних потреб, а потім, поступово, першочергових тощо. На сьогодні, протягом 29-ти років ГШ ЗС України, виконуючи законодавчу норму, визначає і через Міністерство оборони України подає Кабінету Міністрів України потребу Збройних сил України за найскладнішим варіантом розвитку подій.

Найбільш ефективно задоволення потреб оборони держави необхідно вирішувати спочатку через державне оборонне замовлення продукції оборонного та подвійного призначення у мирний час. Це створює умови для завчасної підготовки виробництва, пошуку співвиконавців по кооперації, постачальників вузлів, агрегатів, вирішення питань з безперебійним отриманням сировини в потрібних обсягах і необхідної якості, підготовки трудових ресурсів. Мають бути пов'язані проекти Державного оборонного замовлення, Державна програма розвитку озброєння і військової техніки та Стратегія розвитку оборонно-промислового комплексу України. Позитивом є і те, що замовник продукції та виробник працюють без посередників (Мінекономіки). Бюджетні кошти від замовника (господаря грошей) рухаються після виконання замовлення (у більшості випадків) виконавцю на умовах складених договорів.

Покладання мобілізаційних завдань (замовлень) завдяки укладанню договорів на підприємства виконавця державного оборонного замовлення на ідентичну

оборонну продукцію та послуги сприятиме поступовому створенню резервів необхідних потужностей.

Отже доцільно роботу системи державного оборонного замовлення, мобілізаційну підготовку підприємств організувати центральним органом виконавчої влади в інтересах якого працюватимуть підприємства Міністерства оборони України, Міністерства внутрішніх справ України тощо.

Міністерство повинно мати повноваження на:

пошук виконавців завдань та проведення тендерів;

підготовку проектів Постанов Кабінету Міністрів України щодо визначення мобілізаційних завдань (замовлень) центральним і місцевим органам виконавчої влади, іншим державним органам, підприємствам на особливий період;

підготовку проектів Постанов Кабінету Міністрів України щодо створення мобілізаційних потужностей;

розроблення проекту Схеми мобілізаційного розгортання виробництва оборонної продукції, виконання робіт, надання послуг в особливий період з визначенням підприємств-виконавців оборонного замовлення, мобілізаційних завдань (замовлень), номенклатури продукції та її кількості, строків початку виробництва та виходу на повну потужність, перелік суміжників та постачальників сировини;

підготовку проекту Мобілізаційного плану за підприємства, які виробляють оборонну продукцію, виконують роботу та надають послуги в інтересах міністерства;

доведення мобілізаційних завдань (замовлень) до центральних і місцевих органів виконавчої влади, інших державних органів, підприємств на особливий період;

контроль мобілізаційної готовності виконавців мобілізаційних завдань (замовлень).

Центральний орган виконавчої влади має укладати договори (контракти) на



виконання підприємствами, установами і організаціями державного оборонного замовлення, мобілізаційних завдань (замовлень), фінансувати заходи мобілізації підприємства, контролювати ефективність витрачання ресурсів.

Фінансування заходів дослідно-конструкторських робіт, створення виробництва, виробництво продукції в межах державного оборонного замовлення, створення резервів потужностей (мобілізаційних можливостей) здійснюється за рахунок кошторису міністерства.

Наприклад, Міністерство оборони України створює умови для:

прийняття більш виважених рішень у визначенні номенклатури продукції та послуг, які готуватимуться до виробництва та придбаватимуться в умовах обмежених ресурсів;

підвищення відповідальності посадових осіб за підготовку відповідних рішень, підготовку та захист позицій бюджетного запиту, витрати бюджетних коштів;

гарантованого забезпечення впровадження життєвого циклу озброєння та військової техніки: науково-дослідні, дослідно-конструкторські роботи, серійне виробництво, експлуатація у військах (силах), ремонт, модернізація, утилізація;

підвищення ефективності витрат бюджетних коштів;

поліпшення управління мобілізаційною підготовкою оборонного сектору економіки та гнучкістю мобілізаційним розгортанням виробництва.

**Висновки та напрями подальших досліджень.** Отже, для удосконалення та підвищення ефективності управління мобілізаційною підготовкою оборонного сектору національної економіки України пропонується покласти відповідальність за:

мобілізаційну підготовку щодо функціонування системи управління державою в особливий період – на Кабінет Міністрів України;

мобілізаційну підготовку щодо мобілізаційного розгортання Збройних Сил України, інших військових формувань, Оперативно-рятувальної служби цивільного захисту – на Міністерство оборони України, Міністерство внутрішніх справ України;

мобілізаційну підготовку щодо функціонування оборонного сектору національної економіки в особливий період з питань наукового, методичного, організаційного керівництва, загального

планування та звітності – на Мінекономіки України;

мобілізаційну підготовку щодо функціонування системи забезпечення життєдіяльності населення в особливий період – на Кабінет Міністрів України;

мобілізаційну підготовку підприємств-виконавців державного оборонного замовлення, мобілізаційних завдань (замовлень), планування та звітність – на Міністерство оборони України, Міністерство внутрішніх справ України.

Створити в складі зазначених центральних органів виконавчої влади потужні виконавчі структури.

Удосконалити нормативно-правову базу з метою створення умов для ефективної подальшої роботи в зазначеній сфері.

**Подальші дослідження** спрямувати на моделювання роботи системи управління державою в мирний час та особливий період з питань мобілізаційної підготовки оборонного сектору національної економіки.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про мобілізаційну підготовку та мобілізацію : Закон України від 21.10.1993 р. № 3544-ХІІ. ВВР, 1993, № 44, ст. 417. URL: <https://zakon.rada.gov.ua/laws/show/3543-12> (дата звернення: 02.01.2021).
2. Грінченко О. І. Ворович Б. О., Кутовий О. П. Аналіз системи управління мобілізаційною підготовкою та мобілізацією національної економіки. Визначення проблемних питань її функціонування. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2020. № 1 (68). С. 44–51.
3. Грінченко О. І., Кутовий О. П., Шапталенко М. І. Мобілізаційні спроможності оборонного сектору національної економіки України: погляди на ефективність. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2019. № 2 (66). С. 29–34.
4. Горбулін В. П. Зубарев В. В., Скурський П. П., Кутовий О. П. Проблемні питання формування ефективної системи управління оборонно-промисловим комплексом України. *Національна безпека: український вимір*. 2009. № 4 (23). С. 11–20.
5. Волотівський П. Б., Дупляк П. П. Щодо причин низької якості управління мобілізаційною підготовкою та мобілізацією в державі. *Довготермінові програми мобілізаційної підготовки. Їх роль у забезпеченні готовності держави до функціонування в умовах особливого періоду* : матеріали міжвідом. наук.-практ. конф. м. Київ, 16 квіт. 2015 р. Київ, 2015. С. 77–83.

6. Показники ВВП країн світу. URL: <https://knoema.ru/nwnfkne/%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%BE%D0%B9-%D1%80%D0%B5%D0%B9%D1%82%D0%B8%D0%BD%D0%B3%D1%81%D1%82%D1%80%D0%B0%D0%BD-%D0%BF%D0%BE-%D0%B2%D0%B2%D0%BF-%D0%B2-2019%D0%B3%D0%BE%D0%B4%D1%83%D1%81%D1%82%D0%B0%D1%82%D0%B8%D1%81%D1%82%D0%B8%D0%BA%D0%B0> (дата звернення: 02.01.2021).
7. Рынок и мобилизационные мощности в промышленности (на примере США). URL: [http://svop.ru/wp-content/uploads/2018/10/VoennyVestnik\\_MFIT\\_No3\\_RYNOK-I-MOBILIZACIONNYYE-MOSCHNOSTI.pdf](http://svop.ru/wp-content/uploads/2018/10/VoennyVestnik_MFIT_No3_RYNOK-I-MOBILIZACIONNYYE-MOSCHNOSTI.pdf) (дата звернення: 04.01.2021).
8. Оцінка та управління якістю планів. URL: <https://library.if.ua/book/122/8069.html> (дата звернення: 04.01.2021).
9. Ширалієв Р. Ш. Проблемні питання законодавчого, нормативно-правового та організаційного характеру, що впливають на функціонування національної економіки України в особливий період та забезпечення потреб оборони. *Проблеми своєчасного забезпечення Збройних Сил України озброєнням, військовою технікою, іншими матеріально-технічними засобами в особливий період. Можливі шляхи їх вирішення* : матеріали наук.-практ. семінару. м. Київ, 26 лист. 2015 р. Київ, 2015. С. 19–26.
10. Волотівський П. Б. Питання мобілізаційного планування національної економіки України. Зміст, принципи та підходи щодо його організації в сучасних умовах. *Наука і оборона*. 2018. № 2. С. 17–24.
11. Горовенко В. К., Щипанський П. В. Деякі проблеми організації мобілізаційної підготовки України. *Довготермінові програми мобілізаційної підготовки. Їх роль у забезпеченні готовності держави до функціонування в умовах особливого періоду* : матеріали міжвідом. наук.-практ. конф. м. Київ, 16 квіт. 2015 р. Київ, 2015. С. 23–26.

Стаття надійшла до редакційної колегії 25.01.2021

## Issues of improving the efficiency of management of the mobilization training of the defense sector of the national economy of Ukraine

### Annotation

The system of state management of mobilization training is an integral part of the general system of state management, which directs its activities, including the mobilization readiness of the defense sector of the national economy of Ukraine, resource provision of ongoing activities.

Ways to increase the efficiency of management of mobilization training of the defense sector of the national economy of Ukraine and the role of central executive bodies, public authorities, other state bodies responsible for the implementation of mobilization training in the state are identified.

Mobilization training of the defense sector of the national economy, as provided by the current legal framework of the state, should be considered in four main areas, namely:

mobilization training for the functioning of the state management system in a special period;

mobilization training for the mobilization deployment of the Armed Forces of Ukraine, other military formations, operational and rescue service of civil defense;

mobilization training for the functioning of the national economy in a special period;

mobilization training for the functioning of the system of ensuring the livelihood of the population in a special period.

The decision of questions of mobilization preparation of national economy as a part of operating economy is complicated by incompleteness of branch structuring in many directions. Therefore, in the existing structure of the national economy, mobilization training of enterprises should be organized by the central executive body in the interests of which the enterprise will operate.

It is proposed to create powerful executive structures within these central executive bodies.

**Keywords:** mobilization training of the defense sector of the national economy of Ukraine; management system, resource provision.

Братко А. В., канд. військ. наук, доцент

(0000-0001-5503-3318)

Національна академія Державної прикордонної служби України імені Богдана Хмельницького, Хмельницький

## Удосконалення оборонного планування у Державній прикордонній службі України

**Резюме.** У статті досліджені сучасні підходи та наведені певні рекомендації щодо удосконалення планування у Державній прикордонній службі України на основі спроможностей. Таке планування дасть змогу якісніше планувати оперативно-службову діяльність прикордонного відомства та забезпечувати активніше співробітництво України з НАТО з метою досягнення критеріїв, необхідних для набуття повноправного членства в Альянсі.

**Ключові слова:** планування; спроможності; оперативно-службова діяльність; сили та засоби; Державна прикордонна служба України.

**Постановка проблеми.** Події останніх років змінили умови, у яких функціонує Державна прикордонна служба України (далі – ДПС України), що призвело до нагальної потреби, а саме удосконалення планування оперативно-службової діяльності та подальшого розвитку (реформування) відомства.

Планування в ДПС України на основі спроможностей є одним із перспективних методів планування у сфері забезпечення безпеки державного кордону, особливістю якого є розвиток спроможностей сил для ефективної протидії загрозам і ризикам як воєнного, так і невоєнного характеру з урахуванням імовірних сценаріїв розвитку конфліктних (кризових) ситуацій на довгострокову перспективу. Цей метод планування є основним в країнах - членах НАТО.

**Аналіз останніх досліджень і публікацій.** У наукових працях [1–7] проведено дослідження щодо:

організації і планування діяльності Збройних Сил України (далі – ЗС України) та інших складових сектору безпеки і оборони;

проблем розвитку спроможностей сил безпеки і оборони;

стратегічного планування на основі спроможностей за підходами управління, які орієнтовані на результат;

наявного стану та подальшого розвитку системи оборонного планування в ЗС України.

У монографії [8], яка присвячена оборонному менеджменту, викладені новітні підходи до впровадження у Міністерстві оборони (МО), ЗС України та інших складових сил оборони системного підходу до оборонного менеджменту.

Проте залишається невирішеним актуальне питання щодо впровадження планування на основі спроможностей в діяльність ДПС України.

**Мета статті** є удосконалення планування оперативно-службової діяльності органів управління ДПС України на основі їх спроможностей.

**Викладення основного матеріалу.** Планування оперативно-службової діяльності на основі спроможностей потребує вдосконалення, передусім, за функціональною ознакою. Адже функціональна група спроможностей, відповідно до Порядку організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони, затвердженого наказом МО України від 22.12.2020 № 484, являє собою “сукупність спроможностей складових сил оборони, поєднаних в ієрархічну структуру відповідно до їх функціонального призначення”.

Функції та завдання, що мають виконуватись під час очікуваних (вірогідних, майбутніх) дій сил і засобів, трансформуються у вимоги до спроможностей, на підставі чого планується їх створення, підтримання та розвиток.

Планування в ДПС України на основі спроможностей передбачає створення, розвиток та підтримання оптимального складу необхідних спроможностей в межах наявних ресурсів. Однак матеріальні ресурси не завжди є визначальним фактором розвитку спроможностей.

Ефективними шляхами нарощування спроможностей може бути удосконалення законодавчої бази, основ застосування, структур частин і підрозділів ДПС України,

впровадження нових форм і методів оперативно-службової діяльності, поліпшення системи відбору на військову службу, навчання, підготовка та мотивація персоналу відомства тощо.

На відміну від планування на основі загроз, планування на основі спроможностей в ДПС України потребує зосередження зусиль не на створенні нових організаційних структур для забезпечення протидії правопорушенням, а на розвитку спроможностей наявних сил для ефективного виконання визначених їм завдань за функціональним призначенням.

*Основними завданнями планування оперативно-службової діяльності в ДПС України на основі спроможностей є [8]:*

оцінювання середовища у сфері забезпечення безпеки державного кордону, визначення засад, цілей та основних завдань ДПС України в системі державної політики у сфері оборони держави, пріоритети і напрями розвитку сил безпеки державного кордону з урахуванням реальних і потенційних загроз у прикордонній сфері, демографічних і фінансово-економічних можливостей держави;

визначення вимог до спроможностей, структури, чисельності персоналу, кількісних і якісних показників ОВТ, інших видів МТЗ, прикордонної інфраструктури, підготовленості особового складу сил прикордонного відомства (формування перспективного складу ДПС України, який задовольняє вимогам щодо необхідних спроможностей з урахуванням можливостей держави задовольнити потреби у забезпеченні безпеки державного кордону);

оцінювання стану готовності сил ДПС України до виконання завдань із забезпечення безпеки державного кордону (оцінювання наявних спроможностей ДПС України щодо виконання завдань за всіма визначеними сценаріями), а також результати виконання заходів з їхнього розвитку за попередній період;

формування комплексного документа з розвитку спроможностей ДПС України та потреби на розвиток спроможностей ДПС України у видатках Державного бюджету України, оцінювання ризиків;

планування ресурсного забезпечення ДПС України (формування пропозицій до державного оборонного замовлення, планування закупівель продукції, робіт і послуг, зокрема на особливий період);

планування заходів з мобілізаційної підготовки у ДПС України;

організація виконання завдань та заходів програм і планів, оцінювання стану досягнення спроможностей.

*Принципами такого планування на основі спроможностей в літературі є [9]:*

реалістичність, яка полягає в збалансованості вартості заходів із досягнення спроможностей та виділеними коштами;

результативність, яка полягає у досягненні визначених цілей завдяки виконанню завдань і заходів у плановий період у межах виділених коштів;

ефективність, яка полягає в оптимальному співвідношенні витрачених ресурсів і досягнутого результату;

централізація управління плануванням для забезпечення збалансованого розвитку складових сил оборони;

безперервність управління плануванням та моніторингу спроможностей;

системність і паралельність процесів планування та моніторингу для забезпечення оперативності процесу управління розвитком спроможностей;

об'єктивність і колегіальність під час підготовки пропозицій для прийняття рішень у процесі планування;

цілісність, яка забезпечується взаємоузгодженням документів планування розвитку складових сил оборони на довго-, середньо- та короткостроковий період з урахуванням їх функціонального призначення;

єдине наскрізне планування створення нових і модернізація існуючих видів озброєння, військової та спеціальної техніки, виробничих потужностей для їх розроблення, виготовлення, а також освоєння і впровадження нових технологій військового призначення;

узгодженість планування в ДПС України із стратегічним плануванням застосування сил оборони, заходами мобілізаційної підготовки національної економіки, системи життєзабезпечення населення і території держави до оборони;

відкритість інформації про цілі, пріоритети, орієнтири планування та прозорість використання ресурсів.

*Вихідними даними для планування є:*

визначені законами України засади внутрішньої і зовнішньої політики, зокрема у сфері оборони держави;

визначені прогнозовані загрози національній безпеці та національним

інтересам України, стратегічні цілі та основні завдання політики національної безпеки у сфері оборони держави та забезпечення безпеки державного кордону, а також уточнені, за необхідності, завдання сил складових сектору безпеки і оборони;

висновки за результатами аналізу досягнень військової науки та новітніх технологій військового призначення, досвіду застосування ДПС України та інших складових сектору безпеки і оборони у воєнних діях та міжнародних операціях з підтримання миру та безпеки;

орієнтовні прогнози показники можливостей держави у задоволенні потреб оборони людськими, фінансовими та матеріально-технічними ресурсами (показники виробництва військової техніки та озброєння підприємствами оборонно-

промислового комплексу в мирний час, після введення в дію мобілізаційного плану національної економіки України на особливий період, закупівлі за кордоном, виробництва в кооперації, лізингу та інших форм військово-технічного співробітництва);

затверджена за результатами огляду стану загальна структура, склад та організація ДПС України (для довгострокового планування – модель (обрис) майбутніх сил ДПС України).

Їх оборонний огляд передбачає проведення таких основних процедур (рис. 1) [8]: оцінювання середовища безпеки; планування сил; планування ресурсів; оцінювання ризиків; формування перспективної моделі (структури) ДПС України; підготовка програмних документів їх розвитку.



Рис. 1. Процедури оборонного огляду ДПС України

За їх результатами опрацьовується перспективний склад та організаційна структура сил, які відповідають завданням ДПС України та збалансованим ресурсам, розділеними між складовими сектору безпеки і оборони, а також програмні документи довго- та середньострокового планування.

Оцінювання наявних спроможностей (оперативних, бойових, спеціальних) здійснюється департаментами Адміністрації ДПС України на стратегічному,

оперативному, тактичному рівні, командирами, начальниками, керівниками структурних підрозділів та організацій під час огляду, огляду спроможностей (1 раз на 2-3 роки за рішенням Голови ДПС України), а також за необхідністю. Воно здійснюється за усіма базовими компонентами (складовими) спроможностей та передбачає оцінювання:

чинних доктринальних документів, які застосовуються (для підготовки, застосування,

організації повсякденної діяльності підрозділу (структурного елементу);

організаційної структури і складу наявних підрозділів ДПС України щодо їх здатності виконувати завдання за кожною ситуацією з необхідним рівнем ефективності;

рівня підготовки персоналу до виконання завдань за призначенням;

забезпеченості необхідними зразками озброєння та військової техніки для виконання завдань за ситуаціями, з урахуванням їх технічного стану та термінів експлуатації;

стану та здатності систем матеріального та технічного забезпечення (логістики), медичного забезпечення до виконання завдань за ситуаціями, зокрема наявність запасів;

якості військової освіти та науки, її здатності забезпечити належний рівень професійної підготовки персоналу і обґрунтування розвитку та застосування ДПС України;

наявності кваліфікованого та мотивованого військового (цивільного) персоналу;

наявної прикордонної інфраструктури і її здатності забезпечувати життєдіяльність прикордонних підрозділів та виконання ними завдань за призначенням;

рівня сумісності з підрозділами сил НАТО.

Розвиток спроможностей здійснюється завдяки розвитку (вдосконаленню) базових компонентів (складових) спроможностей.

Розвиток ОВТ не єдиний шлях розвитку спроможностей. Необхідного ефекту в деяких випадках можливо досягти поліпшенням інших базових компонентів (складових) спроможностей, які не потребують значних ресурсів, зокрема удосконаленням (змінною) доктрин, засад застосування, організаційних структур, поліпшення системи відбору, навчання, підготовки та мотивації персоналу.

Основні етапи розвитку спроможностей включають:

визначення (опис) спроможності (capability definition);

визначення стандартів, необхідних для розвитку спроможності та формування переліку військових вимог (сил і засобів) (definition of standards and military requirements);

закупівлю (постачання) необхідних ОВТ та МТЗ (procurement); розроблення настанов та підготовку персоналу (implementation through instruction and training);

бойове злагодження (навчання) перед застосуванням (deployment preparations);

розгортання та застосування спроможності (deployment / engagement of the capabilities);

оцінювання та висновки (аналіз та опрацювання пропозицій щодо коригування цільових пакетів (документів з розвитку) спроможностей (lessons learned) [9].

Спроможності ДПС України можна розвивати через:

аналіз та оцінювання розвитку воєнно-політичної обстановки для визначення переліку реальних і потенційних воєнних загроз, уточнення варіантів імовірних сценаріїв і ситуацій для планування застосування сил з урахуванням ескалації цих загроз;

визначення завдань за ситуаціями, зокрема кінцевої мети ведення прикордонних операцій;

опис умов виконання визначених завдань;

визначення алгоритмів дій сил і засобів у певних умовах (ситуаціях);

визначення вимог до спроможностей сил і засобів, запланованих для виконання визначених завдань.

*Аналіз та оцінювання розвитку воєнно-політичної обстановки для визначення переліку реальних і потенційних загроз воєнного характеру на державному кордоні передбачає:*

аналіз міждержавних відносин, їх змісту і спрямованості, намірів держав або інших суб'єктів щодо вирішення політичних питань, поглядів їх воєнно-політичного керівництва на роль воєнно-силових методів у вирішенні цих питань;

оцінювання впливу глобальних економічних, політичних, демографічних та інших проблем на безпеку України у сфері забезпечення безпеки державного кордону;

розгляд військових планів та приготувань окремих держав, політичних суб'єктів, оцінювання рівня небезпеки, що походить від окремих воєнно-політичних конфліктів чи конфліктних територій;

з'ясування рівня розвитку способів і засобів збройної боротьби та зусиль окремих держав для їх удосконалення;

дослідження процесу утворення і динаміки розвитку воєнно-політичних союзів (блоків) та аналіз їх цілей;

моніторинг виникнення нових зовнішніх і внутрішніх політичних та (або) економічних умов, які загрожують національним інтересам

України, аналіз тенденцій їх розвитку на державному кордоні;

оцінювання розвитку інформаційного простору та його впливу на прикордонну безпеку;

оцінювання інших суб'єктів, які впливають на стан і систему забезпечення прикордонної безпеки в довготривалій перспективі.

Оцінювання воєнно-політичної обстановки та перспектив її розвитку завершується складанням Переліку викликів і загроз прикордонній безпеці, сценаріїв застосування сил ДПС України, можливих завдань і способів їх виникнення на основі прогнозних характеристик імовірності виникнення можливих кризових ситуацій воєнного характеру та їх негативного впливу на національні інтереси України.

Результатом виконання цього кроку є визначення переліку викликів та загроз у воєнній сфері та сценаріїв їх розвитку на державному кордоні на довгостроковий період.

*Розроблення сценаріїв застосування сил ДПС України* передбачає уточнення завдань, застосування опису географічних районів, визначення ймовірного просторового розмаху воєнних (бойових) дій, визначення протидіючих сил, їх спроможності, військових цілей та відповідних завдань.

Для формування ймовірних сценаріїв і ситуацій можливого застосування сил ДПС України враховують вимоги доктрин, інших стратегічних і концептуальних документів, актів Президента України тощо.

Сценарій має містити низку обов'язкових елементів: об'єкт впливу загрози воєнного характеру та можливі цілі сторін, опис умов виникнення загрози, можливих суб'єктів, які братимуть участь у її реалізації, масштаби реалізації, сили і засоби, які можуть бути задіяні в цьому сценарії, інші особливості його реалізації.

Сценарії конкретизують у ситуаціях, які описують особливості застосування сил ДПС України та засобів, тривалість і наслідки застосування сили, обсяг сил прикордонного відомства, які будуть задіяні в разі виникнення певної ситуації.

Для забезпечення уніфікованого підходу до процесу уточнення сценаріїв, використовують шаблони, структура яких містить такі елементи: загальний опис сценарію; припущення щодо застосування військової сили; політичні та воєнні цілі, яких потрібно досягти; фізико-географічні,

військові та цивільні умови; припущення щодо підтримання сил; загальний задум операції сил.

Пріоритети кожного сценарію визначають експертно-аналітичним шляхом відповідно до ймовірності виникнення та масштабів наслідків для України.

Результатом виконання цих заходів можуть бути висновки з оцінювання воєнно-політичної обстановки, характеристика викликів і загроз, пропозиції до переліку сценаріїв застосування сил ДПС України, перелік можливих ситуацій для планування сил.

*Визначення завдань*, які мають бути виконані для нейтралізації конфліктної (кризової) ситуації певного сценарію. Завдання можуть бути сформульовані лише після опису та аналізу ситуації (або її варіанта) певного сценарію, який потребує застосування (залучення) відповідних складових сил і засобів ДПС України.

Завдання вважають прийнятним, якщо для його виконання залучають мінімальну кількість сил і засобів, очікувані витрати при цьому мінімальні, а виконання можливе в межах відповідних нормативів (часу, фізичних характеристик досягнення тощо).

Завдання для спільного виконання ДПС України, ЗС України та іншими складовими сил сектору безпеки і оборони за визначеними сценаріями (ситуаціями) вирішують на основі вказаних у чинних доктринах і нормативно-правових актах, бойових статутах, настановах тощо завдань з питань підготовки та застосування підрозділів ДПС України, ЗС України та інших складових сектору безпеки і оборони (стандартних завдань), або визначених для прогнозованих за ситуаціями викликів, ризиків і загроз.

В описі цих завдань мають бути вказані заходи, які виконуватиме ДПС України, ЗС України та інші складові сили безпеки і оборони для нейтралізації (запобігання, ліквідації наслідків тощо) конфліктної (кризової) ситуації певного сценарію.

Залежно від рівня завдань визначають їх виконавців:

національні стратегічні – на рівні держави обов'язкові для всіх сил сектору безпеки і оборони;

стратегічні (як частина національних або самостійних) – Адміністрація ДПС України, регіональні управління ДПС України;

оперативні (як частина стратегічних) – окремі оперативні підрозділи ДПС України за їх призначенням;

тактичні (окремі завдання) – частини та підрозділи ДПС України.

Виконання завдань має охоплювати не тільки безпосередні дії під час певних конфліктних (кризових) ситуацій, а й завчасну спільну підготовку сил і їх ресурсне забезпечення.

Для цього формують матрицю завдань, у якій раціонально розподіляють їх між ДПС України та складовими сектору безпеки і оборони. Матриця має містити вихідні дані для планування кожної складової, щоб мати можливість залучати оптимальну кількість сил, забезпечувати їх ефективне застосування та економію ресурсів.

*Опис умов виконання визначених завдань і факторів, які впливатимуть на їх виконання і сукупно становитимуть вимоги до оперативно-службових спроможностей.*

Для опису оперативно-службових спроможностей ураховують умови (географічні, кліматичні, суспільно-політичні, військові, техногенні, криміногенні тощо), у яких триватиме виконання завдань за визначеними сценаріями (ситуаціями). До того ж використовують стандартні каталоги умов, які містять інформацію за трьома напрямками: фізичне середовище; умови застосування сил; цивільне середовище або суспільство.

Крім того використовується Орієнтовний перелік типових організаційних структур, а також орієнтовний каталог спроможностей типових організаційних структур сил і засобів ДПС України, які містять опис характеристик (вимог) основних спроможностей завчасно визначеного переліку базових (типових) структур.

Зазначений каталог розробляють і уточнюють з урахуванням надходження на озброєння нових зразків ОВТ, інженерно-технічного забезпечення, проведення організаційних заходів, розвитку форм і способів застосування сил.

Перелік умов і критеріїв виконання завдань за всіма визначеними сценаріями – це вимоги до оперативно-службових спроможностей, у яких визначено кількісні показники для реальних умов, що можуть виникнути під час виконання завдань. Вимоги ґрунтуються на стандартних характеристиках, визначених керівними документами, але кількісні їх показники можуть відрізнятися від стандартних і відповідати реальним умовам.

Перелік умов і критеріїв виконання завдань формують за окремими напрямками (категоріями): готовність сил; оперативні заходи; наявність резервів; застосування сил; управління та зв'язок; логістика (тилове, технічне та медичне забезпечення); живучість і захист сил тощо.

*Визначення стандартів виконання завдань* передбачає добір згідно зі стандартом відповідного зразка озброєння та військової техніки, інженерно-технічного забезпечення, рівня управління прикордонного підрозділу або за категоріями (складовими) оперативно-службових спроможностей (готовність до виконання, оперативні заходи, наявність резервів, застосування, управління силами та зв'язок, логістика, живучість і захист сил.

Типову структуру сил ДПС України використовують для опису спроможностей як розрахункову (еталонну) одиницю.

Згідно з чинними в Україні концептуальними документами [2, 3] стратегічне планування в секторі безпеки і оборони проводять за адаптованими в Україні стандартами держав – членів НАТО.

Визначення вимог до спроможностей сил і засобів, необхідних для кожного сценарію та можливих ситуацій, для з'ясування сумарних спроможностей сил і засобів, які необхідно мати для ефективного реагування на визначені загрози. Приклад визначення сценарію розвитку обстановки на ділянці відповідальності прикордонного загону та загону морської охорони у разі ускладнення обстановки наведений у табл. 1.

У науковій публікації [10] авторами наведено підхід, за яким можна визначити вимоги до спроможностей сил за певною послідовністю дій, а також поєднати інформацію про наявні спроможності, поставлені завдання, умови їх виконання та прогнозовані сценарії застосування сил. Відповідно, пропонується аналогічна послідовність дій для визначення вимог до спроможностей, а також конкретний варіант виконання визначених завдань за одним зі сценаріїв, а саме:

розробляється перелік імовірних сценаріїв застосування сил і засобів ДПС України;

готується список завдань для виконання визначеними силами у зазначеній конфліктній (кризовій) ситуації;

окреслюються умови виконання визначених завдань (фізичні, військові, цивільні фактори впливу) та складають список



умов, що впливають на виконання визначених завдань;

розробляються стандарти як мінімально необхідні вимоги до виконання певного завдання у визначених умовах;

формується каталог типових структур сил і засобів ДПС України з описом

характеристик (вимог) основних оперативно-службових спроможностей із завчасно визначеного переліку базових частин і підрозділів, органів управління, окремих засобів, а також систем і програмного забезпечення.

Таблиця 1

**Сценарій розвитку обстановки на ділянці відповідальності прикордонного загону та загону морської охорони у разі ускладнення обстановки**

Загрози	Сценарій дій порушника	Кризові ситуації	Ступінь залучення сил і засобів противника	Формулювання завдання прикордонному загону	Наявні спроможності прикордонного загону	Сили і засоби ЗС України (взаємодіючі підрозділи)	Необхідні спроможності прикордонного загону
Збройна агресія РФ проти України з проведенням морських та сухопутних операцій з рішучими воєнно-політичними цілями	Висадка морського десанту на узбережжі України	Збройне вторгнення за допомогою морської техніки на територію України	ПСКА на повітряній подушці, малі катера під вогневим прикриттям ПСКР	Відбиття збройного нападу та недопущення підходу морських сил та засобів до узбережжя України	Сили та засоби ЗМО (КрМО, КаМО, МКаМО)	Висвітлення надводної обстановки ПТС прикриття узбережжя ЗС України (берегова артилерія)	Сили та засоби ЗМО (КрМО, КаМО, МКаМО), протидиверсійні групи
	Обстріл території України з території РФ	Обстріл пунктів управління, нарядів та підрозділів ДПС України на узбережжі та іншої інфраструктури	Використання систем залпового вогню, ракетних комплексів. Використання озброєння з малих катерів по береговій смузі. Обстріл з використанням авіації та БПЛА	Відбиття збройного нападу та недопущення ведення вогню по території України. Викриття місць знаходження агресора, передавання даних на ЦУС для залучення сил і засобів старшого начальника для знищення противника	Сили і засоби прикордонного загону, ЗМО (КрМО, КаМО, МКаМО) висвітлення надводної обстановки ПТС	Прикриття узбережжя ЗС України (берегова артилерія). Військова авіація. Сили та засоби ВМС, ППО	Сили та засоби прикордонного загону, ЗМО (КрМО, КаМО, МКаМО) висвітлення надводної обстановки ПТС

За результатами формується Каталог спроможностей типових структур ДПС України, а також визначаються вимоги до необхідних спроможностей сил і засобів, які залучатимуться до нейтралізації (запобігання, ліквідації наслідків) конфліктної (кризової) ситуації на державному кордоні певного сценарію та описують вимоги до спроможностей сил і засобів ДПС України для виконання визначених завдань за цим сценарієм.

Складовими спроможностей вважають: організацію, систему управління; кадрову систему та персонал; військову освіту і науку, спільну підготовку військ (сил); основні системи забезпечення ОВТ; матеріальне, інженерно-технічне та медичне забезпечення; прикордонну інфраструктуру.

Процедуру планування сил безпеки і оборони та спільної їх підготовки та застосування у конфліктних (кризових) ситуаціях воєнного характеру реалізують на основі визначених ситуацій, завдань і вимог

до оперативних (бойових) та службових спроможностей. Процедура передбачає оцінювання наявних спроможностей складових сил безпеки і оборони, визначення їх відповідності вимогам до виконання завдань за окресленими сценаріями та відмінностей між необхідними і наявними спроможностями.

Визначені відмінності вважають основою для планування сил і засобів, з'ясування необхідності утримувати наявні або формувати нові спроможності, чи нарощувати їх, або позбавлятися від зайвих.

**Висновки.** Планування оперативно-службової діяльності ДПС України на сьогодні потребує вдосконалення завдяки активнішому впровадженню запропонованого МО України оборонного планування на основі спроможностей.

Упровадження у ДПС України планування на основі спроможностей дасть змогу якісніше здійснювати планування розвитку сил і засобів ДПС України;

гармонізувати оборонне та бюджетне планування; відійти від ручного, ситуативного планування; у якості кінцевого результату – зміцнити обороноздатність держави.

Запровадження у діяльність ДПС України планування на основі спроможностей дасть змогу поліпшити якість планування; підвищити здатність ДПС України до виконання завдань за призначенням; поширити отриманий досвід на інші складові сил оборони; забезпечити активне співробітництво України з НАТО з метою досягнення критеріїв, необхідних для набуття повноправного членства в Альянсі.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Оборонне планування на основі спроможностей: особливості та перспективи впровадження / І. С. Руснак та ін. *Наука і оборона*. 2017. № 2. С. 3–10.
2. Горбулін В. П. Розвиток оборонного планування як складової національної системи планування у сфері безпеки і оборони за умов наближення до процедур та стандартів НАТО : аналітична записка. Київ : НІСД, 2017. 17 с.
3. Буняк О. В., Бондарь Р. Г., Романюк І. М. Проблеми розвитку спроможностей сил оборони. *Проблеми формування ефективної політики, системи планування і управління ресурсами в секторі оборони з використанням сучасних євроатлантичних підходів* : матеріали міжнар. наук.-практ. конф., м. Київ, 24 берез. 2017 р. Київ, 2017. С. 16–19.
4. Романченко І. С., Крикун П. М., Богданович Ю. В., Денсжкін М. М. Стан і перспективи розвитку системи оборонного планування в Збройних Силах України. *Наука і оборона*. 2017. № 1. С. 25–30.
5. Хоффман Ф. Г. Большая стратегия: основное соображения. *Орбис*. 2014. № 58 (4). С. 472–485. DOI: <https://doi.org/10.1016/j.orbis.2014.08.002> (дата звернення: 15.02.2021).
6. Development and Implementation of the Target Function in the Decision-Making Process in the System of Providing the Military Security of the State / V. O. Kosevtsov et al. *Eastern-European Journal of Enterprise Technologies*. 2020. Vol. 5, No 3. P. 17–23. <https://doi.org/10.15587/1729-4061.2020.215128>.
7. National Resiliences A Determinant of National Security of Ukraine / S. Bondarenko et al. *Journal of Optimization in Industrial Engineering*. 2021. Vol. 14, No 1. P. 111–117. DOI: <https://doi.org/10.22094/JOIE.2020.677837>.
8. Оборонна реформа: системний підхід до оборонного менеджменту : монографія / А. Павліковський, В. Фролов, Ф. Саганюк та ін. ; за заг. ред. д-ра військ. наук А. Сиротенка. Київ : НУОУ, 2020. 274 с.
9. Оборонний огляд: український вимір 2014–2018 : монографія / Ф. Саганюк, А. Павліковський, П. Щипанський, В. Павленко та ін. ; за заг. ред. д-ра військ. наук, проф. І. Руснака. Київ : МО та ГШ ЗС України, НУОУ, 2019. 196 с.
10. Троцько В. В., Цурко Ю. В. Підхід до визначення вимог до необхідних можливостей для проведення оборонного огляду. Сектор безпеки і оборони України: теорія і практика : монографія. Київ : Академпрес, 2017. С. 68, 165–169.

Стаття надійшла до редакційної колегії 24.03.2021

### Improving defense planning in the State Border Guard Service of Ukraine

#### Annotation

The article provides recommendations for improving the planning in the State Border Guard Service of Ukraine, which is based on the methodology of defense planning. Capability-based planning will allow for better planning of operational activities of the border agency and will ensure active cooperation between Ukraine and NATO in order to achieve the criteria necessary for full membership in the Alliance. The main tasks of planning in the State Border Guard Service of Ukraine on the basis of capabilities are formed, the principles and initial data are determined. Procedures for reviewing the state of the border agency are considered, namely environmental assessment, force planning, resource planning, risk assessment, formation of a promising model and structure of the State Border Guard Service of Ukraine that meets the accepted risks, preparation of development program documents. The process of developing the capacity of the department to perform certain tasks is defined and the main procedures are indicated. Requirements are identified for the capabilities of the forces and means required for each scenario and possible situations, to determine the total capabilities of the forces and means that must be available to respond effectively to identify threats. The procedure of planning security and defense forces and their joint training and application in conflict (crisis) situations of a military nature is implemented on the basis of certain situations, tasks and requirements for operational (combat) and service capabilities. The procedure involves assessing the available capabilities of the components of the security and defense forces, determining their compliance with the requirements for the tasks in the outlined scenarios and the differences between the required and available capabilities. The advantages of the implementation of capacity-based planning in the operational and service activities of the State Border Guard Service of Ukraine are determined.

**Keywords:** planning; capabilities; operational and service activities; forces and means; State Border Guard Service of Ukraine.

Яким'як С. В., канд. військ. наук, доцент  
Вдовицький Є. А.

(0000-0002-1530-271X)  
(0000-0003-0930-525X)

Кафедра Військово-Морських Сил командно-штабного інституту застосування військ (сил) Національного університету оборони України імені Івана Черняхівського, Київ

## **Аналіз чинників, які впливають на виконання завдань Військово-Морськими Силами під час захисту економічної діяльності держави на морі в умовах гібридних дій противника**

**Резюме.** У статті проведено аналіз зовнішніх і внутрішніх чинників, які впливають на ефективність застосування Військово-Морських Сил Збройних Сил України під час виконання завдань захисту економічної діяльності держави на морі в умовах гібридних дій Російської Федерації.

**Ключові слова:** військово-морські сили; захист економічної діяльності на морі; зовнішні та внутрішні чинники; гібридні дії.

**Постановка проблеми.** Унаслідок захоплення Криму та встановлення контролю Російською Федерацією (РФ) над значною частиною територіального моря, виключної (морської) економічної зони (далі – В(М)ЕЗ) України, об'єктів виробничої діяльності на морі, морської інфраструктури та інших складових морського потенціалу України, наша держава понесла величезні економічні збитки.

Так, агресором (РФ) захоплено та контролюється понад 50 % територіального моря та внутрішніх вод України у межах Чорного й Азовського морів; порушуються суверенні права України на економічну діяльність у межах В(М)ЕЗ України, понад 90 % якої захоплено та контролюється підрозділами військових формувань РФ; здійснюється незаконне управління судноплавством в акваторії захопленої ним Керченської протоки та отримується відповідна економічна вигода; захоплені та експлуатуються морські нафтогазодобувні платформи на українській частині шельфу; РФ захоплено та незаконно експлуатуються морські порти, промисловий флот, судноремонтні та суднобудівні заводи України, які були розміщені у Криму, зокрема значні збитки економіці України наносяться через захоплення причального фронту портів, які забезпечували експортно-імпорتنі операції України [1, 2].

Ці втрати Україна несе і дотепер, тому керівництвом держави вживаються відповідні заходи із забезпечення захисту національних інтересів на морі.

Зокрема, у вересні 2020 р. Президентом України було затверджено Стратегію національної безпеки України, згідно з якою

реалізація потенціалу України як морської держави є одним з основних напрямів зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки [3].

До цього, постановою Кабінету Міністрів України від 18.12.2018 № 1108 була оновлена та видана в новій редакції Морська доктрина України на період до 2035 року, яка визначає стратегію та основні напрями подальшого розвитку України як морської держави, зокрема і її економічної складової [2].

Проте реалізації стратегії, що визначена Морською доктриною, щодо ведення Україною економічної діяльності на морі, перешкоджають гібридні дії РФ. Це обумовлює необхідність залучення до її захисту сил (військ) Військово-Морських Сил Збройних Сил України (далі – ВМС ЗС України), на ефективність застосування яких впливає низка чинників, недостатньо вивчених на сьогодні.

**Аналіз останніх досліджень і публікацій.** У наукових дослідженнях останніх років питання ведення гібридних дій РФ у Чорному та Азовському морях, їх вплив на ведення економічної діяльності нашою державою та застосування ВМС ЗС України для виконання завдань щодо протидії противнику вивчали І. Веремій, М. Паламарчук, А. Тарасов, І. Кабаненко, А. Риженко, Б. Бабін, С. Соколюк, А. Клименко [4–11], а також розглядалися в [12, 13], проте аналіз впливу чинників на ефективність застосування сил (військ) не проводився.

Окремі питання аналізу чинників, які впливають на ефективність застосування ВМС під час виконання завдань захисту

економічної діяльності держави на морі досліджували С. Г. Санніков, Й. К. Раджапакса в [14], однак у зазначеній праці розглядалися умови регіону, відмінного від Чорноморського, без урахування гібридних дій противника.

Отже, аналіз праць зазначених науковців та інших наукових джерел свідчить, що питання впливу чинників на ефективність застосування ВМС під час виконання завдань захисту економічної діяльності держави на морі в умовах гібридних дій противника комплексно не розглядалися і не були предметом окремого дослідження.

**Метою статті** є визначення чинників та аналіз характеру їх впливу на застосування ВМС під час виконання завдань захисту економічної діяльності держави на морі, зокрема в умовах гібридних дій противника.

**Виклад основного матеріалу.** В умовах зростання негативного впливу РФ на економічну діяльність України на морі постає необхідність проведення дослідження щодо розвитку способів застосування сил (військ) ВМС під час виконання завдань захисту економічної діяльності держави на морі в умовах гібридних дій противника.

Аналіз досвіду дій флотів та поглядів іноземних і вітчизняних фахівців на застосування сил (військ) ВМС щодо захисту економічної діяльності на морі дав змогу визначити такі основні чинники, які впливають на виконання силами (військами) завдань:

зовнішні – вимоги міжнародних і національних нормативно-правових актів, які регламентують питання захисту економічної діяльності на морі; види та характер економічної діяльності держави на морі, яка потребує захисту; існуючий і прогнозований характер дій РФ, що негативно впливає на економічну діяльність на морі; умови району застосування сил (військ) ВМС;

внутрішні – наявний склад, стан, оперативні (бойові) спроможності сил (військ) ВМС, які можуть залучатися до виконання завдань захисту економічної діяльності на морі; рівень підготовки особового складу органів військового управління, військових частин до виконання завдань захисту економічної діяльності на морі, а також існуючі способи виконання зазначених завдань.

Розглянемо вплив зазначених чинників на ефективність застосування ВМС під час виконання вказаних завдань.

Відповідно до Конвенції ООН з морського права 1982 р., прибережні держави мають суверенні права у виключній

економічній зоні щодо розвідування, розроблення і збереження природних ресурсів як живих, так і неживих, у водах, що покривають морське дно, на морському дні та в його надрах, а також для управління цими ресурсами, та щодо інших видів діяльності з економічної розвідки та розроблення зазначеної зони [15].

Правовий режим такої економічної зони України в Чорному морі визначається Законом України “Про виключну (морську) економічну зону”. До того ж, в Азовському морі подібна зона юрисдикції України обмежена, а економічна діяльність держави регламентується Договором між Україною і РФ про співробітництво у використанні Азовського моря і Керченської протоки від 24.12.2003 (далі – Договір про співробітництво) [16].

Анексія Кримського півострова призвела до подвійного тлумачення статусу внутрішніх морських вод, територіального моря та частини В(М)ЕЗ України навколо півострова, оскільки РФ, у порушення міжнародного законодавства, заявила права на них.

Прикриваючись внутрішнім законодавством, суб’єкти економічної діяльності РФ під захистом сил Чорноморського флоту Південного військового округу РФ (далі – ЧФ ПдВО РФ) з 2014 р. ведуть активну діяльність у В(М)ЕЗ України та на її шельфі, а сили ЧФ ПдВО РФ – гібридні дії щодо перешкоджання веденню такої діяльності Україною.

У порушення норм міжнародного права та національного законодавства, 25 листопада 2018 р. відбулося захоплення військових кораблів ВМС ЗС України поблизу Керченської протоки спеціально створеним міжвидовим угрупованням РФ під прикриттям кораблів Берегової охорони Прикордонної служби Федеральної служби безпеки РФ. Указані дії противник обґрунтував “неправомірним заходом у територіальні води РФ”, хоча встановлення РФ в односторонньому порядку суверенітету над зазначеною акваторією прямо суперечить положенню Договору про співробітництво, відповідно до якого врегулювання питань, які стосуються акваторії Керченської протоки, здійснюється за угодою між сторонами [16]. До того ж, відповідно до резолюції 3314 (XXIX) Генеральної Асамблеї ООН від 14 грудня 1974 р., напад збройними силами однієї держави на сухопутні, морські чи повітряні сили, або морські та повітряні флоти іншої держави кваліфікується як акт агресії.

Водночас, від керівництва РФ лунають заяви щодо неприпустимості перегляду існуючої нормативно-правової бази щодо статусу Азовського моря і Керченської протоки, яка зокрема, забороняє захід військових кораблів або інших державних суден, які експлуатуються в некомерційних цілях, в Азовське море і прохід Керченською протокою без надання дозволу обох держав [16]. Зазначене дає підставу РФ для блокування заходу в цій акваторії військових кораблів третіх держав без її дозволу та не дає змоги залучати сили ВМС країн – партнерів до спільного виконання завдань з ВМС ЗС України.

Українська економіка значно залежить від морської діяльності. Як відомо, існують такі її види: торговельне мореплавство, морський транспорт, суднобудування, військово-морська діяльність, використання водних біоресурсів та інших ресурсів моря, туристична та рекреаційна діяльність, а також діяльність у сферах науки, освіти, екології і захисту моря [2]. Ведення противником гібридних дій щодо перешкоджання її провадження нашою державою обумовлює необхідність захисту вказаної діяльності. До видів морської діяльності, що потребують захисту, належать: торговельне мореплавство (зокрема, захист портів); морський транспорт; використання водних біоресурсів та інших ресурсів моря; діяльність щодо вивчення, розвідки, видобування, використання, збереження невідновних і відтворення відновних ресурсів, які не належать до водних біоресурсів.

Так, на сьогодні сили ЧФ ПдВО РФ активно ведуть гібридні дії щодо перешкоджання морегосподарській діяльності нашої держави та забезпечення незаконної економічної діяльності РФ у В(М)ЕЗ України. До основних видів такої діяльності відноситься видобуток мінеральних ресурсів і промисловий вилов риби. До того ж, Росія не лише продовжує видобуток енергетичних ресурсів з родовищ Чорного та Азовського морів, які розроблялись Україною до анексії Кримського півострова, а й розглядає можливість видобутку інших видів ресурсів – прісної води з дна шельфу для забезпечення питною водою населення окупованого Криму, залізо-марганцевих конкрецій для потреб медицини та ін. [17].

Найбільші збитки Україна несе від втрати доступу до нафтогазових родовищ на шельфі. До анексії Криму наша держава видобувала нафту і газ з десяти родовищ, а нині під контролем України лише одне з них –

родовище “Стрілкове” в західній частині Азовського моря.

Загальний об’єм незаконного видобутого РФ газу у 2014 – 2019 рр. становить 9,4 млрд м<sup>3</sup> (у середньому – 1,57 млрд м<sup>3</sup>), об’єм прогнозованого видобутку до 2025 р. – 9,5 млрд м<sup>3</sup> [18].

Як наслідок, збитки України у 2014 – 2019 р. лише через незаконний видобуток РФ газу становлять близько 1,88 млрд дол., а прогнозовані збитки до 2025 р. – 1,9 млрд дол. (при середній ціні газу 200 дол. за 1000 м<sup>3</sup>). До того ж, ціна нового корабля класу “корвет” становить близько 300 млн дол. Отже, співвідношення втрат, які наша держава несе внаслідок незаконного видобутку РФ газу, є неспіврозмірними необхідним витратам на розвиток сил ВМС ЗС України для перешкоджання протиправній економічній діяльності противника на морі.

Дії противника щодо перешкоджання нашій економічній діяльності на морі характеризуються гібридним впливом на цю діяльність.

До гібридних дій сил ЧФ ПдВО РФ щодо перешкоджання економічній діяльності України на морі відносяться:

обмеження судноплавства в Азовському морі шляхом будівництва мосту через Керченську протоку;

затримка та тривала перевірка торговельних суден на підходах до Керченської протоки, які рухаються до/з портів України в Азовському морі;

необґрунтоване і неправомірне закриття для судноплавства районів моря, через які проходять рекомендовані шляхи суден до/з портів України в Чорному морі;

періодичні затримання рибальських суден у Чорному та Азовському морях, арешт їх екіпажів.

Не виключається можливість залучення сил ЧФ ПдВО РФ, які виконують завдання з охорони газових родовищ у районах, наближених до території України, до затримання та доглядів суден за азовським сценарієм [11].

До того ж, аналіз складу та стану корабельного складу ЧФ ПдВО РФ, який може залучатись до виконання завдань щодо перешкоджання веденню нашою державою економічної діяльності на морі [19], свідчить про його суттєву кількісну перевагу над корабельним складом ВМС ЗС України (табл. 1). Як наслідок, ця перевага не дає змогу ефективно виконувати завдання нашими

силами щодо захисту зазначеної діяльності в усій акваторії Чорного та Азовського морів.

Як відомо, ефективність застосування сил (військ) значною мірою залежить від умов навколишнього середовища. Зазначене потребує проведення аналізу району виконання завдань силами (військами) ВМС ЗС України під час виконання завдань захисту економічної діяльності держави на морі.

Просторові розміри Чорного моря характеризуються значними відстанями (найбільша протяжність із заходу на схід – 1150 км, з півночі на південь – 580 км), що обумовлює необхідність виконання силами завдань захисту економічної діяльності

держави у віддаленні від пунктів базування. Просторові розміри Азовського моря значно менші (найбільша протяжність із заходу на схід – 380 км, з півночі на південь – 200 км), що дає змогу надводним кораблям здійснювати розгортання в райони виконання завдань у короткі терміни.

Клімат у цілому сприяє діям військ, однак вплив атлантичних циклонів узимку може ускладнювати плавання кораблів і застосування ними зброї, а низькі температури можуть призвести до потужного льодоутворення, що зі свого боку ускладнює або зовсім виключає плавання кораблів і застосування ними зброї.

Таблиця 1

**Співвідношення кількості бойових кораблів та катерів ВМС ЗС України та ЧФ ПДВО РФ, які можуть залучатися до виконання завдань захисту / перешкоджання веденню економічної діяльності України на морі**

Сили та засоби сторін	ВМС ЗС України	Співвідношення	ЧФ ПДВО РФ
крейсери	–		1
сторожові кораблі / фрегати	1	1 : 5	5
малі ракетні кораблі	–		7
протичовнові кораблі	–		6
десантні кораблі	1	1 : 7	7
патрульні кораблі	–		2
мінно-тральні кораблі	1	1 : 7	7
розвідувальні кораблі	1	1 : 4	4
підводні човни	–		7
ракетні катери	1	1 : 5	5
артилерійські катери	11		–
патрульні катери	2	1: 4,5	9
десантні катери	1		–
протидиверсійні катери	1		–
<b>Загальне співвідношення сил сторін</b>	<b>20</b>	<b>1 : 3</b>	<b>60</b>

Хвилювання понад 4 бали, яке можна очікувати взимку з імовірністю до 30 %, ускладнює застосування бойових катерів [20].

Система базування ВМС ЗС України на Чорному морі не розвинена та налічує лише два пункти базування (Одеса, Очаків), що не дає змоги здійснювати розосереджене базування сил.

Відсутність пунктів базування ВМС ЗС України в Азовському морі негативно впливає на організацію всебічного забезпечення та відновлення боєздатності катерів і суден (базування корабельного складу здійснюється на орендованих причалах у портах Бердянськ і Маріуполь).

Система берегового спостереження ВМС ЗС України забезпечує висвітлення морської обстановки лише в ближній морській зоні.

Загалом, характеристика районів і їх оперативне обладнання частково сприяє виконанню завдань.

Одним з основних внутрішніх чинників, який впливає на ефективність застосування ВМС ЗС України, є наявний склад, стан, оперативні (бойові) спроможності сил (військ), які можуть залучатися до виконання завдань.

Як зазначалося, на сьогодні до складу ВМС ЗС України входить 20 бойових кораблів і катерів [21]. Більшість бойових катерів (за винятком патрульних), має низькі морехідні якості та обмежену автономність [22], яка не дає змоги залучати їх протягом тривалого часу до виконання завдань поза межами територіального моря та в осінньо-зимовий період.

Пріоритети розвитку спроможностей ВМС ЗС України до 2035 року визначено в [23]. Аналіз цього документа свідчить про можливість набуття спроможностей щодо контролю В(М)ЕЗ (Sea Control) не раніше 2030 р., оскільки їх розвиток сплановано здійснити протягом другого етапу (2025 –

2030 рр.) розвитку спроможностей ВМС ЗС України.

І хоча на сьогодні відпрацювання документів середньострокового планування у сферах національної безпеки і оборони за напрямом розвитку ЗС України (Державна програма розвитку ЗС України до 2025 року, Програми розвитку видів (родів) ЗС України тощо) не завершено, напрями розвитку корабельного складу ВМС ЗС України та їх спроможностей можливо визначити за інформацією з офіційних джерел та інформаційних ресурсів, які спеціалізуються на висвітленні питань розвитку озброєння.

Так, відповідно до інформації з відкритих інформаційних ресурсів, у найближчий період бойовий склад флоту планується поповнити завдяки: отриманню як міжнародної технічної допомоги патрульних катерів типу "Island"; придбанню патрульних катерів Mark VI; отриманню катерів вітчизняного будівництва за контрактами, які були укладені в попередніх роках та створенню і будівництву ракетних катерів за спільним українсько-британським проектом. До того ж, переважна більшість з них (патрульні катери Mark VI, десантно-штурмові та броньовані артилерійські катери) за своїми тактико-технічними характеристиками [22, 24] не спроможні до довготривалого виконання завдань поза межами територіального моря та в осінньо-зимовий період. Отже прийняття їх до складу ВМС ЗС України хоча і підвищить бойовий потенціал флоту в цілому, але суттєво не вплине на підвищення спроможностей щодо захисту економічної діяльності на морі.

Водночас, слід відмітити низький рівень укомплектованості органів військового управління ВМС ЗС України, управлінських дивізіонів та екіпажів кораблів, що негативно впливає на якість підготовки та виконання силами завдань у морі.

Крім того, на ефективність застосування (військ) впливає також наявність і якість керівних документів, які визначають їх завдання та способи виконання цих завдань.

Так, відповідно до Тимчасової доктрини застосування ВМС ЗС України, виконувати завдання із захисту економічної діяльності держави на морі передбачається як у воєнний час, так і в умовах гібридних дій противника [25]. Однак обґрунтованого та докладного переліку завдань захисту економічної діяльності та способів виконання таких завдань керівними документами ВМС ЗС України не визначено. Як наслідок, указані

завдання виконуються несистемно та епізодично.

## Висновки

1. В умовах збройної агресії РФ Україна продовжує нести значні економічні збитки. Зазначене обумовлює необхідність вирішення питання обґрунтування переліку завдань щодо захисту економічної діяльності держави на морі та способів їх виконання силами (військами) ВМС ЗС України.

2. Невирішеність питання щодо делімітації державного кордону між Україною та РФ в Азовському морі та Керченській протоці, а також умови Договору про співробітництво, дають змогу противнику сприймати всю їх акваторію як свої внутрішні води та територіальне море, а також блокувати вільний прохід в Азовське море військових кораблів як третіх країн, так і України. Це дає змогу діяти силам ЧФ ПдВО РФ у всій акваторії Азовського моря, обмежує можливості щодо нарощування корабельного складу ВМС ЗС України в Азовському морі та не дає змоги залучати кораблі ВМС країн – партнерів до спільних дій, що негативно впливає на виконання завдань силами (військами) ВМС ЗС України в цій акваторії.

3. Після анексії Криму та втрати контролю над прилеглими до півострова водами і більшою частиною В(М)ЕЗ, характер економічної діяльності України на морі зазнав суттєвих змін, які потребують врахування під час визначення переліку завдань щодо захисту економічної діяльності держави на морі.

4. Основними загрозами веденню Україною економічної діяльності на морі на середньострокову перспективу залишаються дії сил ЧФ ПдВО РФ щодо перешкоджання морегосподарській діяльності нашої держави в контрольованих противником акваторіях.

5. Кількісна та якісна перевага ЧФ ПдВО РФ над ВМС ЗС України обмежує просторові розміри району виконання завдань захисту економічної діяльності держави на морі силами (військами) ВМС ЗС України.

6. Переважна частина корабельного складу ВМС ЗС України не спроможна виконувати завдання щодо захисту економічної діяльності держави на морі протягом тривалого часу поза межами територіального моря та в осінньо-зимовий період. Зазначене потребує врахування під час визначення способів виконання завдань силами (військами) ВМС ЗС України.

7. В існуючих керівних документах з питань застосування ВМС не визначено

перелік завдань щодо захисту економічної діяльності держави на морі та способи їх виконання, що негативно впливає на ефективність виконання цих завдань силами (військами) ВМС ЗС України.

#### Напрями подальших досліджень.

Проведений аналіз чинників, що впливають на ефективність застосування ВМС для виконання завдань захисту економічної діяльності держави на морі в умовах гібридних дій противника, надалі дає змогу обґрунтувати перелік завдань щодо захисту економічної діяльності держави на морі та способи їх виконання силами (військами) ВМС ЗС України.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Яким'як С. В. Розвиток України як морської держави: пріоритети державної морської політики в умовах збройної агресії РФ. *Морська стратегія держави. Розвиток та реалізація морського потенціалу України* : матеріали міжнар. наук. форуму, м. Київ, 24-25 трав. 2016 р. Київ, 2016. С. 12–25.
2. Морська доктрина України на період до 2035 року : затв. Постановою Кабінету Міністрів України від 07.10.2009 р. № 1307 (у редакції Постанови Кабінету Міністрів України від 18.12.2018 р. № 1108). URL: <https://zakon.rada.gov.ua/laws/show/1307-2009-%D0%BF#Text> (дата звернення: 01.12.2020).
3. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року “Про Стратегію національної безпеки України” : Указ Президента України від 14.09.2020 р. № 392/2020. URL: <https://www.president.gov.ua/documents/3922020-35037> (дата звернення: 01.12.2020).
4. Російська політика в Чорноморському регіоні: загрози й виклики для України : аналіт. доп. / О. Александров, А. Филипенко, Р. Власенко та ін.] ; за заг. ред. І. Веремія, М. Паламарчука. Київ : НІСД, 2020. 37 с.
5. Кабаненко І. В., Риженко А. О. Військово-Морські Сили України: час діяти. *Чорноморська безпека* : аналітичний часопис. Київ, 2020. № 2 (38). С. 33–38.
6. Бабін Б. В. Силові органи України та окупація Криму. *Чорноморська безпека* : аналітичний часопис. Київ, 2020. № 2 (38). С. 76–82.
7. Тарасов А. А. Основні погляди на концепцію розвитку Військово-Морських Сил Збройних Сил України. Реформа та модель Військово-Морських Сил Збройних Сил України. *Морська стратегія держави. Розвиток та реалізація морського потенціалу України* : матеріали міжнар. опер.-стратег. семінару в межах міжнар. наук. форуму, м. Київ, 28 квіт. 2015 р. Київ, 2015. С. 7–19.
8. Клименко А. В. Російське озеро. Дев'ять аспектів сучасного Чорноморського контексту. *Морська стратегія держави. Розвиток та реалізація морського потенціалу України* : матеріали міжнар. наук. форуму, м. Київ, 22-23 трав. 2019 р. Київ, 2019. С. 12–19.
9. Риженко А. О. Сфера діяльності Військово-Морських Сил Збройних Сил України щодо забезпечення морської безпеки України. *Морська стратегія держави. Розвиток та реалізація морського потенціалу України* : матеріали міжнар. наук. форуму, м. Київ, 22-23 трав. 2019 р. Київ, 2019. С. 19–24.
10. Соколюк С. М. Захист морської діяльності у виключній (морській) економічній зоні України та інших районах відкритого моря. *Морська стратегія держави. Розвиток та реалізація морського потенціалу України* : матеріали міжнар. наук. форуму, м. Київ, 24-25 трав. 2016 р. Київ, 2016. С. 59–63.
11. Клименко А. В. Сценарії дій на морі на 2020 рік. *Протидія гібридній війні на морі: уроки та висновки* : матеріали круглого столу, м. Київ, 25 лют. 2020 р. Київ, 2020. С. 32–42.
12. Яким'як С. В. Проблемні питання протидії гібридному впливу противника на морі та шляхи їх вирішення. *Наука і оборона*. 2020. № 2. С. 31–36.
13. Воєнні аспекти протидії “гібридній агресії”: досвід України : монографія / колектив авторів ; за заг.ред. А. М. Сиротенка. Київ : НУОУ імені Івана Черняхівського, 2020. 176 с.
14. Санніков С. Г., Раджапакса Й. К. Аналіз чинників, які впливають на ефективність застосування Військово-Морських Сил у інтересах забезпечення безпеки економічної діяльності держави. *Труди університету* : зб. наук. праць. Київ, 2013. № 5 (119). С. 53–60.
15. United Nations Convention on the Law of the Sea. URL: [https://www.un.org/depts/los/convention\\_agreements/texts/unclos/unclos\\_e.pdf](https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf) (дата звернення: 01.12.2020).
16. Договір між Україною та Російською Федерацією про співробітництво у використанні Азовського моря і Керченської протоки. URL: [https://zakon.rada.gov.ua/laws/show/643\\_205#Text](https://zakon.rada.gov.ua/laws/show/643_205#Text) (дата звернення: 01.12.2020).
17. Пасынков А. А. Минеральные и топливно-энергетические ресурсы Черного моря (перспективы развития). *Моря России: наука, безопасность, ресурсы* : тезисы докл. научн. конф., г. Севастополь, 3-7 октября 2017 г. Севастополь, 2017. С. 100–102.
18. Чорноморнефтегаз в 2019 г. остановил падение добычи газа. URL: <https://neftegaz.ru/news/dobycha/501855-udalos-chernomorneftegaz-v-2019-g-ostanovil-padenie-dobychi-gaza> (дата звернення: 01.12.2020).
19. Чорноморський флот. URL: [https://www.kchf.ru/ship/today/today\\_all.htm](https://www.kchf.ru/ship/today/today_all.htm) (дата звернення: 01.12.2020).
20. Військово-географічні умови застосування сил (військ) Військово-Морських Сил : навч. посіб. / колектив авторів ; під заг. ред. С. В. Яким'яка. Київ : НУОУ імені Івана Черняхівського, 2019. 172 с.



21. Військово-Морські Сили Збройних Сил України. URL: <https://www.ukrmilitary.com/p/ukrainian-navy.html> (дата звернення: 01.12.2020).
22. Озброєння та військова техніка Військово-Морських Сил Збройних Сил України : навч. вид. / колектив авторів ; за заг. ред. С. В. Яким'яка. Київ : НУОУ імені Івана Черняхівського, 2020. 96 с.
23. Стратегія Військово-Морських Сил Збройних Сил України 2035. Відновити – Захистити – Перемогти. Одеса – Київ, 2018.
24. US Navy fields new Mark VI patrol boats. Navaltoday.com URL: <https://www.navaltoday.com/2019/05/23/us-navy-fields-new-mark-vi-patrol-boats/> (дата звернення: 01.12.2020).
25. Тимчасова доктрина застосування Військово-Морських Сил Збройних Сил України : затв. наказом Командування ВМС ЗС України від 08.04.2019 р. № 80. Одеса, 2019, 207 с.

Стаття надійшла до редакційної колегії 17.12.2020

### **Analysis of factors that may effect on the effectiveness of use the Navy duties during the protection of the economic activities of the state at sea in the context of hybrid enemy actions**

#### **Annotation**

After the capture of Crimea, the Russian Federation exercises control over a large part of the territorial sea, (maritime) economic zone of Ukraine. Many production facilities at sea, maritime infrastructure and other components of Ukraine's maritime potential have been affected. In addition to the above, the Russian Federation not only conducts illegal economic activities but also carries out hybrid operations to prevent Ukraine from implementing maritime economic activities. All this necessitates the involvement of units of the Navy of the Armed Forces of Ukraine in the protection of the national interests of our state.

The issues of conducting hybrid actions by the Russian Federation at sea, their impact on the conduct of economic activities in Ukraine, the use of the Navy of the Armed Forces of Ukraine to perform tasks to counter the enemy are well covered in recent scientific papers. This paper highlights the analysis of the impact of factors on the effectiveness of the use of forces (troops) in carrying out the tasks of protecting the economic activities of the state at sea during hybrid actions of the enemy. The analysis of this area has not been previously conducted comprehensively and has not been the subject of a separate study in previous works.

In research paper external and internal factors that affect the use of the Navy of the Armed Forces of Ukraine in carrying out tasks to protect the economic activities of the state at sea is identified. The general analysis of features and character of their influence on efficiency of use of forces (troops) is carried out also.

A number of restrictions have been identified, due to these factors, on the spatial and temporal indicators of the performance of tasks by the forces of the Navy of the Armed Forces of Ukraine, as well as the methods of their performance.

It is established that currently a clear list of tasks to protect the economic activity of the state at sea and ways to implement them in the current guidelines on the application of the Navy of the Armed Forces of Ukraine are not defined, so their implementation is unsystematic and sporadic.

The necessity of substantiation of the list of tasks and expedient ways of their performance by the forces (troops) of the Navy of the Armed Forces of Ukraine for effective protection of economic activity of Ukraine in the sea is pointed out.

**Keywords:** naval forces; protection of maritime economic activities; external and internal factors; hybrid actions.

УДК 355.02 (477) DOI: <https://doi.org/10.33099/2304-2745/2021-1-71/82-86>

Лобко М. М., канд. військ. наук, доцент<sup>1</sup> (0000-0002-3848-8772)  
Фучко А. Й.<sup>1</sup> (0000-0002-8941-2217)  
Копистира В. М.<sup>2</sup> (0000-0002-3712-6809)

<sup>1</sup> – Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ;

<sup>2</sup> – Національний університет оборони України імені Івана Черняхівського, Київ

## Інституційна модель системи оборони України

**Резюме.** У статті на основі аналізу вітчизняного законодавства розглядаються питання оборони, системи оборони, інституційної моделі системи оборони України з використанням системного підходу, її сутність, побудова. Розкриваються поняття “оборона України”, “система оборони”, “модель системи оборони України”. Сформовано структурно-описовий обрис “інституційної моделі системи оборони України”. Визначаються структура інституційної моделі системи оборони України: відношення, зв’язки та взаємодія між її елементами (компонентами) під час виконання покладених функцій і завдань оборони.

**Ключові слова:** оборона України; система оборони; інституційна модель системи оборони; складові моделі системи оборони.

**Постановка проблеми.** Вивчення досвіду відсічі збройної агресії Російської Федерації (РФ) проти України показало, що існуюча система оборони не повною мірою забезпечила виконання завдань оборони. Унаслідок збройної агресії Росією був анексований і тимчасово окупований Крим та частка території Донецької і Луганської областей. Отже, виникла нагальна потреба у суттєвому оновленні діючої системи оборони та формуванні її перспективної моделі, основаної на принципах і стандартах НАТО.

**Аналіз останніх досліджень і публікацій.** Питання, так чи інакше пов’язані із системою оборони держави та її моделлю, розглядали як вітчизняні, так й іноземні вчені, фахівці, експерти. Однак дослідження авторів здебільшого проводились стосовно певних складових цієї моделі. Так, у [1, 2] розглядалися питання розбудови сучасної європейської моделі сектору безпеки і оборони України як важливого компонента моделі системи оборони, моделі управління постачанням сил сектору безпеки і оборони у єдиній системі матеріально-технічного забезпечення та ін. У [3, 4] досліджувалась модель оборонного планування за аналогією з НАТО та модель бойових дій сил і засобів протиповітряної оборони оперативного угруповання військ. Цілісно модель системи оборони нашої держави в наукових публікаціях не розглядалась.

У статті [5] автор визначає гіпотези щодо моделей оборони для ліпшого розуміння систем оборони, які існують у різних державах, та цілей кожної моделі й фактичних результатів її існування.

Слід зазначити, що в Україні триває оборонна реформа. Одним із наріжних завдань оборонної реформи є формування перспективної моделі Збройних Сил України та інших складових сил оборони. Водночас, проводиться трансформація органів державної влади, інших державних органів, які пов’язані з обороною держави.

**Мета статті** – на основі аналізу вітчизняного законодавства, наукових публікацій розкрити сутність, склад і структуру моделі системи оборони України та надати структурно-описовий обрис інституційної моделі системи оборони України.

**Викладення основного матеріалу.** Оборона України базується на положенні Конституції України: “захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу”.

**Оборона України** становить собою *систему* політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших *заходів* держави щодо *підготовки* до збройного захисту та її *захисту* у разі збройної агресії або збройного конфлікту.

Однак сама “система заходів держави” є суто переліком встановлених заходів, виконання яких забезпечать підготовку та оборону держави. Для реалізації встановленої “системи заходів держави” потрібно визначити відповідні суб’єкти державної

влади, які мають бути наділені відповідними повноваженнями, функціями і завданнями з їх виконання та задіяти необхідні сили і засоби держави. Сукупність визначених суб'єктів, діяльність яких спрямована на досягнення єдиної мети щодо забезпечення оборони та задіяні для цього сили і засоби держави становлять собою “систему оборони України”.

Отже, **система оборони України** - це організована державою сукупність органів державної влади, інших державних органів, органів місцевого самоврядування, усіх складових сектору безпеки і оборони України, єдиної системи цивільного захисту, національної економіки, інших складових, об'єднаних метою і завданнями, що здійснюють законодавчо встановлені повноваження, функції і завдання щодо забезпечення підготовки до оборони, оборони держави, захисту її суверенітету, територіальної цілісності та інших національних інтересів у разі збройної агресії.

Для проведення наукових досліджень, пошуку шляхів подальшого реформування та розвитку системи оборони необхідно сформувати модель системи оборони України.

**Довідка.** Під моделлю слід розуміти (“модель”, фр. *modèle* від лат. *modulus* “міра, аналог, взіреть”) аналог (як правило зменшений або уявний образ) об'єкта – оригінала (процесу, явища, системи), що підлягає науковому дослідженню з певною метою, прообраз, опис або зображення якогось об'єкта.

Модель це проект, інформаційне, натурно-матеріальне чи описово-макетне уявлення об'єкта.

Існують різні види моделей і вони мають відповідати певним вимогам. Формуючи модель системи оборони слід зазначити, що вона має включати певну кількість елементів, які виконують визначені їм функції з оборони держави.

Модель системи оборони є складною і охоплює всі інституції державного устрою встановленого законодавством держави, які мають повноваження, функції і завдання в частині підготовки, здійснення оборони та її забезпечення (сприяння). Вона має об'єднувати воєнні, невоєнні, виробничі, інформаційні, ресурсні та інші можливості всіх її складових.

Сформована модель є відповідним структурно-описовим обрисом, що утворює сукупний образ, загальний вигляд системи оборони. Вона надає уявлення про систему оборони, її призначення, склад, структуру, розкриває характер та ті чи інші властивості. Сформована модель дає змогу досліджувати

систему оборони, проводити певні експерименти, вносити необхідні зміни, уточнення, вдосконалювати та формувати її перспективну модель.

Необхідно зазначити, що модель системи оборони України пройшла певний шлях становлення і розвитку та формувалась протягом тривалого часу незалежності нашої держави. Відтак, сформована модель системи оборони України є “інституційною”.

Інституційність моделі системи оборони полягає в тому, що основні її складові, їх повноваження, функції і завдання у сфері оборони встановлені положеннями вітчизняного законодавства, вона складалась і вдосконалювалась залежно від зміни світових геополітичних процесів, безпекового середовища, розвитку воєнно-політичної, воєнно-стратегічної обстановки довкола України, зростання загроз у воєнній сфері, збільшення обсягу завдань оборони та їх важливості.

Розглядаючи інституційну модель системи оборони України слід зазначити, що вона є складною, ієрархічною, функціональною і, як зазначалось, включає значну кількість елементів, які за функціональною ознакою доцільно умовно розділити за відповідними компонентами (рис. 1).

**Довідка.** Поняття “компонент” слід розуміти як складову цілого, що становить собою сукупність певних елементів об'єднаних за функціональною ознакою.

Першою складовою моделі доцільно визначити ті її елементи, на які покладається виконання функцій управління щодо проведення комплексу заходів з підготовки держави до оборони та керівництво обороною під час відсічі збройної агресії. Такою складовою має бути **керуючий компонент**.

До керуючого компонента слід віднести: Президента України; Верховну Раду України; Раду національної безпеки і оборони України, Воєнний кабінет; вищий колегіальний стратегічний орган воєнного керівництва обороною держави в особливий період (Ставка Верховного Головнокомандувача), Кабінет Міністрів України; міністерства, центральні та інші органи виконавчої влади; місцеві державні адміністрації, ради оборони (Автономної Республіки Крим, областей, міст Києва та Севастополя), військово-цивільні (військові) адміністрації (у разі їх утворення) (ВЦА, ВА); органи військового управління; органи місцевого самоврядування на які

покладено здійснення повноважень у сфері оборони.

Наступною складовою моделі необхідно визначити *виконавчий компонент*. До нього слід включити такі елементи: сектор безпеки і оборони України; національну економіку та інші підприємства, установи промисловості усіх форм власності, що беруть участь у забезпеченні оборони.

До наступної складової моделі необхідно віднести *забезпечуючий компонент* до якого необхідно віднести такі елементи: військового

обов'язку та військової служби (ВО та ВС); мобілізаційної підготовки та мобілізації (МП та мобілізації); територіальної оборони України; єдиної державної системи цивільного захисту (ЄДС ЦЗ); єдиної транспортної системи України в особливий період; паливно-енергетичного комплексу в особливий період (ПЕК); єдиної системи державного матеріального резерву України (ЄСДМР); забезпечення інформаційної безпеки; національна система кібернетичної безпеки; підготовка населення і території держави до оборони.

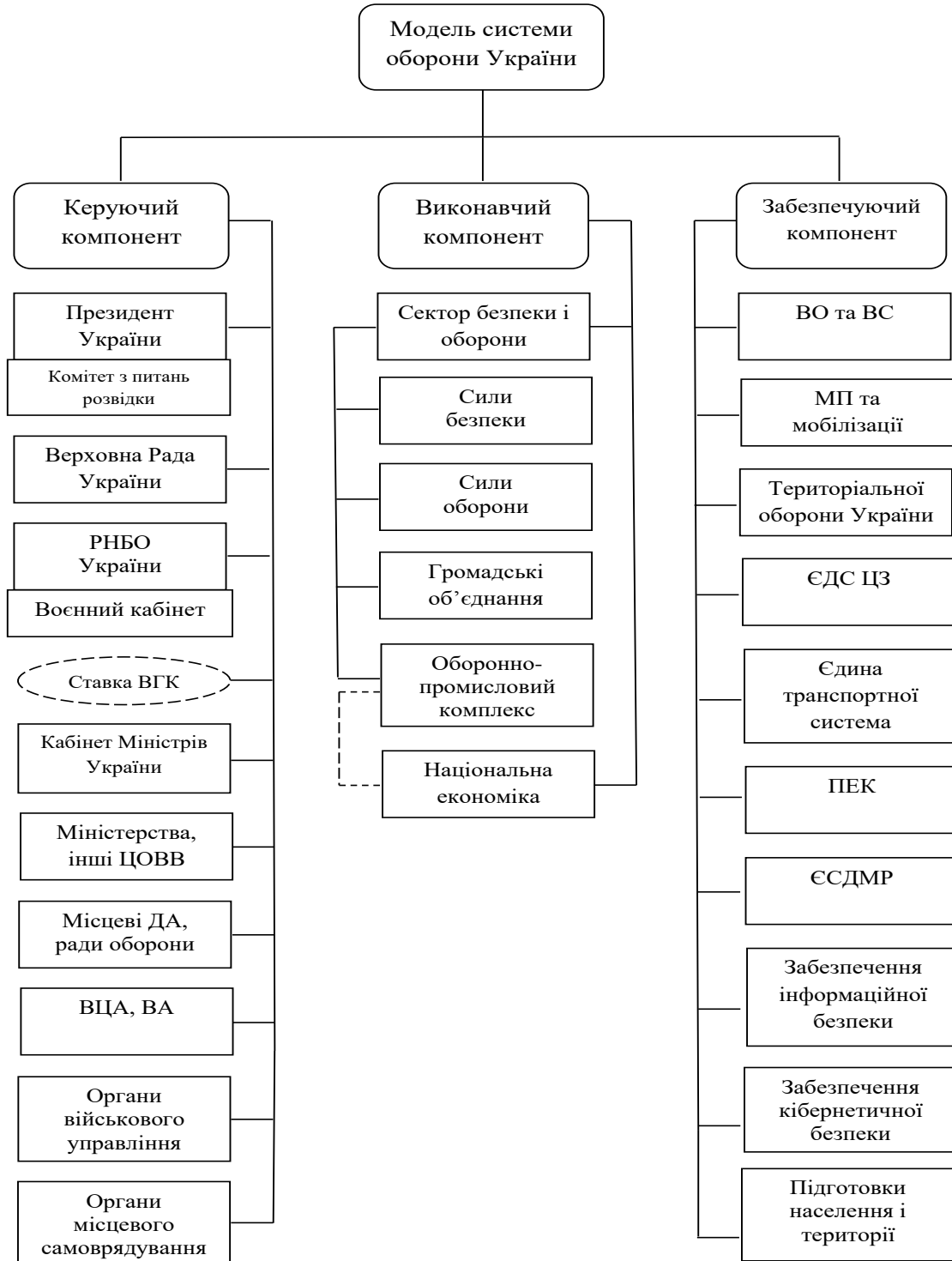


Рис. 1. Структура інституційної моделі системи оборони України

Указані елементи безпосередньо не виконують завдання оборони, однак вони здійснюють різноманітні функції з її підготовки та забезпечення (сприяння).

Зазначені складові системи оборони під час функціонування щодо виконання заходів і завдань оборони знаходяться у відповідних відносинах та взаємодіють між собою.

Наприклад, міністерства та інші органи виконавчої влади взаємодіючи організовують і забезпечують виконання законодавства у сфері оборони, сприяють Збройним Силам України, іншим військовим формуванням, розвідувальним і правоохоронним органам у виконанні ними завдань, належно забезпечують їх за напрямками діяльності, узгоджують з Генеральним штабом Збройних Сил України та забезпечують проведення заходів щодо розвитку системи зв'язку, шляхів, транспорту, інших об'єктів інфраструктури і території держави та підготовку своїх галузей до оборони, забезпечують їх територіальну оборону, планують, організовують і контролюють виконання заходів з мобілізаційної підготовки відповідних органів управління, установ, організацій і підприємств усіх форм власності та взаємодіють під час виконання інших повноважень, які належать до сфери їх управління.

**Висновки.** В Україні триває оборонна реформа одним із важливих завдань якої є реформування та подальший розвиток основних складових системи оборони держави.

Існуюча система оборони має бути спроможною реалізувати визначений комплекс заходів держави щодо підготовки до оборони та її захист у разі збройної агресії. Для цього вона має об'єднувати воєнні, невоєнні, виробничі, інформаційні, ресурсні та інші можливості всіх її складових.

Модель системи оборони держави слід розглядати як відображення сукупності елементів (компонентів) органів державної влади, інших державних органів, органів місцевого самоврядування, об'єднань громадян, національної економіки, сектору

безпеки і оборони, цивільного захисту, інших складових державного устрою, яким законодавчо визначені повноваження, функції і завдання з реалізації системи заходів держави щодо підготовки оборони та її захисту у разі збройної агресії.

Сформовану модель системи оборони України потрібно розглядати як інституційну, що базується на положеннях вітчизняного законодавства і набула свого сучасного обриса протягом тривалого часу незалежності та розвитку нашої держави і її обороноздатності.

Під час функціонування з виконання покладених завдань оборони складові системи оборони вступають у відповідні відносини та взаємодіють між собою.

#### ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Турчинов В. Україна розбудовує сучасну європейську модель сектору безпеки і оборони. URL: [https://galinfo.com.ua/news/ukraina\\_rozbudovuie\\_suchasnu\\_ievropeysku\\_model\\_sektoru\\_bezpeky\\_i\\_oborony\\_307255.html](https://galinfo.com.ua/news/ukraina_rozbudovuie_suchasnu_ievropeysku_model_sektoru_bezpeky_i_oborony_307255.html) (дата звернення: 02.02.2021).
2. Сисоев В. В. Модель управління постачанням сил сектору безпеки і оборони держави в єдиній системі матеріально-технічного забезпечення. *Проблеми економіки = Theproblems of economy*. 2014. № 2. С. 144–153. URL: <http://repository.kpi.kharkov.ua/handle/KhPI-Press/37703> (дата звернення: 02.02.2021).
3. Зміцнення обороноздатності: модель оборонного планування за аналогією з НАТО. *Оборонний вісник*. URL: <http://defpol.org.ua/index.php/aleia-heroi/v705-zmitsnennya-oboronozdatnosti-model-oboronnoho-planuvannia-za-analohiieiu-z-nato> (дата звернення: 06.02.2021).
4. Зварич С. С. Модель бойових дій сил та засобів протиповітряної оборони оперативного угруповання військ. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2012. № 3. С. 97–100. URL: [http://nbuv.gov.ua/UJRN/sitsbo\\_2012322](http://nbuv.gov.ua/UJRN/sitsbo_2012322) (дата звернення: 06.02.2021).
5. Глен Грант. Модель оборони: як зрозуміти стиль оборони країни. *Виклики і ризики. Безпековий огляд ЦДАКРВ*. URL: <https://cacds.org.ua/?p=2239> (дата звернення: 06.02.2021).

Стаття надійшла до редакційної колегії 15.03.2021

### Institutional model of the Defense System of Ukraine

#### Annotation

An analysis of the experience of repelling the armed aggression of the Russian Federation showed that the existing Defense System of Ukraine did not fully ensure the fulfillment of defense tasks that time. As a result during the armed aggression, Russian Federation annexed the Ukrainian Autonomous Republic of Crimea and occupied part of the territory of Donetsk and Luhansk regions. In order to

increase the defense capabilities of our country, it was decided to upgrade Ukraine's Defense System and build a promising model based on modern principles and standards which are currently applied in NATO member countries.

The formed model is a corresponding structural and descriptive outline, which forms an aggregate image, a general view of the defense system. It provides an idea of the defense system, its purpose, composition and structure, reveals the nature and other properties. Created model provides an opportunity to study the Defense System for conducting a certain experiments, making changes and clarifications, with the purpose to making it better and use it for planning next long-term actions.

The institutional model of the Defense System is that its main components, their powers, functions and tasks in the field of defense are established by the provisions of domestic law. The Defense System was built and improved considering on the changes in the next spheres:

- geopolitical;
- security environment;
- development of military-political, military-strategic situation around Ukraine;
- growing threats in the military sphere; increasing the volume of defense tasks and other important processes.

According to the functional feature, the institutional model of the Defense System of Ukraine can be divided into appropriate components: management, executive and support.

**Keywords:** Defense System; defense of Ukraine; institutional model of the Defense System; components of the Defense System model.

Галаган В. І., канд. військ. наук, доцент

(0000-0001-9578-0895)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

## Пропозиції щодо розроблення та впровадження аналітичного модуля контролю за процесом закупівель товарів, робіт та послуг для потреб Збройних Сил України

**Резюме.** У статті на основі детального аналізу функціонування системи електронних торгів надано пропозиції щодо розроблення та впровадження аналітичного модуля контролю за процесом закупівель товарів, робіт та послуг для потреб Збройних Сил України.

**Ключові слова:** система електронних торгів; аналітичний модуль контролю; аналітична система.

**Постановка проблеми.** Відповідно до положень Стратегічного оборонного бюлетеня України [1] очікуваним результатом є створення за принципами та стандартами, прийнятими в державах – членах НАТО, ефективних, мобільних, оснащених сучасним озброєнням, військовою та спеціальною технікою сил оборони зразка 2020 р., здатних гарантовано забезпечити оборону держави та адекватно і гнучко реагувати на воєнні загрози національній безпеці України, а проте раціонально використовувати наявний потенціал (спроможності) та ресурси держави.

Для виконання поставлених завдань у Збройних Силах (ЗС) України на сьогодні проводиться оборонна реформа, під час якої здійснюється перехід на нову відкриту, позбавлену корупційної складової систему оборонних закупівель.

Крім того, проведення ЗС України Операції об'єднаних сил та залучення для цього великої кількості з'єднань, частин і підрозділів значно підвищують потреби в логістичному забезпеченні, яке досить суттєво залежить від процесу закупівель товарів, робіт і послуг.

Для контролю за закупівлями товарів, робіт і послуг у державному масштабі створена та використовується система електронних торгів *ProZorro*. Після початку роботи системи електронних торгів *ProZorro* Міністерство оборони України активно включилося в роботу та стало одним із лідерів за кількістю укладених угод серед інших учасників, що призвело до значної економії бюджетних коштів.

Суттєве спрощення процедур призвело до залучення до роботи в системі електронних торгів тільки визначених окремих категорій посадових осіб (фахівців) Міністерства оборони України, переважно Департаменту державних закупівель та постачання

матеріальних ресурсів Міністерства оборони України, які готують документацію та контролюють проходження тендерних процедур.

Водночас більша частина зацікавлених безпосередніх замовників товарів, робіт, послуг не має доступу до детальної інформації щодо тендерного процесу, що часто призводить до вибору учасників торгів, які не стануть добросовісними постачальниками та партнерами, не виконуватимуть належним чином узяті зобов'язання (як правило, це терміни поставок, виконання робіт і їх якість). На часті випадки невиконання своїх зобов'язань постачальниками неодноразово зверталася увага і керівництва Міністерства оборони України [2].

Отже, проблема забезпечення всіх зацікавлених осіб (до ланки начальника служби частини, з'єднання) необхідною аналітичною інформацією щодо процесу закупівель товарів, робіт, послуг є досить актуальною задачею. Тим більше, що саме вказані категорії є найбільш обізнаними з діяльністю, спроможностями та порядністю місцевих (гарнізонних) постачальників.

**Аналіз останніх досліджень та публікацій.** На сьогодні більшість фахових публікацій [3–5] з питань розроблення та впровадження інформаційно-аналітичних систем стосуються бізнес-сектору, не враховуючи специфіку діяльності державних структур, зокрема і Міністерства оборони України.

Досвід роботи та проведений аналіз показав, що нині питанням забезпечення інформацією щодо процесу закупівель товарів, робіт і послуг у Міністерстві оборони України приділяється недостатня увага.

У межах створення та функціонування єдиної інформаційної системи управління оборонними ресурсами (DRMIS), яка

включатиме інформаційні системи (управління інфраструктурою, особовим складом, видами забезпечення та ін.) планується циркуляція значної кількості даних, які також мають ураховувати і майбутні закупівлі товарів, робіт і послуг для забезпечення потреб ЗС України. Водночас обмін даними між інформаційною системою DRMIS та системою електронних торгів *ProZorro* поки не планується.

Указаний стан потребує розроблення власного аналітичного інструментарію, доступного для всіх категорій посадових осіб (фахівців), які мають відношення до процесу закупівель у ЗС України та дасть змогу контролювати його хід (аналізувати, проводити моніторинг закупівель та їх учасників). Отримана деталізована інформація може використовуватися керівним складом ЗС України для подальшого прийняття обґрунтованих рішень щодо забезпечення потреб військ (сил).

Це завдання особливо актуалізується на етапі проведення заходів трансформації системи об'єднаного керівництва силами оборони та військового управління в ЗС України під час реорганізації підрозділів Генерального штабу ЗС України та перерозподілу функцій між ними.

З огляду на викладене, **метою статті** є проведення детального аналізу, обґрунтування та надання відповідних пропозицій щодо розроблення власного аналітичного модуля контролю за процесом закупівель товарів, робіт і послуг для потреб Збройних Сил України.

**Виклад основного матеріалу.** Система електронних торгів стала невід'ємною частиною українських державних закупівель, зокрема і для забезпечення потреб ЗС України.

У державному масштабі закупівля товарів, робіт і послуг здійснюється через електронну систему *ProZorro*, правовий статус якої закріплений у Законі України “Про публічні закупівлі” від 25.12.2015 № 922-VIII, де була запроваджена обов'язковість проведення публічних електронних процедур закупівель для головних розпорядників коштів і монополістів [6].

Загалом система *ProZorro* – це база даних, що знаходиться на окремому сервері та доступ до якої здійснюється тільки через електронні майданчики, які мають доступ до системи, наприклад, Української Універсальної Біржі (на сьогодні використовується 19 електронних

*майданчиків*). Завдяки такій організації процесу закупівель, держава не зможе втручатися у торги, лобіювати або відсіювати учасників, чи впливати на них.

Сутність роботи *ProZorro* полягає у проведенні зворотного аукціону, у якому учасники змагаються за право постачати замовнику певний товар чи послугу. Під час проведеного аукціону переможе той, у кого ціна виявиться найнижчою, а технічні характеристики товару або послуги відповідають тим, що заявлені замовником у тендерній документації.

Отже, з 2016 року основна частина публічних закупівель здійснюється за допомогою електронних торгів. Конкурентний діалог застосовується у випадках, коли замовнику важко визначитись зі специфікацією та технічними характеристиками запланованих робіт або коли закуповуються інформаційні послуги та наукові дослідження. Переговорна процедура є винятком і застосовується здебільшого для проведення архітектурних конкурсів і закупівлі творів мистецтва.

Після запуску системи *ProZorro* та отримання великої кількості відкритих даних в Україні виникла необхідність проведення їх упорядкування та аналізу, що призвело до появи багатьох інструментів і сервісів, які допомагають аналізувати, проводити моніторинг закупівлі та їх учасників.

На сьогодні існують аналітичні інструменти для контролю та моніторингу публічних закупівель як від команди розробників системи *ProZorro*, так і від сторонніх команд. На жаль, ЗС України не мають власних і не використовують аналітичних засобів інших розробників.

Найбільш розвиненим і досконалим є моніторинговий портал *DoZorro* – платформа, де кожен учасник системи (постачальник, замовник, контролюючий орган, громадянин) може дати зворотній зв'язок державному замовнику чи постачальнику, обговорити та оцінити умови конкретної закупівлі, провести аналіз закупівлі окремого державного органу чи установи, підготувати та подати офіційне звернення до контролюючих органів та ін.

Розроблення індивідуальних аналітичних програм пояснюється тим, що у кожного учасника публічних закупівель існують певні пріоритети, і, відповідно, свої потреби в аналізі інформації, але спільним, для кожного учасника, є ефективне використання коштів і мінімізація ризиків пов'язаних з недобросовісними



постачальниками товарів і послуг та стороннім втручанням будь-яких зацікавлених осіб.

Негативний приклад був і в діяльності ЗС України, а саме будівництво табірної містечка на території військового полігону “Широкий лан”. Забудовником, згідно з умовами договору, об’єкт мав бути готовим і зданим в експлуатацію в 2018 році, проте донині частина будівельних робіт досі не виконана. Цей факт указує на недостатню інформованість керівного складу (фахівців), які приймали відповідні рішення, щодо можливостей і порядності забудовника [7].

Команда розробників електронної системи *ProZorro* пропонує за аналітичний інструмент використовувати в моніторинговому порталі *DoZorro* два основних модулі “Публічний модуль аналітики” та “Професійний модуль аналітики”. Кожен з модулів має свою визначену направленість на користувача.

“Публічний модуль аналітики” дає змогу замовникам знайти типову документацію, перевірити постачальників і додатково оцінити рівень власної ефективності. Цей модуль у режимі онлайн відображає усі закупівлі, що проводяться через електронну систему *ProZorro*, має широкий функціонал (від загальної інформації про стан системи до викриття порушень і змов).

“Публічний модуль аналітики” має великий перелік критеріїв, за якими можна фільтрувати та сортувати закупівлі, плани, постачальників і замовників, щоб отримати потрібну інформацію. Модуль аналітики нараховує близько 450 полів відборів, які користувач може застосувати під час детального аналізу. Усі поля відборів поділені на групи, які структурують їх і поєднують за функціональними особливостями. За допомогою цієї інформації є можливість оцінити стан ринку та своє положення на ньому, оцінити позиції конкурентів та поведінку партнерів, а також знайти кращі практики із закупівель.

Відмінність “Публічного модуля аналітики” від “Професійного модуля аналітики” полягає в можливості останнього створювати власні напрями аналізу, загалом “Професійного модуля аналітики”.

“Професійний модуль аналітики” забезпечує розгорнутий аналіз закупівлі через систему *ProZorro* завдяки понад 1000 різноманітним показникам. Крім того, модуль дає змогу налаштувати під свої потреби

таблиці та графіки об’єктів, або навіть створити власні показники.

Загалом, моніторинговий портал *DoZorro* – це платформа, де кожен учасник системи (постачальник, замовник, контролюючий орган, громадянин) може дати зворотній зв’язок державному замовнику чи постачальнику, обговорити та оцінити умови конкретної закупівлі, проаналізувати закупівлі окремого державного органу чи установи, підготувати та подати офіційне звернення до контролюючих органів та багато іншого. Крім того, портал дає змогу обговорити конкретний тендер із потенційними та наявними постачальниками, дізнатись їхню експертну думку про правильність формувань у тендерній документації, отримати професійну експертизу тощо. Державні замовники можуть не лише дати оцінку конкретному постачальнику, але й проаналізувати зворотній зв’язок від бізнесу та внести відповідні зміни до закупівельного процесу і створити власну систему ризик-менеджменту [8].

Обидва модулі створені за допомогою програмного забезпечення *Qlik*, основною технологічною особливістю якого є реалізація асоціативної архітектури, технології обробки даних в оперативній пам’яті (в пам’яті), інтуїтивно зрозумілого користувальницького інтерфейсу, сумісного з новими технологіями даних.

У системі *Qlik* реалізована унікальна запатентована технологія резидентного (in-memory, тобто в оперативній пам’яті) асоційованого аналізу, яка створила фундамент для створення *BI* (*Business intelligence*) – платформи нового покоління *Qlik*. *BI*-технологія *Qlik* – сучасна розпорядча аналітична система з наданням завдань на виконання, яка складається з комбінацій “традиційної” або дескриптивної аналітики (відповідає на запитання “що?”), діагностичної аналітики (“чому?”), прогнозної аналітики (“що станеться?”).

Кожний з модулів аналітики, який розглядається, побудований на різних функціональних рішеннях *Qlik* – *Qlik View* (“Професійний модуль аналітики”) та *Qlik Sense* (“Публічний модуль аналітики”), які виконані на одній програмній платформі.

Насамперед, слід зазначити, що *QlikView* і *Qlik Sense* – аналітичні інструменти з єдиною логікою і на єдиній платформі. Ключова відмінність у позиціонуванні: *QlikView* – подається як корпоративна платформа, а

*Qlik Sense* – інструмент персонального дослідження даних кінцевим користувачем.

*Qlik View* – програмне забезпечення, яке дає змогу користувачам будь-якого рівня, від новачків до фахівців, отримувати і співставляти дані з будь-якого джерела: баз даних, аналогічних *SQL Server* або *Oracle*, а також файлів *Excel*, *XML* або текстових файлів. Додатки для підприємств, наприклад, *SAP (ERP-система для планування ресурсів підприємств)*, можуть бути також використані в якості джерела даних для виконання аналізу *QlikView*.

*Qlik Sense* – додаток для самостійної візуалізації, дослідження і моніторингу даних, який має інтуїтивно зрозумілий інтерфейс, що дає змогу користувачам не мати спеціальних знань з обробки даних та полегшує створення нових діаграм без написання кодів і формул. Має можливість обробки даних безпосередньо в оперативній пам'яті та дає змогу оперувати великими обсягами інформації. *Qlik Sense* належить до класу аналітичних систем самообслуговування *Self-Service BI*.

Аналітична система *Qlik* може використовувати методи штучного інтелекту для оперативного прогнозування. Отже, значною перевагою цього програмного забезпечення є можливість виконувати роботу на будь-яких пристроях (ноутбук, планшет, телефон, комп'ютер), що є досить вагомим фактором для ЗС України. Система автоматично масштабується під розмір екрану, має змогу роботи з даними *Offline (без доступу до мережі)*, сумісної роботи з декількома вікнами та майже необмежені можливості візуалізації аналітичних даних.

Утім, згадані модулі аналітики мають певні особливості, які впливають на можливість їх повноцінного впровадження та застосування в діяльності ЗС України. Насамперед, незначна кількість безкоштовних ліцензій та обмежений термін безкоштовної ліцензії на користування (1 місяць), у разі покупки комерційної ліцензії значна її вартість (1350 \$ - одна ліцензія).

Отже, з огляду на наведене, можна дійти висновків:

в Україні розроблена та ефективно використовується в інтересах державного сектору система публічних закупівель *ProZorro*, яка здійснюється за допомогою електронних торгів;

для контролю та моніторингу публічних закупівель у системі *ProZorro* є можливість використовувати аналітичні інструменти (моніторинговий портал *DoZorro*);

цінова політика та політика доступу розробника програмного забезпечення *DoZorro* до використання аналітичних модулів обмежує їх широке застосування для дієвого контролю за процесом закупівель товарів, робіт і послуг для потреб ЗС України;

керівний склад (фахівці), які готують і приймають управлінські рішення та контролюють процес закупівель товарів, робіт і послуг для потреб ЗС України мають тільки загальну інформацію із системи *ProZorro* (без необхідної деталізації);

для моніторингу та контролю закупівель для потреб ЗС України керівному складу (фахівцям) Міністерства оборони та Генерального штабу ЗС України потрібен власний аналітичний модуль, який дасть змогу відслідковувати будь-які фінансові дії щодо організацій (структур) та здійснювати прогноз на основі отриманих реальних статистичних даних.

Для впровадження пропозиції щодо розроблення власного аналітичного модуля для потреб ЗС України бажано використовувати програмні продукти, які розповсюджуються безкоштовно або були раніше закуплені для потреб Міністерства оборони України, що призведе надалі до значної економії бюджетних коштів.

На сьогодні закуплена та знаходиться у користуванні Міністерства оборони України сучасна аналітична платформа з асоціативною технологією аналізу *QlikView*. За допомогою програмного забезпечення *QlikView* вже було розроблено макет автоматизованого робочого місця керівного складу Міністерства оборони України за напрямом управління нерухомим військовим майном, який проходить етап тестування в структурах, що займаються інфраструктурним забезпеченням [9]. Тобто, для розроблення та налаштування власного аналітичного модуля є підготовлені досвідчені спеціалісти та отриманий певний досвід з розроблення програмних продуктів на базі *Qlik*.

Крім того, для розроблення, налаштування та впровадження власного аналітичного модуля контролю за процесом закупівель товарів, робіт і послуг для потреб ЗС України необхідно виконати певні заходи з організаційної та технічної підтримки, а саме: розгортання на базі Головного управління зв'язку та інформаційних систем Генерального штабу ЗС України серверного обладнання з доступом до мережі "Інтернет", забезпечення його працездатності та підтримки цілодобової роботи;

організація та проведення консультаційної підтримки з розробником програмного забезпечення *DoZorro* (ТОВ “АрБіСі Груп”);

отримання у розробника програмного забезпечення *DoZorro* моделі аналітичної системи (у вигляді виконуваного файлу) та розміщення його на серверному обладнанні Генерального штабу ЗС України;

налаштування та перевірка процесу обміну даними із системою *ProZorro*;

організація та налаштування доступу користувачів (за переліком ролей і повноважень);

налагодження процесу впровадження програмного продукту та супроводження роботи користувачів, подальший розвиток власної асоціативної систему аналізу.

Тобто, розроблення, впровадження та використання власного модуля *BI*-аналітики для структур (організацій) ЗС України з доступом до системи *ProZorro* дає змогу одразу отримати необхідну інформацію, яка стосується безпосередньо Міністерства оборони України, мати на початковому екрані саме ті показники, які є специфічними для посадової особи (фахівця) та проводити аналіз закупівель за особисто вибраними критеріями, або створити їх для себе і використовувати надалі.

Окрім того, наявність власного аналітичного модуля дає змогу поєднувати дані з різних джерел інформації як з Міністерства оборони України, так і інших державних і недержавних відкритих і закритих реєстрів. Так, наприклад, поєднання даних щодо закупівель структурами (організаціями) ЗС України (юридичним особами) з даними реєстру декларацій посадових осіб, фізичних осіб (і їх близьких родичів), може значно знизити корупційні ризики під час проведення закупівель, або визначити ймовірність корупційної складової вже проведених тендерів.

**Висновки.** Отже, проведений аналіз показує, що розроблення та впровадження власного аналітичного інструментарію дасть змогу контролювати процес закупівель і надавати деталізовану інформацію керівному складу Міністерства оборони України та Генерального штабу ЗС України для подальшого прийняття обґрунтованих рішень щодо забезпечення потреб військ (сил). До того ж, етап розроблення та впровадження аналітичного модуля контролю за процесом

закупівель товарів, робіт і послуг може бути максимально спрощеним і фінансово незатратним завдяки отриманому раніше досвіду роботи з програмним забезпеченням і наявними ліцензіями на його використання.

Напрацювання, які будуть реалізовані у власному аналітичному модулі можуть бути успішно використані під час побудови DRMS та під час створення робочого макету базового рівня інформаційної інфраструктури Міністерства оборони України.

**Подальші дослідження** за доцільно зосередити на питаннях розроблення та впровадження аналітичних модулів за видами матеріально-технічного забезпечення військ (сил).

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року “Про Стратегічний оборонний бюлетень України” : Указ Президента України від 06.06.2016 р. №240/2016. URL: <http://www.president.gov.ua/news/prezident-zatverdiv-strategichnij-oboronnij-byulet-en-ukrayin-37309> (дата звернення: 15.04.2020).
2. Виступ Міністра оборони України від 10.01.2019. URL: <https://ukurier.gov.ua/uk/articles/ministr-oboroni-stepan-poltorak-use-sho-zakupovuye/> (дата звернення: 15.04.2020).
3. Бородулин А. Разработка информационно-аналитических систем корпоративного управления. *Вестник Тверского государственного университета. Экономика и управление.* 2016. № 2. С. 159–165.
4. Белов В. Информационно-аналитические системы. Основы проектирования и применения : учебн.-практ. пособ. изд. 2-е, перераб. и доп. Москва : МГУ экономики, статистики и информатики, 2005. 111 с.
5. Бусол О. Перспективи використання інформаційно-аналітичних систем. Тези доповіді на міжнародній конференції. URL: <http://conference.nbu.gov.ua/report/view/id/335> (дата звернення: 15.04.2020)
6. Про публічні закупівлі : Закон України від 25.12.2015 р. № 922-VIII. URL: <https://ukurier.gov.ua/uk/articles/ministr-oboroni-stepan-poltorak-use-sho-zakupovuye/> (дата звернення: 15.04.2020).
7. Державне бюро розслідувань. ДБР розслідує розтрату 37 млн під час будівництва на полігоні “Широкий лан”. URL: <https://dbr.gov.ua/news/dbr-rozslidue-roztratu-37-mln-pid-chas-budivnictva-na-poligoni-shirokiy-lan> (дата звернення: 15.04.2020).
8. Аналітичні інструменти для контролю та моніторингу публічних закупівель. URL: <https://dozorro.org/tools> (дата звернення: 15.04.2020).
9. Галаган В., Бондарчук С., Полішко С. Формування загального обрису інформаційно-аналітичного автоматизованого робочого місця керівного складу управління нерухомим військовим майном ЗС України. *Оборонний вісник.* 2018. №2.

## **Proposals for development and implementation of an analytical module for monitoring the process of procurement of goods and services for the needs of the Armed Forces of Ukraine**

### **Annotation**

Since the time when ProZorro e-trading system has been created and used to control the procurement of goods, works and services on a national scale the Ministry of Defense of Ukraine became one of the leaders in the number of concluded agreements among other participants, and this is led to save significant amount of funds in budget resources.

Currently there is a problem of providing all interested persons (up to the level of the head of the service of the unit, connection) with the necessary analytical information about procurement process. These categories of servicepersons are more aware about the activities, capabilities and decency of local suppliers.

An analysis shows that the development and implementation of own analytical tools will control the procurement process and provide detailed information to the leadership of the Ministry of Defense of Ukraine and the General Staff of the Armed Forces of Ukraine for further decisions to meet the needs of units of the Armed Forces. The development and implementation of such analytical module can be simplified and financially inexpensive due to previous experience with software and existing licenses for its use.

The developments that will be implemented in our own analytical module can be successfully used even in the construction of a single information resource management system DRMIS (Defense Resources Management Information System) and the creation of a working layout of the basic level of information infrastructure of the Ministry of Defense of Ukraine.

**Keywords:** electronic bidding system; analytical control module; analytical system.

Руденська Г. В.

(0000-0002-4719-3765)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

## Шляхи удосконалення тестування спеціального програмного забезпечення інформаційної системи управління оборонними ресурсами на етапі експлуатації

**Резюме.** Проаналізовано методи тестування спеціального програмного забезпечення на етапі експлуатації, які відповідають регламентам міжнародних стандартів STANAG та ISO/ДСТУ і спрямовані на виявлення потенційної вразливості (*vulnerability*). Запропоновано шляхи удосконалення тестування спеціального програмного забезпечення інформаційної системи управління оборонними ресурсами DRMIS (*Defense Resources Management Information System*) для впровадження на етапі експлуатації.

**Ключові слова:** управління оборонними ресурсами; інформаційна система; спеціальне програмне забезпечення; тестування; процедури тестування, уразливість; міжнародні стандарти; система менеджменту; початкові коди.

**Постановка проблеми.** Використання інформаційних систем (ІС) у сфері державного військового управління і оборонного планування передбачає застосування відповідного спеціального програмного забезпечення (СПЗ). Однією з вимог до СПЗ є забезпечення потрібного рівня його захищеності під час можливих кібератак та несанкціонованого доступу.

Основні заходи, які використовуються для захисту ІС – мережеві екрани, системи виявлення і попередження вторгнень та антивірусні системи на основі аналізу сигнатур трафіку, спрямовані на відбиття атак з мережі [1]. Високий рівень уразливості СПЗ може мати такі наслідки, як отримання доступу до конфіденційної інформації неавторизованими користувачами, порушення нормального режиму функціонування (виконання довільного коду), виконання команд з підвищеними привілеями користувачем, який їх не має та ін. Крім того,

є проблеми довіри до СПЗ ІС воєнного призначення, в розробленні або тестуванні яких взяли участь компанії інших країн і рівень його уразливості не підтверджений.

Отже, актуальним стає впровадження сучасних процедур тестування та виявлення вразливості СПЗ, яке використовується або планується до використання в сучасних ІС воєнного призначення, зокрема DRMIS.

**Аналіз останніх досліджень та публікацій.** Концептуальний підхід до тестування СПЗ викладено в [2]. Існує значна кількість сучасних наукових досліджень з питань загального менеджменту ІС, аналізу коду, проведення тестування на проникнення [3, 4]. Агенція передових оборонних дослідницьких проєктів (DARPA) Міністерства оборони США, яке відповідає за розроблення нових технологій для Збройних сил США, на етапі розроблення нового СПЗ застосовує чотири основні процедури тестування (табл. 1).

Таблиця 1

Дослідження DARPA щодо тестування СПЗ ІС воєнного призначення

Процедура	Мета процедури
Перевірка програмних і апаратно-програмних засобів (VET)	Контроль відповідності заявленим спроможностям, виявлення закладок у СПЗ ІС
Аналіз програм для забезпечення кібербезпеки (APAC)	Автоматизація виявлення вразливостей СПЗ ІС у реальному часі
“Великий кібервиклик” (CGC) та академічні дослідження вразливостей	Упровадження нових процедур тестування
Системний аналіз програмних комплексів	Підвищення надійності СПЗ та удосконалення процедур верифікації, зокрема статичних аналізаторів

Однак процедури тестування та виявлення уразливості СПЗ безпосередньо на етапі експлуатації ІС вивчені недостатньо та розглядаються як питання технічного регулювання [5]. Дослідження з цього питання

носять фрагментарний характер або обмежені внутрішніми “кращими практиками” розробників програм. Так, у [6] добре опрацьовані загрози ланцюжків поставок, а

процедури виявлення уразливості СПЗ на етапі експлуатації описані недостатньо.

Водночас понятійний і методичний апарат тестування СПЗ та оцінювання вразливості програм уже склався і знаходиться на відповідному рівні ітераційного розвитку. У статті використанні визначення, прийняті міжнародними організаціями зі стандартизації, у яких бере участь Україна, а саме: STANAG, ISO, IEC, ITU.

**Метою статті** є аналіз методів тестування СПЗ для виявлення уразливості та шляхів удосконалення тестування СПЗ DRMIS на етапі експлуатації.

**Виклад основного матеріалу дослідження.** Тестування СПЗ (*Custom Software Testing*) – це процес аналізу і визначення надійності функціонування програмного продукту в інформаційному середовищі, у якому він використовується. Надійність функціонування програмного продукту (*Software Reliability*) визначається

ймовірністю його роботи без відмов протягом встановленого періоду часу, з урахуванням вартості кожної відмови [8]. Ймовірність роботи СПЗ без відмов на практиці визначається ймовірністю того, що оператор не зможе ввести в систему деякий конкретний набір даних, що визначається як відмова в обслуговуванні, яка впливає на результат функціонування DRMIS, наприклад, своєчасне направлення необхідних боєприпасів на вогневу позицію артилерії, що зрештою призводить до суттєвих втрат. Під уразливістю СПЗ (*System Vulnerability*) розумітимемо нездатність протистояти впливу певної кіберзагрози або сукупності кіберзагроз: помилок програмування, недоліків проектування, ненадійних паролів, вірусів та інших шкідливих програм, використання мов програмування загального призначення (наприклад, PHP скриптів) і SQL-ін'єкцій [9]. Тобто, це певні недоліки в СПЗ, які можуть порушити її цілісність та надійність експлуатації.

#### **Примітка**

*PHP* – скриптова мова загального призначення, інтенсивно застосовується для розроблення вебдодатків. На сьогодні підтримується переважною більшістю хостинг-провайдерів і є одним з лідерів серед мов, які застосовуються для створення динамічних вебсайтів.

*SQL* ін'єкція – один з поширених способів злому сайтів і програм, які працюють з базами даних, заснований на впровадженні в запит довільного SQL-коду.

*Програма-експлоїт* (en: exploit – експлуатувати) – комп'ютерна програма, фрагмент програмного коду або послідовність команд, які використовують уразливості в програмному забезпеченні та застосовують для проведення атаки на обчислювальну систему. Метою атаки може бути як захоплення контролю над системою (підвищення привілеїв), так і порушення її функціонування (DoS-атака).

Повний перелік процедур тестування СПЗ на етапі експлуатації включає [9]:

- аналіз початкового коду для визначення уразливості;
- визначення причин виникнення уразливості;
- забезпечення надійності функціонування СПЗ.

Аналіз початкового коду. Аналіз початкового коду СПЗ для виявлення уразливості базується на різних методах тестування: статичному, динамічному, експертно-документальному, фазінгу. Це пов'язано з тим, що помилки і уразливості СПЗ мають різну природу і різні характерні ознаки.

*Статичний метод* базується на ідентифікації початкових кодів, які беруть участь у компіляції об'єкта сертифікації для фіксування повного переліку файлів вихідних текстів. Під час застосування *динамічного методу аналізу початкового коду* проводиться формування переліку шаблонів атак, які є актуальними для СПЗ із використанням

послідовності дій, які представлені в розділі 6.1 стандарту ISO/IEC TR 20004. Під час застосування *експертно-документального аналізу* крім інформації, представленої в початкових кодах СПЗ, експерти використовують представлену для тестування документацію (технічну, програмну, експлуатаційну), інформацію про вразливості СПЗ об'єкта, схожого з об'єктом сертифікації. *Фазінг-тестування* базується на визначенні актуальних вразливостей СПЗ за результатами виконання тестів на проникнення.

Результативність застосування цих методів аналізу початкового коду СПЗ, визначеної через відсоток від загальної кількості виявлених вразливостей, наведена на рис. 1 [9].

Отже, не зважаючи на використання різних методів тестування СПЗ, допустимий рівень надійності функціонування СПЗ неможливо забезпечити без надання доступу до початкового коду СПЗ. Динамічний метод і фазінг-тестування не дають змоги виявити “плаваючі” помилки і програмні закладки,

ініціювання яких пов'язане з рідкісними комбінаціями вхідних даних, і які, за статистикою, є однією з найбільших проблем

функціонування СПЗ. Тільки доступ до початкових кодів СПЗ дає високу ймовірність усунення уразливості.

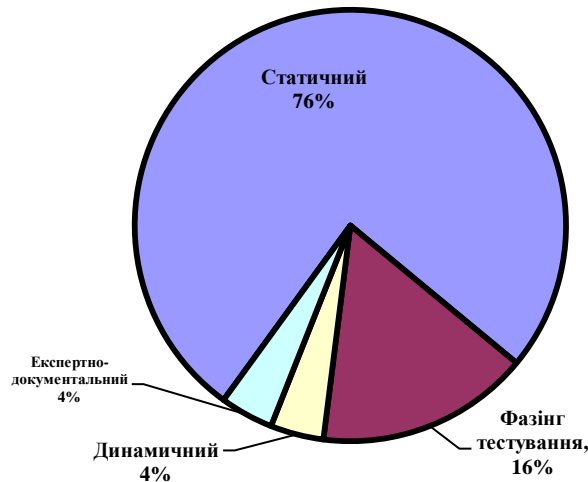


Рис. 1. Методи аналізу початкових кодів СПЗ DRMIS

Визначення переліку причин виникнення уразливості СПЗ базується на двох методах:

статистичному, з використанням статистики провідних баз даних уразливості програмного забезпечення, таких як CAPEC, OWASP, *Mitre CVE*;

тестуванні загальновідомими програмами-експлоїтами.

У межах дослідження пілоотної версії DRMIS [10] методом співставлення зі статистичними даними *Mitre CVE*, яка перевищує 100 000 вразливостей [11], встановлений визначальний вплив на причини виникнення уразливості СПЗ рівня менеджменту розробника та критичної структурної складності СПЗ.

*Рівень менеджменту* істотно впливає на ймовірність уразливості та можливості оперативного виправлення СПЗ, встановлена строга зворотна пропорційність вірогідності уразливості рівню менеджменту розробників програм. Цей висновок підтверджується компанією Microsoft, ймовірність уразливостей в програмному забезпеченні якої вдалося знизити на 80 % за умови введення відповідної підсистеми менеджменту (*Microsoft Secure Software Development Life Cycle*) [12].

*Критична структурна складність* СПЗ DRMIS обумовлює значне зниження рівня надійності її експлуатації. Критичною до вразливості вважають структурну складність СПЗ, коли довжина вихідного тексту на мові високого рівня, досягає 20 Гб, а число логічних операторів (вузлів графа програми) може становити близько десятка мільйонів, що знаходиться далеко за рамками

когнітивних спроможностей тестувальника [13]. Відомо багато прикладів, коли помилка кодування або проектування (тобто уразливість, що не ідентифікується як навмисна) ІС воєнного призначення приводила до катастроф і критичних збитків. Крім того, наведені методи аналізу і тестування програм, за винятком експертних методів, потрапляють в зону “прокляття розмірності”. Відповідно, незважаючи на удосконалення процедур тестування, число вразливостей не зменшується. Так, на сьогодні обсяг міжнародної бази вразливостей *Mitre CVE* перевищує 100 000 вразливостей, збільшується і число комп'ютерних атак, зокрема цілеспрямованих АРТ-атак, які використовують уразливості нульового дня, а також загальний збиток від них.

Крім того, під час проведення тестування СПЗ DRMIS необхідне врахування таких потенційних причин виникнення уразливості: відсутність доступу до вихідного коду СПЗ, недоліки проектування, помилки програмування, ненадійні паролі, віруси та інші шкідливі програми, розширення спектру навмисних загроз, особливо в частині віддалених, прихованих і неведених атак і загроз компрометації даних надвеликого обсягу (*Big Data*); недостатня результативність формальних методів аналізу і тестування, за винятком експертних методів у зоні даних з великою розмірністю, використання розробниками послуг краудсорсингу, проведення відкритих конкурсів (*Bugbounty*) з виявлення уразливості в СПЗ; протиріччями між вимогами за колаборативною сертифікацією (на основі

колаборативного профілю захисту) і вимогами міжнародних стандартів; використання програмної продукції, яка пройшла сертифікацію в інших країнах; політика імпортозаміщення і обмежень з використання імпортного СПЗ; дискредитація міжнародної системи технічного та правового регулювання інформаційної та кібербезпеки.

З огляду на викладене, для удосконалення процедур тестування СПЗ DRMIS для виявлення вразливості пропонується:

упровадити єдину систему менеджменту на пост виробничих етапах життєвого циклу DRMIS;

доповнити стандартні процедури управління життєвим циклом DRMIS додатковими, які спрямовані на своєчасне виявлення та усунення вразливості СПЗ;

підвищити рівень технічного регулювання та оцінку відповідності у формі обов'язкової сертифікації СПЗ DRMIS з наданням доступу до вихідних текстів на етапі тестування СПЗ;

удосконалити систему тестування СПЗ через упровадження триетапної процедури та апаратних методів виявлення уразливості в режимі реального часу.

Впровадження єдиної системи менеджменту на етапі експлуатації підвищить надійність функціонування DRMIS завдяки зниженню рівня уразливості та підвищенню оперативності їх виправлення.

Стандартні процедури управління життєвим циклом DRMIS [8] пропонується доповнити чотирма додатковими, які спрямовані на запобігання уразливості СПЗ (рис. 2).

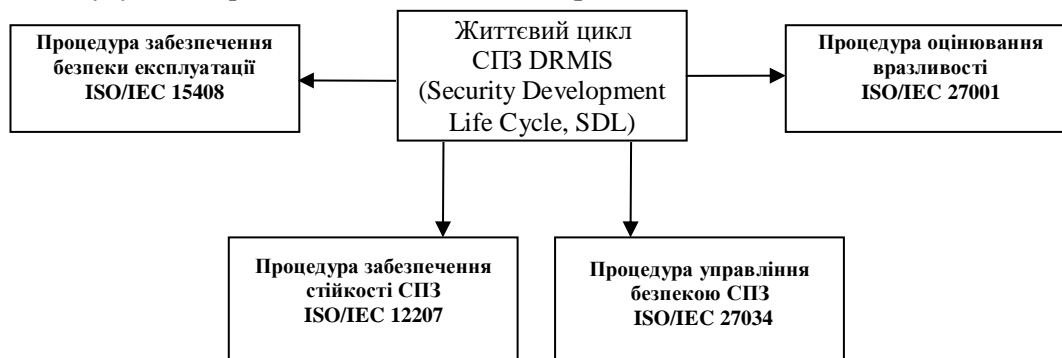


Рис. 2. Додаткові процедури тестування СПЗ DRMIS

Процедура забезпечення безпеки експлуатації встановлює загальні критерії оцінювання надійності функціонування СПЗ на основі вимог ISO/IEC 15408. Процедура оцінювання вразливості встановлює необхідні критерії (рівні) уразливості, за яких можливо введення в експлуатацію СПЗ DRMIS, базується на вимогах ISO/IEC 27001. Процедури забезпечення стійкості визначають граничні параметри, за яких СПЗ DRMIS забезпечує надійність функціонування в умовах впливу кібератак визначеної інтенсивності. Процедури управління безпекою відповідають вимогам ISO/IEC 27034 та забезпечують контроль програмних і апаратних методів тестування.

Підвищення рівня технічного регулювання та оцінки відповідності у формі обов'язкової сертифікації СПЗ DRMIS з наданням доступу до вихідних текстів на етапі тестування на сьогодні є проблемним питанням. Основною загрозою з погляду розробника є загроза крадіжки інтелектуальної власності. Водночас досвід тестування СПЗ показав, що створення автономного захищеного стенду в захищеному

приміщенні або “clean-room” забезпечує повне виконання вимог з безпеки коду У такому приміщенні на території замовника (під контролем служби ТЗІ замовника) на період проведення тестування організовується доступ до вихідного коду програм. У межах такої процедури в закритому захищеному середовищі виконується тестування, фіксуються контрольні суми і проводяться інші необхідні процедури. Без погодження зі службою ТЗІ замовника не допускається винесення будь-якого носія інформації, ініціювання сеансу зв'язку зовні та ін. Усі документальні підтвердження проведених перевірок і висновки обговорюються і затверджуються замовником. Зазначені процедури мають низку переваг і гарантій, а саме:

дають змогу підвищити рівень надійності експлуатації DRMIS завдяки консолідації зусиль розробників і допущених фахівців лабораторії з тестування СПЗ;

виявленні уразливості будуть виправлені в межах сертифікації в обов'язковому порядку, а відомості щодо них не будуть відомі третій стороні;



перевірки абсолютно прозорі, всі дії (організація доступу, контроль і моніторинг роботи, обговорення результатів, підготовка звітних документів тощо) технічно і нормативно забезпечуються службою ТЗІ замовника;

завжди є ймовірність виявити потенційно небезпечний код (або продемонструвати його відсутність), у чому зацікавлені обидві сторони сертифікації.

Зазначений підхід прийнятий і пройшов апробацію в Агенції НАТО з підтримки та

постачання, на сьогодні не зафіксовано жодного компрометуючого його випадку.

Крім того, питання відкриття доступу до вихідного коду для проведення тестування підтримується потужними розробниками програм. Так, Microsoft відкрила доступ до вихідного коду своїх програмних продуктів у понад тридцяти країнах світу.

Для удосконалення системи тестування СПЗ DRMIS пропонується впровадження три етапної процедури (рис. 3).

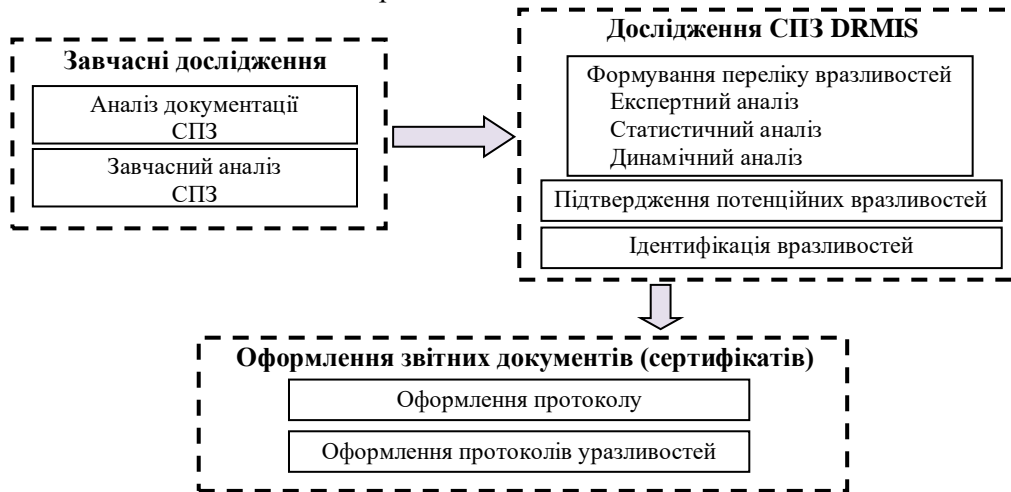


Рис. 3. Порядок тестування СПЗ DRMIS для виявлення вразливостей

Для виявлення вразливостей СПЗ у реальному часі доцільно впровадження апаратних методів [14]. Прикладами таких технологій є механізм *Stack Guard* компілятора *GCC* (внесенням збитковості на етапі виконання перевіряється стан стеку), режим безпеки *GS* компілятора *OCC* (внесенням збитковості на етапі виконання перевірки стану стеку), технологія процесорів *Intel Execute Disable Bit* (забороняє виконання команд у сегменті стеку та сегменті тексту), механізми безпеки *JVM (Java Virtual Machine)* та *CLR (Common Language Runtime)*.

**Висновок.** Отже, представлено дослідження дає змогу вдосконалити тестування СПЗ DRMIS та підвищити надійність її експлуатації.

**Надалі,** за результатами експериментального тестування дослідного зразка СПЗ DRMIS планується розроблення методики тестування та виявлення вразливості СПЗ інформаційної системи управління оборонними ресурсами.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Scambray J., Shema M. Hacking exposed web applications. California : McGraw-Hill, 2002. 416с.

2. ISO/IEC TR 20004:2015. Інформаційна технологія. Методи і засоби забезпечення безпеки. Уточнений аналіз уразливості програмного забезпечення по ISO/IEC 15408 та ISO/IEC 18045.

3. Барабанов А. В., Марков А. С., Цирлов В. Л. Международная сертификация в области информационной безопасности. *Стандарты и качество*. 2016. № 7. С. 30–33

4. Шерстюк В. П. XIV научная конференция Международного исследовательского консорциума информационной безопасности // *Международная жизнь*. 2017. № 14. С. 42–180.

5. Марков А. С., Шермет И. А. Теоретические аспекты сертификации средств защиты информации. *Оборонный комплекс – научно-техническому прогрессу* 2015. № 4 (128). С. 7–15.

6. Клянчин А. И. Каталог закладок АНБ (Spigel). Часть 1. Инфраструктура. Вопросы кибербезопасности. 2014. № 2 (3). С. 60–65.

7. ДСТУ ISO/IEC 27032:2016. Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT). [Чинний від 2018-01-01]. Вид. офіц. Київ, 2018.

8. Руденська Г. В. Моделі і процеси життєвого циклу інформаційної системи управління оборонними ресурсами. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2020. № 1 (68). С. 59–65.

9. Баранов А. В., Марков А. С. Статистика

- виявлення уязвимостей програмного забезпечення при проведенні сертифікаційних випробувань. *Вопросы кибербезопасности*, 2017. № 2 (20). С. 2–8.
10. Сиротенко А. М. Інформаційна система управління оборонним плануванням на спроможностях J-DARTS і можливості її впровадження у Збройних Силах України. *Наука і оборона*. 2018. № 4. С. 29–34.
11. Common Vulnerabilities and Exposures (CVE) – база даних загальновідомої уразливості інформаційної безпеки. URL: <https://cve.mitre.org> (дата звернення: 20.07.2020).
12. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД ТЗІ 1.1-003-99 : затв. наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 р. № 22. Київ : ДСТСЗІ СБ України, 1999. 30 с.
13. Основні вразливості програмного забезпечення (за версією проекту ТОП 10 OWASP). URL: <https://beasthackerz.ru/uk/skype/uyazvimost-eto-cto-takoe.html> (дата звернення: 20.07.2020).
14. Левшенко О. С., Руденська Г. В. Питання воєнно-наукового супроводження створення інформаційних систем військового призначення. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2016. № 2 (57). С. 61–66.

Стаття надійшла до редакційної колегії 25.08.2020

## Ways to improve testing of special software of the defense resource management information system at the operational stage

### Annotation

With the growing role of modern information systems, the complexity of special open source software increases and the likelihood of its vulnerability increases. The exploitation of the DRMIS, which is based on open source software with vulnerability, can have such consequences as gaining access to confidential information by unauthorized users, disrupting the operating mode, and others.

*The purpose of the article* is to analyze testing procedures and identify vulnerabilities in open source software to increase the security level of the DRMIS operation.

Testing special open source software of the DRMIS in order to identify vulnerabilities includes three sequential stages: identifying potential vulnerability of open source software and assessing the possibility of their implementation by modeling cyber-attacks for various purposes; identification and response to incidents related to ongoing cyber-attacks; elimination of the consequences of successful cyber-attacks. With the purpose of decreasing vulnerability of the DRMIS open source software the next requirements were identified:

- Low level of developer management;
- Critical structural complexity of the DRMIS open source software;
- Lack of access to the source code of open source software;
- Design flaws, programming errors, weak passwords, viruses and other malware;
- Expanding the range of intentional threats;
- Insufficient effectiveness of formal methods of analysis and testing;
- Use of crowdsourcing services by developers, holding open tenders to identify open source vulnerabilities;
- Contradictions between the requirements for collaborative certification and the requirements of international standards;
- Use of software products that have passed certification in China and Russia;
- Import substitution policy and restrictions on the use of imported open source software;
- Discrediting of international system of technical and legal regulation of information and cyber security.

Reliable operation of the DRMIS provides that the international system is developed for taking into account procedures that reduce the level of vulnerability. If any vulnerability of the DRMIS open source software detected it will be fixed.

**Keywords:** defense resource management; Information system; special software; testing; vulnerability; the likelihood of vulnerability; operational reliability; international standards; management system.

Бондарчук С. В.

(0000-0003-0624-9782)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

## Обґрунтування підходу щодо підготовки даних до первинного завантаження для проведення тестування інформаційних систем управління оборонними ресурсами

**Резюме.** У статті розглянуто підхід щодо підготовки тестових даних до первинного завантаження в базу даних для проведення тестування інформаційних систем управління оборонними ресурсами. На основі проведеного аналізу визначено проблемні питання під час перетворення даних і шляхи їх вирішення. Запропоновано інструментарій та визначено етапи обробки і перетворення неструктурованої та/або частково структурованої інформації в структуровану.

**Ключові слова:** управління оборонними ресурсами; підготовка даних для тестування; перетворення даних; структурування даних; структуровані дані.

**Постановка проблеми.** Україна, зокрема і збройні сили проходять етап становлення в нових ринкових відносинах. Ефективне використання оборонних ресурсів залежить від швидкого збору, обробки інформації, і як результат – отримання повної і достовірної інформації про стан і наявність ресурсів для правильного прийняття ефективних рішень [1]. Централізація управління і потреба в розумінні кількісного та якісного стану наявних ресурсів спонукає до автоматизації і впровадження інформаційних систем обліку та управління оборонними ресурсами. Підґрунтям для ефективної роботи таких систем є бази даних та інструментарій щодо управління ними.

На етапі створення кожної бази даних виникає потреба в разовому (первинному), але досить масштабному (об'ємному) процесі підготовки даних шляхом перетворення і завантаження великих обсягів неструктурованої (частково структурованої) інформації із зовнішніх джерел для проведення тестування інформаційної системи (ІС). Одним із завдань Оборонної реформи ЗС України є створення *єдиної інформаційної системи управління оборонними ресурсами* (Defense Resources Management Information System – DRMIS), яка передбачає інтеграцію ІС управління особовим складом, управління організаційною структурою, управління оборонним плануванням, матеріально-технічним, медичним та іншими видами забезпечення, управління закупівлями, управління майном, фінансами та бюджетом, адміністративно-господарською діяльністю [2–5]. Отже, одноразова потреба завантаження великого об'єму даних для

конкретної ІС, в масштабі воєнного відомства перетворюється у багаторазову.

До розробника кожної ІС попередньо надходить велика кількість різномірної та непослідовної інформації, яка перебуває в різних стандартах і форматах. Якість підготовки даних і їх формати дуже сильно залежать від людського фактора, потреб і вподобань користувачів на етапі попереднього формування. Використання різномірних джерел даних потребує певного розуміння правил щодо їх поєднання у базі даних ІС, які не дадуть втратити структури зв'язків та суть інформації. Сьогодні також має враховувати існуючі матеріальні, фінансові обмеження, щоб вчасно відпрацювати відповідні етапи життєвого циклу ІС. Тому нагальним практичним завданням є скорочення витрат на підготовку даних на етапі тестування ІС із забезпеченням якості й повноти первинного наповнення бази даних.

**Аналіз останніх досліджень і публікацій.** На сьогодні існують спеціалізовані програмні продукти з аналізу текстів (Textual Analysis Computing Tools (TACT), HTML Batch Editor, Словогроз, ClearText Reader's Edition, xReplacer, xMarkup, TODOS), деякі з них можуть будувати зв'язки. Однак для роботи з ними потрібні чи спеціальні знання, чи замовлення вартісної послуги і залучення відповідного виконавця [6–8]. Саме тому, для підготовки даних до завантаження та проведення тестування новостворюваних ІС, здебільшого застосовують існуючий загальнодоступний інструментарій програм роботи з текстом, подібних до Notepad та Microsoft Office. Зазвичай цей інструментарій використовують

різні розробники ІС незалежно один від одного. Кожний розробник під час створення конкретної ІС одноразово знаходить свій унікальний спосіб перетворення даних, який не розголошується. Отже, обґрунтування методичного забезпечення щодо застосування загальнозживаного інструментарію для первинної підготовки даних є актуальним завданням, відпрацювання якого дасть змогу задовольнити значну частину вимог щодо попередньої підготовки даних, максимально оптимізувати її, за необхідності, повторювати цей процес для проведення тестування різних ІС.

**Метою статті** є формалізація процесу підготовки даних до первинного завантаження в базу даних із застосуванням загальнозживаного інструментарію для проведення тестування інформаційних систем управління оборонними ресурсами.

**Викладення основного матеріалу.** Під час первинного завантаження даних в базу даних, важливо усвідомлювати процеси обробки та перетворення даних, а також

приблизно розуміти структуру первинних (початкових) даних і чітко розуміти структуру кінцевих даних та їх призначення. За суттю, процес первинного завантаження можна віднести до кібернетичної трактовки роботи із сигналами та процесами [9]. Кібернетична трактовка цього поняття передбачає відмову від вивчення фізичних особливостей як первинного процесу, так і носія сигналу. Сигнал ототожнюється з інформацією про фізичні характеристики процесу (об'єкта, явища), який досліджується. До того ж ураховується, що з різних причин початкові дані не містять усієї інформації про певний об'єкт даних, а з іншого боку, початкова інформація може містити сторонню інформацію. На інформаційне наповнення первинних даних впливають способи їх обробки, зберігання, помилки та інші чинники.

Загалом кібернетичний блок (“чорний ящик”) – це блок, для якого встановлено пов’язані причинно-наслідковим відношенням вхідні та вихідні сигнали (рис. 1).

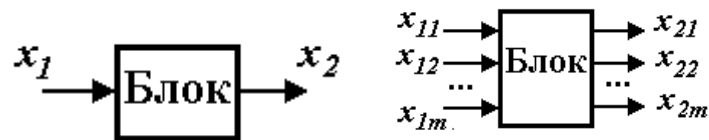


Рис. 1. Одноканальний та багатоканальний кібернетичні блоки

Для отримання необхідного вихідного сигналу блоку  $x_2(t)$ , внутрішні процеси змінюються та повторюються залежно від вхідного сигналу  $x_1(t)$ , який несе інформацію, проте важливо не втратити чи спотворити інформацію. У класичному визначенні кібернетичного блоку відсутня згадка про фізичну природу процесів усередині блоку, що і визначається терміном “чорний ящик”. Залежно від числа вхідних і вихідних сигналів розрізняють одноканальні блоки, тобто блоки з одним входом і одним виходом, і багатоканальні – з декількома вхідними та вихідними сигналами. Для спрощення, процес перетворення даних розглянемо як одноканальний кібернетичний блок.

Для опису кібернетичного блоку використовується одна з форм аналітичного опису зв'язку вхідних і вихідних сигналів. Для одноканального блоку такий опис може бути у вигляді алгебраїчного чи трансцендентного рівняння  $x_2 = f(x_1)$ , де  $f(\cdot)$  – функція перетворення даних. Для завантаження даних, їх необхідно упорядкувати, і цей процес виконується в одноканальному блоці, де вони перетворюючись переходять до бази даних.

Операції з обробки даних необхідно виконувати за певними правилами. Ці правила визначаються структурою (моделлю) даних [10, 11]. За допомогою моделі даних можуть бути представлені об'єкти предметної області та взаємозв'язки між ними [12].

Зазвичай використовується реляційна, або подібна модель даних, яка ґрунтується на добре опрацьованій теорії відносин (*Relation* – відношення). Під час проєктування такої бази даних застосовуються чіткі методи, побудовані на нормалізації відносин. Дані в реляційній моделі представляються у вигляді таблиць, які називаються відносинами, де стовпці таблиці – елементи даних, а рядки – записи. Допустимими відносинами в реляційній моделі є ті, які задовольняють умові: на перетині будь-якого рядка і будь-якого стовпця в таблиці має бути одне, а не безліч значень. Сукупність значень зв'язаних елементів даних утворює запис даних.

Кожен об'єкт в базі даних характеризується деяким набором атрибутів (наприклад, об'єкт людина може мати такі атрибути як прізвище, адреса і, можливо, ідентифікаційний номер). Унікальне значення,

яке приймає атрибут об'єкта, дає змогу ідентифікувати значення, які приймають інші елементи даних цього ж об'єкта (наприклад, знаючи ідентифікаційний номер людини, можна дізнатися прізвище, адресу, дату народження). Елементи даних, за якими можна визначити інші елементи даних, називаються ключовими.

Не кожні відносини матимуть первинний ключ у вигляді єдиного атрибуту, але можна використовувати деяку комбінацію атрибутів, які взяті разом однозначно

ідентифікуватимуть значення у відносинах. Тоді, первинний ключ називатиметься складеним первинним ключем.

Первинна інформація, як правило, зберігається в частково чи повністю неструктурованому вигляді у текстових форматах, які можуть оброблятися за допомогою загальноживаних програмних продуктів Microsoft Office – Word чи Excel. Як приклад, інформація може мати такий вигляд (рис. 2):

№ з/п	П. І. Б.	Рік народження
1	Сидоренко І.І.	1960 р.
2	Петренко Іван Петрович	68 р.н.
.....	.....	.....
5125	Яценко Степан	1972

№ з/п	П. І. Б.
1	Сидоренко І.І. -1960 р.
2	Петренко Іван Петрович - 68 р.н.
.....	.....
5 25	Яценко Степан - 1972

Математично це можна відобразити так:

Атрибут	Заголовок 1	Заголовок 2
$k_1$	$a_{1,1} a_{1,2}$	$d_{1,1} d_{1,2}$
$k_2$	$a_{2,1}$	$d_{2,1} d_{2,2}$
.....	.....	.....
$k_n$	$a_{n,1} a_{n,2} a_{n,3}$	$d_n$

Атрибут	Заголовок
$k_1$	$a_{1,1} a_{1,2} d_1$
$k_2$	$a_{2,1} a_{2,2} d_2$
.....	.....
$k_n$	$a_{n,1} a_{n,2} a_{n,3} d_n$

де  $a, d$  – дані (будь-які дані)

$k$  – атрибути ( $k \neq k_j$ , тільки один для даної таблиці)

Рис. 2. Вигляд даних до перетворення

З прикладу видно, що дані можуть бути як у різних стовпцях, так і в одному; особливий випадок, коли вони являють собою однотипні дані (наприклад, прізвище, ім'я, по батькові). Загалом *опис та обробка текстів, таблиць* – це морфологічний, лексичний і синтаксичний аналіз фраз для виділення інформації щодо об'єктів (людей, географічних понять, наприклад, адреси

організацій, продукти, матеріали та ін.), їх взаємозв'язків. Розуміння цього надалі дасть змогу провести структурування виявлених фактів і зв'язків у вигляді реляційних таблиць, які потім можуть бути завантажені до бази даних [12].

Вигляд, який мають дані після структурування наведено на рис. 3.

Атрибут	Заголовок 1	Заголовок 2	Заголовок 3	.....	Заголовок n
1	Сидоренко	І.	І.	.....	1960
2	Петренко	Іван	Петрович	.....	68
.....	.....	.....	.....	.....	.....
5125	Яценко	Степан	.....	.....	1972

Математично це можна відобразити так:

Атрибут	Заголовок 1	Заголовок 2	Заголовок 3	.....	Заголовок n
$k_1$	$a_{1,1}$	$a_{1,2}$	$a_{1,n}$	.....	$d_1$
$k_2$	$a_{2,1}$	$a_{2,2}$	$a_{2,n}$	.....	$d_2$
.....	.....	.....	.....	.....	.....
$k_n$	$a_{n,1}$	$a_{n,2}$	$a_{n,n}$	.....	$d_n$

Рис. 3. Вигляд даних після перетворення (кінцевих даних)

З рис. 3 видно, що кожне поле таблиці знаходиться окремо на перетині горизонталі та вертикалі, кожний запис має тільки один атрибут і за його допомогою може бути ідентифікований однозначно.

У процесі завантаження та перетворення дані проходять основні стадії, кожна з яких реалізується у вигляді окремої фази процесу перетворення даних (табл. 1).

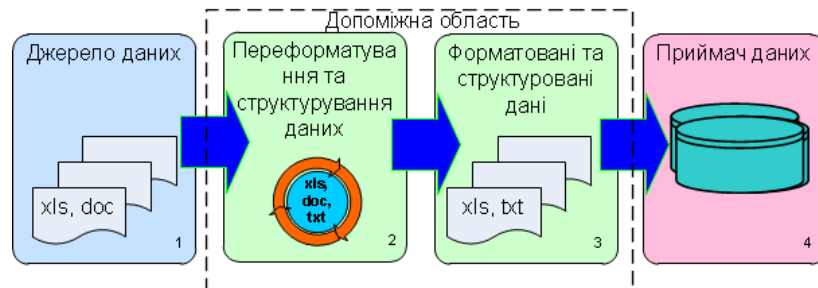
Таблиця 1

**Фази процесу перетворення даних**

№	Назва	Опис
1	Витягування	Стадія витягування даних з джерела і завантаження їх в допоміжну область
2	Виявлення помилок	Дані проходять перевірку на відповідність специфікаціям і потенційну можливість завантаження в базу даних
3	Перетворення	Дані групуються і перетворюються згідно з моделлю даних
4	Розподіл	Дані розподіляються на декілька потоків (формується декілька таблиць), залежно від способу, яким вони мають бути завантажені до бази даних
5	Вставка (завантаження)	Підготовлені дані поступають до бази даних

Фази 1–3 є найбільш громіздкими в обробці та аналізі, потребують значної уваги та одноманітного повторення операцій до досягнення повністю структурованого вигляду даних. Фази 4 та 5 виконуються стандартними засобами системи керування базою даних.

Далі розглянемо перші три фази більш детально. На кожній стадії слід визначитися з початковими джерелами (Word чи Excel), допоміжною областю (Word, Excel та TXT) і кінцевим приймачем – базою даних (рис. 4).



**Рис. 4. Кроки процесу перетворення даних**

Excel найбільш підходить для обробки інформації у форматі чисел, зазвичай, більша частина інформації в джерелах, знаходиться саме в цьому форматі. Також табличний процесор Excel можна використати для заповнення пустих полів визначеними значеннями, яке потім під час аналізу можна використати як *маркер відсутньої інформації*.

Таблиця Excel – це набір рядків, у якому існують більш чіткі, в плані визначень форматів, обмеження, на відміну таблиці Word, у якій не враховується формат даних [13]. Для побудови приймача даних, здатного коректно сприймати всі команди та формати Excel з обробки списків, необхідно керуватися певними принципами та правилами, а саме:

створюваний список повинен мати постійну кількість стовпців;

кількість рядків є змінною, що дає змогу пізніше додати, видалити або переставити записи;

у кожному стовпчику має міститися однотипна інформація;

порожні рядки/записи мають бути видалені, а стовпці заповнені.

*Перша фаза* – витягування. На цій стадії виконується витягування даних із джерела і завантаження їх у допоміжну область (рис. 4). Необхідно проаналізувати та підготувати кінцеву форму приймача даних за принципами описаними вище.

Дані, які отримуємо з джерела, наприклад, мають такий вигляд у форматах Word чи Excel (рис. 5).

У наведеному прикладі таблиці Excel колонки 3 та 14 під час перетворення будуть розділені автоматично на три записи, водночас ці дані стосуються одного запису, тому і в проміжній таблиці мають оброблятися як один запис (запис з одним ідентифікатором). Далі необхідно визначити ключове поле та створити копію форми приймача даних з додатковим (технічним) ключовим полем.

№	Підрозділ	Ім'я	Вік	Статус
2.	м-р запасу	Олександр Вікторович	15	1 (він-1963р.н.) розлучений
3.	майор запасу	Віктор Володимирович	16	1 (він-1958р.н.) розлучений

Рис. 5. Приклад можливого запису у списку Word та Excel

Якщо позначити кінцеву множину записів, по аналогії з “чорним ящиком”, як множину  $M_{вих}(a,b,c)$ , де  $a, b, c$  – упорядкований набір записів (структуровані дані/записи), тоді джерело даних до перетворення можна зобразити як

$$M_{ex}(c,b,a) \Rightarrow M_{дон}(k,c) \cdot M_{дон}(k,b) \cdot M_{дон}(k,a) \Rightarrow M_{вих}(a,b,c)$$

де  $M_{дон}$  – допоміжна множина даних;

$k$  – додаткове (технічне) ключове поле в проміжній таблиці.

Додаткове ключове поле дає змогу врахувати у тимчасових проміжних таблицях відсутність даних (ключове поле = 0), таким чином автоматично визначаючи умову, що ключове поле, за яким визначається однозначність усього запису, має заздалегідь задане відоме і неповторюване значення, а саме значення  $k_i \neq 0$  та  $k_i \neq k_j$ .

Визначившись з кількістю записів та значенням ключового поля, можна переходити до подальшої обробки первинних даних.

Друга фаза перетворення – виявлення помилок. У наведеному прикладі формату Word (див. рис. 5), у другому стовпчику у записах 2 та 3 міститься за змістом ідентична інформація, але за текстом вона відрізняється, отже має бути приведена до одного вигляду. Подальшу обробку доцільно проводити за стовпчиками, щоб оптимально задіяти можливості Word. Після обробки тексту і первинного розділення даних по полях, результат аналізується за стовпчиками з використанням вбудованих інструментів сортування та фільтрації [13, 14]. Ці інструменти доцільно використовувати як у Word, під час попередньої обробки, так і в Excel на кінцевих етапах. Вбудований алгоритм сортування значно прискорює процес обробки інформації, що довів ще в

$M_{ex}(c,b,a)$ , де  $c, b, a$  – невпорядкований набір записів (неструктуровані дані/записи). Для переходу від однієї множини до іншої необхідний заздалегідь підготовлений і відомий набір інформації (шаблон). Перехід від джерела до приймача математично можна відобразити так:

XIX ст. американець Герман Холлерит, коли реалізував машинне сортування “окремо для кожного стовбця” [15].

Через інструмент фільтрації проводиться відсіювання “правильних” даних від “шуму”. Фільтрація на етапі первинної обробки даних знижує гостроту проблеми недостовірності, хоча уникнути усіх помилок неможливо. Результатом роботи на цьому етапі буде таблиця (див. рис. 3), в полях якої знаходиться тільки одне значення.

Отже основні етапи другої фази “виявлення помилок” можна визначити так:

список із потрібною інформацією у складі з технічним ключовим полем і колонкою у якій проводитимуться зміни, із формату Excel копіюються у формат Word;

у Word табличний варіант через інструмент перетворення таблиць, перетворюємо на текст, до того ж як роздільник слід виставляти “знак табуляції”;

заміну пропусків між словами доцільно проводити на “знак табуляції”, і далі використати його як роздільник під час формування нової таблиці;

отриманий варіант тексту (у форматі – “слово, знак табуляції, слово”) перетворюємо у табличний варіант, число стовпців запропонує Word. Отримана таблиця копіюється в Excel;

аналіз отриманого результату слід проводити за стовпчиками за допомогою

інструменту сортування за низхідним/висхідним порядком.

У разі необхідності усі етапи фази “виявлення помилок” повторюються до досягнення необхідного результату – коли поле містить тільки один елемент даних.

*Третя фаза* – перетворення. Кінцевим результатом має бути текстовий файл з розділювачем, який готовий до завантаження у базу даних. Перетворення, так само, як і виявлення помилок доцільно проводити з використанням технічного (допоміжного) ключового поля. Рекомендації щодо кількості стовпців і використання ключового поля аналогічні попередньому процесу.

Під час запропонованого процесу перетворення даних мають використовуватись загальні правила:

1. *Під час формування таблиці у Word*, як розділювач доцільно використовувати знак табуляції.

2. *Проміжні дані*, під час перетворення, необхідно переносити разом з ключовими полями, а у разі відсутності таких ключових полів, необхідно їх створити.

3. *Для масового видалення непотрібних даних*, доцільно створити шаблон видалення з урахуванням ключового поля.

4. *Стандартні ключові поля*, для проміжного перетворення доцільно доповнити додатковими цифровими ключовими полями оптимальної довжини.

5. *Для проміжного перетворення*, таблиці з великою кількістю колонок доцільно розбити на декілька таблиць з максимальною кількістю колонок до шести.

Слід зазначити, що наведений підхід було апробовано під час впровадження підсистем управління нерухомим військовим майном та забезпечення житлом військовослужбовців ІС управління адміністративно-господарськими процесами ЗС України, а також створення макету автоматизованого робочого місця керівника вищого рівня за напрямком управління нерухомим військовим майном. До того ж час на підготовку даних до первинного завантаження із залученням до трьох фахівців було скорочено із запланованого одного року до одного місяця.

Отже на практиці доведено, що дотримання запропонованих правил дає змогу не тільки спростити та оптимізувати первинну підготовку даних для наповнення реляційної бази даних, а також, спростити тестування ІС на етапі її створення. Це також позбавляє розробників можливості зробити “власні

помилки”, дає змогу поєднати технологічні прийоми з програмами незалежних розробників, які виконують спеціалізовані функції, унікальні для конкретного випадку.

**Висновок.** Процес підготовки тестових даних є складним, тривалим і циклічним, тому його оптимізація дасть змогу більш якісно та ефективно використовувати людський і фінансовий ресурс, а під час наповнення бази даних, частково автоматизувати цей процес та звести виникнення помилок, які залежать від людини, до мінімуму.

У статті розглянуто підхід щодо автоматизації процесу підготовки та обробки даних до первинного завантаження в базу даних. У результаті запропоновано послідовність дій на основі використання загальноживаного інструментарію, проведено формалізацію процесу підготовки даних до первинного завантаження для проведення тестування інформаційних систем.

Напрямом **подальших наукових досліджень** може бути вирішення питань інтеграції баз даних під час перетворення даних, їх передавання і обробки в інформаційних системах.

#### СПИСОК ВИКОРСТАНОЇ ЛІТЕРАТУРИ

- Діджиталізація як основний фактор розвитку бізнесу. URL: <http://confmanagement.kpi.ua/proc/article/view/201186> (дата звернення: 02.08.2020).
- План дій щодо впровадження оборонної реформи. URL: <https://www.mil.gov.ua/diyalnist/reformi-ta-planuvannya-u-sferi-oboroni/22082016-04.html> (дата звернення: 06.08.2020).
- Концепція інформатизації Міністерства оборони України : затв. наказом Міністерства оборони України від 17.09.2014 р. № 650.
- Пріоритетні напрямки реформи Міністерства оборони та Збройних Сил України на 2019–2020 роки. URL: <https://www.mil.gov.ua/prioritetni-napryamki-reformi-ministerstva-oboroni-ta-zbrojnih-sil-ukraini-na-2019-2020-roki.html> (дата звернення: 03.08.2020).
- ERP-системи. URL: <http://tehasu.ru/tehasu/articles/160-articles2.html> (дата звернення: 02.08.2020).
- Основи інформаційних систем : навч. посіб. / за ред. проф. В. Ф. Ситника. Київ : КНЕУ, 2007. 252 с.
- Комп’ютерний контент-аналіз: проблеми та перспективи вирішення. *Методологія, теорія та практика соціологічного аналізу сучасного суспільства* : зб. наук. праць. Вип. 15. Харків : ХНУ, 2009. С. 335–340.
- ІТ-платформа онтологічних інформаційно-аналітичних експертних систем. URL: <http://ontology4.inhost.com.ua/?fname=TODO&detail=ТОДОС> (дата звернення: 02.08.2020).



9. Живицкая Е. Н., Едемская О. П. Системный анализ и проектирование информационных систем : учебно-метод. пособ. для студентов специальности I-40 01 02-02 Информ. системы и технологии в экономике. Минск : БГУИР, 2005. 59 с.
10. Этапы проектирования данных. URL: [http://www.mstu.edu.ru/study/materials/zelenkov/ch\\_5\\_1.html](http://www.mstu.edu.ru/study/materials/zelenkov/ch_5_1.html) (дата звернення: 03.08.2020).
11. Проектирование баз данных. URL: [http://ru.wikipedia.org/wiki/Проектирование\\_баз\\_данных](http://ru.wikipedia.org/wiki/Проектирование_баз_данных) (дата звернення: 04.08.2020).
12. База данных. URL: [http://ru.wikipedia.org/wiki/База\\_данных](http://ru.wikipedia.org/wiki/База_данных) (дата звернення: 02.08.2020).
13. Office: довідка та інструкції. URL: <http://office.microsoft.com/uk-ua/support/#> (дата звернення: 04.08.2020).
14. Устранение неполадок и решение проблем в Microsoft Office XP. URL: <http://support.microsoft.com/ph/2533/uk-ua> (дата звернення: 02.08.2020).
15. Холлерит Г. Галерея портретов. URL: [http://informat444.narod.ru/museum/1\\_17\\_115.htm](http://informat444.narod.ru/museum/1_17_115.htm) (дата звернення: 06.08.2020).

Стаття надійшла до редакційної колегії 24.09.2020

## The justification of approach concerning of data preparation for initial loading for testing Defense Resource Management Information Systems

### Annotation

The implementation of the Unified Defense Resources Management Information System for requires a prudent approach in design of not only the infrastructure, but also unified data model that will be stored in a unified repository.

Creation of such model requires a properly design data, which in turn requires proper formation and its preparation. This process is quite long, complex and cyclical and will include certain stages of transformation, extraction and structuring of information.

*The main purpose of the article* is to simplify the process of preparing primary data for loading into a repository with relational connections. Make this process repetitive and as independent as possible from person. Using this approach, we can minimize or even avoid the use of expensive software platforms and not involve third-party professionals. Such optimization will allow more efficient and rational use of software and human resources partially automate it and, if necessary, parallel the process and minimize errors.

The article considers a modern approach how to automate the process of preparation and processing of data for initial uploading data into the database. As a result, a sequence of actions based on the use of commonly used set of tools is proposed, the process of data preparation for the initial download for testing information systems is formalized.

The approach is given was tested during the introduction of subsystems for the management of military real estate and the provision of housing for servicemen of the Information System Management of administrative and economic processes of the Armed Forces of Ukraine. All at once, the time for preparing data for the initial download with the involvement of up to three specialists was reduced from the planned one year to one month.

**Keywords:** defense resource management; preparation of data for testing; data conversion; data structuring; structured data.

УДК 004.056 DOI: <https://doi.org/10.33099/2304-2745/2021-1-71/106-115>

Беляченко В. В. (0000-0003-3938-5158)  
Бобров С. В., канд. техн. наук, доцент (0000-0002-9647-9700)  
Утюшев М. К. (0000-0002-7386-7831)  
Мулявка А. С. (0000-0002-3113-0719)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського

## Основні відмінності та особливості структурного та об'єктно-орієнтованого підходів до проектування інформаційних систем військового призначення

**Резюме.** У статті розглянуто переваги та недоліки двох підходів щодо проектування інформаційних систем. Вибір структурного і об'єктно-орієнтованого підходу залежить від переваг обраної методології, стану цільового інформаційного середовища, обсягу та складності системи, яку необхідно проектувати. Запропоновано алгоритм вибору методології проектування на етапі концепції на основі семи ключових критеріїв.

**Ключові слова:** інформаційна система; проектування інформаційних систем; структурний аналіз; об'єктно-орієнтований аналіз; критерії вибору моделі проектування.

**Постановка проблеми.** Закріплення в Конституції України стратегічного курсу на набуття членства України в ЄС та НАТО зумовило зростання необхідності використання інформаційних технологій управлінської діяльності у військовій сфері. Управлінська діяльність у військовій сфері охоплює матеріальний, інформаційний та фінансовий потоки ресурсів і потребує інтелектоємних інструментів високого рівня. Досвід збройних конфліктів за участю збройних сил провідних країн світу (ПКС) свідчить, що без автоматизації процесів управління матеріальними та нематеріальними ресурсами неможливо ефективно забезпечити операції військ (сил). Створення автоматизованих систем управління логістичним забезпеченням як інформаційної системи військового призначення (ІС ВП) були першочерговими завданнями комплексної інформатизації процесів управління оборонними ресурсами та військами в США й інших країнах – членах НАТО. Ускладнення під час реалізації проектів створення ІС ВП у ПКС загострили увагу до низки проблемних питань, зокрема, проблеми вибору методології проектування, які зменшували б складність проектних завдань і мінімізували проектні ризики.

**Аналіз останніх досліджень та публікацій.** Вимоги до сучасних ІС ВП і їх складність постійно зростає, відповідно, загострюється проблема ефективного управління процесами створення, тестування та впровадження ІС ВП в інформаційне середовище військового відомства. Комплексне вирішення цієї проблеми –

складна і довготривала робота, яка потребує високої кваліфікації задіяних у ній спеціалістів. Попри технологічний прогрес, завдання у сфері проектування ІС ВП виконуються на інтуїтивному рівні згідно з досвідом і прогностичними здібностями учасників проекту і обґрунтовуються суб'єктивними оцінками з ознаками конфлікту інтересів. Експериментальна перевірка проектних рішень на наступних стадіях розроблення може виявити помилку вибору методології і технології проектування як один з наслідків недостатньо ретельного підходу до збору вимог до майбутньої ІС ВП і точності опису процесів. Досвід виконання ДКР “Ніка-1” та ін. ІС ВП в Збройних Силах України, а також досвід розроблення ІС ВП у Збройних силах США та інших ПКС, свідчить, що вартість виправлення помилок, які було зроблено на ранніх стадіях проекту, з часом значно зростає [1, 3–5].

Зокрема, під час впровадження Системи Підтримки Бою в Експедиції (англ. – ECSS) у Військово-повітряних силах США спостерігались значні відхилення від попередніх оцінок обсягів проектних ресурсів і часу реалізації [1], що разом з іншими причинами підтверджує необхідність критичного розгляду методологій проектування ІС ВП для обґрунтованого вибору з урахуванням комплексної інформатизації та реінжинірингу процесів управління потоками ресурсів. У сфері економіки, згідно з щорічним звітом Інституту проектного менеджменту (англ. – PMI) за 2016 р. про результати опитування учасників проектів з усіх галузей економіки (сфера ІТ

становила 17 % від загального числа опитаних учасників проєктів), неточність збору вимог і первинних даних, на підставі яких серед інших проєктних стратегій обирається методологія і технологія проєктування ІС, посідає третє місце серед причин невдалих проєктів (у 37 % проєктів респонденти називали ці причини серед інших трьох основних причин) [2, 8]. Виправлення помилок структурного та/або об'єктно-орієнтованого аналізу, виявлених на стадії робочого проєктування, збільшують вартість і тривалість проєкту. Виявлення та усунення помилок на етапі тестування ще дорожче і довше. Усунення помилок на етапі експлуатації може перевищувати вартість усього проєкту та в деяких випадках призводити до відмови від розроблення загалом і дискредитації як розробників, так і замовників.

Вибір методології проєктування, засобів супроводження ІС, тестування її компонентів та інкрементів на всіх стадіях розроблення є складними та відповідальними *управлінськими рішеннями*, від яких залежить результативність та ефективність проєкту загалом. Порядок розв'язання проблеми вибору з погляду теорії прийняття рішення розглянуто в роботі [3]. Під час пошуку рішення визначаються критерії, які впливають на це рішення, їх вагомість і порядок розгляду, збираються та аналізуються дані щодо альтернатив, визначаються і оцінюються ризики та обмеження щодо об'єкта. Відомості про переваги та недоліки структурного та об'єктно-орієнтованого підходу, які придатні на роль чинників впливу на управлінські рішення були описані дослідниками раніше та зафіксовані в багатьох джерелах 90-х – початку 2000-х, зокрема [4–10]. Проте дані щодо новітнього проєктного досвіду [2] свідчать, що на етапах розроблення, тестування програмних рішень продовжують виявлятися ускладнення, зумовлені неточністю збору вимог до проєкту, поспішністю висновків щодо первинних даних, недбалістю під час моделювання тощо.

Структурний і об'єктно-орієнтований підходи до проєктування системи, результатом яких є сукупність моделей об'єкта інформатизації попри особливості, переваги і недоліки, описані в роботах [4–6, 12–14], мають спільне – об'єкт інформатизації, що дає змогу зробити припущення про можливість успішного комбінування обох підходів у межах ширшої концепції – архітектурного підходу [12].

Комбінація підходів реалізована в методології моделювання діяльності організації ARIS (англ. Architecture of Integrated Information Systems), яка об'єднує структурні та об'єктно-орієнтовані методи для формування цілісного погляду на процеси, об'єкти та потоки інформації в організації. Близькість методів моделювання предметної сфери в структурному та об'єктно-орієнтованому підходах проілюстрована в роботі [11], у якій обґрунтовується раціональність їх поєднання. Результатом проєктування на етапі концепції є “моделі, які дають змогу зрозуміти структуру майбутньої ІС, досягти узгодження суперечливих вимог та окреслити план реалізації” [9]. Висновки дослідників щодо вибору методології проєктування, або їх комбінації, сходяться на тому, що кінцевий вибір архітектора системи значною мірою зумовлений критеріями, які безпосередньо залежать від такого: що (процеси та об'єкти); у якому обсязі (вимоги) передбачається автоматизувати; що відомо про існуюче інформаційне середовище (початкові дані); чи існує типове проєктне рішення; яке передбачено ресурсне забезпечення (час, фінанси, кадровий потенціал); які є проєктні обмеження; у якому організаційному та інформаційному середовищі перебуватиме розроблення на кожному етапі ЖЦ системи та які проєктні ризики потребують оброблення.

Проте більшість проєктів усе ж виконуються з використанням одного з підходів, що дає змогу авторам статті зробити припущення про можливість швидко обрати методологію проєктування завдяки використанню декількох ключових критеріїв. Швидкий вибір дасть змогу зосередитись на зборі загальних вимог до системи та аналізі первинних даних, згідно з якими архітектор системи обирає остаточне рішення щодо організаційних і технологічних форм, у яких створюватиметься АС, або її компоненти, та який підхід застосувати для опису і проєктування системи – структурний чи об'єктно-орієнтований, або комбінацію підходів, з урахуванням складності поєднання, якщо є необхідність узгодження розроблюваної системи з ієрархією вже існуючих систем та актуальним інформаційним середовищем.

**Метою статті** є огляд підходів щодо проєктування ІС, систематизація особливостей та обґрунтування критеріїв, на які розробники ІС ВП можуть спиратись під час первинного вибору методології та технології проєктування.

### **Виклад основного матеріалу.**

*Проектування* – це процес пошуку, досліджень та реалізації способів створення системи, що задовольняє вимогам до її функціональності з огляду на обмеження часу, коштів і доступність технології та охоплює три сфери:

проектування об'єктів даних, які будуть реалізовані в базі даних;

проектування програм, екранних форм, звітів, які забезпечуватимуть виконання запитів до даних;

проектування певного середовища, топології мережі, конфігурації апаратних засобів, використовуваної архітектури (файл-серверної або клієнт-серверної), способів обробки даних (паралельна, розподілена).

Мета проектування полягає у забезпеченні надійного та ефективного функціонування ІС ВП та конструктивної взаємодії замовника (користувачів) і розробників ІС ВП. У процесі проектування ІС ВП удосконалюється як інструмент реінжинірингу управлінських процесів органів військового управління.

Основу проекту будь-якої ІС складають такі компоненти [3–5, 12]:

методологія проектування;

технологія проектування;

стандарты і методики проектування;

інструментальні CASE-засоби

проектування як окремих елементів життєвого циклу програмного засобу (надалі ЖЦ ПЗ), так і інтегровані набори інструментів, які підтримують ЖЦ ПЗ, у яких реалізована підтримка процесів створення ІС.

Між компонентами діє щільний зв'язок, а саме: реалізація методології здійснюється через конкретні технології, кожна технологія підтримується відповідними стандартами і методиками, а інструментальні засоби забезпечують реалізацію процесів проектування, що описані у методиках і стандартах. *Методологія проектування* – це знання про організацію процесу розроблення системи, методи управління цим процесом, які гарантують дотримання вимог як до самої системи, так і до характеристик процесу її розроблення і засоби проектування. Найважливіші завдання, які мають виконуватись учасниками проекту під час створення ІС:

відповідність розроблюваної ІС меті та завданням організації, а також вимогам щодо обсягів автоматизації її функціональних процесів;

гарантоване створення системи з обмеженням часу та бюджету;

підтримання порядку супроводження, модифікацій і масштабування системи для забезпечення її адаптації до зміни умов;

забезпечення відповідності ІС вимогам до відкритості та здатності до масштабування;

забезпечення можливості спадкоємності розробки через використання елементів існуючого інформаційного середовища організації.

Головний зміст *технології проектування* – це технологічні інструкції, які є сукупністю з трьох складових:

послідовності виконання технологічних операцій, передбачених процесом проектування;

критеріїв щодо оцінювання результатів виконання технологічних операцій;

нотацій (тобто графічних і текстових засобів) для опису системи, що проектується.

Кожна технологічна операція потребує матеріальних, інформаційних і людських ресурсів, зокрема:

даних, отриманих від попередньої операції;

методичних матеріалів, інструкцій, нормативів, стандартів;

програмних і технічних засобів; виконавців.

Результати здійснення операції мають бути подані у стандартному вигляді, що гарантує його адекватне сприйняття під час виконання наступної технологічної операції для якої вони є вхідними даними.

Низка *загальних вимог до технології проектування*, розроблення і супроводження ІС є такою:

підтримувати повний ЖЦ ІС;

гарантувати досягнення цілей розроблення із заданою якістю та у межах встановленого часу;

забезпечувати можливість розподілу (декомпозиції) великої ІС на кілька складових частин (підсистем), які розробляються окремими групами виконавців із подальшою інтеграцією цих частин;

надавати можливість проектування підсистем малими групами, що гарантує керованість колективом та підвищує продуктивність унаслідок мінімізації кількості зв'язків із зовнішнім середовищем;

забезпечувати мінімальний час для отримання працездатної системи;

давати можливість керувати конфігурацією проекту, вести облік і

синхронізацію версій проекту та його складових;

забезпечувати незалежність проектних рішень від засобів реалізації, – систем управління базами даних, операційної системи, мов програмування тощо.

Існують дві основні парадигми проектування, які реалізують два різних підходи до опису систем [3–5]:

структурна (процесно-орієнтована), яка спирається на каскадну модель ЖЦ ІС;

об'єктно-орієнтована, яка спирається на ітеративну модель ЖЦ ІС.

Основні відмінності та особливості використання цих підходів у такому [6]:

1. Структурний аналіз (англ. – Structured Analysis або SA) і структурне проектування (англ. – Structured Design або SD) бере свій початок від класичного системного аналізу [7]. Сутність структурного підходу до початку розроблення ІС полягає в декомпозиції опису системи за допомогою ієрархічного набору діаграм та виокремлення функцій, які підлягають автоматизації. Система розкривається до функціональних підсистем, які зі свого боку розподіляються на окремі завдання. Процес деталізації триває до рівня окремих процедур, у яких ще є вхід і вихід. Спроба подальшої деталізації призводить до втрати цілісності та пов'язаності з іншими елементами системи. Під час виконання структурного аналізу система має зберігати цілісність, взаємопов'язаність складових компонентів і загальне підґрунтя. Якщо розробляти систему у напрямку “знизу-догори”, тобто від окремих завдань до всієї системи, то втрачається цілісність і виникають проблеми взаємодії окремих компонентів. Усі найпоширеніші методології структурного підходу [8] базуються на шести загальних принципах [9], два з яких є основними:

принцип “розділяй і володай” – декомпозиційний підхід до розв'язання складних проблем завдяки їх розкладанню на низку простіших і відносно незалежних один від одного завдань, придатних для аналізу та удосконалення під час практичної реалізації;

принцип ієрархічного упорядкування – принцип організації складових частин проблеми та упорядкування як ієрархічної деревоподібної структури з додаванням нових деталей на кожному рівні.

Додаткові принципи:

принцип абстрагування – виділення суттєвих аспектів системи серед несуттєвих;

принцип формалізації – необхідність чіткого методичного підходу до аналізу;

принцип несуперечності – обґрунтованість та узгодженість елементів;

принцип структурування даних – усі дані мають бути структуровані та ієрархічно впорядковані.

У структурному аналізі використовуються дві головні групи методологій, які застосовуються для опису системи:

1) функцій, які виконує система (SADT-моделювання);

2) відношень між даними, яким відповідають функціональні моделі та моделі потоків даних (SSADM-моделювання).

На етапі проектування системи функціональні моделі та моделі потоків даних доповнюються діаграмами, що відображають архітектуру системи та ПЗ. Склад діаграм у моделях залежить від необхідного рівня повноти опису системи. Найпоширенішими засобами структурного аналізу є:

SADT (від англ. Structured Analysis and Design Technique) – функціональні моделі та відповідні функціональні діаграми;

DFD (англ. – Data Flow Diagrams) – діаграми потоків даних;

ERD (англ. – Entity Relationship Diagrams) – діаграми “сутність-зв'язок”;

EED (англ. – Entity Event Diagrams) – діаграми “сутність-подія”.

SADT-моделі є типовими для структурного підходу під час проектування систем.

Процес моделювання за методологією SADT складається з етапів:

збір і аналіз інформації щодо предметної області;

документування отриманої інформації;

коригування моделей за допомогою ітеративного рецензування.

На сьогодні методологія SADT використовує формалізовані методи моделювання систем (найчастіше в нотаціях IDEF0 та IDEF3 [7]), які дають змогу отримати опис ІС в обсязі, необхідному для аналізу вимог до системи та ПЗ та переходу до концептуального проектування.

Методологія SSADM (англ. Structured Systems Analysis and Design Method) також базується на структурному аналізі систем і графічному поданні інформації у вигляді комплексу структурних моделей: логічної структури даних (DFD високого рівня + ERD), деталізованої структури інформаційних потоків (DFD), змін структур у динаміці (EED) – змін життєвого циклу сутностей. Процес моделювання за методологією SSADM

аналогічний як SADT. Побудова цих моделей дає змогу перейти до процесу проектування архітектури системи та програмного засобу під час створення ІС.

**Методологія структурного підходу** використовуються в каскадній моделі ЖЦ ІС, результативність якої була перевірена на практиці:

однорідних ІС, де кожен додаток становить єдине ціле;

ІС, для яких на початку розроблення точно сформульовані вимоги, що сприяє пошуку розробниками оптимальних програмно-технічних рішень для ІС зі складними обчисленнями та необхідністю роботи в режимі реального часу.

На базі каскадної моделі було створено популярний в кінці 90-х – початку 2000-х програмний комплекс розробника Oracle Designer [3].

Нині існує достатня кількість інструментальних засобів проектування, що входять до складу програмних засобів, які підтримують повний життєвий цикл програмних засобів та ІС, створених з їх використанням. Наприклад, клієнти SAP безоплатно отримують комплексне програмне рішення SAP Solution Manager 7.2 з управління життєвим циклом усіх ІТ-компонентів організації в мультисистемному інформаційному середовищі і підтримкою моделей проектування від каскадної, V-подібної, спіральної до інкрементно-ітеративної та інших різновидів “гнучких” (agile).

**Основні переваги структурного підходу** до проектування [3, 4, 7, 9]:

засновані на класичному системному аналізі, є процесно-орієнтованими, підходять для описання будь-яких систем, зручні для дослідження предметної області, реінжинірингу бізнес-процесів тощо;

структурні методології дають зрозумілу і просту візуалізацію системи, їх легко сприймають і користувачі, і розробники проекту;

у структурних методологіях акцент зроблено на командній роботі;

чітко визначені етапи, які полегшують управління проектом і дають змогу розробляти системи високої якості;

структурні методології допускають використання засобів перевірки вимог;

SADT і SSADM – класичні, поширені методології в області проектування ІС, існують упродовж тривалого часу і добре перевірені на практиці.

**Основні недоліки структурного підходу** [3–5]:

оскільки структурна методологія є процесно-орієнтованою, то вона ігнорує нефункціональні вимоги до системи, тобто результатом її використання можуть бути не ідеальні рішення з точки зору використання об’єктно-орієнтованих мов програмування на етапі реалізації проекту (методологія краще відповідає структурним мовам);

оскільки SSAD і SSADM не є ітеративними, то зміна вимог може призвести до перезавантаження практично всього процесу розроблення;

під час використання структурного підходу можуть виникати труднощі у визначенні глибини декомпозиції, тобто моменту, коли доцільно зупинитися та перейти до практичної реалізації моделей.

**Об’єктно-орієнтований підхід до проектування** (від англ. Object-Oriented Analysis and Design, OOAD) – це підхід до інженерії ПЗ, що розглядає систему як групу взаємодіючих об’єктів. Об’єктно-орієнтований аналіз OOA (від англ. Object-oriented Analysis, OOA) використовує методи об’єктного моделювання для аналізу функціональних вимог до системи. Об’єктно-орієнтоване проектування (ООП) (від англ. Object-oriented Design, OOD) має на меті розробити моделі процесів, придатні для аналізу та подальшого створення специфікацій для їхньої реалізації.

Одним з найважливіших результатів специфікацій є технічне завдання. Концептуальною основою ООП є об’єктна модель, яка будується з урахуванням принципів абстрагування, інкапсуляції, модульності, ієрархії, типізації, паралелізму, стійкості. Основними поняттями ООП є клас і об’єкт. Для взаємодіючих між собою об’єктів можна створити моделі, які характеризують їхню статичну структуру або поведінку в динаміці під час розгортання системи (run-time deployment).

Наступну групу важливих понять об’єктного підходу складають поліморфізм (здатність класу належати більш ніж одному типу) та успадкування (побудова нових класів на основі існуючих із можливістю додавання або коригування даних і методів).

У сучасній практиці використовують велику кількість методів моделювання під час ООП, зокрема **IDEF4**. Цей метод дає змогу відображати структуру об’єктів і принципи їхньої взаємодії у контексті різних нотацій і об’єктних моделей. Для опису об’єктно-

орієнтованих моделей використовують спеціальні мови.

Найпопулярнішою мовою ООП є UML (англ. - the Unified Modeling Language). UML – це відкритий стандарт, який використовує графічні позначення для створення абстрактної моделі системи та був створений для визначення вимог до системи, візуалізації, проектування та документування програмних рішень. Методи описання результатів аналізу та проектування UML семантично близькі до методів програмування на сучасних об'єктно-орієнтованих мовах. За допомогою CASE-засобів на підставі UML-моделей реалізована генерація програмного коду. На UML можна розробити докладний план системи, що містить системні функції і бізнес-процеси, схеми баз даних, програмні компоненти багаторазового використання тощо [3, 8].

*Основні переваги об'єктно-орієнтованих методологій.* Більшість цих переваг є наслідком об'єктно-орієнтованого програмування, а саме [3–5, 13, 14]:

мультимодельне представлення складних інформаційних систем дає змогу уніфікувати та інтегрувати знання з різних дисциплін усіх учасників проекту для адекватного бачення майбутньої системи з максимально можливих точок зору;

під час розроблення об'єктів зі складною взаємодією аналітик акцентує увагу на іншому рівні деталізації, ніж це можливо в структурному підході, а стандартизація об'єктів збільшує рівень розуміння проекту;

спрощення та прискорення програмної реалізації системи на відміну від структурних методологій завдяки автоматизованим засобам візуального та імітаційного програмування з можливістю прямого і зворотного генерування коду найпоширенішими мовами програмування;

модульність, розширення атрибутів і поведінки об'єктів, можливість повторного використання коду в інших проектах (як наслідок незалежності об'єктів та їх інкапсуляції), що підвищує продуктивність розроблення коду порівняно з традиційними методами програмування, скорочує вартість і тривалість проектування, програмування і тестування ІС та сприяє поліпшенню якості подальших проєктів;

відсутність чіткого розподілу між фазами аналізу і розроблення, що забезпечує взаємодію з користувачами до завершення проєкту;

швидке генерування коду вивільняє час і ресурси проєкту на ретельне опрацювання

вимог замовника до системи, об'єктно-орієнтований аналіз і проектування, що зменшує проєктні ризики розробки системи і збільшує цінність впровадження для замовника;

якісніше опрацювання вимог до ІС, моделювання та швидке розроблення загалом вивільняє час і ресурси проєкту на ретельніше тестування розроблених ІС, що дуже важливо в гетерогенному середовищі вже існуючого інформаційного середовища;

відсутність жорстких обмежень щодо впровадження системи, що дає змогу реалізувати проєкти створення ІС для функціонування у різних середовищах;

велика кількість програмістів, які використовують об'єктно-орієнтовані мови програмування і, відповідно, суттєвіша підтримка виробників ПЗ і розробників мов програмування, які надають великі бібліотеки перевірених практикою об'єктів з коректними кодами, що зменшує ризики під час розроблення складних ІС і їх подальшого супроводження завдяки модульному дизайну;

модульний дизайн дає змогу працювати над одним проєктом різним командам розробників та організувати процеси розроблення з використанням аутсорсінгової моделі з використанням принципів спільного розроблення застосунків JAD (Joint Application Development);

модульний дизайн дає змогу оновлювати окремі частини ІС у разі виникнення проблем без необхідності внесення значних змін у дизайн інших частин ІС.

*Недоліки об'єктно-орієнтованих методологій* [3–5, 10, 13, 14]:

об'єктно-орієнтований підхід надмірно фокусується на коді, внаслідок чого поєднання об'єктного програмування з аналізом функцій системи є проблематичним;

читання об'єктно-орієнтованого коду не дає бачення загальної картини і часто неможливо переглянути всі функції, які викликаються функцією, яка була змінена;

ускладнений пошук причин виникнення помилок у коді через необхідність відстеження потоку виконання по всіх об'єктах і класах через які він пройшов та який до того ж може багато разів переміщуватись між декількома функціями-членами, перш ніж потік перейде до іншого об'єкта. Унаслідок цього іноді неможливо швидко виявити помилки потоку виконання за допомогою простого перегляду коду, створеного під час об'єктно-орієнтованого

проектування на відміну від коду, створеного мовою низького рівня (Assembly code);

проблематичність відстеження потоків виконання і, відповідно, визначення більш ефективного з них під час виконання функцій;

визначення всіх класів і об'єктів, необхідних для розроблення складних інтегрованих інформаційних систем, є непростим завданням і потребує специфічної і довгої підготовки розробників ІС та залучення бізнес-аналітиків;

програми, які створюються на основі взаємодії об'єктів є складнішими для розуміння, а деякі методи програмування, зокрема успадкування та поліморфізм, викликають когнітивні ускладнення;

об'єктному підходу до моделювання даних складніше співіснувати з реляційними моделями даних, які присутні в переважній більшості вже існуючих ІС, тому нові ІС часто розробляються, або модифікуються з використанням комбінації об'єктно-орієнтованих мов програмування і реляційних баз даних;

наслідком об'єктного підходу та програмування різних модулів окремими командами програмістів під час створення великих ІС є також випадки нерозуміння яким чином обробляти помилки потоку виконання, якщо програміст або команда програмістів не були знайомі з об'єктами, з якими працювала інша команда програмістів;

програми, створені об'єктно-орієнтованими мовами загалом працюють повільніше, ніж програми створені процесно-орієнтованими мовами, оскільки потребують виконання більшої кількості інструкцій і є більш вибагливими до продуктивності апаратної платформи;

не підходить для всіх типів завдань: є завдання, які краще піддаються стилю функціонального програмування, стилю логіки програмування або стилю програмування на основі процедур, а застосування об'єктно-орієнтованого програмування в таких ситуаціях не призводить до ефективних програм.

З огляду на велику кількість чинників, які можуть впливати на рішення з вибору підходу до моделі проектування та методів програмування ІС ВП, пропонується під час передпроектної підготовки скоротити кількість можливих варіантів проектних моделей, технологій, методик та інструментів проектування через застосування алгоритму вибору моделі проектування та методу програмування за сімома критеріями (рис. 1).

**Критерій 1.** *“Оцінка ймовірності та складності проектних ризиків”*. Якщо передбачається велика кількість інноваційних рішень і не існує близьких аналогів розроблюваної АС ВП, то високий рівень ризикованості обумовлює вибір моделі спірального проектування, під час якого розробник реалізує частину загального набору вимог на прототипі “Х”, оцінює ризики та відповідність прототипу вимогам і переходить до наступного кола проектування з розроблення прототипу “Х+1” з додаванням наступного набору функцій, або поліпшення продуктивності вже розроблених. Для такого проекту підходить **об'єктно-орієнтоване програмування**.

**Критерій 2.** *“Сталість вимог до АС ВП”* застосовується у разі, якщо кількість ризиків незначна, алгоритми рішення добре відомі, є ринкові аналоги для порівняння та оцінювання, то чи передбачає замовник часту зміну вимог. Якщо не передбачає, що є традиційною практикою у сфері безпеки і оборони України, хоча і застарілою через безпрецедентне зростання можливостей сучасних програмно-технічних рішень, розроблюваних програмною індустрією і новітнім підходом до оборонного планування, з урахуванням загроз майбутнього, зокрема у кіберпросторі, то для уточнення додається третій критерій – “складність вимог”. Якщо складність незначна, то оптимальним вибором є класична “каскадна модель” і процесний підхід з використанням методів структурного аналізу.

**Критерій 3.** *“Складність вимог”*. Якщо вимоги складні, що актуально в умовах гетерогенного інформаційного середовища, типового для бюджетних організацій сектору безпеки і оборони із значною кількістю історичних систем, з якими необхідно інтегрувати новий компонент, або здійснити міграцію даних з історичних систем у нову АС ВП і до того ж передбачати дотримання жорстких вимог щодо кібербезпеки вже на етапі концептуального проекту, особливо в контурах інформаційного середовища, де циркулюють дані та інформація з обмеженим доступом, то доцільним є використання “V-моделі” (різновид “каскадної” моделі). При цій моделі розробник на кожному етапі здійснює детальне планування сценаріїв тестування функцій, інтеграції в інфосередовище та окремих модулів, що можливе за умови застосування **процесного підходу** та результатів структурного аналізу.



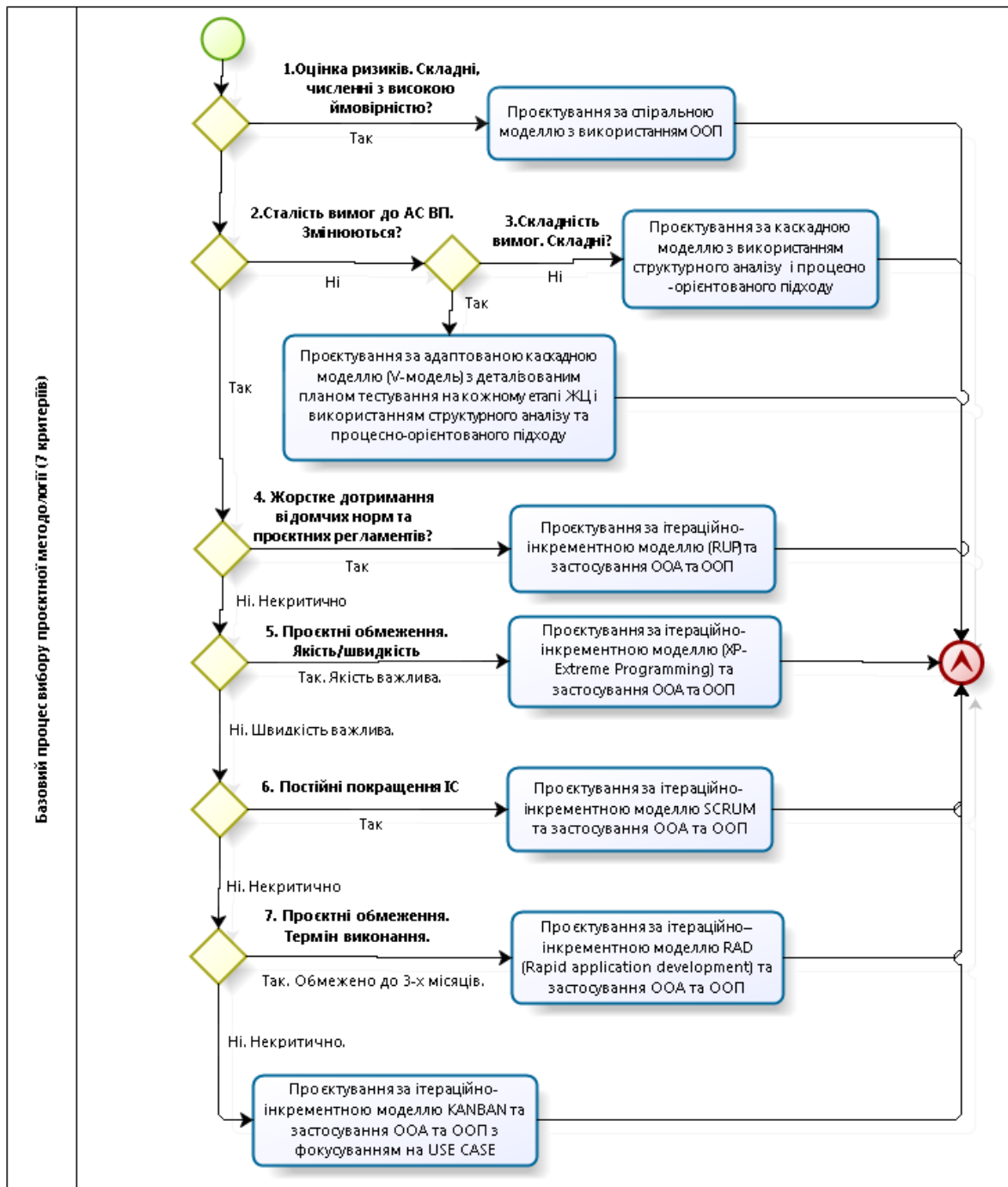


Рис. 1. Алгоритм вибору моделі проектування та методу програмування за сімома критеріями

**Критерій 4.** “Дотримання галузевих вимог і відомчого регламенту” - передбачається необхідність гнучкого реагування на можливу зміну вимог до ІС ВП унаслідок швидких змін інформаційного середовища ЗС України та/або поява проривних технологічних рішень в управлінні військами та/або зброєю. Тоді доцільним є використання ітераційно-інкрементної моделі проектування (наприклад UP, RUP від IBM, або модифікація OpenUP для невеликих проєктів з фокусуванням на управлінні ризиками) та застосування

**об’єктно-орієнтованого аналізу та об’єктно-орієнтованого програмування.**

**Критерій 5.** Проектні обмеження за швидкістю релізів і якістю. У разі, якщо *якість важливіша*, то доцільним є використання ітераційно-інкрементної моделі проектування (наприклад, XP – Extreme Programming), у якій новий функціонал додається в ІС мінімально можливими обсягами одночасно з тестуванням, практикується спільне розроблення застосунків (JAD) та інтеграція з уже розробленою архітектурою системи під час кожного додаванні. Модель придатна для

малих і середніх проєктів. У цьому разі найдоцільніше використовувати ООА та ООП, а проєктній команді потрібно мати архітекторів, аналітиків та розробників, які вже мають досвід використання цієї моделі.

**Критерій 6.** У разі, коли вимога швидкості додавання нових функціональних можливостей в ІС критично важлива, тоді необхідно застосувати шостий критерій – *“необхідність постійних покращень додатків”*, при якому доцільно використовувати модифікацію ітераційно-інкрементної моделі проєктування SCRUM, у якій практикуються періодичні уточнення щодо змісту майбутніх покращень та критичний розгляд щодо результатів додавання попереднього покращення, а також метод спільного розроблення застосунків (JAD) за допомогою ООП. Цей підхід спрацьовує у разі розроблення інноваційних інформаційних технологій, нестандартних програмних рішень, які не мають аналогів і коли команда розробників потребує злагодження.

**Критерій 7.** Проєктне обмеження за терміном виконання. Якщо нагальної потреби в постійному покращенні немає, але є проєктне обмеження за часом, тоді використовується сьомий критерій – *“обмеження часу на цикл розроблення від задуму до релізу від двох до трьох місяців”*. У цьому разі доцільно використовувати ітераційно-інкрементну модель розроблення згідно з методологією RAD (Rapid Application Development), створеної як розвиток спіральної моделі, та методи об’єктно-орієнтованого проєктування, а якщо обмеження на час відсутні або незначні та потрібно додавати нові можливості до ІС згідно з дорожньою картою рівномірного удосконалення, тоді доцільно застосувати різновид методології Agile ітераційно-інкрементну модель проєктування – KANBAN, у якій доцільне використання ООП на основі клієнтських сценаріїв користування системою (USE CASE) для наближення готового продукту до користувацьких потреб.

**Висновок.** Вибір рішення щодо застосування методології та технології проєктування залежить від особливостей проєкту в конкретній організації, вимог до майбутньої ІС, особливостей тієї чи іншої технології, ресурсного забезпечення. Доцільно обирати методологію та методи проєктування, які відповідають рівню складності об’єкта автоматизації, інформаційному середовищу, у якому функціонуватиме ІС ВП, організаційній

зрілості суб’єкта-замовника і проєктним обмеженням (час, бюджет, доступність технологій і кадрів). Метою використання методології та технології проєктування є зменшення складності процесу створення ІС та зменшення ймовірності виникнення типових проєктних проблем завдяки адекватному за витратами набору моделей ІС ВП. З метою зменшення складності прийняття рішення пропонується використати на передпроєктному етапі алгоритм відбору моделі проєктування та методу програмування за сімома критеріями.

Зважаючи на підвищений рівень загрози національній безпеці під час використання ІС ВП створених неналежним чином, критерій наявності досвіду використання проєктних методологій і технологій програмування має входити до загального переліку вимог до виконавців, тому доцільно на стадії попередньої кваліфікації та оцінювання пропозицій претендентів на роль виконавців створення ІС ВП застосовувати критерій *“досвід використання проєктних методологій і технологій програмування окремо чи в комбінації”* у розрізі двох показників: 1) *“доступність персоналу, який виконував роботи з використанням проєктної методології та технології програмування”*, 2) *“кількість проєктів, здійснених з використанням проєктної методології та технології програмування”* за участі заявленого персоналу претендента за 5 років до подачі пропозиції.

Уточнення критеріїв і методів оцінювання проєктного досвіду претендентів на роль виконавців створення ІС ВП є **напрямом подальших досліджень.**

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. John McCain, Carl Levin. Report on the Air Force’s Expeditionary Combat Support System (ECSS). U.S. Senate Committee on Homeland Security & Governmental Affairs. Permanent Subcommittee on Investigations. URL: <https://www.hsgac.senate.gov/subcommittees/investigations/media/permanent-subcommittee-on-investigations-releases-report-on-ecss-program> (дата звернення: 05.06.2020).
2. 8th Global Project Management Survey of Project Management Institute “Pulse of profession 2016”. URL: <https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/pulse/pulse-of-the-profession-2016.pdf> (дата звернення: 05.06.2020).
3. Инюшкина О. Г., Кормышев В. М. Исследование систем управления при проектировании информационных систем : учеб. пособ. Екатеринбург : Форт-Диалог Исеть, 2013. 370 с.

4. Инюшкина О. Г. Проектирование информационных систем (на примере методов структурного системного анализа) : учеб. пособ. Екатеринбург : Форт-Диалог Исеть, 2014. 240 с.
5. Рудаков А. В. Технология разработки программных продуктов : учебник для студ. сред. проф. образования / 7-е изд., стер. Москва : Академия, 2012. 208 с.
6. Карпенко М. Ю., Манакова Н. О., Гавриленко І. О. Технології створення програмних продуктів та інформаційних систем : навч. посіб. Харків : ХНУМГ імені О. М. Бекетова, 2017. 94 с.
7. Черемных С. В., Семенов И. О., Ручки В. С. Структурный анализ систем: IDEF-технологии. Москва : Финансы и статистика, 2003. 208 с.
8. Арлоу Д., Нейштадт А. UML2 и Унифицированный процесс. Практический объектно-ориентированный анализ и проектирование. Санкт-Петербург : Символ-Плюс, 2007. 624 с.
9. Буч Г. Объектно-ориентированный анализ и проектирование с примерами приложений. Москва : И. Д. Вильямс, 2008. 720 с.
10. Asaf Shelly. Flaws of Object Oriented Modeling. Intel Software, Developer Zone, Blogs. URL: <https://software.intel.com/en-us/blogs/2008/08/22/flaws-of-object-oriented-modeling/> (дата звернення: 08.06.2020).
11. Вичугова А. А. Методы и средства концептуального проектирования информационных систем: сравнительный анализ структурного и объектно-ориентированного подходов. *Прикладная информатика*. Москва, 2014. № 1(49). С. 56–65.
12. Коцюба И. Ю., Чунаев А. В., Шиков А. Н. Основы проектирования информационных систем : учеб. пособ. Санкт-Петербург : Университет ИТМО, 2015. 206 с.
13. Alshamranil A., Bahattab A. A Comparison Between Three SDLC Models Waterfall Model, Spiral Model, and Incremental/Iterative Model. *IJCSI International Journal of Computer Science Issues*. Vol. 12, Iss. 1, No 1. January 2015. P. 106–111. URL: <https://www.ijcsi.org/papers/IJCSI-12-1-1-106-111.pdf> (дата звернення: 08.06.2020).
14. Nabil Mohammed Ali Munassar, Govardhan A. A Comparison Between Five Models Of Software Engineering. *International Journal of Computer Science Issues*. Vol. 7, Iss. 5. September 2010. P. 94–100. URL: [https://www.researchgate.net/publication/258959806\\_A\\_Comparison\\_Between\\_Five\\_Models\\_Of\\_Software\\_Engineering](https://www.researchgate.net/publication/258959806_A_Comparison_Between_Five_Models_Of_Software_Engineering) (дата звернення: 09.06.2020).

Стаття надійшла до редакційної колегії 01.07.2020

### The main differences and features of structural and object-oriented approaches into designing of military information systems

#### Annotation

The experience of world's leading countries conflicts shows that it is impossible to ensure the operation of troops (forces) effectively, without the automation of the management of tangible and intangible resources.

The article considers the differences and features, advantages and disadvantages of two methodologies for designing information systems. The paper proves that the application of methodologies and the final choice of methods and means of designing military information systems depends on the following important components:

- of the general requirements to the system;
- of the level of technology innovation and complexity of the system;
- of the volume and details of the description of the object of automation;
- regulatory and design restrictions to the system;
- needs for iterative improvement of the system;
- the needs for integration with previous created systems;
- the level of organizational and technological maturity of the customer organization;
- of the availability and experience of performers of the system.

The value of the article in providing next recommendations:

- for architects of the system - criteria to facilitate the solution of the problem of choosing the design methodology and tools for implementing the information system;
- for project managers - information on the risks associated with methodologies;
- for heads of functional groups of information developers - for the selection of qualified specialists who are able to effectively use the methods and tools of design that was selected by the architects of the system;
- customers may have a better understanding of the importance of clearly formulating system requirements and providing primary data for further modeling.

In total the use materials of the article provides an opportunity for all project participants to optimize resources and time for pre-project preparation and improve the likelihood of successful implementation of project objectives.

**Keywords:** information system; design of Information Systems; structural analysis; object-oriented analysis; criteria for selecting a design model.

Андрощук О. В., канд. психол. наук

(0000-0002-1032-7459)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

## Аналіз застосування світових підходів для створення інформаційної інфраструктури Міністерства оборони України

**Резюме.** У статті розглядаються методологічні підходи щодо управління створенням інформаційної інфраструктури корпоративного рівня, що в світовій практиці застосовуються протягом її життєвого циклу. Унаслідок проведеного дослідження запропоновано підходи щодо застосування кращих світових практик для створення інформаційної інфраструктури Міністерства оборони України.

**Ключові слова:** інформаційна інфраструктура; IT-менеджмент; інформаційне забезпечення; управління вимогами.

**Постановка проблеми.** Перехід до нових стратегій реалізації державної інформаційної політики в Україні та використання інформації в цивільному та оборонному секторі доводить, що на сьогодні наша держава не може претендувати на конкурентоспроможність без ефективної інформаційної інфраструктури. У сфері інформатизації під поняттям *інформаційна інфраструктура* розуміють сукупність територіально розподілених інформаційних систем, інформаційно-телекомунікаційних мереж, систем і засобів захисту інформації, а також організаційних структур, які забезпечують її ефективне функціонування [1].

Особливо актуальною в сучасних умовах є проблема інформатизації Збройних Сил (ЗС) України, одним з напрямів якої є створення сучасної інформаційної інфраструктури Міністерства оборони (МО) України. Наявна інформаційна інфраструктура не повною мірою відповідає завданням, покладеним на МО України та ЗС України, має децентралізовану архітектуру, що призвело до виникнення великої кількості розрізнених інформаційних систем (ІС), для підтримки яких потрібно використовувати значні ресурси та утримувати великий штат чергового і обслуговуючого персоналу. Інформаційна взаємодія між цими системами практично відсутня або здійснюється фрагментарно за окремими напрямками, що призводить до дублювання та недостатньої достовірності та повноти інформації.

З аналізу стану використання ІС, інформаційно-телекомунікаційного, технічного, інженерного обладнання та нормативно-правового забезпечення, зрозуміло, що існуючий стан обумовлено недосконалістю підходів щодо управління

створенням інформаційної інфраструктури, основними недоліками яких є:

1) організаційна розпорошеність і функціональна розрізненість існуючих ІС;

2) відсутність централізованого планування розвитку інформаційної інфраструктури та аудиту стану впровадження інформаційних технологій;

3) недосконалість та неповнота нормативно-правового регулювання у галузі створення ІС на всіх етапах їх життєвого циклу (від проєктування до утилізації);

4) відсутність єдиних методологічних, технічних та організаційних принципів і підходів щодо створення ІС та впровадження інформаційних технологій;

5) відсутність стандартів обміну даними між ІС для забезпечення взаємосумісності;

6) відсутність організаційно-технічної платформи з централізованими сервісами доступу, збереження, обробки і обміну даними;

7) недостатня розгалуженість інформаційно-телекомунікаційних мереж і швидких каналів передачі даних;

8) недостатня розробленість питань захисту інформації (інформаційних ресурсів) та висока вартість проведення заходів зі створення комплексних систем захисту інформації;

9) відсутність єдиної технічної підтримки забезпечення функціонування ІС, навчання та підтримки користувачів.

Відповідно, актуальним завданням є пошук шляхів створення сучасної інформаційної інфраструктури МО України.

**Аналіз останніх досліджень та публікацій.** Процес створення інформаційної інфраструктури є багатоступінчастим. Як будь-який складний високотехнологічний процес, проєкт створення інформаційної інфраструктури має свій *життєвий цикл*

(ЖЦ), який представляється як сукупність взаємопов'язаних процесів послідовної зміни стану інформаційної інфраструктури, які відбуваються під час створення, функціонування та супроводження складових інфраструктури від визначення вимог до завершення їх використання [2].

У світі існує низка методологій і стандартів, які регламентують етапи створення інформаційної інфраструктури та процеси ЖЦ її складових. Серед найвідоміших слід виділити:

*Business System Planning (BSP)* – методологія організаційного планування компанії IBM на основі методу структурування інформації з використанням матриць перетину бізнес-процесів, функціональних підрозділів, функцій системи обробки даних, інформаційних систем, інформаційних об'єктів, документів і баз даних [3].

*Custom Development Method (CDM)* – методика компанії Oracle з розроблення прикладних ІС на основі використання заготовок проектних документів, розрахованих на використання класичної моделі ЖЦ [58].

*Rational Unified Process (RUP)* – методологія розроблення програмного забезпечення (ПЗ) компанії IBM, яка пропонує модель розроблення, що включає у себе чотири фази: початок, дослідження, побудова та впровадження. Кожна фаза може бути розбита на етапи (ітерації). Проходження через чотири основні фази називається циклом розроблення, який може повторюватися, якщо робота над проектом не завершується [4].

*Microsoft Solution Framework (MSF)* – методологія ідентична до RUP, що також включає чотири фази: аналіз, проектування, розроблення, стабілізація, і є ітераційною та передбачає використання об'єктно-орієнтованого моделювання [5].

*Extreme Programming (XP)* – методологія розроблення ПЗ, яка отримала назву екстремального програмування, базується на прийомах організації командної роботи, ефективної комунікації між замовником та виконавцем в період усього проекту [6].

*Continuous Acquisition and Life cycle Support (CALS)* – концепція безперервної інформаційної підтримки ЖЦ продукту на всіх його стадіях, яка призначена для підвищення ефективності та якості процесів ЖЦ продукту завдяки застосуванню безпаперових технологій.

*ГОСТ 34.601-90* – стандарт, що розповсюджується на автоматизовані системи та встановлює стадії та етапи їх створення. Крім того, у стандарті міститься опис робіт на кожному етапі.

*ISO/IEC/IEEE 12207:2017* – стандарт на процеси та організацію ЖЦ програмного забезпечення. Стандарт не містить описів фаз, стадій та етапів [7].

*ДСТУ ISO/IEC/IEEE 15288:2016* – стандарт на процеси ЖЦ систем, що стосуються різноманітних областей: системної інженерії, програмування, управління якістю, людськими ресурсами, безпекою та ін. [8].

Незважаючи на досить широкий вибір наведених підходів, їх застосування на практиці здебільшого орієнтовано на управління ЖЦ окремих складових інформаційної інфраструктури. Складність створення інформаційної інфраструктури військового відомства пов'язана з наявністю значної кількості модифікацій її складових, постійними змінами функціонального середовища, проблемами стандартизації, уніфікації, що потребує застосування багаторівневої моделі ЖЦ. Саме тому актуальним є завдання аналізу практичного застосування світових підходів для створення інформаційної інфраструктури МО України.

**Метою статті** є обґрунтування шляхів створення інформаційної інфраструктури Міністерства оборони України на основі застосування найкращих світових практик.

**Виклад основного матеріалу.** На цей час у провідних країнах світу розробляється цілий пласт проблем, пов'язаних з архітектурним підходом до управління складними організаційно-технічними об'єктами (рівня підприємства, організації, військового відомства тощо) та їх інформаційною інфраструктурою. Стандарт ДСТУ ISO/IEC/IEEE 15288:2016 визначає поняття *системної архітектури*, як концептуальну організацію складної системи, яка втілюється в її елементах, їх взаємодії між собою та із середовищем, а також принципах, що є основою для прийняття рішень щодо її проектування і еволюціонування. Такий підхід з погляду управлінської діяльності розглядає архітектуру інформаційної інфраструктури як складову більш загального поняття – архітектури організації (Enterprise Architecture).

Відомі міжнародні компанії IBM, Hewlett Packard, Microsoft виділяють чотири основні погляди на архітектуру інформаційної інфраструктури організації [9]:

бізнес-архітектура – описуються функціональні процеси організації, а також стратегії розвитку організації;

інформаційна архітектура – описуються необхідні для реалізації функціональних процесів дані та використовується як зв'язок між даними і процесами;

архітектура застосунків – вказується, яке прикладне ПЗ використовується або має використовуватися для обробки даних;

технологічна архітектура – описується структура апаратного забезпечення, необхідного для підтримання архітектури застосунків та інформаційної архітектури.

Як видно з наведених визначень, концепція архітектури інформаційної інфраструктури організації полягає у визначенні підходів щодо використання інформаційних і технологічних ресурсів відповідними функціональними процесами. Зазначені архітектурні підходи отримали широке визнання, і за ініціативою різних організацій і фондів, що займаються впровадженням інформаційних технологій (ІТ), були опубліковані у вигляді бібліотек найкращих практик, що описують фреймворки (англ. *frameworks* – робочі моделі) управління процесами на різних рівнях архітектури інформаційної інфраструктури (далі – ІТ-процесами). Мета ініціативи – зібрати і поділитись передовим досвідом управління застосуванням ІТ між організаціями по всьому світу.

Відповідно до наведених рівнів архітектури інформаційної інфраструктури слід виділити такі передові підходи:

*Business Information Services Library* (BISL) – бібліотека, що описує ІТ-процеси забезпечення надання інформації з погляду задоволення потреб її споживачів;

*Control Objectives for Information and related Technology* (COBIT) – збірка принципів управління застосуванням ІТ-процесів та проведення їх аудиту з погляду стратегічного керівництва організації;

*Application Services Library* (ASL) – бібліотека, що описує ІТ-процеси управління розробленням, супроводженням та оновленням прикладного ПЗ;

*Information Technology Infrastructure Library* (ITIL) – бібліотека, що описує ІТ-процеси управління технологічною інфраструктурою.

Наведені підходи розглядають функціональні процеси організації, як множину завдань, для вирішення яких інформаційною інфраструктурою надається

певний набір послуг – так званих ІТ-сервісів. З позиції загальної теорії систем, ІТ-сервіси є системоутворюючими факторами, які виконують роль керованих об'єктів у системі управління інформаційною інфраструктурою. Вироблення керуючих впливів здійснюється керівниками функціональних процесів (функціональним ІТ-менеджментом), який відображає потреби підрозділів організації в інформаційному забезпеченні та є засобом управління інфраструктурою і застосунками. Такий підхід до управління ІТ-сервісами характеризується орієнтованістю на функціональні процеси і їх максимально тісною зв'язкою з можливостями технологічної інфраструктури. Це забезпечується такими обов'язковими етапами створення інформаційної інфраструктури:

ідентифікація функціональних та інформаційних процесів організації (як існуючих, так і запланованих) і їх вимог до ІТ-сервісів;

відображення інформаційних процесів на елементи застосунків і технологічної інфраструктури;

визначення вимог до мережевих компонентів, серверного обладнання, систем зберігання даних і застосунків для забезпечення продуктивності та доступності конкретних технологічних компонентів;

моніторинг заданих параметрів якості надання ІТ-сервісів і звітність за його результатами (дає змогу контролювати їх досягнення).

Рекомендації BISL, COBIT, ASL та ITIL відрізняються за діапазоном завдань, які вони вирішують, і підходами, які використовують. Для розуміння можливостей використання зазначених підходів слід проаналізувати кожен з них і порівняти.

BISL – описує такі види діяльності із забезпечення надання інформації: ефективне планування, збір, організація, використання, контроль, поширювання і знищення інформації. Ця інформація пов'язана з активним управлінням, супроводженням і підтриманням функціональних процесів. Розроблення моделі інформаційної політики організації знаходиться в зоні відповідальності функціонального ІТ-менеджменту. Вихідними даними для формування моделі інформаційної політики є опис основних функціональних процесів, зв'язки між стратегічними цілями організації і функціональними процесами; зв'язки між застосунками, що виконують обробку даних, і функціональними процесами; зв'язки між

застосунками. Функціональні процеси умовно розділяються залежно від рівня деталізації на процеси і функції, що визначають діяльність з використання інформації, інформаційних технологій і технологічної інфраструктури.

У BISL визначено 23 IT-процеси, об'єднані в сім кластерів, що утворюють три рівні процесів управління інформаційним забезпеченням: операційний, управлінський і стратегічний [10].

Процеси операційного рівня відповідають за визначення вимог до інформаційного забезпечення і безперервне підтримання відповідних функціональних процесів.

На управлінському рівні розглядаються специфічні вимоги користувачів до прикладного ПЗ, забезпечуючи управління його використанням з погляду планування, рентабельності, потреб, рівнів якості надання IT-сервісів.

На стратегічному рівні розглядаються зв'язки між функціональними процесами і їх інформаційною підтримкою. На рівні функціонального-процесу формуються вимоги до інформації, що пред'являються окремими функціональними процесами. Цей рівень забезпечує визначення політики майбутнього інформаційного забезпечення, формуючи стратегію його розвитку.

COBIT – визначає набір універсальних методів управління IT-процесами для контролю за їх виконанням, аудиту та надання звітності [11]. Згідно з COBIT, процес – це дія, спрямована на досягнення результату за умови оптимального використання ресурсів, яка може коригуватися під час її виконання. Усі ресурси, задіяні у процесі, структуруються таким чином, щоб максимально ефективно виконувати цей процес. Більшість процесів є сталими або змінюються нечасто, порівняно з організаційними об'єктами (співробітники, відділи, департаменти та ін.). Упровадження методології COBIT, як правило, не обмежується рамками одного відділу або департаменту, а зачіпає всю структуру організації.

COBIT охоплює усі IT-процеси, які згруповані за напрямками:

планування та організація – група процесів, які визначають напрями щодо впровадження рішень і забезпечення IT-сервісів;

придбання і впровадження – група процесів, які забезпечують впровадження рішень і надання на їх основі IT-сервісів;

експлуатація та супроводження – група процесів, які реалізують функціональні процеси і роблять їх доступними для кінцевих користувачів;

моніторинг – група процесів, які виконують спостереження за всіма IT-процесами для вчасного реагувати на інциденти і проблеми.

Особливістю підходу COBIT є наявність у ньому моделі зрілості інформаційної інфраструктури. Використання моделі зрілості робить цей підхід найбільш ефективним для визначення цілей у сфері IT, побудови системи збалансованих показників для проведення внутрішніх і зовнішніх аудитів IT-процесів. Усі ресурси, які використовуються об'єктами контролю, оцінюються з погляду їх відповідності критеріям, які впливають із завдань організації: ефективність, технічний рівень, безпека, цілісність, придатність, узгодженість, надійність. На підставі результатів аудиту за рівнями зрілості можливо сформувати повну, об'єктивну та актуальну інформацію про поточний стан IT-процесів, визначити можливі рішення щодо зміни ситуації, заходи щодо вдосконалення IT-процесів, перспективи та ризики щодо їх реалізації.

ASL – описує види діяльності щодо управління застосунками протягом їх ЖЦ, а саме проектуванням, тестуванням, супроводженням, обслуговуванням, розширенням і оновленням економічно виправданими методами [12].

Важливим аспектом підходу ASL є проактивний підхід до надання IT-сервісів. Він дає змогу передбачити розвиток ситуації і забезпечувати виявлення можливих сценаріїв роботи на декількох рівнях управління:

на рівні політики і стратегії управління застосунків, де здійснюється коригування способів надання IT-сервісів на ранніх стадіях, для задоволення майбутніх потреб;

на рівні стратегії, де планується створення застосунків, проводиться актуалізація сценаріїв і методів, які призводять до бажаного результату;

на рівні процесів управління, де проводиться управління якістю застосунків (зокрема управління проблемами);

на операційному рівні (у процесі експлуатації), для здійснення активної взаємодії всіх зацікавлених сторін і надання звітності.

Рекомендації ASL можуть бути використані як:

інструмент структурування діяльності (описує діяльність з управління застосунками, допомагаючи визначити, де і яка робота проводиться чи не проводиться, або здійснюється неявно);

інструмент комунікацій (забезпечує чітку понятійну основу, даючи визначення різним поняттям та видами діяльності, забезпечуючи взаємодії між зацікавленими сторонами на основі загальної системи понять);

інструмент проєктування і впровадження застосунків (встановлює систему взаємозв'язків між різними видами діяльності, надаючи інструменти для впровадження ПЗ).

ІТІЛ – описує процесний підхід до надання і підтримки ІТ-сервісів [13]. Він пропонує структурований опис найбільш часто використовуваних ІТ-процесів, їх цілей і параметрів, а також зв'язків між окремими ІТ-процесами. Кожен процес детально описаний, надано рекомендації щодо його впровадження та реалізації. Згідно з підходом ІТІЛ виділяють три основні групи процесів:

планування розвитку ІТ-сервісів: проєктування, планування, розширення;

надання ІТ-сервісів: управління інцидентами і проблемами, управління конфігурацією і змінами, управління релізами;

управління наданням (підтримка) ІТ-сервісів: управління рівнем обслуговування, фінансове управління ІТ-сервісами, управління готовністю, управління безперервністю обслуговування, управління потужностями.

Однією з основних цілей впровадження ІТІЛ є підвищення якості надання ІТ-сервісів в умовах обмеженого бюджету, низької кваліфікації персоналу, складної конфігурації систем, швидких змін функціональних процесів. Ця методологія передбачає надання ІТ-сервісів на основі попередньої домовленості, яка виражається угодою про рівень послуг (SLA – Service Level Agreement). Контроль за якістю послуг ґрунтується на процесі управління рівнем сервісу (SLM – Service Level Management). Параметри якості ІТ-сервісу і результати їх вимірювання мають формулюватися з погляду функціонального ІТ-менеджменту, тобто мають визначати вимоги до можливостей ПЗ (які послуги ПЗ має надавати, яку реакцію демонструвати у відповідь на певні дії і в певних ситуаціях).

Однією з найважливіших умов побудови ефективної інформаційної інфраструктури є *підтримка ІТ-сервісів* (Service Support). Для

якісної підтримки ІТ-сервісів необхідні: *служба технічної підтримки* (Service Desk), *система управління інцидентами* (Incident Management), *система управління проблемами* (Problem Management), *система управління конфігураціями* (Configuration Management), *система управління змінами* (Change Management) і *система протоколювання версій реалізації* (Release Management). У разі потреби поліпшення надання ІТ-сервісів, проводять їх змінення в рамках процесу управління змінами (Change Management) під час надходження запиту на зміну (RFC – Request For Change) до служби технічної підтримки. Це дає змогу підвищити якість ІТ-сервісів для виконання службових завдань і зменшити витрати на їх надання.

Для забезпечення максимальної ефективності надання ІТ-сервісів в ІТІЛ пропонуються ключові процедури, що включають в себе *управління сервісами мережі* (Network Service Management), *станом елементів технічної інфраструктури* (Operations Management), *локальними комп'ютерами* (Management of Local Processors), а також *інсталяцією і експлуатацією обчислювальних систем* (Computer Installation and Acceptance). В ІТІЛ також описані зв'язки між етапами розроблення та підтримки ПЗ, зокрема розглядається *управління життєвим циклом ПЗ* (Software Lifecycle Support) і *тестуванням ІТ-сервісів* (Testing an IT Service for Operational Use).

Порівняння підходів. BISL, COBIT, ASL і ІТІЛ розглядають управління інформаційною інфраструктурою з різних боків:

BISL – розглядає необхідні види діяльності з управління інформаційним забезпеченням функціональних процесів організації та дає чітке розмежування між стратегічним керівництвом функціональними процесами, управлінням інформацією, користувачами та постачальниками ІТ-сервісів;

COBIT – управління діяльністю, ресурсами і ризиками щодо забезпечення надання ІТ-сервісів;

ASL – описує види діяльності щодо управління ПЗ, що реалізує функціональність ІТ-сервісів;

ІТІЛ – описує множину аспектів взаємодії з користувачами ІТ-сервісів, визначає ролі та обов'язки, пов'язані з підтримкою технологічної інфраструктури.

Таким чином, рекомендації BISL, COBIT, ASL і ІТІЛ можна розглядати як



взаємодоповнюючі підходи. Можлива рівнях архітектури інформаційної взаємодія розглянутих підходів на різних інфраструктури наведена на рис. 1.

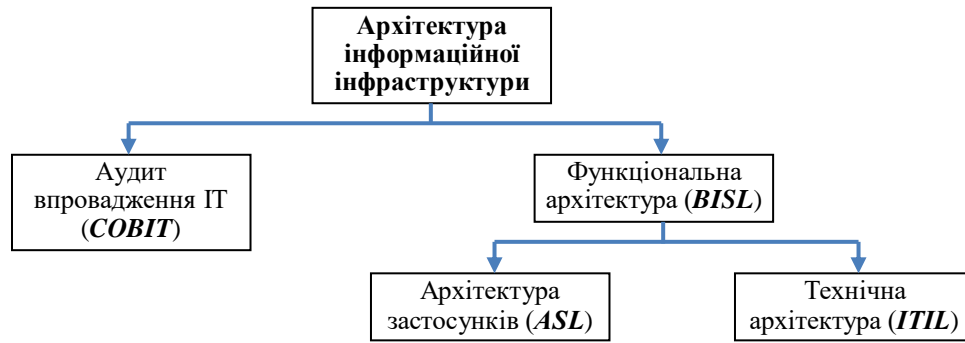


Рис. 1. Схема взаємодії підходів BISO, COBIT, ASL і ITIL

Взаємне використання підходів BISO, COBIT, ASL і ITIL дає змогу забезпечити усунення основних недоліків щодо створення інформаційної інфраструктури МО України: BISO – недоліки 1-2, COBIT – 2-4, 6; ASL – 4, 5; ITIL – 6-9.

**Висновки.** У статті проведено аналіз світових підходів, що запропоновані рекомендаціями бібліотек найкращих практик управління ІТ-процесами на різних рівнях архітектури інформаційної інфраструктури. Визначено, що доцільним є застосування інтегрованого підходу на основі найкращих практик BISO, COBIT, ASL і ITIL, що дасть змогу підняти на якісно новий рівень процеси створення та управління інформаційною інфраструктурою МО України.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про затвердження Концепції інформатизації Міністерства оборони України : наказ Міністерства оборони України від 17.09.2014 р. № 650. URL: <https://zakon.rada.gov.ua/rada/show/v0650322-14#Text> (дата звернення: 04.06.2020).
2. Інженерія систем і програмного забезпечення. Процеси життєвого циклу програмного забезпечення (ISO/IEC 12207:2008, IDT). [Чинний від 2016-01-01].
3. Zachman John. Business Systems Planning and Business Information Control Study: A

comparisment. *IBM Systems Journal*. Vol 21, No 3, 1982. P. 31–53.

4. Вернадов А. М. Программирование программного обеспечения экономических информационных систем. Москва : Финансы и статистика, 2002. 349 с.
5. Кратчен Филипп. Введение в Rational Unified Process. Москва : Вильямс, 2002. 240 с.
6. Обзор Microsoft Solutions Framework (MSF) URL: [https://msdn.microsoft.com/ru-ru/library/jj161047\(v=vs.120\).aspx](https://msdn.microsoft.com/ru-ru/library/jj161047(v=vs.120).aspx) (дата звернення: 04.06.2020).
7. Ауер К., Миллер Р. Экстремальное программирование. Санкт-Петербург : Питер, 2004. 368 с.
8. Инженерия систем і програмного забезпечення. Процеси життєвого циклу систем (ISO/IEC 15288:2008, IDT). [Чинний від 2016-01-01].
9. Обзор архитектуры Microsoft URL: <https://msdn.microsoft.com/ru-ru/library/ee872883.aspx> (дата звернення: 06.06.2020).
10. Ван дер Полс Р., Донац Р., Ван Аутфорст Ф. BiSL. Сборник описаний процессов для управления бизнес-информацией. Москва : 2014. 191 с.
11. COBIT. An ISACA Framework. URL: <http://www.isaca.org/cobit> (дата звернення: 06.06.2020).
12. ASL BiSL Foundation. URL: <http://www.aslbislfoundation.org/ru/bisl> (дата звернення: 04.06.2020).
13. What is ITIL Best Practice. ITIL. AXELOS. URL: <https://www.axelos.com/best-practice-solutions/itil/what-is-itil> (дата звернення: 04.06.2020).

Стаття надійшла до редакційної колегії 06.07.2020

### Analysis of the application of global approaches to the creation of information infrastructure of the Ministry of Defense of Ukraine

#### Annotation

The transition to new strategies for the implementation of state information policy in Ukraine and the use of information in the civil and defense sectors, proves that today our state cannot claim competitiveness without an effective information infrastructure. The existing information infrastructure

does not fully meet the tasks assigned to the Ministry of Defense of Ukraine and the Armed Forces of Ukraine, has a decentralized architecture, which has led to a large number of disparate information systems (IS), which require significant resources and large staff.

As the analysis of the state of use of IP, information and telecommunication, technical, engineering equipment and regulatory support, the current state is due to the imperfection of approaches to managing the creation of information infrastructure. The main disadvantages are:

- organizational dispersion and functional diversity of existing IP;
- lack of centralized planning of information infrastructure development and audit of the state of information technology implementation;
- Lack of common methodological, technical and organizational principles and approaches to the creation of IP and implementation of information technology and others.

The article analyzes the global approaches proposed by the recommendations of libraries of best practices in IT process management at different levels of information infrastructure architecture. It is determined that it is expedient to apply an integrated approach based on the best practices of BISO, COBIT, ASL and ITIL, which will allow to raise to a qualitatively new level the processes of creating and managing the information infrastructure of the Ministry of Defense of Ukraine.

**Keywords:** system architecture; IT management; information support; information support management; defense sector; requirements management.

Литовченко Г. Д.

(0000-0002-8625-1438)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

## Аналіз процесів управління інформаційним забезпеченням інформаційних систем у сфері управління оборонними ресурсами

**Резюме.** У статті проаналізовано підхід Business Information Services Library (бібліотеки найкращих практик управління інформаційним забезпеченням) щодо його застосування для інформаційного забезпечення інформаційних систем стратегічного управління оборонними ресурсами. Визначено процеси формування інформаційної політики і специфікації вимог до інформаційного забезпечення функціональних процесів управління оборонними ресурсами.

**Ключові слова:** управління оборонними ресурсами; інформаційна система; інформаційне забезпечення; функціональні процеси; функціональні сервіси.

**Постановка проблеми.** В умовах високої багатоаспектності та складності завдань, які стоять на сьогодні перед Збройними Силами (ЗС) України, важливим стає забезпечення розроблення, впровадження і використання інформаційних технологій (ІТ), починаючи з постановки цілей, визначення джерел отримання інформації до застосування математичних засобів інформаційно-аналітичної підтримки у сфері стратегічного управління оборонними ресурсами. Під управлінням оборонними ресурсами розуміють специфічну форму адміністративно-господарської діяльності ЗС України, а саме підтримку процесів оборонного та мобілізаційного планування, матеріально-технічного, медичного та інших видів забезпечення, управління фінансово-економічною діяльністю, особовим складом, організаційною структурою, майном, закупівлями, іншими видами адміністративної діяльності [1].

Нині у ЗС України за кожним з напрямів управління оборонними ресурсами створені окремі компоненти інформаційної інфраструктури та інформаційних систем (ІС), але вони є різнорідними за часом створення, ступенем завершеності, використаними технологіями, обсягом охоплення процесів, обсягом розгортання та наповнення даними [2]. Зважаючи на це, вдосконалення системи управління оборонними ресурсами та стрімкий розвиток новітніх інформаційних технологій потребують застосування нових підходів як до побудови ІС управління оборонними ресурсами, так і до управління їх інформаційним забезпеченням. До того ж *під інформаційним забезпеченням* розуміються такі представлення та організація інформації, які відповідатимуть потребам користувачів ІС

та вимогам автоматизованої обробки даних. Під *управлінням інформаційним забезпеченням* розуміють наявність чітких процесів руху інформації від моменту її створення до використання, застосування систем класифікації та кодування, створення інформаційно-логічних моделей масивів інформації, управління змінами наявних ІС, рішення рутинних завдань щодо якості функціонування ІС тощо.

Контроль відповідності наданої інформації до потреб користувачів є ключовою функцією управління інформаційним забезпеченням. Інша важлива функція полягає в наданні технологій, на базі яких узгоджуються інтереси всіх сторін, залучених в інформаційну діяльність. Складність управління інформаційним забезпеченням у сфері управління оборонними ресурсами визначається постійними змінами функціонального середовища, появою нових цілей і пошуку нових рішень. Зміни в функціональному середовищі потребують зміни процесів управління для забезпечення відповідності новим вимогам множини учасників, що залучені до створення і використання інформаційних ресурсів. Отже аналіз процесів управління інформаційним забезпеченням щодо їх застосування для ІС управління оборонними ресурсами є актуальною задачею.

**Аналіз останніх досліджень і публікацій.** У роботі [2] розглядаються сучасна методологія і передові підходи до створення ІС в оборонному секторі. Роботи [3, 4] присвячені основним засадам побудови єдиної інформаційної системи управління оборонними ресурсами. У працях [5–7] висвітлено особливості управління функціональними сервісами ІС. Незважаючи

на певні досягнення у цій сфері, дослідження є фрагментарними, вирішення питань ефективності функціонування ІС управління оборонними ресурсами обмежене, не приділена належна увага вимогам до процесів управління інформаційним забезпеченням.

**Метою статті** є аналіз сучасних підходів управління інформаційним забезпеченням інформаційних систем щодо застосування у сфері управління оборонними ресурсами.

**Виклад основного матеріалу.** З наведеного аналізу тенденцій інформатизації у сфері управління оборонними ресурсами можна дійти висновку, що управління, контроль і зміна інформації з погляду попиту на неї є критичними факторами успіху, які показують, наскільки добре інформаційне забезпечення відповідає потребам користувачів і вимогам автоматизованої обробки даних. Важливо управляти інформаційним забезпеченням таким чином, щоб воно повністю відповідало існуючим функціональним процесам управління оборонними ресурсами. Побудовування цієї відповідності може бути успішним лише тоді, коли різні рівні управління інформаційним забезпеченням сходяться і взаємно пов'язуються.

Основні компоненти сучасної ефективної системи управління інформаційним забезпеченням можна розділити таким чином:

управління стратегічними і тактичними запитамися щодо потреб в інформаційному забезпеченні ІС;

управління портфелем проєктів щодо створення нових ІС;

управління програмним офісом, тобто певною множиною ІС;

управління рутинними операціями щодо підтримки функціонування ІС.

На сьогодні у світовій практиці у сфері управління інформаційним забезпеченням використовують такі відомі методологічні підходи, як збірник найкращих практик управління інформаційним забезпеченням (ІТ-менеджменту) – бібліотека сервісів бізнес-інформації BISL (Business Information Services Library) [8].

Згідно з підходами, визначеними у BISL, управління попитом на інформацію, перетвореним у вимоги до інформаційного забезпечення, може бути успішним тоді, коли споживачі інформації і ті хто її надає розділені відносно інформаційного забезпечення. Сторона споживача управляє попитом на інформацію через трансляцію вибору,

зробленого на стороні попиту, на вимоги до інформації на стороні пропозиції. Далі фактична послуга надається третьою стороною – постачальником ІТ-сервісів або відповідним підрозділом.

Інформаційне забезпечення є важливим для підтримання функціональних процесів. З огляду на те, що інформаційне забезпечення важливе, насамперед, для функціональних процесів, контроль над ними має здійснювати не тільки постачальник ІТ-сервісів. Цей контроль має взяти на себе сторона споживача ІТ-сервісів.

Управління інформаційним забезпеченням, визначення вимог до інформації потребує спеціальних знань і досвіду в роботі з функціональними процесами, який відрізняється від технічного досвіду у сфері ІТ. Управління інформацією з боку управляючого функціональним процесом (менеджера або адміністратора функціонального процесу) забезпечує підтримання функціонального процесу в оптимальному режимі.

Отже, управління інформаційним забезпеченням впливає на процеси проєктування і надання ІТ-сервісів. Ця діяльність потребує, щоб управління інформаційним забезпеченням було невід'ємною частиною діяльності сторони споживачів ІТ-сервісів.

На управління інформаційним забезпеченням впливають чотири чинники:

інформаційне забезпечення функціональних процесів у частині визначення вимог до інформації;

автоматизоване інформаційне забезпечення та ІТ-підтримка в частині процедури замовлення ІТ-сервісів і моніторинг їх якості;

організаційні заходи щодо управління ІТ-сервісами – функція, яка безпосередньо управляє інформаційним забезпеченням;

політика щодо інформаційного забезпечення.

Важливою передумовою ефективного управління інформаційним забезпеченням є спеціалізоване знання функціональних процесів, яке досягається різними способами. Оскільки неможливо, щоб одна посадова особа мала усі необхідні спеціальні знання, персонал необхідно поділяти на різні інформаційні групи або галузі знань.

Інформаційне забезпечення в рамках організації можна розглядати на трьох рівнях. Управління інформаційним забезпеченням відбувається на кожному з цих рівнів.

На корпоративному рівні інформаційне забезпечення управляється в межах всієї організації. Беруться до уваги зв'язки між різними функціональними процесами і їх вплив на інформаційне забезпечення. На практиці за цим рівнем стежать окремі підрозділи у межах організації, оскільки тут необхідні спеціальні знання, навички та контакти.

На рівні функціонального процесу відбувається управління всім інформаційним забезпеченням, яке підтримує цей процес. На цьому рівні основними є вимоги до інформаційного забезпечення, які висувуються окремими функціональними процесами.

На системному рівні передбачаються специфічні вимоги користувачів до роботи ІС. Інформаційні системи часто підтримують тільки частину функціонального процесу, і навпаки, єдина інформаційна система часто використовується для підтримки декількох функціональних процесів. Це означає, що можуть існувати кілька ІС, що підтримують функціональний процес загалом, що зі свого боку може призвести до необхідності управління інформаційним забезпеченням на системному рівні.

Таким чином, сфера відповідальності щодо управління інформаційним забезпеченням є досить широкою. Управління

має інтерпретуватися ширше, ніж просто роль операційного адміністратора функціонального процесу. У рамках BISL визначені три рівні:

- операційний;
- управлінський;
- стратегічний.

Зазвичай ролі, які відповідають цим рівням, визначаються адміністраторами функціональних процесів і власниками системи.

*Операційний рівень* процесів управління відповідає за використання інформаційного забезпечення та визначає вимоги, яким воно має задовольняти. На практиці сюди включаються завдання, які виконуються адміністраторами функціональних процесів.

*Управлінський рівень* відповідає за витрати, повернення інвестицій, ведення договорів і планування. Власник системи, замовник, власник бюджету тощо відповідають за зазначену сферу діяльності. У разі, коли постачальники ІС також управляють інформаційним забезпеченням, цей рівень переводиться в зону їх відповідальності.

*Стратегічний рівень* стосується майбутнього інформаційного забезпечення. За цей рівень відповідає керівництво вищого рівня.

Відповідна такому розподілу модель управління інформаційним забезпеченням визначає сім груп процесів (рис. 1).



Рис. 1. Рівні управління інформаційним забезпеченням

Група процесів 1 – управління використанням – спрямовані на безперервне підтримання інформаційного забезпечення. Ці процеси надають підтримку користувачам щодо інформаційного забезпечення для

здійснення діяльності в межах функціонального процесу, операційного управління постачальниками ІТ-сервісів, а також забезпечують і здійснюють моніторинг своєчасності надання даних.

*Група процесів 2* – управління функціональними можливостями – описують рівень, на якому відбувається проектування і реалізація інформаційного забезпечення. Мета цієї групи полягає в здійсненні змін таким чином, щоб вони вписувалися в набір структур і вимог та одночасно з цим задовольняли цілі функціональних процесів і запити користувачів.

*Група процесів 3* – зв'язувальні процеси операційного рівня – пов'язують між собою групи процесів управління використанням і управління функціональними можливостями, які не можуть функціонувати окремо. Метою цих взаємодіючих процесів є прийняття рішень щодо необхідних змін в інформаційному забезпеченні та якою має бути фактична реалізація цих змін.

*Група процесів 4* – управлінських процеси – забезпечує інтегральне управління згаданими групами процесів. Управлінські процеси здійснюють моніторинг діяльності щодо узгоджених витрат, вимог, договорів та планування.

*Група процесів 5* – інформаційної стратегії – відповідає за розроблення майбутньої стратегії інформаційного забезпечення. Як безпосередньо в самій організації, так і у функціональних процесах постійно відбуваються різного роду зміни, які впливають на потреби щодо інформаційного забезпечення. Важливо, щоб інформаційне забезпечення відповідало майбутнім вимогам, а структурні недоліки поточної ситуації були вирішені.

*Група процесів 6* – стратегії розвитку організації – координує управління, структурування методів роботи, прийняття рішень у сфері інформаційного забезпечення. Це може бути застосовано до відносин зі сторонами, що знаходяться поза межами управління інформаційним забезпеченням, такими як ІТ-постачальники і споживачі.

*Група процесів 7* – зв'язувальні процеси стратегічного рівня – пов'язують між собою зміст (група процесів 5) і стратегією розвитку (група процесів 6).

**Висновки.** Отже, підходи BISL на практиці доцільно використовувати для створення єдиної інформаційної системи управління оборонними ресурсами. Їх успішне застосування значною мірою визначається зв'язками між різними групами і різними рівнями процесів управління інформаційним забезпеченням. До того ж забезпечується взаємодія та комунікація між визначеними групами процесів управління, що є

вирішальними факторами створення ефективної інформаційної інфраструктури МО України і якості інформаційного забезпечення функціональних процесів у сфері управління оборонними ресурсами.

У сучасних умовах складність інформаційних систем сфери оборони зростає, а методи і технології ефективного управління інформаційним забезпеченням динамічно розвиваються. У подальших дослідженнях доцільно розглянути нові архітектурні підходи до побудови програмних платформ ІС стратегічного управління оборонними ресурсами, орієнтованих на надання відповідних функціональних сервісів.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Романченко І. С., Богданович В. Ю., Денешкін М. М. Теоретико-методологічні засади побудови системи управління ефективністю планування та виконання програм розвитку Збройних Сил України. *Наука і оборона*. 2015. № 3/4. С. 50–55.
2. Кірпічніков Ю. А., Утюшев М. К., Закалад М. А. Аналіз світового досвіду застосування інтеграційних технологій в автоматизованих системах управління. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2016. № 3 (58). С. 131–135.
3. Кірпічніков Ю. А., Андрощук О. В., Головченко О. В., Петрушен М. В. Визначення технологічних рішень щодо створення єдиної інформаційної системи управління оборонними ресурсами. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2019. № 1(65). С. 86–91.
4. Кірпічніков Ю. А., Андрощук О. В., Петрушен М. В., Васюхно С. І. Теоретичні підходи до побудови архітектури інформаційної системи управління оборонними ресурсами на основі сервісно-орієнтованої моделі. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2018. № 1 (62). С. 80–85.
5. Беляченко В. В., Педан Ф. П., Романченко О. А. Підходи до створення, підтримки і вдосконалення АСУ логістичного забезпечення ЗС України з урахуванням досвіду країн – членів НАТО. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2018. № 3 (64). С. 54–60.
6. Головін О. О. Єдиний інформаційний простір – основа ефективної реалізації принципів програмно-цільового планування розвитку озброєння та військової техніки. *Наука і техніка Повітряних Сил Збройних Сил України*. Харків, 2018. № 2 (31). С. 41–46.

7. Долженко А. И. Управление информационными системами : курс лекций. Ростов-на-Дону, 2007. 191 с.

8. Ван дер Полс Р., Донац Р., Ван Аутфорст Ф. ViSL. Сборник описаний процессов для управления бизнес-информацией. Москва : 2014. 191 с.

Стаття надійшла до редакційної колегії 01.02.2021

### **Analysis of information management processes for information systems in the field of defense resource management**

#### **Annotation**

At present time in the Armed Forces of Ukraine have already created separate components of information infrastructure and information systems in each of the areas of defense resources management. But these components are heterogeneous in time of creation, degree of completion, technologies used, scope of processes, volume of deployment and data filling.

Therefore, the improvement of the defense resources management system and the rapid development of technology require new approaches, both to the construction of information systems for the management of defense resources, and to their information support.

*Information support* in this paper means the presentation and organization of information that meets the needs of users of information systems and the requirements of automated data processing. Therefore, the analysis of management processes of information support of information systems of defense resources management remains an urgent task for today.

The information management model defines seven groups of processes:

- management of the use of information support;
- functionality management;
- operational level binding processes;
- management processes;
- information strategies;
- organizational development strategies;
- strategic-level linking processes.

Management of information support should take place in such a way that it fully corresponds to the existing functional processes of defense resources management. Building such a match can only be successful when the different levels of information management converge and interconnect.

**Keywords:** sphere of defense; defense resource management; information system; information support; functional processes; functional services.

УДК 355.451 DOI: <https://doi.org/10.33099/2304-2745/2021-1-71/128-133>

Семененко В. М., канд. техн. наук, ст. наук. співроб.<sup>1</sup> (0000-0001-5774-0868)  
Шидлюх В. В.<sup>2</sup> (0000-0002-3792-3592)  
Сівоха І. М.<sup>2</sup> (0000-0001-5377-2520)

<sup>1</sup> – Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ;

<sup>2</sup> – Навчально-науковий центр стратегічних комунікацій у сфері забезпечення національної безпеки та оборони Національного університету оборони України імені Івана Черняховського, Київ

## Культура стратегічних комунікацій як основа таргетингу

**Резюме.** У статті проаналізовано ролі культури стратегічних комунікацій як основи таргетингу, надано рекомендації щодо формування культури стратегічних комунікацій у процесі реалізації і розвитку комунікаційних можливостей держави.

**Ключові слова:** стратегічні комунікації; культура; таргетинг.

**Постановка проблеми.** Декілька років поспіль чинні національні програми під егідою Комісії Україна – НАТО [1, 2], затверджені відповідними указами Президента України, задекларували розвиток в Україні культури стратегічних комунікацій на інституційному рівні, налагодження більш тісного співробітництва з неурядовими організаціями й сприяння розвитку їх спроможності здійснювати стратегічні комунікації в інтересах України.

Згідно з визначеннями Доктрини зі стратегічних комунікацій [5], *стратегічні комунікації* – скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків з громадськістю, військових зв'язків, інформаційних і психологічних операцій, інших суб'єктів інформаційної діяльності для виконання заходів, спрямованих на просування цілей держави.

Стратегічні комунікації у Збройних Силах (ЗС) України – об'єднання комунікативних спроможностей та військової діяльності з метою формування інформаційного середовища для розуміння, підтримання українським суспільством та міжнародною спільнотою діяльності ЗС України, створення сприятливих умов для виконання ними завдань за призначенням [5].

Однак на сьогодні наукові підходи до стратегічних комунікацій як культури, а також до обґрунтування ролі культури стратегічних комунікацій у прийнятих країнами НАТО процесах таргетингу залишаються недостатньо розкритими та науково-обґрунтованими.

**Аналіз основних досліджень і публікацій.** У [3] обґрунтована структура системи стратегічних комунікацій Міністерства оборони (МО) та ЗС України як

складника загальнодержавної системи комунікацій, доведена направленість процесів, які відбуваються під час комунікацій, на підвищення результативності процесів управління військами.

Автори [4] обґрунтовують доцільність формування Ситуаційного центру стратегічних комунікацій МО України та ЗС України, визначають його роль і місце у загальнодержавній системі, структуру, основні завдання та алгоритм роботи.

У [5] окреслюється роль і місце стратегічних комунікацій у структурі ЗС України, а [6] відображає систему поглядів, керівні принципи, умови і шляхи досягнення мети військового лідерства та практичного впровадження у підготовку і застосування військ (сил), як концепту внутрішніх комунікацій. У [7] проведено аналіз результатів роботи високомобільної групи внутрішніх комунікацій у штабах і підрозділах Об'єднаних сил, надано рекомендації щодо застосування технологій внутрішніх комунікацій у процесах управління збройними силами, як складової стратегічних комунікацій. Джерела [8–15] розкривають підходи НАТО щодо реалізації стратегічних комунікацій та їх складових.

Однак питання сутності культури стратегічних комунікацій в означених роботах не розглядаються.

**Метою статті** є аналіз культури стратегічних комунікацій, як основи таргетингу та розроблення пропозицій щодо її формування.

**Виклад основного матеріалу.** У сучасному інформаційному середовищі послідовне і своєчасне застосування стратегічних комунікацій має вирішальне значення для загального успіху, особливо у протистоянні загрозам, які створюються



агресором у гібридній війні. Для досягнення успіху, сили безпеки і оборони мають максимально ефективно застосовувати всі елементи стратегічних комунікацій, бути гнучкими і активними, намагатись завоювати панування в межах інформаційного середовища, тобто досягнути такого стану, коли взаємодія між суб'єктами стратегічних комунікацій підсилює зусилля один одного, робить оптимальним використання дефіцитних ресурсів.

Характер сучасних загроз в інформаційній сфері розмиває традиційні рамки миру і війни, тому стратегічні комунікації мають бути організовані та діяти ефективно як в мирний час, так і у складних умовах криз і воєнних конфліктів. Основним фактором формування складних умов є нестача або неефективне використання наявних людських і матеріальних ресурсів. Подолання цих умов потребує точного *таргетингу* (націлювання) і постійного удосконалення як політики, так і безпосередньо функцій стратегічних комунікацій, зокрема, організаційної (планувальної), виконавчої (координаційної) і контрольної (коригувальної) складових комунікаційної діяльності.

У НАТО справедливо вважають [15], що використання летальних і нелетальних можливостей впливає на інформаційне середовище або позитивно, узгоджуючи дії зі словами, або негативно, суперечачи повідомленням НАТО для аудиторії або завдаючи шкоди місії в зоні операцій і поза нею. Усі цільові заходи мають узгоджуватися із замислом стратегічних комунікацій НАТО та наративом місії (наратив – соціальна конструкція, когерентно взаємопов'язана між собою послідовність історичних і поточних подій [10], яка пояснює мотив місії).

За визначенням НАТО [15] таргет (ціль) – це структура, об'єкт, особа чи група осіб, проти яких може бути застосовані летальні чи нелетальні можливості для створення конкретних психологічних чи фізичних ефектів. Поняття “особа” включає мислення, процес мислення, її ставлення до чогось і поведінку.

Процес таргетингу – це спільні, системні та цілеспрямовані летальні та нелетальні дії стратегічного, оперативного і тактичного рівнів для створення конкретних ефектів, досягнення військових цілей і бажаного кінцевого стану [15]. Згідно з принципами, викладеними в Конституції України, бажаним кінцевим станом для

України можна вважати такий стан національної безпеки і оборони, який гарантуватиме захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки.

Для того, щоб інформаційні та комунікаційні аспекти летальних та нелетальних дій були зрозумілими та прийнятними для суспільства і всіх рівнів військового управління, процеси стратегічних комунікацій МО і ЗС України мають бути цілеспрямованими, узгодженими, продуктивними, простими і своєчасними, опиратись на досвід, бути ціннісноорієнтованими, а також гармонійно інтегрованими в життєдіяльність сил безпеки та оборони.

Усе це потребує створення у внутрішньому та зовнішньому середовищі матеріальних і духовних цінностей через реалізацію комунікативних можливостей держави, постійний розвиток і удосконалення цих можливостей завдяки максимальному використанню набутого досвіду і ефективному використанню ресурсів для гармонізації заходів, спрямованих на просування цілей держави, тобто потребує таргетингу і підходів до стратегічних комунікацій, як культури, яка забезпечить досягнення військових цілей і бажаного кінцевого стану.

З огляду на загальноприйняте визначення поняття “культура” (від лат. culture – “обробіток”, “обробляти”) і “стратегічні комунікації” [5] пропонується таке визначення *культури стратегічних комунікацій* – сукупність матеріальних і духовних цінностей, створених у процесі реалізації комунікативних можливостей держави, історично набутий досвід і рівень їх розвитку для удосконалення та гармонізації заходів, спрямованих на просування цілей держави в майбутньому.

Хоча культура стратегічних комунікацій не є кінцевим продуктом, вона є важливим фактором, який гарантує залучення великої кількості людей-одномумців, значну результативність, сприяє розвитку структури, зокрема, ЗС України і суспільства, і міжнародних відносин України.

У НАТО стратегічні комунікації розглядаються як спосіб мислення, який передбачає ширше розуміння комунікацій, як таких, що виходять за межі традиційних засобів масової інформації та некінетичних

підходів до досягнення бажаних ефектів в інформаційному середовищі.

*Менталітет* (англ. *mindset* – система мислення, ментальність, свідомість) – сукупність соціально-психологічних настанов, загальна духовна налаштованість, установка до навколишнього світу.

Менталітет виконавців і планувальників операцій має забезпечувати розуміння того, як ті чи інші дії або слова НАТО будуть сприйняті в інформаційному середовищі в будь-який час. Це мислення має пронизувати всі рівні від стратегічного (оперативного) до тактичного. Персонал має включати фахівців (експертів) за всіма напрямками

комунікативних спроможностей та інформаційних функцій персоналу, що дасть змогу забезпечити розуміння наративів Альянсу завдяки культурній обізнаності, єдності зусиль, послідовності, достовірності та застосовності продуктів стратегічних комунікацій [10].

З огляду на це можна дійти висновку, що “mindset” є основою культури стратегічних комунікацій НАТО.

У НАТО [10] також задекларовані та діють принципи стратегічних комунікацій, які є складовими культури стратегічних комунікацій (рис. 1).

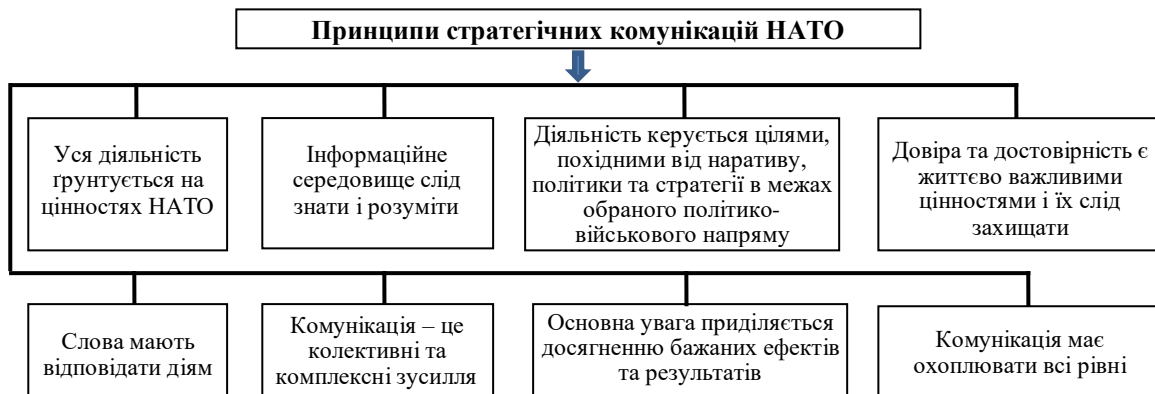


Рис. 1. Принципи стратегічних комунікацій НАТО

В Україні реалізація згаданих принципів ускладнюється тим, що управління кризовими ситуаціями та кризові комунікації часто знаходяться під впливом політичної боротьби і рідко ґрунтуються виключно на реальності. Ситуація, яку можна охарактеризувати як кризову, і яка є поширеною у ЗМІ, зазвичай пов’язана з намаганням якоїсь політичної сили використати гучну подію як інформаційний привід для дискредитації МО та ЗС України для досягнення власних політичних інтересів.

У цій ситуації військові структури не мають великої кількості можливостей цілісних комунікацій із зовнішніми аудиторіями, оскільки не мають доступу до засобів масової інформації, які здебільшого належать приватним особам і ведуть свою редакційну політику.

Зважаючи на це доцільно ширше використовувати різні доступні види комунікацій. За поглядами НАТО види комунікацій наведено на рис. 2.



Рис. 2. Види комунікацій

*Комунікація віч-на-віч.* Спілкування віч-на-віч вважається найвпливовішим засобом комунікації. Командири і старші посадові особи відіграють життєво важливу роль у справі надання (поширення повідомлень) (меседжів) завдяки їх взаємодії з головними лідерами (керівниками) важливих груп та організацій. Спілкування віч-на-віч не є

спонтанним процесом. Кожне таке залучення керівників має бути добре підготовленим, організованим, проведеним та оціненим. Для підготовки командувача потрібна допомога експертів з комунікації (фахівців з інформаційних операцій, психологічних портретів тих, з ким він зустрічатиметься, аналітиків із соціокультурних аспектів).

Традиційні друковані, радіо- та телевізійні засоби масової інформації. Наполегливо рекомендується, щоб увесь особовий склад отримав підготовку зі спілкування з журналістами, дотримуючись інформаційної стратегії та наративів, розроблених правил забезпечення безпеки операцій.

Традиційні тактики в спілкуванні і відносинах із ЗМІ, є надзвичайно важливими, хоча вони часто функціонують на основі традиційної моделі одностороннього спілкування, реагування на кризові ситуації.

Стандартними інструментами зв'язків із ЗМІ, які застосовуються в установах, є прес-конференція, брифінг у пресі, прес-реліз, відвідування театру, фотосесія, інтерв'ю, публічна заява тощо. Якість інформаційного продукту значно впливає на висвітлення подій у засобах масової інформації, це також один з основних обов'язків практикуючого командира або комунікатора. Незалежно від проактивності, фахівці зі стратегічних комунікацій, командири мають усвідомлювати, що кожна комунікація дорогоцінна. Втративши її один раз, відновити довіру або інтерес буде дуже важко. Отже новини не мають базуватися лише на інформації, яку організація хоче бачити у відкритому доступі, а на потребах цільових аудиторій.

Соціальні мережі (соціальні медіа). Останніми роками соціальні мережі стають популярнішими. Середовище соціальних засобів масової інформації постійно засвідчує зміни в технологіях і комп'ютерних системах. Для багатьох соціальних груп соціальні мережі є невід'ємною частиною їх щоденного споживання інформації. Соціальні мережі надають безліч можливості спілкуватися, взаємодіяти або ділитися контентом різного типу – від тексту до відео, від зображень до геолокаційних даних тощо. Військові недостатньо розуміють соціальні мережі та їх значення у військових операціях, тому їм краще вивчити простір соціальних мереж, їх користувачів, їх інтереси і способи комунікації, і те, як соціальні мережі можуть бути використані як додатковий канал комунікації. Як і всі інші засоби масової інформації, соціальні мережі треба використовувати скоординовано. Перед початком ведення комунікації на каналах соціальних мереж ретельно оцінюють вихідні умови. До того ж військовим необхідно зрозуміти, які соціальні групи використовують соціальні мережі, з якою

метою, як вони спілкуються в Інтернеті, їх інтереси і перебування соціальних груп. Також треба оцінювати відповідну інфраструктуру, ступінь доступу до Інтернету, чи використовує більшість людей смартфони для доступу в Інтернет тощо. Цю базову оцінку потім використовують для розроблення комунікаційної (інформаційної) стратегії, яку вибирає, й інформує про комунікаційні аспекти соціальних мереж.

Цифровізація (діджиталізація), особливо факт збільшення осіб, які використовують Інтернет і Facebook на щоденній основі, запропонували нові можливості спілкування з цільовими аудиторіями. Ці нові технології змінили спосіб спілкування культурних інституцій зі своєю аудиторією з нуля, тобто нові технології здійснили революцію середовища, де споживачі культурних продуктів отримують поінформованість і спосіб комунікації.

Знання реалій та вміння налагоджувати комунікації, вміння ефективно і успішно взаємодіяти з лідерами (керівниками) важливих груп та організацій, представниками та використовувати їх можливості, опираючись на загальнолюдські та загальнодержавні цінності, також є важливим елементом культури стратегічних комунікацій.

Успішні стратегічні комунікації потребують не лише взаємодії суспільних суб'єктів, сукупності ціннісних характеристик щодо розуміння, мотивації, поведінки, ставлення, сприйняття, думок, скарг і проблем суб'єктів, які змінюються з плином часу, а й чіткого таргетингу (націлювання) на конкретні цілі.

В умовах обмежених ресурсів робота професіонала – фахівця стратегічних комунікацій МО та ЗС України – має бути зорієнтована на вироблення якісного продукту і досягнення конкретних цілей. Зазначене потребує інноваційних підходів, творчості, постійного моніторингу інформаційного середовища і технологій задля адаптації продукту стратегічних комунікацій до змін і тенденцій розвитку комунікацій в інформаційному середовищі. У командному контексті культура стратегічних комунікацій розуміється як мистецтво внутрішніх комунікацій, спосіб життя організації, тому можна припустити, що культура стратегічних комунікацій становить основу таргетингу.

Таргетинг (націлення) передуює створенню комунікативних стратегій, на які впливає політична та фінансова стабільність,

нормативні документи, кадрове забезпечення, технологічний розвиток, стихійні лиха, демографічні, духовні та матеріальні здобутки населення.

Цифровізація (діджиталізація), особливо факт збільшення осіб, які використовують Інтернет і Facebook на щоденній основі, запропонували нові можливості спілкування з цільовими аудиторіями. Ці нові технології змінили спосіб спілкування культурних інституцій зі своєю аудиторією з нуля, або краще сказати, що нові технології здійснили революцію середовища, де споживачі культурних продуктів отримують поінформованість і спосіб комунікації.

Після розуміння сутності культури стратегічних комунікації важливим є вироблення пропозицій щодо формування культури стратегічних комунікацій в МО та ЗС України.

Погляд у майбутнє є надзвичайно важливим для формування культури стратегічних комунікацій в МО та ЗС України. Основні пропозиції щодо формування культури стратегічних комунікацій в МО та ЗС України можуть бути представлені такими вимогами до компетентностей суб'єктів стратегічних комунікацій: розуміння процесу планування та управління, знання інструментів і методів, специфічних для виконання функцій стратегічних комунікацій, розуміння спеціалізованих засобів комунікації, розуміння бажань і потреб споживачів – цільової аудиторії, моніторинг тенденцій, гнучкість, прийняття нових тенденцій і усвідомлення того, що інструменти, канали та тенденції постійно змінюються технологічним прогресом.

Продукт стратегічних комунікацій, як і будь-який інший інформаційний продукт, стає все більш чутливим до втручань і впливів, що викликає необхідність стратегічного передбачення та систематичного аналізу нових тенденцій розвитку внутрішнього і зовнішнього інформаційного середовища.

Аналіз інформаційного середовища і стану стратегічних комунікацій дає уявлення про інституцію з трьох аспектів: внутрішнє оточення (місія, бачення та внутрішня структура), сприйняття суспільства (репутація) та зовнішнє оточення (зацікавлені сторони).

Після аналізу внутрішнього і зовнішнього інформаційного середовища, аналізу потреб цільових аудиторій і визначення стратегії, яка має коригувати організаційну (планувальну), виконавчу

(координаційну) функції стратегічних комунікацій, необхідно визначити реальні роль і місце стратегічних комунікацій у свідомості (mindset) військових керівників – лідерів.

Визначення ролі та місця стратегічних комунікацій у свідомості лідерів є вкрай важливим для вибору стратегії і тактики реалізації проекту формування культури стратегічних комунікацій у МО і ЗС України, водночас і найскладнішою частиною процесу удосконалення пов'язаних з цим відносин. Адже, будь-яка спроба удосконалення завжди наражається на скепсис, саботаж, прихований або відкритий спротив. Будь-яке поліпшення, зазвичай, йде в розріз з інтересами окремих особистостей. Це можуть бути іміджеві, статусні, фінансові або інші інтереси. Причиною конфлікту інтересів також можуть бути особисте несприйняття нового, слабо розвинуті ціннісні та фахові компетенції тощо.

Стратегія є основою, на якій будується модель формування цієї культури. Ця стратегія має містити бачення, як досягти встановлених цілей і подолати проблеми в тій тактиці реалізації програми змін, які поєднують в собі набір форм, методів і часових показників.

Лідерство і воля керівника проекту, засновані на ідеї позитивних змін, чітке бачення цілей і результатів, коаліція союзників мають стати рушійними силами реалізації цієї стратегії.

Креативна стратегія формування культури стратегічних комунікацій допоможе інституції наростити імідж і репутацію, отримати конкурентні переваги та зміцнити інституцію, досягнути необхідних ефектів, зокрема визнання лідера суспільством. Таргетинг забезпечить оптимальні шляхи досягнення лідером своєї місії.

**Висновок.** Успішна комунікація потребує сукупності ціннісних характеристик суб'єктів стратегічних комунікацій щодо розуміння, мотивації, поведінки, ставлення, сприйняття думок щодо вирішення проблем налагодження комунікацій із суспільством.

Культура стратегічних комунікацій являє собою сукупність матеріальних і духовних цінностей, створених у процесі реалізації комунікативних можливостей держави. Покладена в основу таргетингу, вона дає змогу досягнути кращого порозуміння з цільовими аудиторіями, постійно розширювати їх для підвищення ефективності комунікацій, а грамотне використання таргетингу дає змогу

раціонально використовувати ресурси, отримуючи максимальний ефект.

Військові лідери є важливими суб'єктами стратегічних комунікацій, особливо в умовах відсічі збройної агресії Російської Федерації проти України. Стратегічні комунікації – це важливий інструмент, який забезпечує ефективне виконання конституційних завдань, які покладуються на ЗС України військовими лідерами, завдяки формуванню у них культури стратегічних комунікацій.

Аналіз показав, що саме культура стратегічних комунікацій сучасних військових лідерів становить основу розвитку комунікаційних спроможностей МО і ЗС України, а окремі пропозиції щодо її формування знайшли відображення у цій статті.

Надалі матеріал статті може бути використано для розроблення теоретико-методологічних основ формування культури стратегічних комунікацій і їх складових в МО та ЗС України.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про затвердження Річної національної програми під егідою Комісії Україна – НАТО на 2017 рік : Указ Президента України від 08.04.2017 р. № 103/2017. URL: <https://www.president.gov.ua/documents/1032017-21670> (дата звернення: 12.10.2020).
2. Про затвердження Річної національної програми під егідою Комісії Україна – НАТО на 2018 рік : Указ Президента України від 28.03.2018 р. № 89/2018. URL: <http://www.president.gov.ua/documents/892018-23882> (дата звернення: 12.10.2020).
3. Сальнікова О. Ф., Міщенко В. Б., Шидлюх В. В., Антоненко С. І. Використання технологій стратегічних комунікацій в системі управління Збройними Силами України. *Сучасні інформаційні технології у сфері безпеки та оборони*. Київ, 2017. № 3 (30). С. 61–66.
4. Вербицька А. М., Савченко В. А. Система стратегічних комунікацій Міністерства оборони України та Збройних Сил України. *Наука і оборона*. 2017. № 1. С. 34–39.
5. ВКП 10-00(49).01. Доктрина зі стратегічних комунікацій. Київ, 2020.
6. ВКП 7-00(03).01. Доктрина розвитку військового лідерства у Збройних Силах України. Київ, 2020.
7. Семененко В. М., Іващенко А. М., Шидлюх В. В. Організація внутрішніх комунікацій у штабах і підрозділах Збройних Сил України під час виконання завдань у районі операції Об'єднаних сил. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2020. № 1 (68). С. 6–12.
8. PO (2009) 0141, NATO Strategic Communications Policy. NATO. 2009.
9. MC 0628, NATO Military Policy on Strategic Communication. NATO. 2017.
10. NU 0692, NATO StratCom Handbook. NATO. 2017.
11. MC 0457, NATO Military Policy on Public Affairs, NATO. 2011.
12. AJP-3.10, Allied Joint Doctrine for Information Operations. NATO. 2015.
13. MC 0402, NATO Military Policy on Psychological Operations. NATO. 2012.
14. MC 0411, NATO Military Policy on Civil-Military Cooperation (CIMIC) and Civil-Military Interaction (CMD). NATO. 2014.
15. AJP-3.9, Allied Joint Doctrine for Joint Targeting. NATO. 2016.

Стаття надійшла до редакційної колегії 15.12.2020

### The culture of Strategic Communication as the basis for targeting

#### Annotation

Strategic communications in the Armed Forces of Ukraine is a combination of communication capabilities and military activities in order to form an information environment to understand of support by Ukrainian society and the international community of the Armed Forces of Ukraine that creates a auspicious conditions for performing assigned task. However, scientific approaches to strategic communications as a culture, as well as to the rationale for the role of strategic communications culture in NATO-adopted targeting processes, remain insufficiently open and scientifically sound.

*Targeting process* is a joint, systematic and targeted lethal and non-lethal actions of strategic, operational and tactical levels of action, carried out in order to create specific effects, achieve military goals and desired results, with the purpose to protect Ukraine's sovereignty and territorial integrity, ensure its economic and information security.

*The culture of strategic communications* is a set of material and spiritual values created in the process of realization of communicative opportunities by the State on the basis of historically acquired experience and the level of its development in order to improve and harmonize measures to promote future goals.

Performed analysis showed that the culture of strategic communications of modern military leaders is the basis for the development of communication capabilities of the Ministry of Defense and the Armed Forces of Ukraine, and some proposals for its formation are reflected in this paper.

The material of the article can be used for developing theoretical and methodological foundations for the formation of a culture of strategic communications and their components in the Ministry of Defense and the Armed Forces of Ukraine.

**Keywords:** strategic communications; culture; targeting.

Фролов С. М., канд. іст. наук<sup>1</sup>  
Крилов І. О.<sup>2</sup>

(0000-0001-9873-4413)

(0000-0002-9810-5139)

<sup>1</sup> – Кафедра Військово-Морських Сил Національного університету оборони України імені Івана Черняховського, Київ;

<sup>2</sup> – Науково-дослідний центр Збройних Сил України “Державний океанаріум” Інституту Військово-Морських Сил Національного університету “Одеська морська академія”, Одеса

## Класифікація тематичних груп військово-морських термінів

**Резюме.** Розглянуто джерельну базу, яка стосується військово-морської термінології, надано пропозиції з визначення кількості та складу тематичних груп військово-морських термінів для обґрунтування структури термінологічного словника.

**Ключові слова:** військово-морська термінологія; класифікація тематичних груп; словник.

**Постановка проблеми.** В умовах триваючої збройної агресії Російської Федерації проти України та проведення спільних заходів оперативної підготовки Військово-Морських Сил Збройних Сил України з країнами – членами НАТО військово-морська термінологія потребує певного унормування та подальшого її впровадження у практичну діяльність сил (військ) та освітню діяльність вищих військових навчальних закладів. Вона тісно пов’язана з розвитком військово-морської справи, науки, освіти, зумовлена загальним соціально-історичним розвитком і підпорядкована фонетичним, словотвірним, лексико-семантичним і граматичним закономірностям української мови.

Відсутність українського військово-морського термінологічного словника з урахуванням сучасних термінів країн – членів НАТО, морського озброєння та застосування сил (військ) Військово-Морських Сил Збройних Сил України значно знижує рівень володіння спеціальною термінологією військовослужбовців.

Для створення військово-морського термінологічного словника, як системи військово-морських термінів, для їх єдиного розуміння та поступового впровадження в діяльність Військово-Морських Сил Збройних Сил України воєнної термінології країн – членів НАТО Командуванням Військово-Морських Сил Збройних Сил України проводиться науково-дослідна робота. Результатом роботи є розроблення до кінця 2022 р. проекту військово-морського термінологічного словника та надання його на затвердження Командувачу Військово-Морських Сил Збройних Сил України.

Актуальність теми зумовлена потребою визначення тематичних груп військово-

морських термінів Військово-Морських Сил Збройних Сил України для обґрунтування структури військово-морського термінологічного словника з урахуванням бойової діяльності національного військового флоту та країн – членів НАТО.

**Аналіз останніх досліджень і публікацій.** Про військово-морську термінологію йдеться як у нормативних документах, так і в наукових працях вітчизняних фахівців [1–10].

У сучасних доктринальних документах і словниках військових термінів [1–5] здійснена спроба поєднання окремих термінів для застосування їх на стратегічному і оперативно-стратегічному рівнях.

У дисертаційному дослідженні [6] визначається поняття “військово-морська термінологія”, розглядається процес формування української військово-морської термінології, зокрема шляхи її виникнення, лексико-семантичні та структурні особливості.

У публікації [7] приділяється увага актуальності використання військово-морської термінології в контексті захоплення російськими військовими трьох військових кораблів Військово-Морських Сил Збройних Сил України в Керченській протоці 25 листопада 2018 р.

У роботах [8, 9] розкривається специфіка понять “тематична група” і “морська справа”, надається класифікація, визначається склад основних тематичних груп української морської терміносистеми.

У тезах доповіді [10] наголошується на необхідності перегляду та систематизації військової терміносистеми України у зв’язку з процесами євроінтеграції.

У країнах – членах НАТО немає таких видань як військово-морський словник, в

іноземних виданнях [11–12] визначаються окремі військово-морські терміни лише для використання їх у тому документі, де вони наведені, зокрема, для підготовки та проведення операцій за стандартами НАТО.

**Метою статті є** надання пропозицій з визначення тематичних груп військово-морських термінів з урахуванням бойової діяльності національного військового флоту та країн – членів НАТО для обґрунтування структури термінологічного словника.

**Виклад основного матеріалу.** Авторами пропонується розглянути джерельну базу для визначення кількості та складу тематичних груп військово-морських термінів для обґрунтування структури військово-морського термінологічного словника. Для цього були обрані керівні та доктринальні документи [1–4], словник військових термінів [5], енциклопедичні видання [13–15], наукові праці у яких висвітлюється українська морська терміносистема [8, 9] та іноземні видання, у яких не розглядаються тематичні групи, а лише окремі військово-морські терміни країн – членів НАТО у вигляді Глосарія [11–12].

За результатами дослідження та з урахуванням сучасного стану і перспектив розвитку Військово-Морських Сил Збройних Сил України [2] пропонується визначити класифікацію тематичних груп військово-морських термінів:

#### 1. Загальні положення.

1.1. Військово-Морські Сили – як вид Збройних Сил.

1.2. Оперативне мистецтво Військово-Морських Сил.

2. Організація та підготовка сил (військ) Військово-Морських Сил.

2.1. Організація та підготовка підводних сил, морської авіації до виконання завдань за призначенням, а також особового складу.

2.2. Організація та управління силами (військами) у мирний і воєнний час.

2.3. Організація та підготовка органів військового управління, надводних сил (кораблів, суден, угруповань, загонів, тактичних груп) до виконання завдань за призначенням, а також особового складу.

2.4. Організація і підготовка військових частин (підрозділів) морської піхоти та артилерійських підрозділів берегових ракетно-артилерійських військ до виконання завдань за призначенням, а також особового складу.

3. Застосування сил (військ) Військово-Морських Сил.

3.1. Застосування підводних сил (підводних човнів, загонів, тактичних груп) в операціях (бойових діях).

3.2. Застосування надводних сил (кораблів, суден, угруповань, загонів, тактичних груп) в операціях (бойових діях).

3.3. Застосування морської авіації в операціях (бойових діях).

3.4. Застосування морської піхоти (тактичних груп) в операціях (бойових діях).

3.5. Застосування артилерійських підрозділів берегових ракетно-артилерійських військ в операціях (бойових діях).

3.6. Застосування в операціях (бойових діях) сил і засобів забезпечення Військово-Морських Сил.

3.7. Ведення видів бойових (спеціальних) дій, підтримання (виконання завдань) силами (військами) Військово-Морських Сил (протиповітряна оборона, протичовнове забезпечення, протипідводно-диверсійне забезпечення, протимінне забезпечення, спостереження і розвідка, радіоелектронна боротьба, радіоелектронне забезпечення, ХБРЯ захист, пошуково-рятувальне забезпечення, геопросторове та гідрометеорологічне (метеорологічна) підтримання, навігаційно-гідрографічне забезпечення).

4. Морське озброєння і військова техніка.

4.1. Класифікація, типи, ранги, найменування, нумерація кораблів (суден).

4.2. Будова корабля (приміщень, систем, вузлів, механізмів) і літальних апаратів (БПЛА) морської авіації.

4.3. Морехідні (льотні), бойові й тактичні властивості кораблів (суден) і літальних апаратів (БПЛА) морської авіації (морського озброєння і техніки).

4.4. Проектування, будівництва, експлуатації та ремонту кораблів (суден), літальних апаратів морської авіації (морського озброєння і техніки);

4.5. Озброєння, системи, вузли, механізми і засоби корабля.

4.6. Позначення дій (елементів руху) корабля.

4.7. Позначення предметів такелажного обладнання та рангоуту корабля.

5. Кораблеводіння, військово-морська географія, гідрографія, морська навігація, гідрометеорологія.

У табл. 1 наведено порівняння морських термінів із документами [11–12].  
 запропонованих тематичних груп військово-

Таблиця 1

№ з/п	Термінологічний словник		Джерело НАТО	Примітки
	тематична група	рубрики		
1	<i>Загальні положення</i>	1.1. Військово-Морські Сили – як вид ЗС	Allied Joint Doctrine for Maritime Operations [12]	Співпадає частково (обумовлено застосуванням ВМС НАТО як військово-політичної основи солідарності та взаємних зобов'язань)
		1.2. Оперативне мистецтво ВМС	Allied Joint Doctrine for Maritime Operations [12]	Співпадає
2	<i>Організація та підготовка сил (військ) Військово-Морських Сил</i>	2.1. Організація та підготовка підводних сил, морської авіації до виконання завдань за призначенням, а також особового складу	NATO Glossary of Terms and Definitions [11] Allied Joint Doctrine for Maritime Operations [12]	Співпадає
		2.2. Організація та управління силами (військами) у мирний та воєнний час	NATO Glossary of Terms and Definitions [11]	Співпадає частково (відсутня така назва, обумовлено специфікою використання в НАТО)
		2.3. Організація та підготовка органів військового управління, надводних сил (кораблів, суден, угруповань, загонів, тактичних груп) до виконання завдань за призначенням, а також особового складу	Allied Joint Doctrine for Maritime Operations [12]	Співпадає
		2.4. Організація і підготовка військових частин (підрозділів) морської піхоти та артилерійських підрозділів берегових ракетно-артилерійських військ до виконання завдань за призначенням, а також особового складу	NATO Glossary of Terms and Definitions [11]	Співпадає частково (відсутня така назва, визначені окремі терміни щодо морської піхоти, взагалі відсутні терміни щодо берегових ракетно-артилерійських військ)
3	<i>Застосування сил (військ) Військово-Морських Сил</i>	3.1. Застосування підводних сил (підводних човнів, загонів, тактичних груп) в операціях (бойових діях)	NATO Glossary of Terms and Definitions [11] Allied Joint Doctrine for Maritime Operations [12]	Співпадає
		3.2. Застосування надводних сил в операціях (бойових діях)	NATO Glossary of Terms and Definitions [11] Allied Joint Doctrine for Maritime Operations [12]	Співпадає
		3.3. Застосування морської авіації в операціях (бойових діях)	NATO Glossary of Terms and Definitions [11] Allied Joint Doctrine for Maritime Operations [12]	Співпадає
		3.4. Застосування морської піхоти (тактичних груп) в операціях (бойових діях)	NATO Glossary of Terms and Definitions [11] Allied Joint Doctrine for Maritime Operations [12]	Не співпадає
		3.5. Застосування артилерійських підрозділів берегових ракетно-артилерійських військ в операціях (б/д)	NATO Glossary of Terms and Definitions [11] Allied Joint Doctrine for Maritime Operations [12]	Не співпадає
		3.6. Застосування в операціях (бойових діях) сил і засобів забезпечення ВМС	NATO Glossary of Terms and Definitions [11] Allied Joint Doctrine for Maritime Operations [12]	Співпадає частково (обумовлено специфікою забезпечення ВМС в НАТО)
		3.7. Ведення видів бойових (спеціальних) дій, підтримання (виконання завдань) силами (військами) ВМС	NATO Glossary of Terms and Definitions [11] Allied Joint Doctrine for Maritime Operations [12]	Співпадає частково (обумовлено специфікою бойових (спеціальних) дій,



**ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ЗБРОЙНИХ СИЛ**

№ з/п	Термінологічний словник		Джерело НАТО	Примітки
	тематична група	рубрики		
				підтриманням (виконання завдань) силами (військами) ВМС в НАТО)
4	<i>Морське озброєння і військова техніка</i>	4.1. Класифікація, типи, ранги, найменування, нумерація кораблів (суден)	NATO Glossary of Terms and Definitions [11]	Співпадає частково (обумовлено специфікою класифікації кораблів (суден) ВМС у НАТО)
		4.2. Будова корабля (приміщень, систем, вузлів, механізмів) і літальних апаратів (БПЛА) морської авіації	NATO Glossary of Terms and Definitions [11]	Співпадає частково (обумовлено специфікою побудови кораблів і літальних апаратів (БПЛА) морської авіації в НАТО)
		4.3. Морехідні (льотні), бойові й тактичні властивості кораблів (суден) і літальних апаратів (БПЛА) морської авіації (морського озброєння і техніки)	NATO Glossary of Terms and Definitions [11]	Співпадає частково (обумовлено специфікою кораблів і літальних апаратів (БПЛА) морської авіації в НАТО)
		4.4. Проектування, будівництво, експлуатації та ремонту кораблів (суден), літальних апаратів морської авіації (морського озброєння і техніки)	NATO Glossary of Terms and Definitions [11] Allied Joint Doctrine for Maritime Operations [12]	Не співпадає (обумовлено специфікою національного проектування, будівництва, експлуатації та ремонту кораблів (суден), літальних апаратів морської авіації (морського озброєння і техніки))
		4.5. Озброєння, системи, вузли, механізми і засоби корабля	NATO Glossary of Terms and Definitions [11] Allied Joint Doctrine for Maritime Operations [12]	Не співпадає (обумовлено специфікою національного озброєння, систем, вузлів, механізмів і засобів корабля)
		4.6. Позначення дій (елементів руху) корабля	NATO Glossary of Terms and Definitions [11] Allied Joint Doctrine for Maritime Operations [12]	Співпадає частково (обумовлено специфікою елементів руху корабля ВМС у НАТО)
		4.7. Позначення предметів такелажного обладнання та рангоуту корабля	NATO Glossary of Terms and Definitions [11] Allied Joint Doctrine for Maritime Operations [12]	Не співпадає
		5	<i>Кораблеводіння, військово-морська географія, гідрографія, морська навігація, гідрометеорологія</i>	5.1. Кораблеводіння
5.2. Військово-морська географія	NATO Glossary of Terms and Definitions [11]			Співпадає
5.3. Гідрографія	NATO Glossary of Terms and Definitions [11]			Співпадає
5.4. Морська навігація	NATO Glossary of Terms and Definitions [11]			Співпадає
5.5. Гідрометеорологія	NATO Glossary of Terms and Definitions [11]			Співпадає

Аналіз табл. 1 дає змогу дійти висновків, що запропоновані рубрики співпадають (зокрема частково) з рубрикацією НАТО на 70 %.

Аналізуючи ці джерела варто зазначити, що в них наведена лише частина існуючих тематичних груп і військово-морських термінів.

Визначену класифікацію тематичних груп військово-морських термінів пропонується погодити з Командуванням Військово-Морських Сил Збройних Сил України.

**Висновки.** Визначена класифікація тематичних груп дасть змогу обґрунтувати структуру військово-морського термінологічного словника як системи військово-морських термінів з урахуванням термінології країн – членів НАТО, для їх єдиного розуміння і поступового впровадження в діяльність Військово-Морських Сил Збройних Сил України та освітній процес вищих військових навчальних закладів.

**Надалі** перелік військово-морських термінів (дефініцій) за напрямом діяльності Військово-Морських Сил Збройних Сил України з урахуванням термінів країн – членів НАТО може бути використаний під час розроблення військового стандарту.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про затвердження Морської доктрини України на період до 2035 року : Постанова Кабінету Міністрів України від 07.10.2009 р. № 1307. Дата оновлення: 28.10.2020. URL: <https://zakon.rada.gov.ua/laws/show/1307-2009-%D0%BF#Text> (дата звернення: 20.03.2021).
2. Доктрина. Військово-Морські Сили Збройних Сил України : затв. Головнокомандувачем ЗС України 19.01.2021 р.
3. Доктрина з навігаційно-гідрографічного забезпечення військ (сил) в об'єднаних операціях : затв. нач. ГШ ЗС України 29.12.2020 р.
4. Про затвердження Положення про корабельну службу у Військово-Морських Силах Збройних Сил України : наказ Міністра оборони України від 17.12.2003 р. № 415.

5. Словник військових термінів та скорочень (аббревіатур). Київ : ВНУ ГШ ЗС України, 2020. 52 с.
6. Андріянова О. Я. Військово-морська термінологія української мови: етапи формування та семантика : дис. ... канд. філол. наук : 10.02.01 / Запорізький національний університет. Запоріжжя, 2011. 199 с.
7. Новітні тенденції функціонування української військової терміносистеми / Жалай В. Я., Линник Т. Г., Миронюк Т. М., Пархоменко А. Ф., Рубашова Л. М. // Лінгвістика XXI століття: нові дослідження і перспективи : часопис. Київ : Центр наукових досліджень та викладання іноземних мов НАН України, 2018. 43 с. URL: [http://langcenter.kiev.ua/Chasopys\\_2018.html](http://langcenter.kiev.ua/Chasopys_2018.html) (дата звернення: 22.03.2021).
8. Дакі О. А. Українська морська терміносистема: предметно-семантична організація. *Наукові праці Кам'янець-Подільського національного університету імені Івана Огієнка. Філологічні науки.* Кам'янець-Подільський, 2015. Вип. 38. С. 126–130.
9. Дакі О. А., Тематичні групи в українській морській терміносистемі. *Наукові записки Національного університету "Острозька академія". Серія: Філологія.* Острог, 2015. Вип. 54. С. 97–100.
10. Войцішук А. Етапи становлення української військової термінології. *Природничі та гуманітарні науки. Актуальні питання : матеріали VIII Всеукр. студентської наук.-техн. конф., м. Тернопіль, 23–11 квіт. 2015 р. Тернопіль, 2015, Том 2. С. 129–130.*
11. NATO Glossary of Terms and Definitions (AAP-6). North Atlantic Treaty Organization NATO Standardization Office (NSO), 2020.
12. Allied Joint Doctrine for Maritime Operations (AJP-3.1, Edition A Version 1). Brussels (Belgium): NATO Standardization office, 2016.
13. Военный энциклопедический словарь / гл. ред. Н. В. Огарков. Москва : Воениздат, 1983. 863 с.
14. Военно-морской словарь / гл.ред. В. Н. Чернавин. Москва : Воениздат, 1989. 511с.
15. Военно-морской энциклопедический словарь / под. ред. В. И. Куроедова. 2-е изд., испр. и доп. Москва : Воениздат, 2003. 960 с.

Стаття надійшла до редакційної колегії 24.04.2021

### Classification of thematic groups of naval terms

#### Annotation

In the context of the ongoing armed aggression of the Russian Federation against Ukraine and the implementation of joint measures of operational training of the Naval Forces of the Armed Forces of Ukraine with NATO member countries, naval terminology needs to be standardized and further implemented in practice.

The purpose of the article is to provide proposals for defining thematic groups of naval terms, taking into account NATO standards, in order to substantiate the structure of the glossary.

The general scientific methods used are analysis and synthesis. These methods provided the formulation of mandatory formal attributes of the article, namely: the formulation of the problem, its relevance, purpose, theoretical provisions, conclusions and justification of further research.

According to the results of the study, the following classification of thematic groups is determined: general provisions; organization and training of forces (troops) of the Naval Forces of the Armed Forces of Ukraine; use of forces (troops) of the Naval Forces of the Armed Forces of Ukraine; naval armaments and military equipment; navigation, naval geography, hydrography, maritime navigation, hydrometeorology.

The list of naval terms (definitions) by area of activity, taking into account the terms of NATO member countries can be used in the development of the Military Standard.

**Keywords:** naval terminology; classification of thematic groups; dictionary.

Гудима О. П., канд. техн. наук, ст. наук. співроб.

(0000-0002-3494-8583)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

## Аналіз науково-методичного апарату формування організаційно-функціональних структур систем стратегічного рівня

**Резюме.** Проведено аналіз використання традиційних підходів до реалізації структурного синтезу складної системи та використання ситуаційного підходу. Збільшення кількості та щільності потоку кризових ситуацій відпрацьовується в системах збільшенням елементів структури, що потребує удосконалення методів структурно-параметричного синтезу складних організаційно-функціональних структур систем.

**Ключові слова:** науково-методичний апарат; організаційно-функціональна структура системи; ситуаційне управління; кризова ситуація; надмірність; структурно-параметричний синтез.

**Постановка проблеми.** Сучасні міжнародні конфлікти на сьогодні не можна оцінювати з погляду традиційних підходів до ведення бойових дій, їх можна охарактеризувати терміном “гібридна війна”, яка є комбінацією традиційних і нетрадиційних методів ведення війни.

Водночас, кожна країна світу постійно стикається в різних сферах своєї діяльності із загрозами, які можуть вплинути на економічні показники та стабільність функціонування самої держави. Кожна загроза (потенційна та реальна) може перерости в кризову ситуацію (КС) різного рівня. КС вважається крайнє загострення протиріч, гостра дестабілізація становища в будь-якій сфері діяльності, регіоні, країні [1].

Зазначене підтверджує і поява пандемії COVID-19, яка змусила всі держави світу ситуативно реагувати на загрози та приймати непопулярні рішення щодо зменшення її наслідків [2].

Можливими варіантами дій щодо реагування на КС є: реагування на виникаючі КС; прогнозування появи КС і завчасне запобігання їх виникненню.

Раннє запобігання (реагування) створює сприятливе підґрунтя для визначення цілей, вироблення можливих планів дій і їх порівняння, аналізу можливого застосування обраного варіанта і реакції конфлікуючих сторін, а також розроблення вірогідних сценаріїв розвитку ситуації. Зважаючи на важливість раннього запобігання, в усіх заходах, спрямованих на врегулювання криз і запобігання конфліктам, значна увага приділяється отриманню, оцінюванню та аналізу інформації на ранніх етапах [3].

Як за першим так і за другим варіантом дій спостерігається певна закономірність. За

умови достатньої частоти появи КС (за певними напрямками) створюються додаткові організаційно-функціональні структури (ОФС) в складі відповідних систем (постійні чи тимчасові) для відпрацювання відповідного потоку КС.

Так, наприклад, у разі збільшення щільності появи загроз, які можуть призвести надалі до КС в інформаційній сфері відповідно до [4] створено Центр протидії дезінформації. Центр протидії дезінформації створюється для досягнення цілей і завдань Стратегії національної безпеки України, протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері, а також для забезпечення інформаційної безпеки України, ефективної протидії пропаганді, деструктивним дезінформаційним впливам та кампаніям, недопущення маніпулювання громадською думкою [4].

Як показує практика, під час побудови ОФС систем стратегічного рівня широкого використання набули експертні методи, які мають низку суттєвих обмежень і недоліків, основними з яких є суб'єктивність і великий час для набуття відповідних спроможностей щодо реагуванню на КС.

Під *ОФС систем стратегічного рівня* розуміється система взаємозв'язків і підпорядкованість організаційних одиниць (підрозділів), які характеризуються чітким розподілом функцій для забезпечення поставлених завдань та проектування організаційних форм управління на рівні вищого державного (військового) керівництва.

Прикладами ОФС систем стратегічного рівня є: система протиповітряної оборони України; Командування повітряно-космічної оборони Північної Америки

(NORAD) - об'єднана система аерокосмічної оборони США та Канади, основними завданнями якої є забезпечення контролю за повітряним і навколосезним простором Північної Америки, раннього попередження про повітряно-космічний напад, протиповітряної і протиракетної оборони двох країн.

З огляду на зазначене, доцільно провести аналіз існуючого науково-методичного апарату синтезу ОФС систем, виявити його недоліки та обмеження застосування, а також провести аналіз можливостей використання ситуаційного підходу для формування ОФС систем стратегічного рівня.

**Аналіз основних досліджень і публікацій.** Структурний синтез складної системи, зокрема: етапи формування вимог до системи; вибір складових системи, рівня їх деталізації, формування варіантів побудови та опис взаємодії компонент; вибір оптимального варіанта побудови системи розглядались у працях [5–10]. Розв'язанню задачі параметричного синтезу складних систем присвячено роботи [5, 7–9].

У роботах [11–13] проведено аналіз використання ситуаційного підходу під час управління великими системами. Використання ситуаційного підходу під час синтезу системи забезпечення інформаційної безпеки було розглянуто в роботах [14–15].

Загалом, існуючі дослідження проводились, як правило, в межах існуючих підходів для вирішення певних часткових проблемних питань, але не було опрацьовано питання щодо формування ОФС систем стратегічного рівня (удосконалення ОФС систем стратегічного рівня) з урахуванням збільшення щільності появи КС.

**Мета статті.** Аналіз науково-методичного апарату формування ОФС систем стратегічного рівня (зокрема, можливості використання ситуаційного підходу), що дасть змогу визначити основні шляхи його подальшого розвитку з урахуванням збільшення щільності появи КС.

**Виклад основного матеріалу.** Будь-яка складна система визначається трьома категоріями: елементами, відношеннями, властивостями. Однозначний і повний опис цих категорій визначають систему, її структуру, параметри та ефективність. Метою синтезу системи є конкретизація і визначення оптимальних (раціональних) рішень для вказаних категорій. Зі свого боку синтез складної системи передбачає розв'язання задач структурного та параметричного синтезу.

Формування властивостей системи, вимог до неї та виконуваних функцій здійснюється на підставі аналізу особливостей застосовності розробленої системи та виконуваних з її використанням завдань. Традиційні підходи до реалізації **структурного синтезу** складної системи можна умовно поділити на два класи. *Перший* полягає в евристичному синтезі структури, який базується на визначенні складових системи та відношень між ними на підставі аналізу виконуваних функцій і вимог до неї. Результатом такого підходу є суто суб'єктивні рішення про склад і структуру системи у вигляді одного безальтернативного варіанта. Такий підхід застосовується, як правило, у разі складного математичного опису (формалізації) задачі синтезу, а етап формування структури найчастіше називають розробленням [16, 17]. *Другий* клас реалізації процесу побудови (синтезу) структури складної системи базується на використанні методів оптимізації і полягає у виборі з надмірної кількості варіантів побудови системи оптимальної структури за обраним критерієм, або системою критеріїв. Альтернативні варіанти побудови системи можна формувати як евристичними методами, так і з використанням методів математичного синтезу. Зі свого боку процедуру вибору оптимальної структури системи із сукупності альтернатив можна реалізувати з використанням оптимізаційних методів як за однокритеріальною, так і за багатокритеріальною моделлю [9, 18]. Однокритеріальні оптимізаційні моделі мають відносну простоту реалізації етапів структурного синтезу, однак порівняно з багатокритеріальними моделями не забезпечують всебічного врахування в остаточних результатах синтезу усієї сукупності суперечливих вимог.

Для багатокритеріальних задач властиве застосування низки (вектора) суперечливих критеріїв. Саме наявність суперечності між частинними критеріями оптимальності системи не дає змоги розв'язувати задачу синтезу підходами, характерними для однокритеріальних задач. Суперечливість частинних критеріїв оптимальності виявляється в тому, що не можливо досягти оптимуму за всіма критеріями одночасно. Поліпшення одного критерію призводить до погіршення інших. У цьому разі застосовуються спеціальні методи розв'язання багатокритеріальних задач [9, 19]. Можна виділити чотири класи основних методів розв'язання задач векторної оптимізації [19]:

оптимізація послідовності частинних критеріїв у разі введення пріоритетів і призначенні поступок;

виділення парето-оптимальних рішень;

оптимізація на основі компромісних відношень;

наближення до певного ідеального значення.

Перевагою методів *першого* класу є упорядкування критеріїв за значущістю і побудова процедур послідовної оптимізації за кожним частинним критерієм. Його недоліком можна вважати складності в обґрунтованості ранжування частинних критеріїв.

Суть методів *другого* класу полягає у визначенні сукупності рішень з області Парето з подальшим наданням права вибору єдиного з них особі, яка приймає рішення. Зазначені методи мають досить значну обчислювальну складність, а необхідність прийняття остаточного рішення із сукупності альтернатив, які належать області Парето, накладає додаткові обмеження на його використання. Особливо це виявляється саме у виборі оптимальних структур складних систем.

Методи *третього* класу (оптимізація на основі компромісних відношень) полягають у визначенні певного оптимального розв'язку з відомою поступкою між частинними критеріями оптимальності. У цьому разі формується узагальнений критерій оптимальності із сукупності частинних за певним правилом і визначається його екстремум відносно шуканого параметра оптимізації. Тобто фактично багатокритеріальна задача зводиться до однокритеріальної форми. Існує велика кількість способів формування узагальненого критерію [9, 19]. Перевагою цього класу методів є належність розв'язку області Парето. Саме ці методи широко застосовують для аналізу складних систем. До складностей методів третьої групи слід віднести обмеження, пов'язані із визначенням вагових коефіцієнтів частинних критеріїв.

Методи *четвертого* класу полягають у введенні певної ідеальної точки, яка належить області Парето, і наближенні оптимальних значень шуканих параметрів до неї за всіма частинними критеріями. Різноманітність критеріїв наближення породжує відповідно різноманітність існуючих методів цього класу за квадратичною, лінійною нормою та ін. [9, 19]. Основним недоліком таких методів є невизначеність або складності у формуванні ідеальної точки.

З аналізу випливає, що найбільшого

поширення набули методи багатокритеріальної оптимізації, які належать до третього і четвертого класів, однак щоразу вибір для використання певного методу залежить від специфіки та особливостей конкретної задачі. Практичній реалізації процесу структурного синтезу складних систем присвячено значну кількість робіт. Найбільш показові результати цього процесу подано в працях [17–20].

**Параметричний синтез** складної системи полягає у визначенні параметрів елементів заданої структури [19]. Розв'язання задачі параметричного синтезу потребує встановлення показників або критеріїв ефективності, формування оптимізаційної моделі параметричного синтезу системи та визначення оптимальних параметрів.

Система критеріїв може встановлюватись евристичним методом і мати ієрархію функцій – факторів – показників – критеріїв. Перший підхід має більш обумовлений характер показників (критеріїв) і застосовується, як правило, на етапі розроблення системи. Другий підхід характерний для типу систем із достатнім досвідом їх розроблення. Якщо встановлено єдину цільову функцію ефективності щодо вибору параметрів системи, задача матиме однокритеріальну модель [19]. Для параметричного синтезу систем за однокритеріальними моделями використовуються методи теорії операцій. Однокритеріальні моделі є простими для формування та аналізу і визначення параметрів системи, однак вони не забезпечують високої достовірності отримуваних рішень через спрощення відображення початкових задач. За наявності вектора критеріальних вимог матимемо багатокритеріальну оптимізаційну модель [9]. У цьому разі всі вимоги до параметрів системи враховуються у формі критеріїв. Задача параметричного синтезу за багатокритеріальною моделлю розв'язується або методом зведення її до однокритеріальної за певним критерієм [9], або альтернативними методами [19]. Для перших характерним є отримання математично обґрунтованого єдиного розв'язку, що, як правило, належить до області Парето. Для альтернативних методів отримується низка розв'язків в області Парето і має місце значний суб'єктивізм в алгоритмі зведення їх до єдиного розв'язку [19].

Аналіз існуючих підходів показує, що в більшості випадків структурний і параметричний синтез ОФС систем здійснюється за однокритеріальними

моделями, що не забезпечує повною мірою врахування усього спектра суперечливих вимог до системи і призводить до зниження якості результатів синтезу.

Окрім того, у кожному конкретному випадку для визначення оптимальної за структурою і параметрами ОФС систем обираються відповідні методи з урахуванням специфіки розв'язуваних цільових задач. Через це необхідним є запровадження багатокритеріальних підходів до структурного і параметричного синтезу складних ОФС систем.

У [21] авторами запропоновано методіку обґрунтування раціональної структури системи інформаційної безпеки Міністерства оборони та Збройних Сил України на основі методу кластерного аналізу, метою якого є пошук наявних структур, що виражається в утворенні груп схожих між собою об'єктів – кластерів. Зазначений підхід дає змогу класифікувати об'єкти не за однією, а за декількома ознаками одночасно як сукупність взаємопов'язаних функціональних підсистем із визначенням функцій кожної з них.

У [22] авторами розглядається системно-концептуальні положення о моделюванні процесів функціонування складних багатоструктурних систем військового призначення і управління їх структурною динамікою в умовах змінювання оперативно-тактичної обстановки в районі ведення бойових дій.

Аналіз відомих методологічних підходів до реалізації процесів та побудови ОФС систем і результати їх практичного застосування переконливо доводить наявність проблем у принципах побудови та методологічній базі обробки в них інформації.

Побудова відомих ОФС систем орієнтована на формування статичної надмірної структури системи і алгоритмів їх функціонування з рівномірним розподілом завдань між усіма її складовими та вибірковістю елементів лише за їх призначенням і ієрархією горизонтально-вертикальних зв'язків.

Так, наприклад, збільшення кількості та щільності потоку КС і їх типів відпрацьовується через збільшення елементів структури за відповідними призначенням і рівнем, що породжує інформаційну надмірність даних для обробки. Зазначене ускладнює реалізувати динамічний перерозподіл обмежених сил і засобів спостереження і дій за загрозами та функціонування ОФС в умовах реального часу,

що може призвести до зриву виконання цільових завдань реагування на КС.

Утім останнім часом широкого розвитку набули впровадження синергетичні методи в задачах управління, обробки інформації і побудови складних ОФС систем. Зокрема це стосується методів ситуативного управління.

Так у [17] авторами розроблена багатокритеріальна методика ситуаційного управління структурою і параметрами системи забезпечення інформаційної безпеки.

У [23] авторами опрацьовано математичний апарат для розв'язання задач щодо підтримання прийняття рішень під час ситуаційного управління операцією.

Організація відповідно до ситуаційного підходу розглядається як складна комплексна і багаторівнева система, у яку закладені адаптивні принципи. Завдання ситуаційної теорії - вивчати залежність методів управління від того, у якій ситуації, в яких унікальних умовах знаходиться їх організація [24].

Технологія ситуаційного аналізу передбачає виділення типових ситуацій у зовнішньому середовищі та об'єднанням цих ситуацій у блоки на основі схожих стратегій і дій керівників. За умови такого підходу головне завдання полягає в розпізнаванні ситуації, ідентифікації її з еталонною ситуацією і передбачення на цій основі подальшого розвитку подій [24].

Зважаючи на значні розміри ОФС систем стратегічного рівня, застосування ситуаційного підходу під час синтезу ОФС загалом призведе до підвищення інерційності роботи.

З огляду на зазначене, можна стверджувати, що традиційні підходи до побудови ОФС систем з упровадженням принципів ситуаційного управління спрямовані на ситуативну зміну властивостей системи завдяки формуванню унікального переліку дій відповідно до виниклої КС. Ця обставина у жодному разі не розв'язує методологічних і технологічних проблем структурного характеру, притаманних традиційним підходам до побудови складних ОФС систем і не розв'язує проблему їх ефективного функціонування в умовах значної динаміки зміни поточної ситуації і підвищення потоку КС. Зазначене потребує розвитку методів структурно-параметричного синтезу складних ОФС систем з упровадженням методів багатокритеріального аналізу та ситуаційного управління.

Доцільно здійснити декомпозицію ОФС системи (системи управління Збройних Сил України та ін.) у вигляді постійної та

флуктуаційної складових. Під *постійною складовою* розуміється лінійна організаційна структура підсистеми, яка характеризується: чіткістю, простотою взаємодії і управління; узгодженістю дій виконавців та інше, і, як правило, призначена для виконання завдань, які постійно повторюються. Під *флуктуаційною складовою* підсистеми розуміється функціональна організаційна структура, до якої закладені адаптивні принципи. Ця складова характеризується інформаційною оперативністю, розв'язаністю вищого керівництва.

Використання такого наукового методу як декомпозиція дасть змогу замінити вирішення одного великого завдання вирішенням серії менших завдань, нехай і взаємопов'язаних, але більш простих. Декомпозиція, як процес розділення, дає змогу розглядати будь-яку досліджувану систему як складну, що складається з окремих взаємопов'язаних підсистем, які, зі свого боку, також можуть бути розділеними на частини.

Так, наприклад, реалізація або адаптація, функціональної організаційної структури підсистеми під КС буде здійснюватися так: розглянемо дві ситуації – потік загроз (потенційних КС) в інформаційному просторі не змінюється, потік (потенційних КС) в інформаційному просторі суттєво збільшується і перевищує заздалегідь визначений поріг.

У першій ситуації, функціональній організаційній структурі підсистеми (ситуаційному центрі, інформаційно-аналітичному підрозділу) достатньо спроможностей для виконання визначених завдань і структура системи не змінюється. У другій ситуації – ситуаційний центр (інформаційно-аналітичний підрозділ) не спроможний опрацювати потік (потенційних КС) в інформаційному просторі, тому створюється додатковий підрозділ для опрацювання зазначеного потоку КС. У разі зникнення загроз (потенційних КС) в інформаційному просторі зазначений підрозділ буде реорганізовуватися.

Так, наприклад, під час побудови державної системи управління силами оборони в кризових ситуаціях воєнного характеру здійснюватимемо декомпозицію системи державного управління на дві складові:

лінійна організаційна структура – Верховна Рада України, Президент України, Кабінет Міністрів України, Міністерство оборони України, центральні органи виконавчої влади, Головнокомандувач Збройних Сил України, Генеральний штаб

Збройних Сил України, Командування об'єднаних сил);

функціональна організаційна структура – системи ситуаційних центрів (пунктів управління) для інформаційно-аналітичної підтримки процесу управління у разі виникнення кризових ситуацій (невоєнного і воєнного характеру).

**Висновки.** Отже, результати проведеного аналізу свідчать, що існуючий науково-методичний апарат синтезу ОФС систем стратегічного рівня не дає змоги повною мірою врахувати нарощування інформаційних потоків, які потрібно обробляти. Особливо це є критичним під час прогнозування та реагування на КС. Найбільш перспективним підходом з означеного питання, який дасть змогу врахувати нові чинники, що набули актуальності за останній час, є використання ситуаційного управління.

Доцільно опрацювання науково-математичного апарату щодо декомпозиції ОФС систем стратегічного рівня на дві складові: постійної (відносно незмінної) і флуктуаційної. Синтез структури та параметрів постійної складової доцільно здійснювати за класичним трактуванням задачі параметричного синтезу складної системи. Під час синтезу структури та параметрів флуктуаційної складової доцільно використовувати ситуаційний підхід. Саме на це має сенс зосередити увагу під час **подальших досліджень**.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про Раду національної безпеки і оборони України : Закон України від 05.03.1998 р. № 183/98-ВР. URL: <https://zakon.rada.gov.ua/laws/show/183/98-%D0%B2%D1%80#Text> (дата звернення: 08.03.2021).
2. Гудима А. О., Гудима О. П. Ситуаційний підхід при реагуванні на глобальну фінансову кризу 2020 року. Cambridge: Education and science of today: intersectoral issues and development of sciences: Collection of scientific papers “ΛΟΓΟΣ” with Proceedings of the I International Scientific and Practical Conference. (Vol. 1). Cambridge-Vinnitsia : 19 March, 2021. P. 93–96. URL: <https://doi.org/10.36074/logos-19.03.2021.v1.33> (дата звернення: 08.03.2021).
3. Кріндлер Джон. Передбачення кризи. Врегулювання кризових ситуацій. *НАТО Ревю*. НАТО, Брюссель, Бельгія. Зима, 2002. С. 17–19. URL: [www.nato.int/review](http://www.nato.int/review) (дата звернення: 04.03.2021).
4. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року “Про створення Центру протидії дезінформації” : Указ Президента України від 19.03.2021 р. № 106/2021

- URL: <https://www.president.gov.ua/documents/1062021-37421> (дата звернення: 02.03.2021).
5. Воронин А. Н. Многокритериальное распределение ограниченных ресурсов. *Проблемы управления и информатики*. 2010. № 4. С. 143–150.
  6. Цвиркун А. Д. Основы синтеза структуры сложных систем. Москва : Наука, 1982. 200 с.
  7. Антушев Г. С. Методы параметрического синтеза сложных технических систем. Москва : Наука, 1986. 88 с.
  8. Баранов Г. Л., Макаров А. В. Структурное моделирование сложных динамических систем. Киев : Наук. думка, 1986. 272 с.
  9. Брахман Т. Р. Многокритериальность и выбор альтернатив в технике. Москва : Радио и связь, 1984. 288 с.
  10. Вермишев Ю. Х. Методы автоматического поиска решений при проектировании сложных технических систем. Москва : Радио и связь, 1982. 152 с.
  11. Горшенин В. XXI век. Ситуационное управление как основа устойчивого развития государства. URL: [http://www.rau.su/observer/N5-6\\_97/5-6\\_02.htm](http://www.rau.su/observer/N5-6_97/5-6_02.htm) (дата звернення: 02.03.2021).
  12. Клык Ю. И. Ситуационное управление большими системами. Москва : Энергия, 1974. 136 с.
  13. Цветков В. Я. Ситуационное управление образовательными учреждениями. *Методы управления и моделирования в бизнесе и образовании*. 2005. Вып. 9. С. 31–33.
  14. Багатокритеріальні математичні моделі ситуаційного управління та самоорганізації у складних інформаційних системах : монографія / Ю. Г. Даник, О. О. Писарчук, В. І. Шестаков та ін. Житомир : Рута, 2016. 232 с.
  15. Соколов К. О., Писарчук О. О., Гудима О. П. Розроблення багатокритеріальної методики ситуаційного управління структурою і параметрами системи забезпечення інформаційної безпеки. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2016. № 3 (58). С. 24–32.
  16. Анкудинов Г. И. Синтез структуры сложных объектов: логико-комбинированный подход. Ленинград : Леингр. ун-т, 1986. 260 с.
  17. Писарчук О. О. Багатокритеріальна математична модель структурного та параметричного синтезу складної інформаційної системи. *Інформаційна безпека* : зб. наук. пр. СУНУ імені В. Даля. Северодонецьк, 2010. № 1 (3). С. 38–44.
  18. Дубов Ю. А., Травкин С. И., Янищев В. Н. Многокритериальные модели формирования и выбора вариантов систем. Москва : Наука, 1986. 296 с.
  19. Антушев Г. С. Методы параметрического синтеза сложных технических систем. Москва : Наука, 1986. 88 с.
  20. Герасимов Б. М., Дивизинюк М. М., Субач И. Ю. Системы поддержки принятия решений: проектирование, применение, оценка эффективности : моногр. Севастополь : СНИЭ и П, 2004. 320 с.
  21. Косогов О. М., Сірик А. О. Методика визначення структури системи інформаційної безпеки Міністерства оборони та Збройних Сил України. *Збірник наукових праць Харківського національного університету Повітряних Сил*. Харків, 2017. № 3 (52). С. 30–34.
  22. Підтримка вироблення рішень під час ситуаційного управління операцією (боєм): методичне забезпечення / О. М. Загорка, А. А. Корецький, І. О. Загорка, Т. М. Комолаєва // *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. Київ, 2020. № 1 (68). С. 98–109.
  23. Принципи, методи і технології моделювання і дослідження процесів функціонування складних багатоструктурних систем військового призначення і управління їх структурною динамікою / Д. А. Гриб, Б. О. Демідов, Ю. Ф. Кучеронко, А. М. Ткачов, Є. В. Шубін // *Системи обробки інформації*. Харків, 2019. № 1 (156). С. 64–73. DOI: <https://doi.org/10.30748/soi.2019.156.09>.
  24. Ситуаційний підхід в теорії організації. URL: [https://studme.com.ua/1056041211177/ekonomika/situatsionnyu\\_podhod\\_teorii\\_organizatsii.htm](https://studme.com.ua/1056041211177/ekonomika/situatsionnyu_podhod_teorii_organizatsii.htm) (дата звернення: 02.03.2021).

Стаття надійшла до редакції 09.04.2021

## **Analysis of the scientific and methodological apparatus of formation of organizational and functional structures of the strategic level**

### **Annotation**

Modern international conflicts can no longer be assessed in terms of traditional approaches to warfare, they can be described in one term – hybrid warfare, which is a combination of traditional and non-traditional methods of warfare. In addition, each country in the world is constantly faced in various areas of its activities with threats that may affect the economic performance and stability of the state itself. Each threat (potential and real) can turn into a crisis situation of different levels.

The results of the analysis show that the existing scientific and methodological apparatus of synthesis of organizational and functional structures of the strategic level does not allow to fully taking



into account the increase in information flows that need to be processed. This is especially critical when forecasting and responding to crisis situations. The most promising approaches to this issue, which will take into account new factors that have become relevant recently, in particular, such as information redundancy and others are the use of situational management.

It is expedient to study the scientific and mathematical apparatus for the decomposition of organizational and functional structures of the strategic level into two components: constant (relatively constant) and fluctuation. The synthesis of the structure and parameters of the constant component should be carried out according to the classical interpretation of the problem of parametric synthesis of a complex system. In the synthesis of the structure and parameters of the fluctuation component is advisable to use a situational approach.

**Keywords:** scientific and methodical apparatus; organizational and functional structure; situational management; crisis situation, redundancy; structural-parametric synthesis.

### ВІДОМОСТІ ПРО АВТОРІВ

**АНДРІЯНОВА Н. М.** – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського кандидат політичних наук;

**АНДРОЩУК О. В.** – науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат психологічних наук;

**БЕЛЯЧЕНКО В. В.** – науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

**БОБРОВ С. В.** – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат технічних наук, доцент;

**БОГАТОВ О. І.** – доцент кафедри оперативного та бойового забезпечення НУО України імені Івана Черняховського, кандидат технічних наук, доцент;

**БОЙКО В. О.** – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат економічних наук, старший науковий співробітник;

**БОНДАРЧУК С. В.** – науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

**БРАТКО А. В.** – доцент кафедри загальновійськових дисциплін Національної академії Державної прикордонної служби України імені Богдана Хмельницького;

**ВДОВИЦЬКИЙ Є. А.** – ад'юнкт кафедри Військово-Морських Сил командно-штабного інституту застосування військ (сил) НУО України імені Івана Черняховського;

**ВОЗНЯК С. М.** – начальник НДВ ЦВСД НУО України імені Івана Черняховського кандидат технічних наук, старший науковий співробітник;

**ГАЛАГАН В. І.** – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат військових наук, доцент;

**ГОЛОПАТЮК Л. С.** – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат військових наук;

**ГРІНЕНКО О. І.** – старший науковий співробітник НДВ ЦВСД НУО України

імені Івана Черняховського, кандидат військових наук, доцент;

**ГУДИМА О. П.** – докторант ЦВСД НУО України імені Івана Черняховського, кандидат технічних наук, старший науковий співробітник;

**ДОБРОГУРСЬКИЙ В. І.** – заступник начальника НУО України імені Івана Черняховського;

**ЗАГОРКА О. М.** – головний науковий співробітник ЦВСД НУО України імені Івана Черняховського, доктор військових наук, професор;

**ЗАГОРКА І. О.** – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

**КИРИЧЕНКО С. О.** – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського кандидат військових наук;

**КОПИСТИРА В. М.** – провідний науковий співробітник кафедри управління військами НУО України імені Івана Черняховського;

**КРИЛОВ І. О.** – начальник НДВ – заступник начальника НДУ проблем розвитку та застосування ВМС НДЦ ЗС України “Державний океанаріум” Інституту ВМС Національного університету “Одеська морська академія”;

**ЛЕПІХОВ А. В.** – головний консультант Центру безпекових досліджень Національного інституту стратегічних досліджень;

**ЛИТОВЧЕНКО Г. Д.** – науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

**ЛОБКО М. М.** – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат військових наук, доцент;

**МУДРАК Ю. М.** – начальник НДВ ЦВСД НУО України імені Івана Черняховського;

**МУЛЯВКА А. С.** – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

**ПАВЛУНЬКО М. Я.** – професор кафедри оперативного та бойового забезпечення НУО України імені Івана Черняховського, кандидат військових наук, доцент;

**ПОСМІТЮХ О. І.** – доцент ІЗВ(с) та ІТ НУО України імені Івана Черняховського кандидат військових наук, доцент;  
**РУДЕНСЬКА Г. В.** – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;  
**САГАНЮК Ф. В.** – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат юридичних наук, доцент;  
**СЕМЕНЕНКО В. М.** – начальник управління ЦВСД НУО України імені Івана Черняховського, кандидат технічних наук, старший науковий співробітник;  
**СЕРГІЄНКО В. Д.** – доцент кафедри оперативного та бойового забезпечення НУО України імені Івана Черняховського, кандидат технічних наук, доцент;  
**СІВОХА І. М.** – науковий співробітник ННЦ стратегічних комунікацій у сфері забезпечення національної безпеки та оборони НУО України імені Івана Черняховського;  
**УТЮШЕВ М. К.** – начальник НДЛ НДВ ЦВСД НУО України імені Івана Черняховського;  
**ФЕДОРІЄНКО В. А.** – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;  
**ФЕДЯНОВИЧ Д. Л.** – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат військових наук, старший науковий співробітник;

**ФРОЛОВ С. М.** – начальник НДЛ кафедри Військово-Морських Сил командно-штабного інституту застосування військ (сил) НУО України імені Івана Черняховського, кандидат історичних наук;  
**ФУЧКО А. Й.** – начальник НДВ ЦВСД НУО України імені Івана Черняховського;  
**ХРАПАЧ Г. С.** – молодший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;  
**ШИДЛЮХ В. В.** – доцент кафедри стратегії Навчально-наукового центру стратегічних комунікацій у сфері забезпечення національної безпеки і оборони НУО України імені Івана Черняховського;  
**ШПУРА М. І.** – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат військових наук, старший науковий співробітник;  
**ЩИПАНСЬКИЙ П. В.** – заступник начальника НУО України імені Івана Черняховського з наукової роботи, кандидат військових наук, професор;  
**ЯКІМ'ЯК С. В.** – начальник кафедри Військово-Морських Сил командно-штабного інституту застосування військ (сил) НУО України імені Івана Черняховського, кандидат військових наук, доцент.

## ВИМОГИ ДО СТАТЕЙ

Відповідно до Постанови ВАК України № 7-05/1 від 15 січня 2003 року наукові статті мають містити такі елементи:

**постановка проблеми** у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

**аналіз останніх досліджень і публікацій**, у яких започатковано розв'язання даної проблеми і на які спирається автор, виділення нерозв'язаних раніше частин загальної проблеми, яким присвячується стаття;

формулювання **мети статті** (постановка завдання);

виклад **основного матеріалу** дослідження з повним обґрунтуванням отриманих наукових результатів;

**висновки** і перспективи подальших досліджень розвитку в цьому напрямі;

**анотація до статті та ключові слова** – розміщуються після назви статті.

У статті слід дотримуватись загальноприйнятої термінології. Усі скорочення та нові терміни мають бути розкриті автором.

Назва, список авторів, назва установи, анотація (не більше 40 слів), ключові слова (7 слів) готуються на трьох мовах: українській, російській та англійській.

Обсяг статті разом із таблицями, рисунками та списком літератури не більше 10 сторінок А4.

Текст статті набирається в редакторі **Microsoft Word** шрифтом **Times New Roman 14**. Вирівнювання по ширині. Інтервал між рядками тексту – 1,0.

**Формат сторінки** – А4. Поля: ліве – 27 мм; верхнє і нижнє – 20 мм; праве – 20 мм.

Не використовуйте для форматування тексту пропуски, табуляцію тощо. Не встановлюйте ручне перенесення слів, не використовуйте колонитули.

Між значенням величини та одиницею її вимірювання ставте нерозривний пропуск (Ctrl + Shift + пропуск).

Таблиці та рисунки виконуються в одному стилі, нумеруються та подаються після посилань на них у тексті.

Текст усередині таблиці набирається в редакторі **Microsoft Word** шрифтом **Times New Roman** – кегль 10.

Таблиці нумеруються, вирівнювання по центру, без відступів. Слово “Таблиця 1” – кегль 11, вирівняний по правій стороні. Формат назви таблиці: вирівнювання по центру, напівжирний, положення – над таблицею. Після таблиці необхідно залишити один порожній рядок.

Рисунки нумеруються, вирівнювання по центру. Формат назви рисунку – вирівнювання по центру, положення – під рисунком, позначається скороченим словом “Рис.”. Перед рисунком і після його підпису необхідно залишити один порожній рядок.

Текст у середині рисунка набирається в редакторі **Microsoft Word** шрифтом **Times New Roman** – кегль 9–10.

Формули виносяться на середину рядків. Набір здійснюється у редакторі формул **Microsoft Equations** курсивом (крім особливих випадків) без обрамлення і заливки. Забороняється використовувати для набору формул графічні об'єкти, кадри і таблиці.

Вирівнювання по центру, нумерація – у дужках, праворуч. Нумерувати потрібно тільки ті формули, на які є посилання у тексті.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ складається у порядку посилання в тексті та подається наприкінці статті згідно з ДСТУ ГОСТ 7.1:2015. – кегль 12

У редакцію надається друкований примірник рукопису.

На останній сторінці робиться припис – “Стаття не містить відомостей, що розкривають державну таємницю та службову інформацію. Автори надають дозвіл на перевірку праці відповідальними особами, призначеними для перевірки праць на оригінальність і відсутність неправомірних записок. Автори гарантують, що ними одержано всі необхідні дозволи на використання у цій статті матеріалів, що охороняються авторським правом. Автори гарантують, що ця стаття раніше не публікувалась і не подавалась до інших видань”. *Підписи авторів.*

До редакційної колегії подаються такі документи:

1. Файли, які містять **текст статті українською** та **анотації** (не менше 1800 знаків) **українською, російською та англійською мовами** у форматі електронного документа **MS Word версія 2010**.

2. Довідка про авторів українською, російською та англійською мовами (П.І.Б. – повністю, установа, посада, вчений ступінь, вчене звання, контактна інформація).

3. Акт експертизи щодо відкритого публікування (для зовнішніх авторів).

**УВАГА!** Статті, які не задовольняють будь-якій з перелічених вимог, до видання не приймаються.

## ШАБЛОН СТАТТІ

УДК 628. 8 – *Times New Roman кегль – кегль 12 пт*

Бунін В. В., д-р техн. наук, професор<sup>1</sup>; – *Times New Roman кегль – кегль 14 пт*

Іванов В. А.<sup>2</sup>

Бунин В. В., д-р техн. наук, профессор<sup>1</sup>;

Иванов В. О.<sup>2</sup>

V. Bunin, Phd<sup>1</sup>;

V. Ivanov<sup>2</sup>

<sup>1</sup> – Департамент воєнної політики та стратегічного планування Міністерства оборони України, Київ;

<sup>2</sup> – Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ

<sup>1</sup> – Департамент военной политики и стратегического планирования Министерства обороны Украины, Киев;

<sup>2</sup> – Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев

<sup>1</sup> – Defence Policy and Strategic planning Department, Ministry of defence of Ukraine, Kyiv;

<sup>2</sup> – Center for Military and Strategic Studies of the National Defence University of Ukraine named after Ivan Cherniakhovskiy, Kyiv

**Матрична модель OLAP-систем** (кегль 14 пт напівжирний)

**Матричная модель OLAP-систем**

**Matrix model of OLAP-systems**

**Резюме (2-3 речення).** Розглянуто особливості матричних моделей ...

(кегль 12 пт)

**Анотація (1800 знаків).**

**Ключові слова:** модель, OLAP-система, інформаційні технології.

**Аннотация (1800 знаків).**

**Ключевые слова:**

**Annotation (1800 characters)**

**Keywords:**

**Постановка проблеми.** Численні дослідницькі роботи направлені на розв'язання задач зниження енергоємності систем пневмотранспорту. ...

**Аналіз останніх досліджень і публікацій.** У роботах [1, 2] розглянуто прикладні методики щодо ... Проте не визначено...

**Мета статті.** Підвищення ефективності технологічних операцій щодо ...

**Виклад основного матеріалу.** Автором пропонується використання аналітичних методів пошуку оптимального режиму ...

*1 інтервал*

$$\sum_{p=1}^{N^2} X_{nk}^{pk}$$

*1 інтервал*

де  $\sum$  - Times New Roman 18 шрифтом;

$X$  - Times New Roman 14 шрифтом;

$N$ ;  $pk$ ;  $p=1$ ;  $n$  - Times New Roman 10 шрифтом;

$k$ ; 2 - Times New Roman 8 шрифтом.

**Висновки.** ... Найбільш ефективним за критерієм мінімуму витрат ресурсів виявився...

**Напрями подальших досліджень.** Уточнення показників щодо ...

**УВАГА! Під час виконання рисунків та набору формул забороняється використовувати графічні об'єкти, кадри і таблиці.**

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ (згідно з ДСТУ ГОСТ 7.1:2015)

**Відомості про авторів** – прізвище, ім'я, по батькові (повністю); посада; установа; вчений ступінь; вчене звання.

**УВАГА! Документи для включення статті в План до друку потрібно подавати на електронну адресу Редакційної колегії [znp.cvsvd@nuou.org.ua](mailto:znp.cvsvd@nuou.org.ua)**

Наукове видання

**Збірник наукових праць  
Центру воєнно-стратегічних досліджень  
Національного університету оборони України  
імені Івана Черняховського**

**№ 1(71), 2021**

***Відповідальні за випуск:***

Відповідальний за випуск: Рибидайло А. А.

Технічний редактор: Руденська Г. В.

Комп'ютерне верстання: Рибидайло А. А.

Коректори: Андріянова Н. М., Уварова Т. В., Терещенко С. А.

Підтримка вебсайту збірника: Кірпічніков Ю. А., Петрушен М. В.

Підписано до друку 30.04.2021. Формат 60x84 1/8.  
Папір офсетний. Обл.- вид. арк. 8,55. Друк. арк. 18,75  
Зам. 205. Наклад 100 прим.

---

**Видання Національного університету оборони України  
імені Івана Черняховського**

03049, м. Київ, Повітрофлотський пр-т, 28  
<http://znp-cvzd.nuou.org.ua>

Свідоцтво про внесення суб'єкта видавничої справи  
до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої  
продукції, серія ДК № 2205 від 02.06.2005 р.

Надруковано у друкарні Національного університету оборони України  
імені Івана Черняховського  
03049, м. Київ, Повітрофлотський пр-т, 28