

НАУКА і ОБОРОНА

Щоквартальний науково-теоретичний та науково-практичний журнал

Передплатний індекс 74303

Редакція:

Семон Богдан Йосипович (*головний редактор*), доктор
технічних наук, професор;
Бодрик Юрій Григорович (*науковий редактор*), кандидат
технічних наук, старший науковий співробітник;
Колесник Володимир Іванович (*відповідальний*
секретар), кандидат *технічних наук, старший*
науковий співробітник

Редакційна колегія:

Бочарніков Віктор Павлович, *доктор технічних наук,*
професор;
Воробйов Олег Михайлович, *доктор технічних наук,*
професор;
Герасименко Володимир Вікторович, *доктор військових*
наук;
Грицюк Валерій Миколайович, *доктор історичних наук,*
доцент;
Еггінтон Білл, *доктор освіти*;
Загорка Олексій Миколайович, *доктор військових наук,*
професор;
Карабин Василь Васильович, *доктор технічних наук,*
доцент;
Коваль Михайло Володимирович, *доктор військових наук*;
Коваль Володимир Валерійович, *кандидат військових*
наук, старший науковий співробітник;
Косевцов В'ячеслав Олександрович, *доктор військових*
наук, професор;
Мацько Олександр Йосипович, *кандидат військових*
наук, професор;
Машталір Вадим Віталійович, *доктор історичних наук,*
професор;

Медведев Володимир Костянтинович, *кандидат*
військових наук, професор;
Мірненко Володимир Іванович, *доктор технічних наук,*
професор;
Неділько Олександр Миколайович, *кандидат технічних*
наук, доцент;
Осьодло Василь Ілліч, *доктор психологічних наук,*
професор;
Павліковський Анатолій Казимирович, *кандидат*
військових наук, доцент;
Павлюк Олександр Олексійович, *кандидат військових*
наук;
Ракушев Михайло Юрійович, *доктор технічних наук,*
старший науковий співробітник;
Руснак Іван Степанович, *доктор військових наук,*
професор;
Салій Анатолій Григорович, *кандидат військових наук,*
професор;
Самберг Андре, *кандидат технічних наук*;
Серватюк Василь Миколайович, *доктор військових наук,*
професор;
Слюсаренко Андрій Віталійович, *доктор історичних*
наук, професор;
Телелим Василь Максимович, *доктор військових наук,*
професор;
Хомік Микола Миколайович, *доктор технічних наук,*
професор;
Чепков Ігор Борисович, *доктор технічних наук,*
професор;
Щипанський Павло Володимирович, *кандидат*
військових наук, професор

Зміст

Актуальні питання національної безпеки та оборони

Стешенко П. М., Волотівський П. Б., Жевтюк О. А.
Створення спеціального БпЛА-перехоплювача для протидії БпЛА типу «Shahed» – актуальне завдання держави3

Павліковський А. К., Тютюнник В. О., Ткаченко В. А., Ткаченко Н. І. Підвищення ефективності протидії масованому застосуванню ударних безпілотних літальних апаратів11

Тимошенко В. А., Отрошенко В. П., Дрьомов С. В.
Проблеми нормативно-правового регулювання призначення військовослужбовцям винагороди за знищення ворожої техніки18

Розвиток теорії та методології

Чепков І. Б., Можаровський В. М., Нор П. І.
Сучасні загальні тенденції розвитку засобів збройної боротьби27

Машталір В. В., Гусак Ю. А. Розвиток понятійного апарату з питань кібероборони та підходи до створення кіберсил в Україні36

Національна безпека та оборона:

методичний аспект

Коваль М. В., Машталір В. В., Загорка О. М.
Оцінювання результатів війни на виснаження: методичні положення47

Оглядові статті

Кармазіна М. С., Аблазов І. В. Концепт «гібридна війна»: аналіз наукового дискурсу54

Summaries60

Contents

Topical issues of national security and defence

P. M. Steshenko, P. B. Volotivskyi, O. A. Zhevtiuk.
Creation of a special UAV-interceptor to counter UAVs of the «Shahed» type is an urgent task of the state3

A. K. Pavlikovskyi, V. O. Tiutiunnyk, V. A. Tkachenko, N. I. Tkachenko. Increasing the effectiveness of countering the massive employment of strike unmanned aerial vehicles11

V. A. Tymoshenko, V. P. Otroshchenko, S. V. Dromov.
Legislative and regulative problems of awarding military personnel rewards for the destruction and capture of enemy equipment.....18

Development of theory and methodology

I. B. Chepkov, V. M. Mozharovskyi, P. I. Nor.
Modern general trends in the development of means of warfare27

V. V. Mashtalir, Yu. A. Husak. Development of the set of concepts on cyber defence and approaches to the creation of cyber forces in Ukraine36

National security and defence: methodical aspect

M. V. Koval, V. V. Mashtalir, O. M. Zahorka.
Assessment of the results of a war of attrition: methodological provisions47

Reviews

M. S. Karmazina, I. V. Ablazov. The concept of «hybrid warfare»: an analysis of scientific discourse54

Summaries60

DOI 10.33099/2618-1614-2025-28-1-3-10

УДК 355.469.4

П. М. Стешенко,*кандидат технічних наук, старший дослідник,
Державний науково-дослідний інститут авіації,***П. Б. Волотівський,***кандидат військових наук,
старший науковий співробітник,
Державний науково-дослідний інститут авіації,***О. А. Жевтюк,***кандидат технічних наук,
старший науковий співробітник,
Державний науково-дослідний інститут авіації*

Створення спеціального БпЛА-перехоплювача для протидії БпЛА типу «Shahed» – актуальне завдання держави

Серед безпілотних літальних апаратів збройних сил РФ, орієнтованих на виконання більшості завдань так званої «спеціальної воєнної операції», найпоширенішими нині є безпілотні авіаційні комплекси з БпЛА, які вирішують завдання виявлення й нанесення ударів по військах та наземних об'єктах. Протидія цим БпЛА належить до головних завдань протиповітряної оборони України на рівні з протиракетною обороною. Досвід боротьби Збройних Сил України з ворожими БпЛА свідчить про практичну відсутність досконалих спеціалізованих систем і засобів, призначених виключно для протидії БпЛА. Тому пошук способів і засобів протидії БпЛА противника є надзвичайно актуальним завданням для сил оборони України. Серед ефективних засобів для протидії БпЛА нині розглядаються БпЛА-перехоплювачі. Вважається, що розробка безпілотних перехоплювачів стає одним з головних напрямів розвитку безпілотних авіаційних систем. Нині настав час переходити від ідеї щодо необхідності створення відповідного типу спеціальних БпЛА-перехоплювачів до її практичної реалізації, адже безпілотна техніка в недалекому майбутньому стане основною системою зброї.

Ключові слова: протиповітряна оборона, протибезпілотна оборона, авіаційні засоби ураження, безпілотний літальний апарат-перехоплювач, спосіб застосування безпілотного літального апарата-перехоплювача.

Постановка проблеми. Нині, виходячи з аналізу розвитку безпілотних авіаційних засобів повітряного нападу РФ, залежно від рівня вирішуваних завдань визначилися такі групи безпілотних літальних апаратів (БпЛА) в номенклатурі повітряних цілей для сил і засобів протиповітряної оборони (ППО) та протиракетної оборони (ПРО) Повітряних Сил Збройних Сил України (ЗСУ), ППО Сухопутних військ та Військово-морських Сил ЗСУ:

1. Тактичні (тактичні мікро, тактичні міні (поля бою)). До цього класифікаційного типу цілей належать БпЛА із системою «First Person View» (FPV) (типу «мультикоптер», літакового й вертолітного типу) зі злітною масою до 15 кг, радіусом дії до 25 км, масою корисного навантаження до 5 кг, тривалістю польоту до 80 хвилин, швидкістю польоту до 200 км/год, практичною стелею 100–6000 м. Ця група БпЛА призначена для ударних та розвідувальних дій, супроводження дій штурмових груп поблизу лінії бойового зіткнення.

2. Тактичні (малі тактичні). До цієї групи повітряних цілей належать БпЛА, які використовуються для ведення повітряної розвідки, радіоелектронної боротьби, видачі цілевказівок для ударних (вогневих) засобів, виконання завдань контрбатареїної боротьби (БпЛА «Орлан-10», «Zala 421-16E» та «Supercam S350», «Тахион», «Леер-3», «Гранат-4», «Mohajer-6»). Основні їхні характеристики: злітна маса понад 15 кг, корисне навантаження 1–4 кг, радіус дії до 120 км, максимальна висота польоту до 5000 м, швидкість польоту до 140 км/год, тривалість польоту до 2–18 год.

3. Тактичні (оперативно-тактичні). До цієї групи повітряних цілей для сил і засобів ППО слід віднести ударні БпЛА типу «Shahed», що застосовуються для ударів у глибині території нашої країни. Їхні основні характеристики: максимальна злітна маса 200 кг, маса корисного навантаження 40 кг, радіус дії до 2000 км, максимальна швидкість польоту 250 км/год, практична стеля 4000 м, тривалість польоту 12 год. Ці БпЛА застосовуються, як правило, масовано із залученням БпЛА хибних цілей «Пародія», «Гербера».

4. Оперативні і стратегічні БпЛА – БпЛА-цілі (безпілотні літаки) призначаються для нанесення ударів по цілях в оперативній глибині та є, як правило, середньо- і високошвидкісними. Їхні основні типові характеристики: максимальна швидкість до 1000 км/год, стартова маса до 7000 кг, маса корисного навантаження до 2900 кг, максимальна висота польоту до 14000 м, максимальна тривалість польоту 18–24 год. На даний час у РФ у цьому класі перебувають такі БпЛА, як «Орион-Э», С-70 «Охотник».

Нині командуванням ЗСУ, оперативно-тактичних угруповань, загальновійськових з'єднань активно

розробляються способи боротьби з ударними та розвідувальними БпЛА противника як у зоні бойових дій, так і в глибині території нашої держави з урахуванням наявного озброєння, засобів виявлення та радіоелектронної протидії.

Протидія БпЛА I класу (тактичні мікро, тактичні міні (поля бою)) для Збройних Сил України поки що залишається не розв'язаною проблемою. У незначному об'ємі повітряного простору над полем бою поблизу лінії бойового зіткнення на відтинку оборони, наприклад, загальновійськової бригади, застосовуються сотні ударних БпЛА із системою FPV типу «мультикоптер», літакового і вертолітного типу як підрозділами противника, так і підрозділами ЗСУ. У таких умовах є складнощі з ідентифікації та знищенням ударних БпЛА противника із системою FPV, зокрема оснащених оптоволоконною системою керування. Такі засоби, як стрілецька зброя, зенітні артилерійські установки, зенітні кулеметні установки, не повною мірою пристосовані для протидії ударним БпЛА із системою FPV, здатним здійснювати активне маневрування під час виконання польотного завдання. Засоби радіоелектронної протидії неефективні в боротьбі з БпЛА із системою FPV, оснащених оптоволоконною системою керування. Для боротьби з таким типом БпЛА необхідно розробити нові та досконалі способи й засоби протидії.

На сьогодні в Силах оборони України сформувалася нова *спроможність перехоплення російських БпЛА розвідників за допомогою БпЛА-перехоплювачів* із системою FPV. Ця спроможність сформувалася шляхом поєднання наявних технологій радіолокації та простих БпЛА для здійснення бойової функції прикриття. Технічні характеристики БпЛА із системою FPV дають можливість перехоплювати повільніші ворожі БпЛА-розвідники. Однак виявлення цих БпЛА відбувається лише за візуальними або акустичними ознаками. Спроможність ефективно протидіяти БпЛА-розвідникам противника з'явилася після об'єднання трикоординатних радіолокаційних станцій (РЛС) сантиметрового діапазону з підрозділами ударних БпЛА в єдиний розвідувально-вогневий контур. *Саме взаємодія засобів виявлення та ураження дала змогу досягти системних результатів у прикритті повітряного простору поблизу лінії бойового зіткнення.*

Натепер помітна нестача спроможностей сил ППО для недопущення прольотів БпЛА противника до об'єктів ударів у глибині території держави, аж до західного кордону. Наявні українські БпЛА-перехоплювачі, як показав досвід, не мають достатніх характеристик, щоб протидіяти ударним БпЛА противника типу «Shahed». Вони показали хорошу ефективність і результативність у протидії розвідувальним БпЛА, які повільніші та значно довше баражують у зоні дії БпЛА-перехоплювачів та радарів сантиметрового

діапазону. Окремі зафіксовані випадки знищення за допомогою БпЛА-перехоплювачів із системою FPV мультикоптерного та літакового типу ударних БпЛА типу «Shahed» не розв'язують проблему.

Тому на порядку денному постало питання створення спеціальних БпЛА-перехоплювачів для протидії ударним БпЛА тактичного та оперативно-тактичного призначення типу «Shahed» [1].

Основні типи безпілотних літальних комплексів (БпАК) і БпЛА тактичного та оперативно-тактичного рівня, що застосовуються на сьогодні збройними силами РФ у широкомасштабній війні проти України, та їхні основні характеристики наведені в *таблиці 1*.

Аналіз застосування збройними силами РФ безпілотних літальних апаратів у війні проти України показує, що для нанесення ударів по аеродромах та інших об'єктах сил оборони, по об'єктах критичної інфраструктури, житловій забудові противник масово застосовує БпЛА-камікадзе «Shahed-136»/«Герань-2», «Гарпия-А1» у комплексі з БпЛА – хибними цілями «Гербера» та «Пародия». Противник також суттєво наростив кількість розвідувальних БпЛА в тактичній та оперативній глибині бойових порядків сил оборони, які забезпечують роботу всіх засобів вогневого впливу (оперативно-тактичних ракетних комплексів, ствольної чи реактивної артилерії, БпЛА «Ланцет»). Нарощування спроможностей щодо прикриття об'єктів сил оборони, національного господарства від дій розвідувальних та ударних БпЛА противника типу «Орлан», «Shahed» у глибині території України залишається ключовим завданням ППО.

Метою статті є визначення цільового призначення БпАК з БпЛА-перехоплювачами для ураження (знищення) розвідувальних, розвідувально-ударних та ударних БпЛА противника тактичного та оперативно-тактичного призначення, окреслення основних завдань, меж та умов бойового застосування такого БпАК.

Аналіз останніх досліджень і публікацій

Спосіб протидії ударним БпЛА з використанням спеціальних БпЛА-перехоплювачів на сьогодні є одним з найменш опрацьованих [4]. У цій роботі автор повідомляє, що у 2000-х роках проводилась ініціативна робота щодо оцінювання доцільності розробки й застосування безпілотного винищувача БпЛА різного призначення. Однак усі роботи за цим напрямом були припинені з таких причин:

- згідно з проведеними на той час розрахунками в середньому вартість ураження повітряної цілі суттєво (до двох порядків) перевищувала вартість самої повітряної цілі;
- вважалось неможливим застосування бойового винищувача проти груп малогабаритних маневрених БпЛА;

Таблиця 1

Основні характеристики БпЛА, що застосовуються збройними силами РФ у війні проти України, та серійно виробляються промисловістю РФ* [2, 3]

№ з/п	Назва БпЛА (БпЛА)	Кількість літальних апаратів БпЛА (БпЛА)	Тривалість польоту, год	Радіус дії, км	Максимальна злітна маса, кг	Маса корисного навантаження, кг	Практична стеля, м	Максимальна швидкість польоту, км/год	Тип корисного навантаження	Тип двигуна
Розвідувальні та ударні БпЛА тактичного та оперативно-тактичного рівня										
1	«Shahed-136»	5	12	2000	200	40	4000	220	БЧ	ДВЗ
2	«Shahed-131»	–	10	900	135	15	4000	200	БЧ	ДВЗ
3	«Mohajer-6»	1	12	2000	600	100	5400	200	ТВ/ІЧ/фото/РЕБ/АЗУ	ДВЗ
4	«Гарпія-А1»	–	8–12	1500	300	150	4000	185	БЧ	ДВЗ
5	«Куб»	–	0,5	65	–	3	1500	130	БЧ	електр.
6	«Куб-2»	–	0,5	65	–	2,5	1500	130	БЧ	електр.
	«Куб-10»	–	–	–	–	–	2500	>100	БЧ	електр.
7	«Ланцет»	–	0,5	60	12	3	3000	110	ТВ/ІЧ/РР/БЧ	електр.
8	Supercam S350	2	4,5	100	15,5	–	150–5000	120	Змінна ТВ/ІЧ/фото/ЛЦ	електр.
9	«Орлан-10»	1	14	До 120	До 18	5	6000	170	ТВ/ІЧ/фото/ретранс./ЛЦ	ДВЗ
10	«Орлан-30»	1	18	120	До 35	12	6000	170	ТВ/ІЧ/фото/ретранс./ЛЦ	ДВЗ
11	«Гранат-4»	2	6	70	30	3	4000	140	ТВ/ІЧ/фото/ретранс./ЛЦ	ДВЗ
12	ZALA 421-16	2	4 або 8	До 50/70	6,5	1,0	3000	130–200	ТВ/ІЧ/ЛЦ	ДВЗ
13	«Елерон-3»	2	1,7	25	5,5	1	4000	130	ТВ/ІЧ/фото	електр.
14	«Мерлин-ВР»	1–2	5	–	–	7	5000	140	ТВ/ІЧ	ДВЗ
15	«Феникс»	–	–	–	–	8	–	–	ТВ/ІЧ	ДВЗ
16	«Тахион»	2	2	40	6,9	1	4000	120	ТВ/ІЧ/фото	електр.
Розвідувальні БпЛА оперативного рівня										
16	«Орион»/ «Орион-Э»	3–6	24	200	1150	250	7000	200	ТВ/ІЧ/ /ретранс./ЛЦ/ЛД/ РЛС/РЕБ/РТР/АЗУ	ДВЗ
17	«Форпост»	3	17,5	350	454	100	5800	204	ТВ/ІЧ/ /ретранс./ЛЦ/ЛД/ РЛС/РЕБ/РТР/АЗУ	ДВЗ

* Прийняті скорочення: БЧ – бойова частина; ТВ – телевізійна оптико-електронна система повітряної розвідки; ІЧ – інфрачервона оптико-електронна система повітряної розвідки; фото – аерофотоапарат; РЕБ – бортова система радіоелектронної боротьби; РР – система радіаційної розвідки; ретранс. – бортова система ретрансляції сигналів (зв'язку); ЛЦ – лазерний цілевказувач; ЛД – лазерний далекомір; РЛС – бортова радіолокаційна станція; РТР – бортова система радіотехнічної розвідки; АЗУ – авіаційні засоби ураження; ДВЗ – двигун внутрішнього згорання; електр. – електричний двигун.

• суттєво ускладнювалася структура військового формування, якому повинен бути приданий комплекс із бойовим винищувачем, що могло призвести до втрати оперативності й мобільності цього військового формування;

• у зв'язку з безповоротною втратою безпілотної винищувача наступало швидке і різке зниження ефективності комплексу.

На думку автора роботи [4], на той час спосіб протидії ударним БпЛА шляхом застосування БпЛА-винищувача значно випередив свій час.

На думку авторів цієї статті, необхідно було б урахувати вартість об'єкта, який може бути уражений

(знищений) ударним БпЛА, а не лише вартість засобу ППО, застосованого для його ураження.

У роботі [5] поставлене питання про необхідність створення системи протипілотної оборони (ППО) в системі ППО України, в роботі [6] запропонований варіант загального обрисів системи ППО як складової частини стратегічної системи ППО/ПРО України.

У роботі [1] проведений огляд основних способів та засобів протидії БпЛА, їхніх переваг і недоліків і на цій підставі сформовані погляди щодо можливих напрямів ефективного розв'язання цієї проблеми. У висновку вказаної роботи відзначено, що стратегічним завданням для розробників та виробників БпЛА є створення БпЛА-перехоплювачів.

Виклад основного матеріалу

Огляд існуючих проєктів у галузі створення безпілотних перехоплювачів. На сьогодні загальносвітовою тенденцією є використання БпЛА для вирішення різноманітних цільових завдань. При цьому БпЛА стали активно витіснити пілотовані літальні апарати, особливо в тих сферах, де людський чинник відіграє суттєву роль у зниженні бойового потенціалу комплексів озброєння або ефективності їхнього застосування [7].

На початкових етапах розвитку БпЛА переважно застосовувалися для вирішення розвідувальних завдань. Після створення розвідувальних БпЛА в усіх класах розпочалися розробки БпЛА, що значно розширили коло завдань, які вони здатні виконувати. З'явилися БпЛА для виконання завдань з радіоелектронної протидії, БпЛА-ретранслятори, БпЛА пошуково-рятувального забезпечення й інші. Подальшим напрямом розвитку стало створення ударних БпЛА з БпЛА, які здатні застосовувати засоби ураження для нанесення вогневих ударів по противнику.

В останнє десятиліття в локальних війнах та збройних конфліктах, особливо в широкомасштабній війні РФ проти України, відмічається масове застосування БпЛА як безпосередньо в зоні бойових дій, так і за її межами для нанесення ударів по об'єктах критичної та соціальної інфраструктури. *Тому нині гостро постало питання про протидію розвідувальним та ударним безпілотним авіаційним системам. Як один з перспективних засобів боротьби з БпЛА противника нині розглядається застосування спеціальних БпЛА-перехоплювачів [1].*

Активні розробки безпілотних перехоплювачів на даний час здійснюються в багатьох державах. Перше випробування БпЛА як винищувача відбулося 10 травня 1971 р. у районі острова Санта-Каталіна поблизу узбережжя Каліфорнії. БпЛА, що був озброєний керуваною ракетою з тепловою головкою самонаведення (ГСН) та керуваною ракетою з радіолокаційною ГСН, виступав проти двох винищувачів-бомбардувальників F-4 «Фантом» авіації Військово-морських сил США. Ці випробування підтвердили ефективність використання БпЛА як засобу перехоплення повітряних цілей.

У 2010 р. американське агентство DARPA повідомило про завершення створення нових БпЛА-винищувачів (проєкт «Перегрин – Киллер БпЛА»). Ці БпЛА здатні «вирішувати завдання щодо знищення собі подібних – інших БпЛА різного призначення». Завданням такого БпЛА є пошук і знищення БпЛА противника під час патрулювання у визначеному районі.

Було відмічено, що створюваний літальний апарат має підвищену міцність, оснащений GPS та має невисоку вартість виробництва.

Заслужує на увагу інформація про те, що американська компанія Boeing у рамках партнерства з міністерством оборони Австралії створює безпілотний винищувач зі штучним інтелектом. *Згідно із заявами, БпЛА створюється для роботи в парі з перспективними винищувачами н'ятого покоління.* Завдяки впровадженню штучного інтелекту безпілотний винищувач буде здатний здійснювати автономний політ. Крім функцій винищувача, він здатний вести розвідку та радіоелектронну протидію. У перспективі цей БпЛА-винищувач має стати захистом для пілотованого літака.

На даний час у США діють програми розвитку авіаційних безпілотних систем (2005–2030) та програми розвитку безпілотних систем загалом (2007–2032). У цих документах зазначається, що міністерство оборони США основну увагу має зосереджувати на науководслідних роботах і промислових розробках створення засобів розвідки, спостереження та рекогносцировки, засобів придушення та знищення системи ППО противника, пошуку і знищення БпЛА противника, знищення засобів радіоелектронної боротьби, засобів мінування. *Передбачене проведення досліджень для виявлення пріоритетного типу БпЛА, найбільш придатного для виконання того чи іншого бойового завдання.* Для цього широко використовується досвід застосування БпЛА у збройних конфліктах останніх років, у тому числі в російсько-українській війні. За результатами аналізу цього досвіду визначаються характерні системні вимоги як до самих БпЛА, так і до організації їх бойового застосування: *індивідуального, групового, у складі змішаного угруповання за участю пілотованої авіації, з урахуванням захищеності об'єктів противника засобами ППО.*

У РФ також активно проводяться роботи в галузі створення безпілотних винищувачів. Однак російські спеціалісти станом на 2022 р. вважали, що російська оборонна промисловість у цій галузі відстала від провідних зарубіжних країн на ціле покоління.

Кроком у галузі створення БпЛА-винищувача стала розробка авіаційного комплексу далекого перехоплення дозвукових крилатих ракет компанією РСК «МиГ». До БпЛА цього комплексу висувалися такі вимоги:

- висока швидкість і дальність польоту;
- оснащення власними засобами виявлення та супроводження повітряних цілей, а також озброєнням;
- вартість БпЛА-перехоплювача повинна бути низькою, що має забезпечувати можливість їх виробництва у великій кількості.

На підставі аналізу швидкісних і маневрених характеристик пілотованої та безпілотної авіації, крилатих ракет у РФ зроблено висновок, що БпЛА-перехоплювач (винищувач) повинен мати здатність діяти в широкому

діапазоні швидкостей можливих цілей та бути високоманевреним.

Дослідження щодо використання цього засобу протидії БпЛА та крилатим ракетам у РФ тривають. Визначені проблемні питання щодо *створення надманевреного БпЛА, основним завданням якого буде завоювання панування в повітрі*. Розробляються та перевіряються на практиці варіанти цілевказання для БпЛА-перехоплювача, варіанти оснащення засобами ураження та цільового навантаження.

На даний час компанія «ООО НПК «Аэрокон» виконує завдання щодо розробки і виготовлення БпЛА-перехоплювача «Лунь-БпЛА-И». Цей БпЛА, відповідно до задуму, призначається для ураження БпЛА противника середньої та великої дальності. Передбачається, що БпЛА-перехоплювач «Лунь-БпЛА-И» повинен мати такі льотно-технічні характеристики:

- діапазон висот – від 50 м до 5000 м;
- максимальна горизонтальна швидкість – не менше 550 км/год;
- крейсерська швидкість – не менше 250 км/год;
- тривалість польоту на максимальній швидкості – не менше 5 хвилин;
- маса бойового спорядження – не менше 6 кг;
- максимальна дальність польоту – не менше 30 км;
- тип силової установки – турбореактивний двигун.

Спеціалісти РФ, які працюють у галузі створення БпЛА-перехоплювача, вважають, що натеper *практична реалізація завдання його створення ускладнюється відсутністю конструктивних алгоритмів управління такими БпЛА, алгоритмів управління траєкторією їхнього руху в інтересах перехоплення повітряної цілі*. Водночас вони переконані, що *впровадження штучного інтелекту* дасть змогу вирішити всі проблемні питання, пов'язані з управлінням та наведенням безпілотного перехоплювача на ціль, розширить сферу їхнього застосування, підвищить ефективність вирішення завдань, забезпечить можливість прийняття самостійних рішень у передбачених чи екстремальних ситуаціях.

Як бачимо, РФ та інші країни активно займаються розробкою БпЛА-перехоплювачів. У цих умовах Україна має не лише не відставати в розробці БпЛА-перехоплювачів від інших країн, особливо від країни-агресора, а випереджати їх у галузі створення високотехнологічних, багатофункціональних безпілотних авіаційних комплексів (систем) з БпЛА-перехоплювачами.

Потенційними об'єктами прикриття перспективного БпЛА-перехоплювача ЗСУ можуть бути: оперативні аеродроми винищувальної та штурмової авіації Повітряних Сил, майданчики дозаправки армійської авіації, вогневі позиції високовартісних зразків озброєння,

пускові майданчики ударних БпЛА, призначених для ураження об'єктів противника стратегічної глибини, об'єкти критичної інфраструктури, населені пункти тощо.

Цілі для БпЛА-перехоплювача. На даний час сформувався такі групи цілей повітряного нападу збройних сил РФ, котрі є (можуть бути) цілями для перспективного БпЛА-перехоплювача:

1. Ударні БпЛА типу «Shahed», БпЛА іншого функціонального призначення (розвідники, постановники завад, ретранслятори зв'язку) зі швидкостями польоту 90–400 км/год у діапазоні висот 50–4000 м;

2. Ударно-транспортні вертольоти зі швидкостями 0–300 км/год;

3. Легкомоторні літаки типу Як-42, Цесна-172, які залучатимуться для виконання бойових та забезпечувальних завдань в операціях (бойових діях).

Примітка: Натеper можна вважати назрілим питання щодо створення БпЛА-перехоплювача дозвуків крилатих ракет великої дальності, що мають швидкість польоту 600–850 км/год, діапазон висот від 50 м до 1000 м. Звичайно, цей безпілотний перехоплювач повинен мати інші швидкісні характеристики та маневрені можливості.

На даний час найбільшої шкоди об'єктам ЗСУ в оперативній та стратегічній глибині оборони, об'єктам критичної інфраструктури держави, оборонно-промислового комплексу, житловій забудові завдають ударні БпЛА-камікадзе типу «Shahed» і розвідувальні БпЛА типу «Орлан», які забезпечують роботу засобів вогневого впливу противника широкого діапазону. Саме ці цілі пропонується вважати основними для БпЛА-перехоплювача, котрий пропонується для розробки й подальшого виробництва.

Як зазначалося вище, збройні сили РФ для ударів по об'єктах у глибині території нашої країни масово застосовують ударні БпЛА «Shahed 136»/«Герань-2», «Гарпия-А1». Запуск цих БпЛА та їхній проліт у повітряний простір України здійснюється з таких напрямків:

- з території окупованого Криму над акваторією Чорного моря в повітряний простір України (південний напрямок);

- з території Краснодарського краю над акваторією Азовського моря, окупованими територіями Запорізької та Херсонської областей України, лінією зіткнення військ, зоною бойових дій;

- зі східного напрямку над окупованими територіями Донецької та Луганської областей, лінією зіткнення військ, зоною бойових дій;

- з північно-східного напрямку над російсько-українським кордоном у глибину території України.

Застосовуються ці БпЛА групами або парами по визначених цілях з урахуванням протидії системи протиповітряної оборони України.

Звідси, перед системою ППО та її складовою проти-безпілотною обороною постає завдання щодо знищення ударних БпЛА противника типу «Shahed» і розвідувальних БпЛА типу «Орлан» на визначених оперативно-стратегічних напрямках (операційних зонах) для недопущення їхнього прольоту в глибину території України:

- у повітряному просторі над територією держави агресора (до перетину лінії державного кордону України);
- у повітряному просторі над територією прикордонної зони України на суходолі;
- до входження в повітряний простір над територіальним морем України в Чорному морі (південний напрямком);
- у повітряному просторі над територіальним морем України в Чорному морі;
- у повітряному просторі над зоною бойових дій (у тактичній та оперативній глибині бойових порядків сил оборони).

Призначення БпАК з БпЛА-перехоплювачами. БпАК з БпЛА-перехоплювачами багаторазового застосування призначається для перехоплення та знищення ударних БпЛА типу «Shahed» і розвідувальних БпЛА типу «Орлан». Перспективний БпЛА-перехоплювач – це високоінтелектуальний, швидкісний БпЛА тактичного (оперативно-тактичного) рівня застосування II класу літакового типу з бортовою малогабаритною РЛС та комплектом керованих ракет класу «повітря – повітря». Бортова РЛС застосовується для виявлення і супроводження БпЛА-цілей. Бортовий комплекс авіаційного озброєння вирішує завдання забезпечення оптимального положення атакуючого БпЛА-перехоплювача відносно цілі, за якого досягається максимальна ефективність авіаційних засобів ураження, що можуть бути застосовані.

БпЛА-перехоплювач здійснює перехоплення ворожих БпЛА у призначеному йому районі патрулювання. Попереднє цілевказання БпЛА-перехоплювачу здійснюється з наземного пункту управління або з літака далекого радіолокаційного виявлення. Для перехоплення групи ворожих БпЛА розробляється система районів патрулювання з розрахунку один район на один БпЛА-перехоплювач. Райони патрулювання визначаються таким чином, щоб виключити взаємне ураження БпЛА перехоплювачами один одного та їх ураження своїми зенітними артилерійськими комплексами та зенітними ракетними комплексами. Райони патрулювання визначаються в повітряному просторі над морською акваторією, над територією

суходолу (як правило за межами великих населених пунктів, над заболоченою місцевістю, лісними масивами, водосховищами тощо).

Спосіб застосування БпЛА-перехоплювача. Командний пункт, що забезпечує управління засобами виявлення та перехоплення ворожих літальних апаратів у смузі відповідальності, в разі отримання від засобів радіолокаційної розвідки інформації про запуск БпЛА противника та напрямком їхнього руху здійснює обробку даних відповідальними черговими по напрямках відповідно зі структурою командного пункту: обробка радіолокаційної інформації; ідентифікація цілі (РЕБ/РЕР); цілевказання і супроводження дій екіпажів БпЛА-перехоплювачів; наявність дружніх (своїх) літальних апаратів у повітряному просторі. Кожен із чергових у режимі реального часу координує застосування відповідних засобів за своїм напрямком. Після ідентифікації цілі як «свій/чужий/нерозпізнаний» інформація передається черговому по засобах перехоплення, який визначає можливість перехоплення, встановлює потребу в БпЛА-перехоплювачах та визначає кожному з них зони райони патрулювання («чергування в повітрі») для перехоплення літальних апаратів (розвідувальних, ударних та іншого призначення БпЛА), віддає команди екіпажам БпЛА-перехоплювачів. Оператор зі складу екіпажу БпЛА-перехоплювача вводить у бортовий комплекс перехоплювача програму польоту, в якій вказуються:

- координати району патрулювання (зони «чергування в повітрі»);
- маршрут (схема) руху в районі патрулювання, швидкість і висота польоту;
- дані про ціль та її характеристики (тип, швидкість, напрямок і висота цілі);
- час перебування в районі патрулювання (у разі необхідності);
- кодована інформація для забезпечення зв'язку з оператором БпЛА-перехоплювача;
- маршрут повернення БпЛА-перехоплювача на оперативний аеродром (точку зльоту);
- інші дані, передбачені програмою.

У повітря можуть бути підняті декілька перехоплювачів для зайняття визначених зон «чергування в повітрі» для забезпечення гарантованого результату, знищення ворожих літальних апаратів, як одиночних, так і груп БпЛА.

Після старту БпЛА-перехоплювач направляється в призначений район патрулювання (зону «чергування в повітрі»). У районі патрулювання перехоплювач переходить у режим максимальної тривалості польоту, здійснює політ по замкненій траєкторії в межах району. При наближенні ворожих БпЛА за даними командного пункту за командою оператора вмикається

бортова РЛС, перехоплювач направляє в район зустрічі із ціллю (цілями). Після виявлення цілі (цілей) бортовою РЛС бортовий комплекс авіаційного озброєння здійснює розподіл цілей для ураження керованими ракетами «повітря – повітря», дає команду на почерговий пуск ракет. У процесі нанесення ураження ворожим БпЛА перехоплювач здійснює об'єктивний контроль. Залежно від умов обстановки БпЛА-перехоплювач може здійснювати патрулювання з увімкненою бортовою РЛС.

Після ураження цілей (ворожих БпЛА) або витрачання боєкомплекту перехоплювач повертається визначеним маршрутом на аеродром базування або оперативний аеродром (місце посадки).

Якщо знищені не всі цілі та вони продовжують політ, віддається команда на їх знищення перехоплювачу, що здійснює «чергування в повітрі» в сусідньому (іншому) районі патрулювання.

У разі складнощів виявлення зльоту БпЛА противника та їх руху в напрямку території нашої держави, БпЛА-перехоплювачі можуть завчасно по команді командного пункту займати визначені райони патрулювання, здійснювати політ по визначеній траєкторії з увімкненими РЛС. При цьому в оператора є можливість вибору режиму керування БпЛА-перехоплювачем – радіоканалом чи в автономному режимі залежно від бойового завдання або в разі появи нештатної ситуації.

На підставі проведених досліджень, виходячи з призначення БпАК із БпЛА-перехоплювачем ворожих ударних БпЛА типу «Shahed», способу його застосування пропонуються такі оперативні-тактичні вимоги до БпЛА-перехоплювача (табл. 2).

Складність боротьби з БпЛА типу «Shahed», особливо в разі їх групового застосування, зумовлює необхідність створення ефективної цілеспрямованої системи протидії цим засобам повітряного нападу, що охоплює «активну» складову (ураження БпЛА вогнем на землі й у повітрі) та «пасивну» радіоелектронну складову. Ця система має бути глибоко ешелонною, інтегрованою як за можливостями виявлення, так і за можливостями ураження, структурно і функціонально взаємоув'язана з іншими підсистемами (боротьби з низько літаючими засобами повітряного нападу, крилатими ракетами тощо). БпЛА-перехоплювач має стати одним з елементів цієї системи.

Групове застосування ударних БпЛА є серйозним фактором для досягнення воєнних цілей малими витратами. Розвиток технологій групового застосування БпЛА суттєво ускладнює завдання боротьби з ними. Тому потрібен ґрунтовний перегляд ідеології створення перспективних систем озброєння ППО. Для успішного знищення БпЛА на траєкторіях їхнього польоту

Таблиця 2

Орієнтовні вимоги до характеристик БпАК з БпЛА-перехоплювачами

Найменування показника	Значення показника
Тривалість польоту (час у повітрі), год.	Не менше 12
Радіус дії, км	300
Робоча висота польоту, м	Від 400–7000
Швидкість максимальна, км/год	До 500
Швидкість крейсерська, км/год	До 200
Максимальна злітна вага, кг	> 500
Бойове навантаження, кг	> 50
Тип корисного навантаження	Авіаційні засоби ураження (зенітний ракетний комплекс «повітря – повітря»)
Маса корисного навантаження, кг	До 100
Вид зльоту	По-літаковому
Вид посадки	По-літаковому
Погодні обмеження	Повинні літати в тих самих умовах, що й БпЛА-камікадзе типу «Shahed»
Характеристика боєприпасу	Комплект керованих малогабаритних ракет з інфрачервоними ГСН або з пасивними (пасивними) радіолокаційними ГСН, доповненими інфрачервоним підривачем. Можливі інші варіанти

в рамках єдиної системи ППО має створюватися ешелонна система боротьби з ними.

Дану статтю варто розглядати передусім як «відправну точку» в такому актуальному напрямі досліджень, як протидія БпЛА з використанням спеціальних БпЛА-перехоплювачів.

Висновки

1. Нині наявний гострий дефіцит спроможностей сил ППО України щодо перехоплення та знищення розвідувальних та ударних БпЛА збройних сил РФ оперативного-тактичного рівня. Для виконання цього складного завдання має бути створена відповідна підсистема озброєння протиповітряної оборони. Одним з важливих та ефективних елементів цієї системи має стати БпЛА-перехоплювач.

2. БпЛА-перехоплювач розвідувальних, ударних (розвідувально-ударних) БпЛА типу «Shahed» та «Орлан» – це високоінтелектуальний швидкісний БпЛА тактичного (оперативно-тактичного) рівня застосування II класу літакового типу з бортовою малогабаритною РЛС і комплектом керованих ракет класу «повітря – повітря» з відповідною системою наведення.

3. Нині актуальним завданням вітчизняних підприємств оборонно-промислового комплексу є розроблення безпілотного авіаційного комплексу з БпЛА-перехоплювачами багаторазового застосування з комплексом керованих авіаційних засобів ураження.

4. Проведені дослідження показують, що подальший напрям розвитку БпЛА нині визначають: розвиток теорії штучного інтелекту; проєкти, націлені на кардинальне підвищення автономності й «інтелектуальності» управління БпЛА.

Перелік літератури

1. Способи та засоби протидії БпЛА, їхні переваги та недоліки. Погляди щодо напрямів їх розвитку [Електронний ресурс] / П. Б. Волотівський, О. В. Гончаров, В. М. Давиденко, Н. Л. Мамонова // Збірник наукових праць Державного науково-дослідного інституту авіації. – Випуск № 20 (27). – 2024. – С. 37–44. – Режим доступу : <https://doi.org/10.54858/dndia.2024-20-7>.

2. Особливості побудови безпілотних авіаційних комплексів, які застосовуються збройними силами Російської Федерації в ході широкомасштабного вторгнення в Україну : довідник / О. М. Романов, М. В. Топольницький, В. С. Герасимов та ін. – К. : НДІ ВР, 2024. – 566 с.

3. Сучасне озброєння і військова техніка збройних сил Російської Федерації. Довідник учасника ООС / С. П. Корнійчук, О. В. Турінський, Г. В. Певцов та ін. ; за заг. ред. С. П. Корнійчука. – Х. : ДІСА ПЛЮС, 2020. – 1220 с.

4. *Ростопчин В. В.* Ударные беспилотные летательные аппараты и противовоздушная оборона – проблемы и перспективы противостояния [Електронний ресурс] / В. В. Ростопчин // ResearchGate. – Режим доступу : <http://surl.li/fcqaqa>.

5. Погляди і перспективи створення системи протибезпілотної оборони, її роль та місце в системі протиповітряної оборони України [Електронний ресурс] / П. Б. Волотівський, О. В. Самойленко, П. М. Стешенко, П. А. Глущенко // Наука і оборона. – 2024. – № 3. – С. 37–44. – Режим доступу : <https://doi.org/10.33099/2618-1614-2024-26-3-37-44>.

6. Щодо обрисів перспективної системи боротьби з безпілотними авіаційними комплексами [Електронний ресурс] / П. Б. Волотівський, П. М. Стешенко, С. О. Богославець, В. В. Корепанов // Наука і оборона. – 2024. – № 4. – С. 24–32. – Режим доступу : <https://doi.org/10.33099/2618-1614-2024-27-4-24-32>.

7. Беспилотные летательные аппараты: обоснование и расчет основных параметров и характеристик / М. М. Митрахович, В. И. Силков, А. В. Самков, В. Б. Семенов ; под общей редакцией В. И. Силкова. – К. : ЦНИИ ВВТ ВС Украины, 2016. – 268 с.

DOI 10.33099/2618-1614-2025-28-1-11-17

УДК 355.424.4.:623.746.-519

А. К. Павліковський,*кандидат військових наук, доцент,
Національний університет оборони України,***В. О. Тютюнник,***кандидат технічних наук, старший науковий
співробітник, Харківський національний університет
Повітряних Сил ім. І. Кожедуба,***В. А. Ткаченко,***кандидат військових наук, старший дослідник,
Центральний науково-дослідний інститут
Збройних Сил України,***Н. І. Ткаченко,***Національний університет оборони України*

Підвищення ефективності протидії масованому застосуванню ударних безпілотних літальних апаратів

У статті проведено аналіз слабких сторін ударних безпілотних літальних апаратів одноразового використання типу «Shahed-136/131» та обґрунтовано можливість і умови використання артилерійської (стрілецької) зброї для їх вогневого ураження. Показано, що раціональним способом застосування артилерійської (стрілецької) зброї для вирішення цього завдання є дії мобільних вогневих груп із засідок, які оперативно організуються на маршрутах польоту ударних безпілотних літальних апаратів за даними оповіщення про повітряного противника. Визначені вимоги до особливостей організації системи вогню, системи розвідки та засобів прицілювання мобільних вогневих груп, які озброєнні зенітними установками або великокаліберними кулеметами.

Ключові слова: зенітна установка, імовірність влучання, мобільна вогнева група, протиповітряна оборона, раціональний склад засобів, стрілецька зброя, ударні безпілотні літальні апарати.

© А. К. Павліковський, В. О. Тютюнник, В. А. Ткаченко,
Н. І. Ткаченко, 2025

Постановка проблеми. У процесі збройної агресії проти України Російська Федерація вдається до масованого використання керованої високоточної зброї оперативно-тактичного призначення для нанесення вогневого ураження по об'єктах цивільної та військової інфраструктури, розташованих у глибині території України. Для цього, як правило, застосовуються крилаті ракети та ударні безпілотні літальні апарати (БпЛА) одноразового використання (далі – камікадзе) типу «Shahed-136/131», які можуть здійснювати політ на малих та гранично малих висотах на відстань до 1500 км з використанням довільних маршрутів польоту над територією України. Відносно невисока вартість і відносно низькі витрати на виробництво ударних БпЛА-камікадзе типу «Shahed-136/131» зумовлює їхнє масоване застосування, в тому числі в ролі хибних цілей з метою викриття системи протиповітряної оборони (ППО), відволікання та перевантаження засобів ППО, спонукання до зайвих витрат зенітних ракет, які мають значну вартість. Особливість використання частки ударних БпЛА-камікадзе типу «Shahed-136/131» зі складу засобів, які залучаються до масованого удару, в ролі хибних цілей полягає в наявності бойової частини та неможливості відрізнити їх від БпЛА, призначених для нанесення удару. Це зумовлює небезпеку БпЛА, які виконують завдання хибних цілей, та необхідність їх вогневого ураження. Отже, комплексне використання крилатих ракет і ударних БпЛА-камікадзе в масованому ударі забезпечує високу щільність удару, яка може перевищувати бойову продуктивність наявних засобів ППО та знижує ефективність прикриття відповідних об'єктів.

Виникає нагальна потреба в пошуку шляхів протидії масованому застосуванню ударних БпЛА-камікадзе оперативно-тактичного призначення, які здійснюють політ на малих та гранично малих висотах над територією України, з урахуванням критерію «ефективність – вартість».

Аналіз останніх досліджень і публікацій свідчить, що питанням удосконалення систем ППО для протидії новітнім засобам повітряного нападу (ЗПН) та новим способам їхнього застосування приділяється значна увага. У роботі [1] обґрунтовано, що для ефективної протидії якісно новим ЗПН необхідно забезпечити можливість ведення боротьби з ними в усьому повітряному просторі України, а не лише в прикордонних районах та навколо важливих об'єктів. Показано, що для вирішення цього завдання доцільно залучати спеціально призначені для цього сили й засоби ППО. У роботах [2–4] проведений аналіз можливостей існуючих засобів протидії маловисотним, малошвидкісним та малорозмірним БпЛА, та зроблений висновок про необхідність створення нових дешевших засобів для протидії їм

з метою оптимізації балансу «вартість ЗПН – вартість боєприпасів для ураження ЗПН». У роботах [5], [6] зазначені тактичні переваги у формуванні та застосуванні мобільних груп і мобільних вогневих підрозділів порівняно зі штатними традиційними підрозділами як спосіб «асиметричного» реагування на ведення противником бойових дій «нетрадиційними» способами. У [7] розглянуті особливості оцінювання дій зенітних мобільних вогневих груп (МВГ) у складі системи зенітного ракетно-артилерійського прикриття важливих об'єктів чи угруповань військ.

Невирішеним залишається питання обґрунтування оптимальної кількості та складу сил і засобів, а також доцільних способів їхнього застосування для протидії масованому удару з використанням БпЛА-камікадзе оперативного-тактичного призначення на маршрутах їхнього польоту над територією України без прив'язки до завдань прикриття конкретних об'єктів.

Мета статті полягає в обґрунтуванні шляхів підвищення ефективності протидії масованому застосуванню ударних БпЛА-камікадзе оперативного-тактичного призначення, визначення доцільного озброєння та способів застосування зенітних підрозділів для вогневого ураження БпЛА-камікадзе під час їхнього польоту над територією України незалежно від об'єктів, які були призначені для ураження.

Викладення основного матеріалу

Підвищення ефективності протидії масованому застосуванню ударних БпЛА-камікадзе можливе за рахунок оптимізації та гнучкого застосування різноманітних засобів ППО з максимальним використанням слабких сторін побудови і тактики застосування ударних БпЛА-камікадзе. Для досягнення цього необхідно забезпечити раціональне поєднання таких елементів системи ППО:

- системи вогню з урахуванням забезпечення балансу «вартість ЗПН – вартість боєприпасів для ураження ЗПН»;

- системи розвідки з урахуванням забезпечення своєчасності виявлення, визначення координат БпЛА та видачі цілевказання;

- системи управління з урахуванням оптимізації цілерозподілу з метою забезпечення балансу між можливостями відповідного засобу ППО та кількістю цілей, які одночасно перебувають у зоні його ураження.

Обґрунтування шляхів підвищення ефективності протидії масованому застосуванню ударних БпЛА-камікадзе проведемо на основі аналізу слабких сторін ударних БпЛА-камікадзе, з одного боку, та сильних сторін відповідних засобів ППО, з другого.

Аналіз досвіду бойового застосування ударних БпЛА-камікадзе, зокрема, «Shahed-136/131», у процесі

відбиття збройної агресії Росії проти України свідчить про наявність характерних тактичних особливостей їхнього застосування [8], [9]:

- вони застосовуються переважно в темний час доби;

- польоти здійснюються на малих (менше ніж 1000 м) та гранично малих (менше ніж 200 м) висотах;

- застосування відбувається групами до 12 БпЛА кожній, які виконують політ послідовно з певними проміжками часу між групами за однаковими або різними маршрутами, що забезпечує високу щільність удару по об'єкту, що прикривається;

- маршрути польотів, як правило, складаються з прямолінійних ділянок та пролягають, за можливості, в обхід зон виявлення та зон ураження засобів ППО, позиції яких розвідані противником завчасно або за результатами застосування хибних цілей (результатів польоту попередніх груп);

- довжина маршруту польоту БпЛА над територією України від державного кордону (лінії розмежування) до об'єкта ураження, розташованого в глибині території України, складає від 200 км до 600 км зі швидкістю до 200 км/год. Це відповідає часу польоту БпЛА над територією України не менш як одна година.

Особливості застосування ударних БпЛА-камікадзе, з одного боку, вимагають високої вогневої продуктивності засобів ППО, які забезпечують прикриття відповідних об'єктів (унаслідок високої щільності удару), а з другого – забезпечують достатньо часу для підготовки для застосування засобів ППО на маршрутах польоту БпЛА до об'єкта удару (внаслідок значного часу перебування БпЛА над територією України).

Наближення до об'єкта прикриття одночасно значної кількості ударних БпЛА може перевищити вогневу продуктивність засобів ППО, які здійснюють прикриття відповідного об'єкта. Для запобігання цьому необхідно забезпечити зменшення щільності удару шляхом поступового знищення БпЛА на маршрутах їхнього польоту під час наближення до об'єктів удару. Потенційна можливість успішності вирішення цього завдання зумовлена значним часом перебування БпЛА над територією України.

Використання малих та гранично малих висот під час польоту ударних БпЛА над територією України, з одного боку, ускладнює їх своєчасне виявлення засобами розвідки системи ППО, а з другого – зумовлює потенційну можливість застосування зенітних артилерійських установок та стрілецької зброї для ураження БпЛА замість зенітних ракетних комплексів.

Успішність застосування активних засобів ППО залежить від своєчасності виявлення й точності видачі цілевказання по БпЛА на вогневі засоби. Основними демаскуючими ознаками ударних БпЛА-камікадзе

типу «Shahed-136/131», які можуть використовуватися для його виявлення, є:

- радіолокаційна помітність, ефективна площа розсіювання складає не менше ніж 0,2 м² [10];
- акустична помітність, зумовлена роботою двигуна внутрішнього згорання, яка складає до 1,5 км по дальності та до 1 км по висоті [11], і тепла помітність;
- візуальна помітність у світлий час доби, зумовлена габаритами БпЛА.

Найдешевшими засобами боротьби з БпЛА, порівняно із зенітними ракетними комплексами, є артилерійські вогневі засоби та стрілецька зброя. Розгляньмо можливості зенітних установок та великокаліберних кулеметів щодо ураження ударних БпЛА-камікадзе типу «Shahed-136/131» під час їхнього польоту на малих та гранично малих висотах.

Основними показниками стрілецької зброї та зенітних установок, які зумовлюють їхню потенційну можливість здійснювати вогневе ураження БпЛА, (табл. 1) є:

- ефективна дальність стрільби;
- бойова швидкострільність;

- калібр кулі (снарядів);
- технічні характеристики розсіювання (згідно з таблицями стрільби, які визначають середнє відхилення по висоті (B_B), середнє бокове відхилення (B_B)) (рис. 1, табл. 1).

Для великокаліберного кулемету М2 Браунінг відомості щодо таблиць стрільби відсутні, але відомо, що розмір пристріляної групи не повинен перевищувати коло розміром 4 см при стрільбі з відстані 10 м [12], що відповідає радіусу кола, яке вміщує всі влучання $R_{100} = 2$ см. Відомо, що в інтервал $\pm 4 B_B$ ($\pm 4 B_B$) потрапляють 100% влучань [13]. За цих умов для кулемета М2 Браунінг можна оцінити площу кіл розсіювання 100% влучань за виразом:

$$S_{100}(D) = \pi(R_{100}(D))^2 = \pi \left(D \frac{R_{100}(10)}{10} \right)^2 = \pi 4 \cdot 10^{-6} D^2, \quad (1)$$

де $S_{100}(D)$ – площа кола, яке вміщує 100% влучань при дальності стрільби D ;

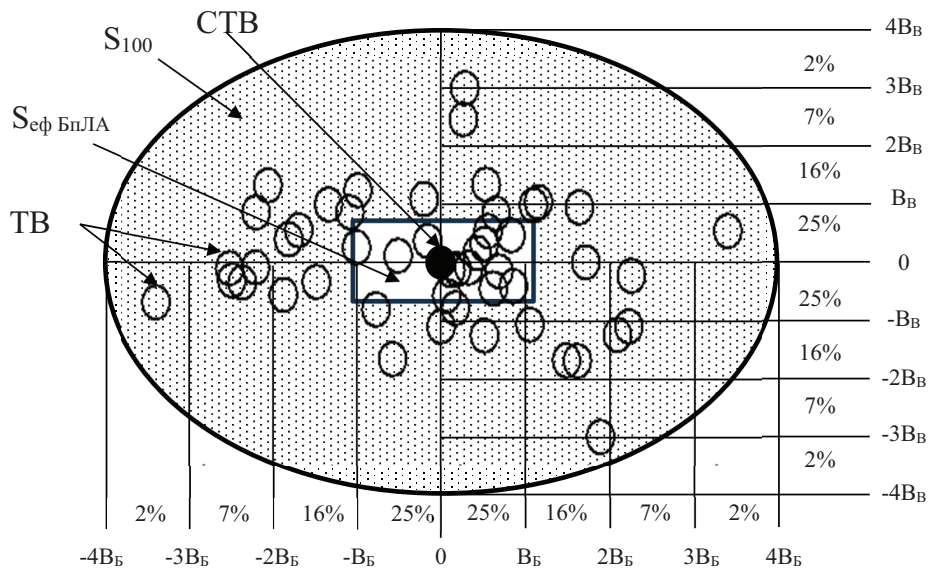


Рис. 1. Розсіювання точок влучання (ТВ) при обстрілі цілі відносно середньої точки влучання (СТВ)

Таблиця 1

Окремі характеристики зброї

Тип зброї	Калібр кулі, мм	Прицільна дальність стрільби, м	Бойова швидкострільність, постріл/хв	Дальність до цілі, м / середнє відхилення, м							
				200		400		800		1000	
				B_B	B_B	B_B	B_B	B_B	B_B	B_B	B_B
Кулемет М2 Браунінг	12,7	2000	100	-	-	-	-	-	-	-	-
Кулемет ДШК	12,7	2400	100	0,13	0,08	0,27	0,19	0,58	0,45	0,76	0,59
Зенітна установка ЗУ-23-2	23	1500	400	0,2	0,1	0,3	0,2	0,6	0,4	0,8	0,5

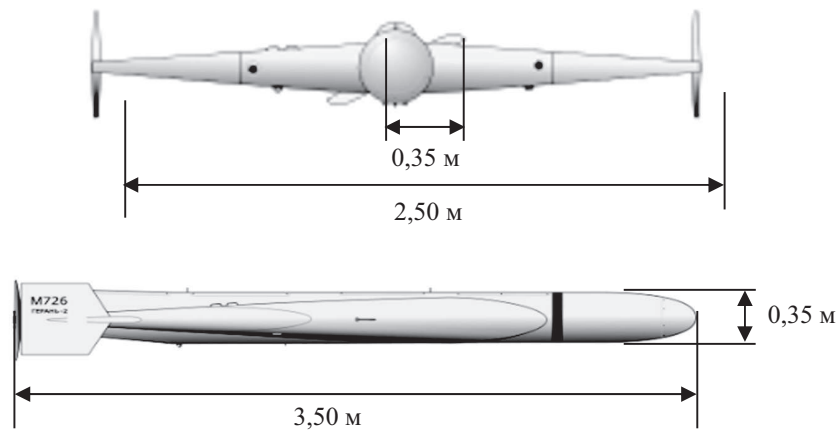


Рис. 2. Розміри ударного БпЛА-камікадзе «Shahed-136/131»

$R_{100}(D)$ – радіус кола, яке вміщує 100% влучань при дальності стрільби D ;

$R_{100}(10)$ – радіус кола пристріляної групи при дальності стрільби 10 м (вміщує всі влучання);

D – дальність стрільби, для якої оцінюється площа кола S_{100} .

Розміри ударного БпЛА-камікадзе «Shahed-136» наведені на *рисунку 2*.

Оцінювання ймовірності ураження ударного БпЛА-камікадзе типу «Shahed-136/131» доцільно здійснювати за умови влучання в центральну частину БпЛА (корпус) без урахування влучань у площину крил, оскільки в центральній частині зосереджена апаратура управління польотом, пошкодження якої призведе до унеможливлення подальшого польоту. Водночас влучання в площу крила може призвести лише до ускладнення подальшого польоту. Переріз центральної частини БпЛА-камікадзе типу «Shahed-136/131» має розмір $0,35 \times 3,5$ м (*рис. 2*) та площу $1,2$ м². БпЛА може спостерігатися стрільцем під різними ракурсами, отже, для оцінювання ймовірності влучання в центральну частину БпЛА припустимо, що значення ефективної площі силуету БпЛА, який спостерігається з боку стрільця, становить не менш ніж $S_{\text{еф}} \text{ БпЛА} = 0,6$ м², а його лінійні розміри не менші ніж $0,35$ м по висоті та $1,72$ м по фронту. Імовірність влучання одного пострілу в центральну частину БпЛА (P_1) за умови, що середня точка влучань (СТВ) збігається із центром БпЛА (*рис. 1*), визначимо за виразом:

$$P_1 = p_B p_{\text{Б}}, \quad (2)$$

де p_B – імовірність влучання одним пострілом з урахуванням розсіювання по висоті;

$p_{\text{Б}}$ – імовірність влучання одним пострілом з урахуванням бокового розсіювання.

Значення ймовірностей p_B та $p_{\text{Б}}$ визначимо за допомогою сітки розсіювання по співвідношенню значень V_B , $V_{\text{Б}}$ (*табл. 1*) та відповідних лінійних розмірів силуету БпЛА (*рис. 1*, *рис. 2*).

Для кулемета М2 Браунінг у зв'язку з відсутністю таблиць стрільби ймовірність влучання одного пострілу в центральну частину БпЛА за умови, що СТВ збігається із центром БпЛА, визначимо за виразом:

$$P_1(D) = \frac{S_{\text{еф}} \text{ БпЛА}}{S_{100}(D)}, \quad (3)$$

де $P_1(D)$ – імовірність одного влучання при дальності стрільби D .

У припущенні (для спрощення розрахунків), що попередні постріли не впливають на влучність наступних пострілів, імовірність того, що із черги пострілів буде не менше ніж одне влучання в ціль визначимо за виразом:

$$P^n = 1 - (1 - P_1)^n, \quad (4)$$

де P^n – імовірність одного влучання із черги пострілів;

n – кількість пострілів у черзі;

P_1 – імовірність одного влучання з одного пострілу.

Результати розрахунків за виразами (1), (2), (3), (4) та кількість пострілів, які необхідно здійснити для забезпечення ймовірності одного влучання не менш ніж $0,9$ ($n_{0,9}$), та час (t), необхідний для здійснення $n_{0,9}$ пострілів, наведені в *таблиці 2*.

З аналізу даних *таблиці 2* видно, що залежно від дальності до цілі й типу зброї кількість пострілів, необхідна для забезпечення ймовірності одного влучання не менш ніж $0,9$, становить від 1 до 45. Час, потрібний для здійснення такої кількості пострілів, складає від $0,6$ с до 27 с. Ураховуючи, що швидкість польоту ударного БпЛА-камікадзе типу «Shahed-136/131» становить 50 м/с (180 км/год), то для забезпечення його

Таблиця 2

Характеристики розсіювання, кількість пострілів та ймовірність влучання

Тип зброї	Дальність до цілі, м											
	200			400			800			1000		
	p_B/p_B	P_1	$n_{0,9}/t, c$	p_B/p_B	P_1	$n_{0,9}/t, c$	p_B/p_B	P_1	$n_{0,9}/t, c$	p_B/p_B	P_1	$n_{0,9}/t, c$
Кулемет М2 Браунінг	–	1	1/0,6	–	0,3	7/4,2	–	0,08	28/16,8	–	0,05	45/27
Кулемет ДШК	0,61/1	0,61	3/1,8	0,32/1	0,32	6/3,6	0,15/0,79	0,12	18/10,8	0,11/0,65	0,07	32/19,2
Зенітна установка ЗУ-23-2	0,43/1	0,43	5/0,75	0,29/1	0,29	7/1,1	0,15/0,84	0,13	17/2,55	0,11/0,73	0,08	28/4,2

обстрілу чергою пострілів необхідно забезпечити супроводження його переміщення під час обстрілу.

Похибки в прицілюванні та дія інших чинників призводить до відхилення СТВ від центру цілі по висоті (ΔB) або фронту ($\Delta \beta$), що зменшує ймовірність влучання в ціль. Ступінь впливу відхилення СТВ від центру цілі на ймовірність влучання залежить від співвідношення значень серединних відхилень по висоті і фронту та лінійних розмірів силуету цілі, який спостерігаються з боку стрільця. Розрахуємо похибки в прицілюванні, які призводять до зменшення ймовірності одного влучання вдвічі. Для цього за допомогою сітки розсіювання, співвідношення значень B_B , V_B (табл. 1) та відповідних лінійних розмірів силуету БпЛА (рис. 1) визначимо відхилення СТВ від центру цілі (ΔB , $\Delta \beta$) та відповідні кутові відхилення ($\Delta \varepsilon$, $\Delta \beta$), які призводять до зменшення ймовірностей p_B та p_B у $\sqrt{2}$. Результати розрахунків наведені в таблиці 3.

З аналізу даних таблиці 3 видно, що максимальна похибка прицілювання за кутовими координатами (азимутом і кутом місця) має бути не більше $0,05^\circ$ (6 кутових хвилин) у режимі супроводження цілі за кутовими координатами під час її обстрілу. Обстріл цілі доцільно здійснювати з відстані не більш ніж 400 м, що забезпечить ймовірність одного влучання не менше ніж 0,9 при кількості пострілів не більше ніж 16. Забезпечення похибок прицілювання за кутовими координатами не більше ніж $0,05^\circ$ можливе лише в разі використання оптичних прицілів.

Таким чином, за результатами аналізу можливостей великокаліберних кулеметів і зенітних артиле-

рійських установок для вогневого ураження ударних БпЛА-камікадзе типу «Shahed-136/131» можна зробити такі висновки:

- влучання в ціль можливе за умови забезпечення її супроводження за кутовими координатами під час обстрілу;

- для забезпечення ймовірності одного влучання в корпус цілі (без урахування площі крил) не менше ніж 0,9 максимальні похибки прицілювання за кутовими координатами мають бути не більше ніж $0,05^\circ$ (6 кутових хвилин);

- обстріл цілі доцільно здійснювати з відстані не більше 400 м, що забезпечить мінімізацію витрат боеприпасів (не більше 16 на одне влучання в корпус із ймовірністю 0,9) та оптимізацію застосування за критерієм «ймовірність влучання – витрата боеприпасів»;

- прицілювання зброї має здійснюватися за допомогою автоматизованих оптичних (тепловізійних) приладів, які обладнані балістичним калькулятором та забезпечують можливість прицілювання по рухомих цілях та їхнє супроводження.

Виходячи з викладеного, типове оснащення мобільної вогневої групи доцільно мати в такому складі (рис. 3):

а) транспортний засіб (автомобіль підвищеної прохідності);

б) вогневий засіб (великокаліберний кулемет або зенітна установка);

в) засоби автоматизації прицілювання;

г) засоби зв'язку та передачі даних (LTE, StarLink).

З урахуванням оцінених вище можливостей вогневих засобів та забезпечення балансу «вартість ЗПН –

Таблиця 3

Похибки прицілювання, кількість пострілів та ймовірність влучання

Тип зброї	Дальність до цілі, м											
	200			400			800			1000		
	$\Delta B/\Delta B$, м	$\Delta \varepsilon/\Delta \beta$, град	$P_1/n_{0,9}/t$, с	$\Delta B/\Delta B$, м	$\Delta \varepsilon/\Delta \beta$, град	$P_1/n_{0,9}/t$, с	$\Delta B/\Delta B$, м	$\Delta \varepsilon/\Delta \beta$, град	$P_1/n_{0,9}/t$, с	$\Delta B/\Delta B$, м	$\Delta \varepsilon/\Delta \beta$, град	$P_1/n_{0,9}/t$, с
Кулемет ДШК	0,19/0,79	0,05/0,23	0,3/7/4,2	0,37/0,71	0,05/0,1	0,16/14/8,4	0,79/0,75	0,06/0,05	0,06/38/22,8	1,1/0,88	0,06/0,05	0,03/76/45,6
Зенітна установка ЗУ-23-2	0,27/0,78	0,08/0,22	0,2/11/1,7	0,4/0,7	0,05/0,1	0,14/16/2,4	0,8/0,77	0,06/0,06	0,06/38/5,7	1,1/0,8	0,06/0,05	0,04/57/8,5

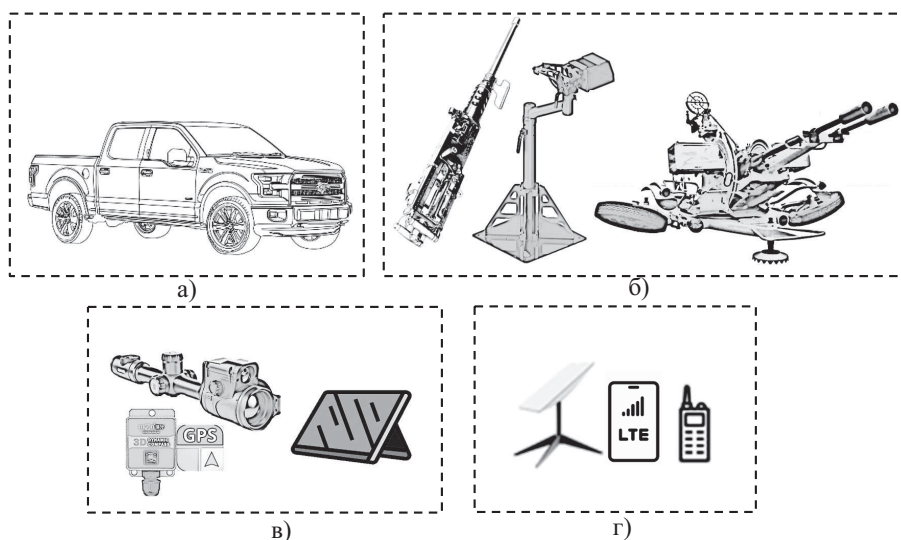


Рис. 3. Типове обладнання МВГ

вартість боєприпасів» ураження БпЛА доцільно здійснювати шляхом організації засідок із декількох МВГ на виявлених маршрутах польотів БпЛА. Припускаючи, що похибка визначення напрямку польоту БпЛА за даними розвідувальної інформації може досягати $\Delta D=1000$ м, система вогню, яка будується МВГ у засідках на маршрутах польоту БпЛА, може мати вигляд, наведений на *рисунку 4*.

Для забезпечення реалізації потенційних можливостей вогневих засобів щодо ураження БпЛА на маршрутах польоту створюється система розвідки повітряних цілей, яка має вирішувати такі завдання:

- завчасне виявлення БпЛА, визначення напрямків їхнього польоту з метою оповіщення та визначення районів організації засідок МВГ;
- видача цілевказання на засоби прицілювання вогневих засобів.

Для вирішення першого завдання доцільно використовувати розвідувальну інформацію, яка здобувається в загальній системі розвідки повітряного противника та оповіщення про нього за допомогою радіолокаційних, радіотехнічних, акустичних та інших засобів.

Для вирішення другого завдання доцільно використовувати мобільні радіолокаційні станції цілевказання (РЛС ЦВ) малої дальності, які діють поблизу вогневих позицій МВГ та видають цілевказання на засоби прицілювання МВГ. Варіант системи розвідки повітряних цілей в інтересах застосування МВГ по БпЛА на маршрутах польоту наведений на *рисунку 5*.

Автоматизована системи управління на основі інформації, яка здобувається системою розвідки, забезпечує оперативне створення системи вогню на маршрутах польоту виявлених БпЛА та управління вогневим ураженням БпЛА.

Висновки та перспективи подальших досліджень

На основі проведеного аналізу слабких сторін ударних БпЛА-камікадзе типу «Shahed-136/131» та сильних сторін артилерійської (стрілецької) зброї можна констатувати, що її застосування за певних умов може забезпечити підвищення ефективності протидії масованому застосуванню ударних БпЛА-камікадзе з урахуванням критерію «ефективність – вартість».

Основним способом протидії масованому застосуванню ударних БпЛА-камікадзе за допомогою артилерійської (стрілецької) зброї є поступове їх знищення

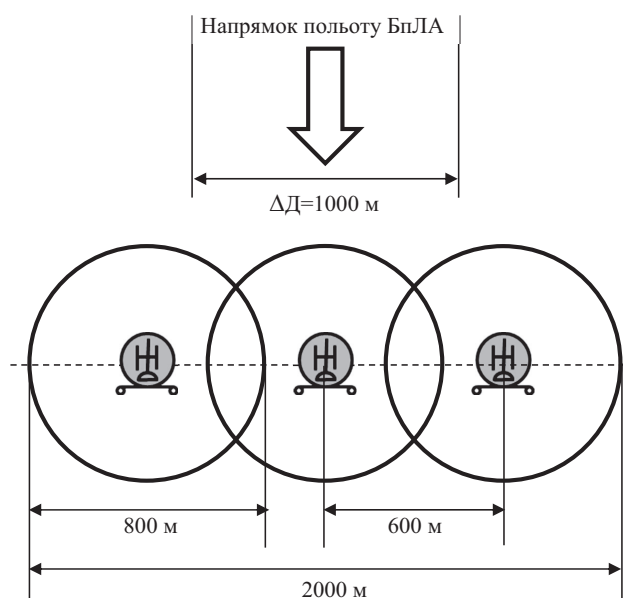


Рис. 4. Система вогню засідки МВГ на маршруті польоту БпЛА

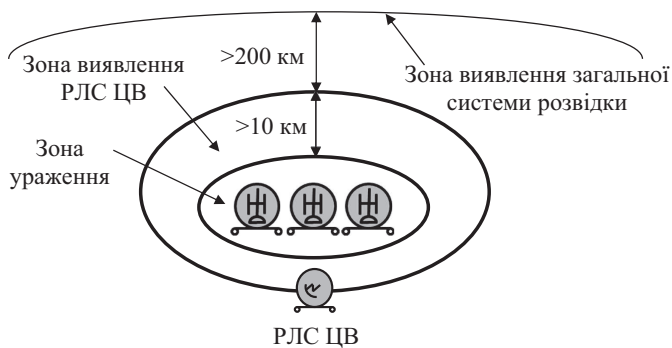


Рис. 5. Система розвідки повітряних цілей в інтересах застосування МВГ по БпЛА на маршрутах польоту

в процесі польоту над територією України до об'єктів удару.

Раціональним вирішенням цього завдання є створення МВГ для дій із засідок, які оперативно створюються на маршрутах польоту ударних БпЛА-камікадзе за даними оповіщення, одержуваними від системи розвідки повітряного противника.

Успішне вирішення завдання вогневого ураження ударних БпЛА-камікадзе в процесі їхнього польоту на малих та гранично малих висотах можливе за умови автоматизації прицілювання артилерійської (стрілецької) зброї по повітряних цілях за допомогою автоматизованих оптичних (тепловізійних) приладів, які обладнані відповідними балістичними калькуляторами і забезпечують супроводження повітряних цілей під час обстрілу, та радіолокаційних засобів малої дальності дії, котрі забезпечують можливість видачі цілевказання на засоби прицілювання.

Напрямок подальших досліджень полягає в удосконаленні алгоритму прицілювання зброї по повітряній цілі та алгоритму взаємодії автоматизованих оптичних (тепловізійних) приладів з радіолокаційними засобами видачі цілевказання.

Перелік літератури

1. Погляди на організацію протиповітряної оборони в сучасних умовах [Електронний ресурс] / В. В. Ткачов, В. В. Камінський, Г. С. Степанов, П. В. Оріховський // Наука і оборона. – 2021. – № 4. – С. 13–16. – Режим доступу : <https://doi.org/10.33099/2618-1614-2021-17-4-13-16>.

2. Munday R. Engagement of Low, Slow and Small Aerial Targets by GBAD : Final Report of NIAG SG-170 Study / R. Munday ; NATO Industrial Advisory Group. – [Brussels] : [NIAG], 2013. – 333 p.

3. Корощенко М. М. Протиповітряна оборона кораблів (катерів) Військово-Морських Сил України у «війні дронів»: проблеми та шляхи підвищення ефективності [Електронний ресурс] / М. М. Корощенко, О. Л. Харитонов, А. М. Гор-

дієнко // Системи озброєння і військова техніка. – 2020. – № 2 (62). – С. 18–23. – Режим доступу : <https://doi.org/10.30748/soivt.2020.62.02>.

4. Захист населених пунктів від ударних та диверсійно-розвідувальних безпілотних літальних апаратів [Електронний ресурс] / І. С. Афтаназів, Р. З. Стоцько, Л. І. Шевчук та ін. // Системи озброєння і військова техніка. – 2023. – № 1 (73). – С. 82–95. – Режим доступу : <https://doi.org/10.30748/soivt.2023.73.10>.

5. Гузченко С. В. Обґрунтування обсягу завдань, що вирішуються мобільними тактичними групами під час ведення бойових дій [Електронний ресурс] / С. В. Гузченко, Д. М. Козлов, С. М. Телюков // Наука і техніка Повітряних Сил Збройних Сил України. – 2020. – № 1 (38). – С. 31–38. – Режим доступу : <https://doi.org/10.30748/nitps.2020.38.03>.

6. Ярош С. П. Обґрунтування організації зенітного ракетно-артилерійського прикриття угруповань військ з застосуванням міжвидових мобільних вогневих підрозділів ППО [Електронний ресурс] / С. П. Ярош, Б. М. Рябуха, Р. А. Соломонович // Наука і техніка Повітряних Сил Збройних Сил України. – 2020. – № 2 (39). – С. 77–82. – Режим доступу : <https://doi.org/10.30748/nitps.2020.39.09>.

7. Пропозиції щодо оцінювання бойових дій зенітної мобільної вогневої групи / М. О. Єрмошин, О. В. Кулешов, О. В. Коломійцев, В. В. Шулежко // Наука і техніка Повітряних Сил Збройних Сил України. – 2017. – № 1 (26). – С. 58–60.

8. Застосування безпілотних літальних апаратів збройними силами Російської Федерації у війні проти України [Електронний ресурс] / О. О. Олексенко, О. В. Авраменко, А. В. Федоров та ін. // Наука і техніка Повітряних Сил Збройних Сил України. – 2022. – № 4 (49). – С. 37–42. – Режим доступу : <https://doi.org/10.30748/nitps.2022.49.05>.

9. Безпілотна авіація Ісламської республіки Іран і досвід її застосування в російсько-українській війні [Електронний ресурс] / С. І. Корсунов, А. Ф. Волков, С. В. Орехов та ін. // Збірник наукових праць Харківського національного університету Повітряних Сил. – 2023. – № 2 (76). – С. 54–66. – Режим доступу : <https://doi.org/10.30748/zhups.2023.76.07>.

10. Дослідження радіолокаційних характеристик моделі баражуючого боеприпасу «Shahed-136» [Електронний ресурс] / О. І. Сухаревський, В. О. Василюк, С. В. Нечитайло та ін. // Наука і техніка Повітряних Сил Збройних Сил України. – 2023. – № 2 (51). – С. 56–62. – Режим доступу : <https://doi.org/10.30748/nitps.2023.51.07>.

11. Ростопчин В. В. Ударные беспилотные летательные аппараты и противовоздушная оборона – проблемы и перспективы противостояния [Електронний ресурс] / В. В. Ростопчин // ResearchGate. – Режим доступу : <http://surl.li/fc9qaka>.

12. Heavy Machine Gun M2 Series : Training Circular TC 3-22.50 / Headquarters, Department of the Army. – [Washington, DC] : [Headquarters, Department of the Army], 2017. – 256 p.

13. Стрільба артилерії : підручник / В. М. Петренко, В. Є. Житник, В. І. Макеєв та ін. – Суми : Сумський державний університет, 2012. – 757 с.

DOI 10.33099/2618-1614-2025-28-1-18-26

УДК 340.134::355.134

В. А. Тимошенко,*доктор юридичних наук, професор,
Національний університет оборони України,***В. П. Отрощенко,***Збройні Сили України,***С. В. Дрьомов,** кандидат юридичних наук,*Збройні Сили України*

Проблеми нормативно-правового регулювання призначення військовослужбовцям винагороди за знищення ворожої техніки

У статті висвітлено результати дослідження проблем нормативно-правового регулювання механізму призначення військовослужбовцям винагороди за знищення та захоплення ворожої техніки. Зазначений механізм розглядається як один з елементів інституту мотивації військовослужбовців сил безпеки та оборони України, який може використовуватися для здійснення впливу на процес формування у військовослужбовця інтересу до військової професії та усвідомлення її суспільного значення. Автори провели аналіз положень нормативно-правових актів, якими регулюються питання призначення військовослужбовцям винагороди за знищення та захоплення ворожої техніки. Зроблено висновки про недосконалість положень зазначених нормативно-правових актів та існування неузгодженості між ними. Запропоновані шляхи вдосконалення законодавства України, яким регулюються питання призначення військовослужбовцям винагороди за знищення та захоплення ворожої техніки.

Ключові слова: національна безпека, суверенітет держави, незалежність, територіальна цілісність, Збройні Сили України, нормативно-правове регулювання, Конституція України, мотивація військової служби, додаткова винагорода військовослужбовцям, знищення ворожої техніки, ураження ворожої техніки, захоплення ворожої техніки, правовий режим воєнного стану, журнал бойових дій.

© В. А. Тимошенко, В. П. Отрощенко, С. В. Дрьомов, 2025

У частині першої статті 17 Конституції України записано, що найважливішими функціями держави, а також справою всього Українського народу є захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки [1].

Надзвичайної актуальності реалізація зазначеного конституційного припису набула у зв'язку з реальною загрозою суверенітету, територіальній цілісності України, викликаною розв'язаною Російською Федерацією воєнною агресією, яка водночас стала чинником, що консолідує зусилля держави та суспільства у справі захисту української державності та національної ідентичності.

Частиною другою статті 17 Основного Закону України визначено, що оборона України, захист її суверенітету, територіальної цілісності й недоторканності покладаються на Збройні Сили України [1].

Відповідно до частини другої статті 1 Закону України «Про Збройні Сили України» під Збройними Силами України розуміють військове формування, на яке згідно з Конституцією України покладаються завдання забезпечувати оборону України, захист її суверенітету, територіальної цілісності та недоторканності [2].

Таким чином, Збройні Сили України [2]:

- забезпечують стримування збройної агресії проти України та відсіч їй;
- здійснюють охорону повітряного простору держави та підводного простору в межах територіального моря України;
- у випадках, визначених законом, беруть участь у заходах, спрямованих на боротьбу з тероризмом.

Водночас держава, зі свого боку, повинна належним чином соціально захищати й мотивувати тих, хто долучився до її захисту. На це неодноразово звертав увагу у своїх рішеннях Конституційний Суд України, зазначаючи, що відповідно до положень статті 17 Конституції України комплекс організаційно-правових та економічних заходів, спрямованих на забезпечення соціального захисту військовослужбовців та працівників правоохоронних органів, зумовлений не їхньою непрацездатністю чи відсутністю достатніх засобів для існування (стаття 46 Конституції України), а особливістю професійних обов'язків, пов'язаних з ризиком для життя та здоров'я, певним обмеженням конституційних прав і свобод, у тому числі права заробляти матеріальні блага для забезпечення собі і своїй сім'ї рівня життя, вищого за прожитковий мінімум (див., наприклад, Рішення Конституційного Суду України № 7-рп/2004 від 17 березня 2004 р. [3]).

Тривалість, інтенсивність і складний характер бойових дій на всіх напрямках фронту вимагає від захисників Вітчизни максимальної віддачі фізичних та

моральних сил. З огляду на це додаткове мотивування (стимулювання), підтримка і повага до них мають забезпечуватися державою й суспільством на належному рівні та вважатися ключовими чинниками під час формування та реалізації державної політики в цій сфері.

Одним з елементів мотивування (фінансового стимулювання) наших оборонців вважається виплата додаткової винагороди за знищену (захоплену) ворожу техніку.

Однак нормативно-правові акти, якими врегульовано порядок підтвердження фактів знищення (захоплення) ворожої техніки, а також визначення розміру винагороди за це, не передбачають належного термінологічного інструментарію, що призводить до неоднозначного та подекуди неправильного тлумачення понять «знищення ворожої техніки», «захоплення ворожої техніки» та навіть до їх отождолення. Це негативно позначається на реалізації положень зазначених нормативно-правових актів, суттєво ускладнює прийняття рішень щодо підтвердження чи спростування фактів знищення ворожої техніки та може призвести до випадків неефективного використання бюджетних коштів і порушення законних прав учасників зазначених правовідносин.

Слід зауважити, що відсутність законодавчого регулювання окремих питань щодо збільшення винагороди військовослужбовцям Збройних Сил України у зв'язку з підтвердженням фактів знищення (захоплення) ними ворожої техніки частково компенсується положеннями постанови Кабінету Міністрів України № 18 від 20 січня 2016 р. [4], Порядком надання військовослужбовцям додаткової відпустки за знищену ворожу техніку, затвердженим постановою Кабінету Міністрів України № 585 від 21 травня 2024 р. [5] (далі – Порядок-1), та Порядком виплати винагороди військовослужбовцям Збройних Сил України та Державної спеціальної служби транспорту за безпосередню участь у воєнних конфліктах, в заходах із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації чи в антитерористичній операції, інших заходах в умовах особливого періоду, затвердженим наказом Міністерства оборони України № 340 від 18 вересня 2020 р., зареєстрованим у Міністерстві юстиції України 22 вересня 2020 р. за № 923/35206 [6] (далі – Порядок-2).

Проте в жодному із цих нормативно-правових актів не наведені визначення таких понять, як «знищення техніки», «захоплення техніки», не встановлені правила диференціації винагороди за ці суспільно корисні дії.

Вважаємо, що такий підхід не узгоджується із закріпленим у частині першій статті 8 Конституції України принципом верховенства права, який вимагає від органів державної влади його втілення у правотворчій та правозастосовній діяльності. Одним з елементів

цього конституційного принципу є принцип правової визначеності, неухильне дотримання якого вимагає чіткості, стабільності, зрозумілості й однозначності правових норм, а також забезпечення передбачуваності їх застосування.

З огляду на викладене метою цієї статті є оприлюднення результатів дослідження проблем нормативно-правового регулювання в Україні механізму призначення військовослужбовцям винагороди за знищення ворожої техніки.

Варто зазначити, що чітке визначення поняття «знищення» відсутнє не лише в постанові Кабінету Міністрів України № 18 від 20 січня 2016 р., Порядку-1 та Порядку-2, а й в інших нормативно-правових актах. Так, у Кримінальному кодексі України (ККУ) слово «знищення» використовується для формулювання ознак об'єктивної сторони складу кримінальних правопорушень. Ідеться, наприклад, про масове знищення людей (частина перша статті 113), погрозу знищення людей (частина друга статті 147), погрозу знищення, пошкодження або вилучення майна потерпілої особи чи її близьких родичів (частина третя статті 154), умисне знищення або пошкодження майна (частина друга статей 194, 347, 352, 378, частини друга та третя статті 399) тощо [7].

Кодексом України про адміністративні правопорушення (КУпАП) передбачена відповідальність за знищення знаків радіаційного забруднення або огорожі зазначеної зони (стаття 46-1), несанкціоноване знищення геопросторових даних та метаданих (стаття 51-4), порушення правил використання земель (стаття 53), знищення межових знаків, геодезичних пунктів і мереж (стаття 56) та інші протиправні діяння, вчинені в зазначений спосіб [8]. Однак і цей нормативно-правовий акт не містить визначення поняття «знищення».

Водночас «знищення майна» та «пошкодження майна» як суспільно корисні чи соціально допустимі дії розглядаються лише в контексті визначення змісту крайньої необхідності (стаття 39 ККУ) як однієї з обставин, що виключають кримінальну протиправність діяння. Так, частиною першою статті 39 ККУ встановлено, що не є кримінальним правопорушенням заподіяння шкоди правоохоронюваним інтересам у стані крайньої необхідності, тобто для усунення небезпеки, що безпосередньо загрожує особі чи охоронюваним законом правам цієї людини або інших осіб, а також суспільним інтересам чи інтересам держави, якщо цю небезпеку в даній обстановці не можна було усунути іншими засобами і якщо при цьому не було допущено перевищення меж крайньої необхідності [7]. У цьому випадку знищення майна являє собою соціально допустиму поведінку особи. Однак і у статті 39 ККУ відсутня відповідна дефініція.

Відповідно до частини другої статті 22 Цивільного кодексу України (ЦКУ) до збитків відносять втрати, яких особа зазнала у зв'язку зі знищенням або пошкодженням речі [9]. Зазначене означає, що знищення майна є обов'язковою умовою для констатації факту нанесення особі збитків та порушення в подальшому питання про відшкодування завданих збитків.

Цивільним законодавством України передбачене також відшкодування особі моральної шкоди, завданої внаслідок порушення її прав. До таких порушень пунктом 3 частини другої статті 23 ЦКУ віднесені душевні страждання, яких фізична особа зазнала у зв'язку зі знищенням чи пошкодженням її майна [9].

Тож, як і у випадку з констатацією факту нанесення особі збитків, підставою для порушення питання про відшкодування фізичній особі моральної шкоди необхідною і достатньою умовою є знищення її майна.

Вельми цікавими в контексті нашого дослідження видаються положення частини першої статті 185 ЦКУ, якими визначено, що споживною є річ, яка внаслідок одноразового її використання знищується або припиняє існувати в первісному вигляді [9].

За своїми природними властивостями будь-які речі є споживними. У процесі їх використання вони втрачають свої споживні якості повністю або частково. До споживних речей належить річ, яка внаслідок одноразового користування нею (тобто вилучення з неї корисних властивостей) знищується або припиняє своє існування в первісному вигляді. До таких відносяться продукти харчування, пальне.

Відповідно до частини другої статті 185 ЦКУ неспоживною є річ, призначена для одноразового використання, яка зберігає при цьому свій первісний вигляд протягом тривалого часу [9]. До неспоживних речей належать ті речі, які в разі їх використання за призначенням піддаються амортизації поступово, протягом тривалого часу, наприклад машини, будинки, споруди.

З огляду на викладене ворожа техніка належить до неспоживних речей, адже в процесі її використання вона піддається зносу, втрачає свої первинні характеристики та може бути пошкодженою або знищеною.

У пункті 96 Типової інструкції про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію, затвердженій постановою Кабінету Міністрів України № 736 від 19 жовтня 2016 р., визначено, що документи, справи, видання з грифом «Для службового користування», вилучені для знищення експертною комісією установи у складі не менше трьох членів, підлягають знищенню шляхом подрібнення носіїв інформації або в інший спосіб (спалювання, розплавлення, розчинення тощо), який виключає можливість їх прочитання та відновлення [10].

Як видно, в цій інструкції недостатньо чітко, але все-таки визначені способи знищення документів.

Однак, встановлюючи порядок знищення електронних носіїв інформації, Кабінет Міністрів України в цій самій інструкції фактично ототожнив знищення та перероблення таких носіїв, вказавши, що спосіб вчинення таких дій повинен виключати можливість повного або часткового відновлення збереженої на них інформації [10].

В Інструкції про порядок розшуку багажу, що не надійшов до аеропорту призначення, затвердженій наказом Міністерства транспорту України № 526 від 1 листопада 1999 р., зареєстрованій у Міністерстві юстиції України 19 листопада 1999 р. за № 799/4092, знищення визначене як фізичні чи хімічні зміни, через які багаж чи вантаж стає цілком знеціненим та не підлягає використанню [11].

Хоча зазначена інструкція втратила чинність 4 грудня 2005 р., використаний її розробниками підхід до формулювання дефініції знищення видається таким, що може бути взятим до уваги при визначенні поняття «знищення ворожої техніки». Це визначення містить вказівку на спосіб вчинення відповідних дій (фізичні чи хімічні зміни багажу), наслідки таких дій – приведення багажу у стан, що його знецінює та робить непридатним до використання, а також причинний зв'язок між діями та їхніми наслідками.

Слід констатувати, що ускладнює ситуацію й відсутність ґрунтовних наукових досліджень проблемних питань у цій царині, хоча на дисертаційному рівні поняття «знищення майна», «знищення інформації» та «пошкодження майна» досліджували Д. Азаров, В. Горбунов, С. Дрьомов, І. Газдайка-Василишин, М. Карчевський, С. Миронюк, Н. Розенфельд, А. Сакун, С. Телешев та інші.

Проте об'єктом їхніх наукових пошуків були кримінально-правові відносини, в яких знищення та пошкодження майна (в тому числі інформації) є суспільно небезпечними протиправними діяннями.

П. Матишевський і М. Мельник знищення майна визначають як доведення його до повної непридатності щодо його цільового призначення, внаслідок якого майно припиняє існувати або повністю втрачає свою цінність. Водночас пошкодженням майна визнають погіршення якості, зменшення цінності або доведення речі на якийсь час у непридатний щодо її цільового призначення стан [12, с. 361; 13, с. 451].

Як видно, запропоноване визначення знищення (у даному випадку майна) відповідає змісту об'єктивної сторони матеріального складу злочину, адже передбачає вчинення особою певного діяння, приведення майна до повної непридатності (наслідок цього діяння) та причинно-наслідковий зв'язок між діянням та наслідком.

Крім того, наведені зазначеними науковцями дефініції дають можливість чітко відмежовувати знищення від пошкодження. Ідеться про наявність чи відсутність можливості відновлення майна до початкового стану за умови відповідних витрат праці та матеріалів.

Децю подібне визначення поняття «знищення» за пропонували М. Бажанов, М. Панов, В. Стапис, В. Тацій. На їхню думку, знищення являє собою протиправний руйнівний вплив на майно, внаслідок якого воно повністю втрачає свою споживчу або економічну цінність. Натомість під пошкодженням вони пропонують розуміти протиправний вплив на предмет, унаслідок якого він частково, не в повному обсязі втрачає свої споживні властивості та економічну цінність, що істотно обмежує можливість його використання за цільовим призначенням [14, с. 150; 15, с. 522].

На думку А. Сакун, під «знищенням майна» слід розуміти протиправне заподіяння шкоди чужому майну, внаслідок чого таке майно стає повністю непридатним для використання за його цільовим призначенням. Натомість при пошкодженні відбувається погіршення якості майна, зменшення цінності або приведення його на якийсь час до непридатності [16, с. 6].

Р. Бондарчук вважає, що внаслідок знищення майно припиняє існувати фізично (наприклад у результаті вибуху газу в балоні) або продовжує своє існування зі зміненою формою, будовою, структурою чи формулою (наприклад отруєне вино в бочках), що зумовлює подальшу неможливість відновлення (ремонт, реставрації тощо) його властивостей та якості. Водночас цінність, мінова та споживча вартість майна, його здатність задовольняти матеріальні та пов'язані з ними потреби людини, шляхом використання цього майна за його цільовим призначенням втрачається повністю й назавжди. Майно втрачає здатність до відокремлення від природного середовища (вилите у водойму пальне) чи відновлення (ремонт) заново шляхом вкладення праці людини, її коштів та матеріалів, власник же чи інший законний володільець позбавляється як права власності на майно, так і можливості володіти, користуватися чи розпоряджатися майном, тому воно випадає з економічного обігу як таке [17, с. 60].

Наведені вище дефініції видаються цілком придатними для формулювання диспозицій статті 194 ККУ. Вважаємо, що запропоновані їхніми авторами підходи до визначення змісту поняття «знищення» можуть бути використанні під час формулювання визначення «знищення ворожої техніки» та відмежування від суміжних видів правомірної поведінки.

Слід зазначити, що в юридичній літературі зверталася увага на те, що в разі буквального тлумачення диспозиції статті 194 ККУ в її чинній редакції під ознаки об'єктивної сторони складу злочину формально потрапляли й випадки правомірного (законного) зни-

щення чужого майна. З огляду на це вносилися пропозиції щодо доповнення частини першої статті 194 ККУ словом «протиправне» після слова «умисне».

Ураховуючи одержані результати дослідження проблем нормативно-правового регулювання механізму призначення військовослужбовцям винагороди за знищення та захоплення ворожої техніки, вважаємо зазначені пропозиції вельми слушними. До того ж, як видається, за такою логікою сформульовані положення статті 25 (Необережність та її види) ККУ. Виокремлюючи види необережності як однієї з форм вини, законодавець указав на кримінальну протиправність самовпевненості та недбалості [7]. Адже самовпевненість і недбалість можуть бути й не суспільно небезпечними, не протиправними та не кримінально караними.

Аналіз матеріалів судової практики вказує на те, що суди також приділяють увагу тлумаченню понять, які не визначені на законодавчому рівні. Так, у постанові Пленуму Верховного Суду України «Про судову практику в справах про знищення та пошкодження державного чи колективного майна шляхом підпалу або внаслідок порушення встановлених законодавством вимог пожежної безпеки» № 4 від 2 липня 1976 р. наведене судове тлумачення поняття «знищення державного або колективного майна». Під таким пропонується розуміти приведення майна в повну непридатність до використання за цільовим призначенням. Унаслідок знищення майно перестає існувати або повністю втрачає свою цінність [19].

Як видно, Верховний Суд України цілком слушно звертає увагу на те, що в разі знищення майно:

- припиняє своє існування, або
- повністю втрачає свою цінність.

Однак у запропонованій Верховним Судом України дефініції має місце ототожнення суспільно небезпечного діяння з його результатом, що видається не зовсім коректним.

Не менш цікавим видається огляд судової практики з розгляду спорів щодо виборів та виборчих правопорушень в Україні (далі – Огляд) [20]. Ідеться передусім про практику застосування положень статті 158-2 КК України (Незаконне знищення або пошкодження виборчої документації або документації референдуму).

Автори Огляду Б. Мохончук, П. Романюк, М. Цуркан звертають увагу на те, що в одних випадках (кримінальні справи № 225/3387/19, № 225/5656/19) суди кваліфікували діяння винуватців як пошкодження виборчих бюлетенів – відрив контрольних талонів у день голосування. Натомість у справах № 344/19623/19 та № 753/14883/19 за цією статтею були кваліфіковані дії виборців, які у стані алкогольного сп'яніння розірвали виборчі бюлетені.

Необхідно зазначити, що в усіх цих випадках громадян визнано винуватими у вчиненні кримінального

правопорушення, передбаченого частиною першою статті 158-2 ККУ, якою встановлена відповідальність за незаконне знищення або пошкодження виборчої документації в державних архівних установах або в Центральній виборчій комісії України та після проведення виборів. Тож для кваліфікації суспільно небезпечного діяння за цією кримінально-правовою нормою не має значення спосіб, у який воно вчинене.

Під знищенням документації автори Огляду пропонують розуміти активні дії, що передбачають повну ліквідацію виборчих документів будь-якими способами, приведення документів у непридатний стан, коли вони втрачають свої властивості і не можуть бути носіями зафіксованої в них інформації [20].

Звертаємо увагу також і на інші недоліки, присутні в нормативно-правових актах, якими врегульоване питання мотивування військовослужбовців до знищення (захоплення) ворожої техніки і які не узгоджені між собою, що ще більше ускладнює їх застосування. Ідеться передусім про відсутність уніфікації термінології, яка використовується у відповідних документах. Так, Порядком-1 регулюються питання додаткової винагороди за «**знищення ворожої техніки**» (виділено нами – В.Т., В.О., С.Д.), у Порядку-2 – за «**знищення (захоплення) техніки**» (виділено нами – В.Т., В.О., С.Д.). Водночас у Методичних рекомендаціях щодо заходів з організації документального підтвердження органами військового управління фактів знищення (захоплення) військовослужбовцями Збройних Сил України техніки противника, затверджених заступником начальника Генерального штабу Збройних Сил України 4 травня 2023 р. (далі – Методичні рекомендації), використовується термін «**знищення (захоплення) техніки противника**» (виділено нами – В.Т., В.О., С.Д.).

Таким чином, у зазначених нормативно-правових актах і Методичних рекомендаціях для визначення одного й того самого предмета правовідносин одночасно використовується різний термінологічний інструментарій.

Привертає увагу й те, що процедура підтвердження знищення (захоплення) ворожої техніки належним чином не унормована ані в постанові Кабінету Міністрів України № 18 від 20 січня 2016 р., ані в Порядку-1, ані в Порядку-2. Натомість така процедура передбачена в Методичних рекомендаціях.

Убачається, що обраний шлях вирішення зазначеної проблеми, на наш погляд, є хибним з таких міркувань.

Відповідно до частини другої статті 19 Конституції України органи державної влади та органи місцевого самоврядування, їхні посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України [1].

Як видно, вказаний конституційний припис вимагає від військових посадових осіб керуватися у своїй діяльності виключно Конституцією та законами України і не містить жодних указівок на підзаконні нормативно-правові акти і методичні рекомендації.

За відсутності законодавчого регулювання питань щодо збільшення винагороди військовослужбовцям Збройних Сил України у зв'язку з підтвердженням фактів знищення (захоплення) ними ворожої техніки учасники цих правовідносин змушені керуватися положеннями постанов Кабінету Міністрів України № 18 від 20 січня 2016 р., № 585 від 21 травня 2024 р. та наказом Міністерства оборони України № 340 від 18 вересня 2020 р., зареєстрованим у Міністерстві юстиції України 22 вересня 2020 р. за № 923/35206.

Звертаємо увагу на те, що зазначеними підзаконними актами не визначено чіткої процедури документального підтвердження органами військового управління фактів знищення (захоплення) військовослужбовцями Збройних Сил України ворожої техніки.

Так, Порядком-2 визначено, що підтвердженням знищення ворожої техніки є [6]:

- 1) журнал бойових дій (журнал ведення оперативної обстановки);
- 2) рапорт (донесення) командира підрозділу, групи (військової частини) за підпорядкованістю, котрий виконував (виконувала) завдання, в якому детально зазначаються обставини, місце (координати), дата, час, спосіб знищення, тип знищеної техніки;
- 3) донесення (повідомлення, рапорт) командирів суміжних (розвідувальних) підрозділів, які за результатами візуального спостереження підтверджують знищення техніки;
- 4) дані відеофіксації, технічних засобів розвідки (спостереження), відеозапис відображення повітряної обстановки бойових машин протиповітряної оборони під час бойової роботи.

Рішення про підтвердження факту знищення ворожої техніки приймається за наявності не менше трьох з наведених підстав. При цьому всі чотири підстави мають однакову юридичну силу.

Дослідження емпіричного матеріалу дає підстави для висновку, що на практиці перших трьох підстав достатньо для констатації (підтвердження) лише власне факту знищення ворожої техніки. Однак відсутність даних відеофіксації, технічних засобів розвідки (спостереження), відеозапису відображення повітряної обстановки бойових машин протиповітряної оборони під час бойової роботи не дає змоги встановити, хто саме знищив ворожу техніку та може розраховувати на одержання додаткової грошової винагороди.

Слід зазначити, що ця проблема частково розв'язана пунктом 8 Порядку-1, яким передбачені такі самі підстави для підтвердження знищення ворожої

техніки, як і Порядком-2. Однак у пункті 9 Порядку-1 записано, що рішення про визнання ворожої техніки такою, що знищена, приймається на підставі обов'язкового підтвердження зазначеним у підпункті 4 пункту 8 цього Порядку способом (дані відеофіксації, технічних засобів розвідки (спостереження), відеозапис відображення повітряної обстановки бойових машин протиповітряної оборони під час бойової роботи) та додатково одним зі способів, зазначених у підпунктах 1–3 пункту 8 цього Порядку, з яких можливо зробити висновок про її знищення, і оформляється розпорядчим документом (наказом) керівника органу військового управління (начальника підрозділу, органу, закладу чи установи СБУ), у складі якого підрозділ виконує завдання згідно з бойовим наказом (розпорядженням) [5].

Таким чином, для надання військовослужбовцям додаткової відпустки за знищену ворожу техніку достатньо двох підстав із чотирьох, передбачених пунктом 8 зазначеного Порядку.

Можна погодитися з тим, що відеофіксація має вирішальне значення для підтвердження факту знищення ворожої техніки. Однак на практиці надані військовими частинами відеоматеріали підтверджують лише факт влучання у відповідний зразок техніки противника, що не дає підстав вважати його знищеним.

Крім того, положення нормативно-правових актів, якими врегульований порядок підтвердження фактів знищення (захоплення) ворожої техніки, а також визначення розміру винагороди за це, мають дискримінаційну складову, оскільки не кожен військовослужбовець, який знищує ворожу техніку, має у своєму розпорядженні засоби відеофіксації, а також можливість застосовувати її належним чином.

Звертаємо увагу на те, що факт знищення ворожої техніки є єдиною підставою для стимулювання (посилення мотивації) військовослужбовців. Ідеться як про виплату додаткової грошової винагороди, так і про надання додаткової відпустки. Однак власне підтвердження факту знищення унормоване різними підзаконними актами.

Убачається, що процедура підтвердження факту знищення ворожої техніки повинна бути уніфікованою. Вважаємо, що, приймаючи рішення про визнання ворожої техніки такою, що знищена, слід керуватися пунктом 9 Порядку-1, оскільки цей Порядок затверджений нормативно-правовим актом, який має вищу юридичну силу.

Таким чином, підставою для прийняття рішення про підтвердження факту знищення ворожої техніки є сукупність:

- даних відеофіксації, технічних засобів розвідки (спостереження), відеозапис відображення повітряної обстановки бойових машин протиповітряної оборони під час бойової роботи);

- одного зі способів, зазначених у підпунктах 1–3 пункту 8 Порядку-1, з яких можливо зробити висновок про її знищення.

Крім того, звертаємо увагу на те, що пунктом 6 Порядку-1 передбачений перелік ворожої техніки, за знищення якої військовослужбовцям надається додаткова відпустка, котрий відрізняється від наведеного в Додатку 3 до Порядку-2. Так, наприклад, відповідно до Порядку-1 додаткова відпустка надається військовослужбовцеві за знищення **військового літака** (виділено нами – В.Т., В.О., С.Д.), а в Додатку 3 до Порядку-2 – за знищення **бойового літака (винищувальної та штурмової авіації)** (виділено нами – В.Т., В.О., С.Д.).

Як видається, поняття «військовий літак» та «бойовий літак» співвідносяться, як частина до цілого. Тобто не кожен військовий літак є бойовим та належить до винищувальної чи штурмової авіації.

З огляду на викладене під час прийняття рішення щодо наявності підстав (доказів) вважати ворожу техніку такою, що знищена, слід керуватися вимогами Порядку-1. Натомість обраний вид заохочення (додаткова грошова винагорода або додаткова відпустка) за знищену техніку визначає, яким з названих двох положень слід керуватися, визначаючи предмет цих правовідносин.

Привертає увагу й те, що Порядком-1 визначені механізми і тривалість надання військовослужбовцям Збройних Сил України, інших утворених відповідно до законів України військових формувань та правоохоронних органів спеціального призначення, державних органів спеціального призначення з правоохоронними функціями, Служби зовнішньої розвідки, розвідувального органу Міноборони додаткової відпустки за знищену ворожу техніку [5].

Зазначена відпустка надається військовослужбовцям, які беруть безпосередню участь у заходах із забезпечення національної безпеки та оборони під час дії особливого періоду, заходах з відсічі і стримування збройної агресії Російської Федерації.

Таким чином, окрім грошової винагороди за знищену ворожу техніку військовослужбовцям може надаватися додаткова відпустка.

Однак видається незрозумілим, чому у випадку виплати грошової винагороди диференціація відсутня. Тобто в нормативно-правових актах, якими врегульоване зазначене питання, за знищення і захоплення ворожої техніки встановлене однакове грошове заохочення. Водночас додаткова відпустка надається лише за **знищення** (виділено нами – В.Т., В.О., С.Д.) ворожої техніки. Невже в такий спосіб Кабінет Міністрів України вирішив виправити помилку та застосувати диференційований підхід до порядку заохочення військовослужбовців? Таким чином, уведення в дію

Порядку надання військовослужбовцям додаткової відпустки за знищену ворожу техніку, на наш погляд, не вирішило всі проблемні питання, створивши натомість нові.

Привертає увагу й те, відповідно до Методичних рекомендацій за результатом розгляду поданих документів керівником угруповання військ (сил) приймається одне з рішень, яким:

- підтверджується факт знищення військовослужбовцями військової частини (окремого підрозділу) техніки шляхом видання відповідного розпорядчого документа (наказу);
- документи повертаються військовій частині (окремому підрозділу) для доопрацювання;
- відмовляється в підтвердженні факту знищення військовослужбовцями військової частини (окремого підрозділу) техніки шляхом направлення відповідного листа із зазначенням причини відмови.

При цьому підставами для відмови в підтвердженні факту знищення (захоплення) військовослужбовцями ворожої техніки визначено:

- неможливість зробити висновок про наявність факту знищення (захоплення) ворожої техніки особовим складом військової частини, що подала відповідні документи;
- наявність підтвердженої інформації лише про пошкодження ворожої техніки;
- наявність інформації про знищення (захоплення) ворожої техніки іншою військовою частиною (окремим підрозділом);
- перебування військової частини (окремого підрозділу) на дату знищення техніки в оперативному підпорядкуванні іншого органу військового управління.

Водночас у Методичних рекомендаціях відсутні підстави повернення документів військовій частині (окремому підрозділу) для доопрацювання.

Звертаємо увагу на те, що в Методичних рекомендаціях доволі ретельно прописаний порядок прийняття органами військового управління рішень щодо підтвердження фактів знищення (захоплення) ворожої техніки. Однак у цих рекомендаціях присутні положення, якими з невідомих міркувань розширюються повноваження військових посадових осіб. Відповідно до цих положень можуть утворюватися не передбачені жодним нормативно-правовим актом робочі групи з підтвердження фактів знищення (захоплення) ворожої техніки. Хоча варто визнати доцільність створення таких груп.

Слід зазначити, що Методичні рекомендації щодо заходів з організації документального підтвердження органами військового управління фактів знищення (захоплення) військовослужбовцями Збройних Сил України техніки противника не мають жодної юридичної сили, а мають рекомендаційний характер. Тому посилення на цей документ при прийнятті рішення

про підтвердження (не підтвердження) фактів знищення (захоплення) ворожої техніки є юридично неспроможними.

Убачається за необхідне також звернути увагу на відсутність диференціації розміру грошової винагороди залежно від того, знищена ворожа техніка чи захоплена. Адаже в разі знищення певного зразка ворожої техніки противник втрачає лише можливість його застосовувати в подальшому, але може використати рештки як металобрухт. Натомість захоплення нашими військовослужбовцями ворожого танка, літака, гелікоптера тощо завдає подвійної шкоди противнику, адже ця техніка обліковується в установленому порядку в підрозділах Збройних Сил України та надалі застосовується в боротьбі з агресором.

Звертаємо увагу також на те, що чинні станом на сьогодні нормативно-правові акти є застарілими, оскільки не враховують того, що на озброєння збройних сил Російської Федерації надходять нові види зброї, вказівка на які відсутня в Додатку 3 до Порядку-2 (пункт 1 глави 4 розділу III). З огляду на це орган військового управління змушений відмовляти у виплаті військовослужбовцям винагороди за знищення нових зразків ворожої техніки, вказівка на які відсутня в зазначеному Додатку.

Слід також зазначити, що в правозастосовній практиці доволі часто трапляються випадки, коли для підтвердження знищення ворожої техніки подаються матеріали, які можуть свідчити не про її знищення, а лише про її ураження (пошкодження).

Також не поодинокими є факти, коли подані до органу військового управління матеріали вказують на спроби видати за знищення ворожої техніки ураження раніше знищених зразків озброєння противника. З огляду на це варто констатувати існування нагальної потреби у створенні автоматизованої системи обліку знищеної та захопленої ворожої техніки, що дасть змогу уникати випадків подвійної виплати винагороди за один і той самий зразок знищеної ворожої техніки. Усе це вказує на потребу належного нормативно-правового закріплення питання автоматизованого збирання, впорядкування, оброблення та зберігання інформації про знищену та захоплену ворожу техніку.

Зауважимо, що перелічені нами та інші проблеми пропонується частково розв'язати проектом Закону України «Про внесення змін до деяких законодавчих актів України щодо мотивації військової служби» (реєстр. № 11012 від 13 лютого 2024 р.), внесеним народними депутатами України (далі – законопроект) [21].

Законопроект пропонується викласти статтю 9-2 Закону України «Про соціальний і правовий захист військовослужбовців та членів їх сімей», якою встановлюється на законодавчому рівні виплата одноразової винагороди за знищення чи захоплення ворожої

техніки, в новій редакції. При цьому визначення поняття «знищення техніки» традиційно не наводиться.

Частину другою цієї статті пропонується встановити розмір одноразової винагороди військовослужбовцям за кожну одиницю знищеної чи захопленої ворожої техніки. Танк оцінюватиметься в 200 000–370 000 гривень; самохідна артилерійська установка або реактивна система залпового вогню – 200 000–370 000 гривень; бойова машина десанту, бронетранспортер, командно-штабна машина, бойова машин піхоти, артилерійська система – 30 000–100 000 гривень тощо.

Впадає в око те, що в законопроекті відсутні будь-які вказівки на порядок здійснення конкретних розрахунків.

Невирішеним залишається питання, за яким критерієм визначатиметься винагорода, наприклад, за знищений танк? Адже різниця між нижньою та верхньою межею розміру винагороди за його знищення є відчутною. Чи братиметься до уваги модель танка, чи враховуватиметься, що саме вчинено: знищення танка чи його захоплення?

Варто погодитися з Головним науково-експертним управлінням (ГНЕУ) Апарату Верховної Ради України, яке звернуло увагу на відсутність логіки встановлення передбачених у запропонованій редакції частини другої статті 9-2 сум, оскільки необхідно у зв'язку із цим зважати на різні наслідки заподіяння шкоди як крилатою ракетою (балістичною), так і безпілотним літальним апаратом ударного типу. До того ж діапазон встановлення сум виплати за знищення ворожої техніки противника вбачається таким, що встановлений довільно. Це вказує на існування в такій редакції норми помітних навіть неозброєним оком корупційних ризиків [22].

ГНЕУ також слушно звернуло увагу на те, що згідно із частиною четвертою статті 9-2 Закону України «Про соціальний і правовий захист військовослужбовців та членів їх сімей» (у редакції законопроекту) винагорода за знищення чи захоплення військової техніки противника розподілятиметься між військовослужбовцями, які брали безпосередню участь у виявленні, знищенні або захопленні техніки противника. Проте порядок такого розподілу в законопроекті не визначається, що свідчить про відсутність завершеного механізму реалізації відповідного припису [22].

Таким чином, ретельний аналіз тексту цього законопроекту дає підстави стверджувати, що його ухвалення не усуне існуючі проблеми, а ще більше їх поглибить.

Ураховуючи все викладене, вбачаємо за доцільне зробити такі узагальнюючі висновки.

Додаткова винагорода за знищену (захоплену) ворожу військову техніку може стати одним з важливих елементів механізму мотивування (фінансового стимулювання) наших оборонців. Таке мотивування потребує належного нормативно-правового регулювання.

Ідеться передусім про необхідність закріплення на законодавчому рівні та подальшої уніфікації відповідної нормативно-правової термінології, що повинно забезпечити точність формулювання і в подальшому вживання дефініцій та загалом підвищити ефективність реалізації правових норм, якими регулюються зазначені правовідносини.

Убачається за доцільне провести систематизацію та ретельний аналіз нормативно-правових актів, якими регулюються питання встановлення та виплати додаткової винагороди за знищену (захоплену) ворожу техніку.

Для досягнення цієї мети вбачається за доцільне підготувати і подати в установленому порядку пропозиції з відповідними правками до тексту проекту Закону України «Про внесення змін до деяких законодавчих актів України щодо мотивації військової служби» (реєстр. № 11012 від 13 лютого 2024 р.), внесеного народними депутатами України, передбачивши:

- закріплення на законодавчому рівні базових принципів формування та реалізації державної політики у сфері поліпшення мотивування до військової служби, зокрема шляхом нормативно-правового закріплення виплати військовослужбовцям додаткового грошового заохочення за знищену (захоплену) ворожу техніку;
- визначення таких дефініцій, як «знищення ворожої техніки», «захоплення ворожої техніки» тощо;
- закріплення на нормативно-правовому рівні процедури документального підтвердження органами військового управління фактів знищення (захоплення) військовослужбовцями Збройних Сил України ворожої техніки було б доцільно передбачити у відповідному наказі Міністерства оборони України (має статус нормативно-правового акта), а також передбачити порядок утворення і визначити повноваження робочої групи та підстави повернення для доопрацювання матеріалів, які надійшли з військових частин для підтвердження знищення (захоплення) ворожої техніки;
- створення автоматизованої системи обліку знищеної та захопленої ворожої техніки, що дасть змогу уникнути випадків подвійної виплати винагороди за один і той самий зразок знищеної ворожої техніки.

Після прийняття зазначеного законопроекту необхідно привести у відповідність до його норм положення нижчих за юридичною силою нормативно-правових актів.

Також вважаємо за необхідне створити механізм своєчасного оновлення Додатку 3 до Порядку виплати винагороди військовослужбовцям Збройних Сил України та Державної спеціальної служби транспорту за безпосередню участь у воєнних конфліктах, у заходах із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації чи в антитерористичній операції, інших заходах в умовах особливого періоду (пункт 1 глави 4 розділу III).

Перелік літератури

1. Конституція України [Електронний ресурс] : прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>.
2. Про Збройні Сили України [Електронний ресурс] : Закон України № 1934-ХІІ від 6 грудня 1991 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/1934-12#Text>.
3. Рішення Конституційного Суду України у справі за конституційним поданням 45 народних депутатів України щодо відповідності Конституції України (конституційності) положень частин третьої, четвертої статті 59 Закону України «Про Державний бюджет України на 2003 рік» (справа про соціальний захист військовослужбовців та працівників правоохоронних органів) [Електронний ресурс] : № 7-рп/2004 від 17 березня 2004 р.: справа № 1-13/2004 // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/v007p710-04#Text>.
4. Деякі питання грошового забезпечення військовослужбовців, осіб рядового і начальницького складу та поліцейських [Електронний ресурс] : постанова Кабінету Міністрів України № 18 від 20 січня 2016 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/18-2016-п#Text>.
5. Порядок надання військовослужбовцям додаткової відпустки за знищену ворожу техніку [Електронний ресурс] : затверджений постановою Кабінету Міністрів України № 585 від 21 травня 2024 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/585-2024-п#Text>.
6. Порядок виплати винагороди військовослужбовцям Збройних Сил України та Державної спеціальної служби транспорту за безпосередню участь у воєнних конфліктах, в заходах із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації чи в антитерористичній операції, інших заходах в умовах особливого періоду [Електронний ресурс] : затверджений наказом Міністерства оборони України № 340 від 18 вересня 2020 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/z0923-20#n23>.
7. Кримінальний кодекс України [Електронний ресурс] : № 2341-ІІІ, прийнятий 5 квітня 2001 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2341-14#Text>.
8. Кодекс України про адміністративні правопорушення (статті 1-212-24) [Електронний ресурс] : № 8073-Х, прийнятий 7 грудня 1984 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/80731-10#Text>.
9. Цивільний кодекс України [Електронний ресурс] : № 435-ІV, прийнятий 16 січня 2003 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/435-15#Text>.
10. Типова інструкція про порядок ведення обліку, зберігання, використання і знищення документів та інших матеріальних носіїв інформації, що містять службову інформацію [Електронний ресурс] : затверджена постановою Кабінету Міністрів України № 736 від 19 жовтня 2016 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/736-2016-п#Text>.
11. Інструкція про порядок розшуку багажу, що не надійшов до аеропорту призначення [Електронний ресурс] : затверджена наказом Міністерства транспорту України № 526 від 1 листопада 1999 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/z0799-99#Text>.
12. Науково-практичний коментар до Кримінального кодексу України / Ю. В. Александров [та ін.] ; відп. ред. С. С. Яценко. – 4-те вид., перероб. та доп. – К. : А.С.К., 2005. – 848 с.
13. Науково-практичний коментар Кримінального кодексу України / А. М. Бойко [та ін.] ; ред. М. І. Мельник, М. І. Хавронюк. – 3-те вид., перероб. та доп. – К. : Атіка, 2003. – 1054 с.
14. Кримінальне право України. Особлива частина : підручник / за ред. М. І. Бажанова, В. В. Сташиса, В. Я. Тація. – К. : Юрінком Інтер, 2003. – 512 с.
15. Кримінальний кодекс України : науково-практичний коментар / Ю. В. Баулін [та ін.] ; заг. ред.: В. В. Сташис, В. Я. Тація ; Акад. прав. наук України, Нац. юрид. акад. України ім. Ярослава Мудрого. – К. : Ін Юре, 2003. – 1193 с.
16. Сакун А. В. Кримінально-правова характеристика умисного знищення або пошкодження майна : автореф. дис. ... канд. юрид. наук : спец. 12.00.08 / Сакун Анна Вікторівна ; Нац. акад. внутр. справ. – К., 2010. – 19 с.
17. Боднарчук Р. О. Поняття, критерії та ознаки знищення чужого майна (статті 194 та 196 КК України) / Р. О. Боднарчук // Форум права. – 2011. – № 3. – С. 53–61.
18. Хавронюк М. І. Довідник з Особливої частини Кримінального кодексу України / М. І. Хавронюк. – К. : Істина, 2004. – 504 с.
19. Про судову практику в справах про знищення та пошкодження державного чи колективного майна шляхом підпалу або внаслідок порушення встановлених законодавством вимог пожежної безпеки [Електронний ресурс] : постанова Пленуму Верховного Суду України № 4 від 2 липня 1976 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/v0004700-76#Text>.
20. Мохончук Б. Огляд судової практики з розгляду спорів щодо виборів та виборчих правопорушень в Україні: за результатами президентських та парламентських виборів 2019 року [Електронний ресурс] / Б. Мохончук, П. Романюк, М. Цуркан ; за ред. М. Цуркана. – К. : АК-Group, 2020. – 147 с. – (Вибори 2019: судові врегулювання виборчих зборів). – Режим доступу : <https://nsj.gov.ua/files/1590748254IFES-Ukraine-Overview-of-court-practices-on-election-dispute-resolution-v1-Ukr.pdf>.
21. Проект Закону про внесення змін до деяких законодавчих актів України щодо мотивації військової служби [Електронний ресурс] : № 11012 від 13 лютого 2024 // Верховна Рада України. Законопроекти. – Режим доступу : <https://itd.rada.gov.ua/billInfo/Bills/pubFile/2209682>.
22. Висновок на проект Закону України «Про внесення змін до деяких законодавчих актів України щодо мотивації військової служби» [Електронний ресурс] // Верховна Рада України. Законопроекти. – Режим доступу : <https://itd.rada.gov.ua/billInfo/Bills/pubFile/2245114>.

DOI 10.33099/2618-1614-2025-28-1-27-35

УДК 623.4

І. Б. Чепков,*доктор технічних наук, професор,
Центральний науково-дослідний інститут озброєння
та військової техніки Збройних Сил України,***В. М. Можаровський,***доктор військових наук, професор,
Центральний науково-дослідний інститут озброєння
та військової техніки Збройних Сил України,***П. І. Нор,***кандидат технічних наук, старший науковий
спієрботник, Центральний науково-дослідний
інститут озброєння та військової техніки
Збройних Сил України*

Сучасні загальні тенденції розвитку засобів збройної боротьби

Проведений аналіз і систематизація перспективних на сьогодні світових тенденцій розвитку засобів збройної боротьби з метою виявлення тенденцій їхнього розвитку, загальних для всіх видів і родів військ. Проаналізований розвиток озброєння і військової техніки більшості передових країн світу та досвід їхнього застосування під час війн і військових конфліктів останніх десятиліть, у тому числі в російсько-українській війні.

Ключові слова: збройні конфлікти, засоби збройної боротьби, озброєння і військова техніка, тенденції розвитку, бойові засоби, ударні засоби.

Аналіз характеру збройної боротьби під час військових конфліктів останніх десятиліть, власного понад десятилітнього досвіду російсько-українського протистояння і широкомасштабної агресії РФ проти України свідчить про різке підвищення впливу засобів збройної боротьби на перебіг і результати воєнних дій. Можна з упевненістю стверджувати, що зразки озброєння та військової техніки (ОВТ), які перебувають на озброєнні збройних сил та інших структур держав світу, становлять основу їхньої бойової могутності та є вирішальним фактором досягнення успіху в можливій війні чи будь-якому збройному конфлікті [1–3].

Номенклатура сучасних засобів збройної боротьби дуже широка й залежить насамперед від виду збройних сил та роду військ конкретних держав. Усі вони мають свої закономірності (тенденції) розвитку, тому виявлення загальних тенденцій розвитку ОВТ даного роду військ чи виду збройних сил уже має свою наукову і практичну цінність. Виявлення загальних тенденцій розвитку практично всієї номенклатури ОВТ усіх видів і родів військ на загальносвітовому рівні – це ще більш складна і методологічно важлива задача. На це і спрямована дана стаття.

Ця тематика раніше вже досліджувалась у Центральному науково-дослідному інституті озброєння та військової техніки (ЦНДІ ОВТ) Збройних Сил (ЗС) України під час виконання низки науково-дослідних робіт, результатами яких стали наукові публікації [2–5]. Зокрема, в них був проведений аналіз актуальних на той час (орієнтовно кінець першого десятиліття XXI ст.), загальних для всіх видів і родів військ тенденцій розвитку ОВТ і тенденцій розвитку форм та способів ведення збройної боротьби, і встановлені їхні взаємозв'язки.

За півтора десятки років, що минули відтоді, під впливом науково-технічного прогресу, як правило, еволюційним шляхом змінюються як способи застосування збройних сил, так і їхній інструментарій, тобто засоби їхньої реалізації. З початком російсько-українського збройного протистояння, а тим більше широкомасштабної російської агресії проти України актуальність порушених питань лише зростає. Перша спроба оновити, тобто осучаснити, матеріал щодо тенденцій розвитку способів ведення збройної боротьби була зроблена наприкінці 2021 р. – на початку 2022 р., результати якої опубліковані в [6, 7].

Мета статті – осучаснити знання про основні загальні тенденції розвитку засобів збройної боротьби (ЗЗБ), тобто зразків озброєння, військової та спеціальної техніки, з урахуванням розвитку на загальносвітовому рівні технологій і досвіду перебігу військових конфліктів і війн за останні десятиліття.

Виклад основного матеріалу

Слід зазначити, що, на відміну від згаданих попередніх наукових публікацій [2–4], у даній роботі дещо змінено підхід до систематизації тенденцій розвитку ЗЗБ, тобто самих зразків, комплексів, систем озброєння військової та спеціальної техніки. Уперше вони розділені на традиційні, або класичні, тенденції розвитку ЗЗБ (зразків ОВТ) і новітні, тобто перспективні, тенденції розвитку ЗЗБ. Крім того, варто виокремити і третю групу тенденцій розвитку ОВТ, котрі були характерні й актуальні як у нещодавньому минулому, так і на цей час.

Крім того, всю номенклатуру традиційних тенденцій розвитку ОВТ розділено на дві великі підгрупи. Перша – бойові засоби (БЗ), а саме зразки, комплекси, системи ОВТ без боєприпасів та інших засобів ураження, а також інші зразки військової техніки, призначені для виконання бойових завдань. Друга складова – це ударні засоби (УЗ), тобто всі види боєприпасів та інших засобів ураження. Такий підхід дає змогу коректніше систематизувати загальні тенденції розвитку ОВТ.

Такий розподіл дає можливість диференціювати підвищення ефективності засобів збройної боротьби за двома визначеними вище напрямками. Перший – тактико-технічні характеристики (ТТХ) зразків ОВТ (БЗ) як платформ для розміщення екіпажу та іншого цільового навантаження, ступеня їхньої захищеності, здатності виявляти загрози та високий рівень ситуаційної обізнаності. Другий – ТТХ безпосередньо УЗ, тобто традиційно боєприпасів (у загальному випадку – ударних засобів). Ці два шляхи як тенденції розвитку можуть розвиватися незалежно один від одного.

Перша тенденція – підвищення ефективності бойових засобів: покращення ТТХ (підвищення дальності дії, динамічності, захищеності, маси корисного навантаження тощо), розширення номенклатури та кількості УЗ (боєкомплекту).

Тенденція належить до традиційних напрямів розвитку ОВТ і проявляється в усіх бойових засобах (зразках, комплексах, системах ОВТ) усіх видів збройних сил та сфер їхнього застосування. Зрозуміло, що підвищення ефективності ОВТ відбувалося практично завжди, але слід відзначити різке підвищення її ролі впродовж останніх десятиліть за рахунок реалізації ефекту синергії, тобто сумісному впливу багатьох тенденцій розвитку ОВТ. Тенденції розвитку ЗЗБ у разі реалізації в окремих зразках ОВТ проявляються, як правило, не окремо, а спільно і підсилюють дію одна одної, що суттєво підвищує загальну ефективність і надає можливість виокремити цю тенденцію як досить вагомую.

Найвиразніше ця тенденція проявляється в розвитку бойових засобів повітряно-космічного базування.

Прикладів можна привести досить багато. Це створення і реальне використання в провідних країнах світу новітніх багаторазових безпілотних повітряно-космічних систем (американський безпілотний Boeing X-37B і його китайський аналог «Шеньлунь»), створення та прийняття на озброєння в останні роки нових багатоцільових бойових літаків п'ятого покоління (три версії американського F-35, китайський J-20, російський Су-57), розвиток у провідних країнах світу наукового доробку для створення бойових літаків шостого покоління, розроблення новітніх високошвидкісних бойових і транспортних вертольотів та конвертопланів (американські експериментальні апарати SB-1 Defiant, S-97 Raider, BELL V-280, V-247) тощо.

Досить масово ця тенденція проявляється також у розвитку зразків ОВТ наземного і морського базування. У сухопутному варіанті це створення багатоцільових платформ бронетанкової та автомобільної техніки, побудованих з використанням модульного принципу, створення новітніх зразків ракетно-артилерійського озброєння. ЗЗБ морського і берегового базування, зокрема кораблі, катери, інші судна забезпечення, а також ракетні протикорабельні комплекси активно реалізуються в рамках даної тенденції розвитку як у плані створення нових зразків, так і модернізації існуючих.

Відмічені ЗЗБ усіх видів збройних сил та сфер їхнього застосування реалізуються за тісної взаємодії з іншими тенденціями розвитку ОВТ, згаданими далі в цій публікації як окремі тенденції. При цьому слід зазначити, що дана тенденція як узагальнююча найтісніше пов'язана з тенденціями створення нових малогабаритних та відносно фінансово низьковитратних зразків ОВТ, тенденціями інтелектуалізації ЗЗБ, тобто передачею багатьох функцій використання ОВТ автоматичі під керівництвом штучного інтелекту, а також тенденцій підвищення скритності і захищеності ОВТ та особового складу.

Друга тенденція з групи класичних, тобто традиційних, тенденцій розвитку – підвищення ефективності ударних засобів: бойової могутності, точності ураження цілі з масовим переходом на високоточні ударні засоби, суттєве зростання швидкості польоту (перехід на гіперзвук) і дальності ураження цілей.

При цьому слід відмітити, що темпи реалізації даної тенденції, на відміну від першої, суттєво вищі за рахунок технічних та економічних факторів. Нові ударні засоби, як правило, сумісні із ЗЗБ (носіями) попередніх поколінь, що дає останнім змогу за рахунок модернізації та розширення боєкомплекту суттєво підвищити свою бойову ефективність.

Як відмічено в попередніх напрацюваннях з даної тематики, ця тенденція стосується практично всіх видів УЗ усіх видів та родів військ збройних сил.

Її характерною рисою є те, що на заміну моноблочним бойовим частинам, спорядженим вибуховими речовинами на базі тротилу, в крилатих ракетах і ракетах інших типів наземного, повітряного і корабельного базування, бомбах, торпедах, снарядах застосовуються бойові частини касетного типу, спрямованої осколкової дії та боеприпаси підвищеної потужності, наприклад термобаричної дії, як правило, без збільшення маси самої бойової частини [2, 3]. При цьому спроможності ураження, властиві їхнім бойовим частинам, у рази більші, ніж у звичайних боеприпасів, що дає можливість досягти в деяких випадках ефективності їхнього застосування, порівняної з потужністю тактичної ядерної зброї.

Упродовж останніх десятиліть у провідних країнах світу активно розробляються УЗ із надвисокими швидкостями руху, так звана гіперзвукова ракетна зброя, яка має значно підвищені можливості щодо подолання системи ППО-ПРО противника та збільшені можливості ураження його цілей.

Науково-технічний доробок останніх двох десятиліть, реалізований у програмах створення експериментальних гіперзвукових ударних засобів передусім у наукових установах США (NASA, DARPA тощо), Китаю та інших країн дав змогу прийняти останніми роками на озброєння перші зразки гіперзвукових ракет. Слід зазначити, що тенденція створення високоточних гіперзвукових ударних засобів виходить нині практично на перший план.

Як приклади і підтвердження реалізації тенденції можна навести такі зразки ОВТ: російські багатоцільові гіперзвукові ракети морського базування «Циркон», аеробалістичні гіперзвукові ракети повітряного базування Х-47М2 «Кинжал», які були використані країною-агресором для ударів по об'єктах інфраструктури України під час широкомасштабної агресії проти нашої країни [8]. При цьому рекламні дані виробника ракет щодо неможливості перехоплення її існуючими засобами ППО були розвіяні за допомогою сучасних зенітних ракетних комплексів «Patriot ПАКЗ», наданих Україні в рамках міжнародної військової допомоги (МВД) урядом США.

Таким чином, за останні десятиліття високоточна зброя зробила якісний стрибок у своєму розвитку. Суттєво розширилися можливості з подолання та вогневого придушення систем ППО, ураження об'єктів практично в будь-якому місці земної кулі, в будь-який час доби і за будь-яких кліматичних умов. Для БЗ, тобто носіїв УЗ, збільшилися рубежі пуску, знизилася її помітність, зросла швидкість польоту, а за рахунок використання комбінованих системи наведення зросла точність ураження цілей.

Вагомі здобутки в плані створення і постачання у війська новітніх зразків високоточної зброї практично

всіх видів базування має й Україна. Це високоефективна ракетна зброя власного виробництва, в тому числі й далекобійна, та поставлені в рамках МВД зразки високоточних УЗ від наших закордонних партнерів [9, 10].

Третя тенденція – інтелектуалізація засобів збройної боротьби: створення і використання роботизованих, дистанційно керованих та повністю автономних ЗЗБ (зразків ОВТ) з використанням технологій штучного інтелекту, виступає як практично найперспективніша тенденція розвитку ОВТ. У провідних країнах світу зразки таких ЗЗБ уже прийняті на озброєння, крім того, тивають широкомасштабні дослідження, спрямовані на розширення їхньої інтелектуалізації, тобто функцій автономності і самостійності в прийнятті рішень новітніх і модернізованих засобів ураження.

Природне середовище їхнього застосування дуже широке: від підводного середовища аж до космічного простору. Відповідно, дана тенденція проявляється й активно реалізовуватиметься в майбутньому в усіх видах збройних сил і родах військ.

Слід зазначити, що процес інтелектуалізації засобів ведення збройної боротьби розпочався практично з появою перших серійних електронно-обчислювальних машин, тобто має вже досить багату історію. Проявом його стало спрощення процесів експлуатації, керування та бойового застосування досить складних зразків (систем, комплексів) ОВТ, передусім пілотованих літальних (ЛА) військового призначення. Але за останні приблизно десять років у зв'язку з бурхливим розвитком комп'ютерних технологій процес інтелектуалізації ЗЗБ набув всеосяжного характеру і має широкі перспективи розвитку.

Як зазначено в попередніх публікаціях, нині керування більшістю автономних безпілотних платформ, як і раніше, здійснюється дистанційно людиною (хоча рівень автоматизації тут постійно зростає), а важливі елементи виконання бойового завдання, наприклад виявлення цілі та ухвалення рішення на її ураження дотепер вимагає контролю людини-оператора [1, 3]. Утім, розвиток науки надає можливості розсунути межі можливостей штучного інтелекту і створити безпілотні платформи, здатні самостійно ухвалювати рішення щодо їхнього бойового застосування.

Результатом реалізації даної тенденції в майбутньому, як зазначають деякі військові аналітики, може стати повне витіснення людини з процесу безпосереднього ведення бойових дій. Основний аргумент – людина-оператор виявилася найслабшою ланкою в багатьох системах озброєнь – її занадто довго і дорого вчити й важко захистити, машини повинні боротися проти машин [1, 2].

На даний час діапазон використання роботів навіть у сухопутних військах (СВ), як у найбільш традиційному

і консервативному виді ЗС, дуже різноманітний. Наземні апарати-роботи вже широко використовуються в останніх війнах та збройних конфліктах, зокрема в інженерних частинах і підрозділах СВ для подолання мінних перешкод, пошуку та знешкодження мін.

Досвід російсько-української війни свідчить, що багатьма розробниками створюються і вже використовуються в бойових умовах новітні наземні бойові дистанційно керовані машини для дій у міських умовах та наземні роботизовані машини для виконання допоміжних та конкретних бойових завдань [11, 12].

Найбільш відомими прикладами реалізації цієї тенденції у СВ є використання легких та відносно недорогих БпЛА поля бою і тактичних БпЛА, що застосовуються в багатьох країнах світу для оперативного одержання розвідувальної інформації та забезпечення зв'язку. Уже натеper і в майбутньому масштаби і сфера застосування таких ЛА тільки розширюватимуться за рахунок як традиційних, так і нових завдань. На підтвердження цього можна навести новітній досвід бойового застосування протиборчими сторонами так званих FPV-дронів в Україні. У цьому плані дана тенденція тісно пов'язана з п'ятою (використання повітряно-космічних систем), а особливо шостою (мінімізація габаритів і цінових параметрів зразків ОВТ) тенденціями з переліку загальних тенденцій розвитку ЗЗБ.

Крім того, останніми десятиліттями суттєво розширився діапазон застосування БпЛА середнього і важкого класу, котрі у складі безпілотних авіаційних комплексів чи наземних розвідувально-ударних комплексів, підпорядковуючись іншим видам і родам військ, застосовуються для вирішення як традиційних, так і нових, суто бойових завдань, з ураження наземних і морських цілей. У майбутньому сфера застосування таких максимально роботизованих та автономних БпЛА практично в усіх видах і родах військ лише розширюватиметься за рахунок витіснення літаків і вертольотів пілотованої авіації. Крім того, прогнозується, що майбутнє шосте покоління літаків тактичної авіації матиме можливість виконувати польоти в пілотованому і безпілотному режимах та діяти в єдиних бойових порядках з керованими ними багатофункціональними БпЛА.

Усе сказане стосовно БпЛА авіації повітряних сил буде характерним і для військово-морських сил (ВМС). Авіація ВМС також переходить на використання БпЛА найрізноманітнішого призначення – від розвідувальних до бойових. Крім того, у ВМС уже зараз застосовуються і, безперечно, розвиватимуться в майбутньому роботизовані автономні й дистанційно керовані надводні та підводні апарати – для вирішення завдань розвідки, виявлення і знищення морських мін, проведення пошукових підводних робіт тощо. Останнім часом у багатьох країнах розробляються і приймаються

на озброєння малогабаритні бойові дрони-камікадзе для ураження плавзасобів противника. Успішний та унікальний досвід створення і бойового застосування вітчизняних роботизованих малогабаритних морських дронів, набутий під час російсько-українського широкомасштабного протистояння на Чорному морі, має і Україна. Завдяки масовому застосуванню таких роботизованих морських дронів удалося повністю витіснити ворожий флот від морського узбережжя України і заблокувати основні наші морські торговельні шляхи.

Четверта тенденція – підвищення ролі спеціальної техніки для ведення інформаційної війни: засобів розвідки, радіоелектронної боротьби (РЕБ), зв'язку, автоматизованого управління військами (АСУ) та їх комплексування, а також новітніх технічних засобів для психологічного впливу на людей.

Однією з найперспективніших тенденцій розвитку засобів військового і взагалі міждержавного протиборства на початку ХХІ ст. стало зростаюче значення інформаційного фактора, який був досить вагомий, але значно обмежений у масштабі й у минулому. Завдяки випереджальному розвитку технічних і програмних засобів їх реалізації інформаційна складова міждержавного протиборства як у військовій, так і в цивільній сферах вийшла на новий якісний рівень, який дав змогу суттєво розширити її вплив передусім за рахунок аудиторії противника.

Об'єктами впливу на противника в сучасній інформаційній війні є спеціалізовані технічні засоби розвідки, управління військами та зброєю, засоби РЕБ, програмні засоби впливу на комп'ютерні мережі і засоби телекомунікації, інші засоби інформаційного впливу на державний апарат, широкі версти населення, а також на особовий склад збройних сил противника.

Найважливішою складовою інформаційної боротьби у військовому плані стали засоби РЕБ, направлені на порушення (зрив) управління об'єднаннями, з'єднаннями, частинами всіх видів (родів) військ, тобто протидія існуючим засобам зв'язку та АСУ противника. Вона реалізована за рахунок постачання у війська потужних багатофункціональних засобів РЕБ, аналогічних засобів на роботизованих платформах ОВТ наземного, повітряного і морського базування (UGV, UAV, USV), малогабаритних та одноразових передавачів завад також різного базування [13, 14].

Другою важливою складовою в системі РЕБ є розвиток технічних засобів боротьби із системами управління (наведення) високоточною зброєю противника, розвиток засобів РЕБ групового й індивідуального захисту пілотованої та безпілотної авіації, бронетанкового озброєння і техніки, автомобільної техніки від ураження радіокерованими вибуховими пристроями (RCID), а також іншими високоточними засобами вогневого ураження [13, 14].

Зростаюча роль РЕБ у досягненні мети операцій у процесі бойових дій змушує провідні країни світу приділяти досить пильну увагу питанням завадозахищеності та завадостійкості своїх радіоелектронних засобів від впливу засобів радіоелектронного придушення противника та забезпечення потрібного рівня їхньої електромагнітної сумісності.

Упровадження АСУ на базі сукупності інформаційно-керівних систем для автоматизації процесів управління вогнем, рухом та захищеністю об'єктів характерне для всіх видів збройних сил, а основні зусилля розробників спрямовані на міжвидову інтеграцію (комплексування) автоматизованих систем бойового управління та ураження.

Як уже зазначалось у попередніх публікаціях, підвищення ролі техніки спеціальних військ, що забезпечує ведення інформаційної боротьби, дає можливість реалізації концепції мережоцентричних бойових дій. Сучасні інформаційні технології як основа мережоцентричних бойових дій стали інструментом досягнення нових бойових можливостей, тобто підвищення ступеня реалізації наявного бойового потенціалу [2–4].

Суттєвим є підвищення ролі засобів ведення інформаційної боротьби в процесі широкомасштабної російської агресії проти України. Вона реалізується обома протиборчими сторонами, і якщо РФ у перший рік війни мала переваги в технічних засобах ведення РЕБ, то згодом ця перевага була практично нівельована.

Уже традиційна, але й досі актуальна *п'ята тенденція*. Це **суттєве підвищення ролі повітряно-космічних систем для вирішення завдань розвідки, управління військами (зв'язок та АСУ), навігації та в перспективі – безпосереднього ураження цілей.**

Слід зазначити, що в даній статі до повітряно-космічних систем (ПКС) не включені традиційні авіаційні бойові засоби та авіаційні ударні засоби, тобто ЛА всіх видів ЗС України та інших країн, що використовуються ними для безпосереднього ураження цілей. До ПКС належать, за запропонованою класифікацією, спеціалізовані (не бойові) зразки авіаційної техніки, космічні та аерокосмічні апарати різного призначення, в тому числі й гіперзвукові БЗ та УЗ.

Тенденція перенесення збройної боротьби в повітряно-космічну сферу – це один з головних трендів розвитку її форм і способів, за якою визначальне майбутнє. Як відмічено у [2, 3], це значною мірою пояснюється тим, що головним носієм високоточної зброї та зброї на нетрадиційних принципах дії, як показав досвід останніх війн і збройних конфліктів, стали ПКС і засоби, тісно пов'язані з ними. Повітряно-космічний простір із фізичного середовища переміщення новітніх літальних і космічних апаратів перетворюється на головний театр воєнних дій зі своїми цілями, завданнями, силами і засобами для всіх видів збройних сил.

Як показує практика останніх років, заборонні міжурядові правові заходи, спрямовані на недопущення мілітаризації космічного простору, стають дедалі менш дієвими.

Отже, в найближчій перспективі успішне ведення воєнних дій у повітряно-космічному просторі стане основою для досягнення успіху в збройній боротьбі як на суші, так і на морі. За цих умов розвиток ПКС для вирішення завдань розвідки, управління, навігації та безпосереднього ураження цілей, а також засобів протидії їм для сторони конфлікту, яка вирішує оборонні завдання, здобуває першорядне і вирішальне значення для перебігу і результатів війни. Це має прямий стосунок до російсько-української війни. Тому використання потужного потенціалу технічних засобів ПКС країн – партнерів України для досягнення переваги в одержанні розвідувальної інформації щодо країни-агресора вкрай важливе.

Розвідувальна інформація, яка одержується за допомогою ПКС, а це космічні апарати, літаки дальнього радіолокаційного виявлення та управління (ДРЛВУ), спеціалізовані розвідувальні літаки та БпЛА різних класів, надзвичайно затребувана практично в усіх видах збройних сил. Зростаючі вимоги її споживачів щодо якості та оперативності одержання спричинили тенденцію розвитку самих розвідувальних ПКС. На зміну спеціалізованим пілотованим літкам прийшли розвідувальні супутники на орбіті Землі, а далі – літаки ДРЛВУ, які давали змогу підвищити оперативність одержуваної інформації.

Усі перелічені вище засоби одержання розвідувальної інформації вимагають наявності у виробника потужного науково-технічного та військово-промислового потенціалу й, відповідно, значних фінансових витрат, що можуть дозволити собі тільки найбільш розвинені країни світу. Упродовж останніх десятиліть на тлі бурхливого розвитку роботизованих безпілотних систем (згадана вище третя тенденція розвитку ЗЗБ) великого значення набули розвідувальні БпЛА всіх класів – від ЛА оперативно-стратегічної до ближньої тактичної розвідки, які дали змогу за значно менших витрат оперативно одержувати необхідну розвідувальну інформацію. Підтвердженням цього є досвід проведення операцій на суходутному театрі воєнних дій у широкомасштабній російсько-українській війні, що триває.

Зрозуміло, що розглянута тенденція (підвищення ролі ПКС) тісно пов'язана з іншими тенденціями розвитку ЗЗБ, що проявляється в тісному взаємозв'язку з ними. Але не виділяти її як окрему й актуальну було б не правильно. Тобто в ній реалізуються значно ширші, але чітко обмежені сферою застосування тенденції розвитку ЗЗБ, які не мають стосунку до інших розглянутих тенденцій.

Шоста тенденція – створення і широке застосування нових високоефективних, малогабаритних та відносно фінансово низьковитратних зразків ОВТ з урахуванням усіх етапів їхнього життєвого циклу.

Основними причинами реалізації даної тенденції є:

- вимоги розробників складних систем (платформ) ОВТ щодо мінімізації габаритів комплектуючого обладнання та озброєння;
- необхідність забезпечення аеромобільності зразків ОВТ, насамперед наземного базування;
- прагнення до створення на базі відносно невеликих автономних безекіпажних платформ усіх видів базування високоефективних бойових та ударних засобів, здатних уражати наземні (надводні) цілі противника;
- суттєве зменшення масо-габаритних показників елементної бази бортового обладнання та озброєння;
- суттєве зростання цінових показників нових традиційних зразків ОВТ, що робить їх надмірно вартісними для більшості традиційних споживачів.

У СВ найвиразніше ця тенденція проявляється під час створення зразків ОВТ з метою забезпечення їхньої аеромобільності й десантопридатності. Це ціле сімейство легких бойових броньованих машин (ББМ) різного призначення, які мають прийти на заміну основним бойовим танкам, самохідним артилерійським установам та іншим важким наземним зразкам ОВТ. При цьому нове покоління відносно легких ББМ за своїми вогневыми можливостями та експлуатаційними характеристиками повинне бути не гіршим, ніж попереднє.

Ця тенденція повною мірою стосується зразків екіпірування солдата майбутнього в широкому сенсі цього слова. А це стрілецька зброя всіх типів, засоби зв'язку та управління, засоби захисту й життєзабезпечення. Інтенсивні пошукові дослідження в даному напрямі з метою зменшення масо-габаритних показників та покращення функціональних показників ведуться в багатьох країнах світу. Тому вже зараз у передових країнах світу прийняті на озброєння (постачання) такі зразки ОВТ, а в найближчому майбутньому слід очікувати вже друге їх покоління.

Реалізується дана тенденція й у всіх родах військ повітряних сил. Це передусім розробка та прийняття на озброєння нових високоефективних відносно легких літаків тактичної авіації та навчально-тренувальних літаків. Поряд зі створенням у провідних країнах світу нових, надзвичайно високовартісних літаків (F-35, Су-57, J-20, J-31), є розуміння необхідності та робляться кроки в плані створення доступних широкому колу споживачів навчально-бойових та легких бойових літаків на їхній базі.

Мінімізація масо-габаритних параметрів авіаційних засобів ураження (бомбового і ракетного озброєння) продиктована бажанням використовувати такі боеприпаси на відносно невеликих БпЛА та необхідністю

розміщення їх у бомбовідсіках новітніх тактичних винищувачів п'ятого покоління. Такі боеприпаси інтенсивно розробляються та приймаються на озброєння в багатьох провідних країнах світу. Крім того, тенденція мінімізації габаритів, а відповідно, і маси ЛА, активно реалізується під час створення самих БпЛА і проявляється в пошукових дослідженнях щодо створення ефективних міні- та мікро-БпЛА.

Як відмічено в попередніх публікаціях [2, 3], у ВМС більшості країн світу відбувається перехід до прийняття на озброєння надводних універсальних кораблів класу «корвет» та багатоцільових катерів з бойовими можливостями, притаганими кораблям вищого класу. Цьому сприяє зменшення маси і габаритів корабельного обладнання та зброї, а відповідно, і їхньої ціни. Активно розробляються та приймаються на озброєння високоефективні малотоннажні надводні та підводні безекіпажні автономні або дистанційно керовані розвідувальні та бойові кораблі, що також підтверджено й останнім досвідом їх застосування українськими Силами оборони в Чорному морі.

Перспективність цієї тенденції підтверджується різким зростанням цін на новостворені зразки ОВТ практично всієї їхньої номенклатури та необхідністю для багатьох країн пошуку альтернативних, більш прийнятних з фінансового погляду варіантів переоснащення збройних сил [2–4]. Ідея створення дешевих високоефективних легких та малогабаритних ЗЗБ має як своїх прихильників, так і противників, але, безсумнівно, є перспективною.

Упродовж останнього десятиліття значного поширення практично в усіх країнах світу набула практика модернізації наявних зразків ОВТ як альтернатива новим надзвичайно вартісним зразкам. І хоча це не має прямого стосунку до даної тенденції розвитку ОВТ, але дає змогу відчутно підвищити технічний рівень модернізованих зразків за значно менших (іноді на порядок) фінансових витрат [15].

Сьома тенденція – розроблення і застосування нових високоефективних транспортних засобів середнього і великого радіусу дії військового (подвійного) призначення.

Реалізація даної тенденції, яку по праву відносять до традиційних тенденцій розвитку ОВТ, зумовлена широким використанням маневру як невід'ємної частини бойових дій, що ведуться на поверхні землі, води й у повітрі. У зв'язку із цим пріоритетний напрям розвитку одержали ЗЗБ, що забезпечують підвищення маневрених можливостей та мобільності зразків, комплексів і систем ОВТ. Вони забезпечують швидке й ефективно переміщення військ зі штатним озброєнням, як правило, повітряним або морським шляхом, на тактичному та стратегічному рівнях. Не залишається осторонь цього процесу й сухопутна складова, що

проявляється через створення і прийняття на озброєння нових високоефективних зразків автомобільної техніки для транспортування військ [2, 3].

Найвиразніше ця тенденція проявляється в розробленні, закупівлі та розширенні використання високоефективних військово-транспортних літаків (ВТЛ) різних класів. Важкі ВТЛ, основним призначенням яких є транспортування військ на стратегічному рівні, модернізуються з метою підвищення ефективності і продовження строків їхньої експлуатації. Найінтенсивніше розвиваються класи середніх і легких ВТЛ, розширюється не лише номенклатура та масштаби випуску, а й географія їхнього виробництва. На рівні найкращих світових стандартів перебувають і аналогічні ВТЛ українського виробництва, насамперед Ан-70 та Ан-178. Серійне виробництво їх у кооперації з новими закордонними партнерами, найімовірніше, після завершення війни з Росією, може бути досить перспективним напрямом розвитку ОПК України.

Практично в усіх провідних країнах світу триває створення і прийняття на озброєння нових і модернізація наявних транспортних і багатоцільових вертольотів легкого та середнього класів. У майбутньому слід очікувати лише розширення їхнього використання у збройних силах практично всіх країн світу для виконання транспортних та інших завдань.

У ВМС для розширення можливостей транспортування військ на великі та середні відстані йде перехід до використання універсальних десантних кораблів з авіаційним компонентом у вигляді бойових і транспортних вертольотів, а також літаків вертикального зльоту і посадки. Для переміщення військ на тактичному рівні та їхньої висадки на берег розробляються і вже використовуються високошвидкісні десантні кораблі з динамічним принципом підтримки (кораблі на підводних крилах та на повітряній подушці) та кораблі, побудовані за принципом багатокорпусної конструкції (катамарани, тримарани).

Наступна, відносно нова, *восьма тенденція – розроблення та застосування ЗЗБ (зразків ОВТ), заснованих на нетрадиційних, зокрема нелетальних, принципах дії.*

На думку більшості провідних воєнних аналітиків, у війнах наступного покоління широке застосування знайдуть засоби ураження цілей, дія яких заснована на використанні різноманітних форм енергії. Деякі елементи такої зброї починають використовувати вже в наш час, в інших перспектива більш туманна. До таких ЗЗБ належать: електромагнітна, лазерна, пучкова, плазмова, акустична, радіологічна, біологічна та геофізична зброя [16].

Найважливішою властивістю перелічених видів зброї є використання спрямованих потоків енергії. Ця зброя може використовуватись як для ураження, так

і для придушення різноманітних об'єктів, у тому числі повітряно-космічних (космічних) апаратів та бойових частин балістичних ракет. Сформовані енергетичні потоки у вигляді лазерних променів здатні вражати органи зору особового складу, оптичні приціли, приймальні пристрої радіоелектронних засобів і головок самонаведення керованих боєприпасів [2, 3]. Електромагнітні імпульси виводять з ладу не лише радіоелектронні засоби, а й звичайні електричні прилади, що може призвести до відмови як системи управління, так і самих сучасних бойових засобів. У зв'язку з усе більшою насиченістю сучасних зразків ОВТ електронікою зброя, заснована на нетрадиційних принципах дії, поступово займатиме дедалі ширшу нішу в арсеналах армій провідних країн світу [1, 2].

Важливою особливістю зброї на нетрадиційних принципах дії, передусім лазерної, електромагнітної, акустичної, в разі використання проти населення і живої сили противника є можливість забезпечення нелетальних наслідків її застосування, що вже зараз використовується та, безперечно, використовуватиметься в майбутньому.

Нині в стадію практичного використання ввійшла лазерна зброя для вирішення завдань розвідки, виведення з ладу оптико-електронних засобів противника, ураження пілотованих і безпілотних літальних апаратів.

Дев'ята тенденція – підвищення скритності і захищеності ОВТ, особового складу та об'єктів інфраструктури від ураження звичайною зброєю, зброєю масового й електромагнітного ураження.

Як показує досвід останніх війн та збройних конфліктів, у тому числі й російсько-української війни, тенденція підвищення скритності і захищеності зразків, комплексів і систем ОВТ тісно пов'язана із загостренням останніми роками найважливішого протиріччя, яке лежить в основі розвитку воєнної справи взагалі, – протиріччя між засобами нападу і засобами захисту. Паралельно зі збільшенням технічних можливостей різних видів повітряної та космічної розвідки і поліпшенням характеристик виявлення цілей, особливо за рахунок використання БпЛА різних класів, практично всіма країнами вживаються і вживатимуться надалі заходи, спрямовані на забезпечення скритності й захищеності особового складу, зразків ОВТ, об'єктів інфраструктури та управління військами [2, 3].

Реалізація даної тенденції для ОВТ наземного базування втілюється у створенні ББМ зі зниженою помітністю в усьому спектрі електромагнітних хвиль, установленні на них комплексів оптико-електронного придушення, використанні комплексів активного та динамічного захисту, які забезпечують їх круговий захист, розробленні високоефективної композитної броні тощо. Указані заходи реалізуються не лише при створенні традиційних зразків ББМ (танки, БМП,

БТР), а й при створенні легкоброньованої автомобільної техніки, що суттєво підвищує їхню протимінну і балістичну стійкість.

Як зазначають закордонні фахівці, підвищення захищеності для ББМ на даний час є однією з головних тенденцій їхнього розвитку. Ще на етапі проектування нових ББМ екіпаж, як правило, розміщують у броньованих капсулах (відсіках), а боекомплект і паливо – окремо від них. Для зменшення ймовірності пробиття броні широке використання знайшли решітчасті та протикумулятивні екрани, а також додаткові модулі захисту, що легко можуть замінюватися.

Для захисту особового складу активно використовуються наявні засоби захисту та ведуться роботи зі створення екіпірування солдата майбутнього, що не лише суттєво розширює можливості з виявлення і вогневого ураження противника, а й значно збільшує шанси на виживання особового складу. Останнє досягається за рахунок використання засобів маскування, високо-ефективного захисту найважливіших ділянок тіла і голови та постійного контролю самопочуття солдата.

В авіації основними шляхами реалізації цієї тенденції є [2]:

- реалізація в нових тактичних літаках п'ятого покоління технологій малопомітності (так званих технологій «Стелс») та її елементів у модернізованих літаках четвертого покоління;
- розміщення авіаційних засобів ураження у внутрішніх відсіках літаків;
- використання практично на всіх ЛА військового призначення окрім пасивних також активних засобів захисту від керованих ракет;
- підвищення скритності РЛС за рахунок перерозподілу електромагнітної енергії по спектру.

У ВМС у цьому плані реалізуються такі основні шляхи [3]:

- мінімізація фізичних полів (електромагнітних, оптичних, гідроакустичних) кораблів і підводних човнів;
- оснащення підводних човнів повітрянезалежними енергетичними установками для збільшення часу перебування під водою, що підвищує їхню скритність;
- розробка за допомогою нанотехнологій і впровадження спеціальних захисних покриттів, що знижують помітність кораблів і нейтралізують імпульси лазерів;
- удосконалення систем і засобів захисту (протиракетного, протиторпедного) шляхом їх комплексування з іншими системами кораблів та підводних човнів.

Дана тенденція, тобто підвищення скритності й захищеності ОВТ, тісно пов'язана й реалізуються разом з іншими вказаними вище тенденціями розвитку ЗЗБ.

Десята тенденція – підвищення ролі загально-військових та загальнотехнічних вимог до ЗЗБ (опера-

тивності застосування, спрощення експлуатації, надійності функціонування, уніфікації та ремонтно-придатності зразків та їх стандартизації згідно з міжнародними стандартами).

Спрощення експлуатації ОВТ на основі уніфікації витратних матеріалів, підвищення надійності роботи апаратури (зростання часу безвідмовної роботи), автоматизованого контролю технічного стану, діагностики відмов разом з резервуванням (дублюванням) роботи основних вузлів та елементів дають можливість значно скоротити чисельність екіпажів та обслуговуючого персоналу ОВТ усіх видів збройних сил і скоротити час приведення їх у бойову готовність.

Воююча сторона, яка має переваги в безперервності функціонування ОВТ за рахунок забезпечення їхньої всесезонності й цілодобовості, одержує додаткові переваги в кількості ОВТ і має можливість використовувати їх у незручний для противника час. Усі ці загальновійськові вимоги вже стали законодавчою нормою та необхідним атрибутом під час створення нових чи модернізації існуючих зразків ОВТ.

На практиці ця тенденція реалізується в зразках ОВТ у вигляді вбудованих систем самоконтролю працездатності і діагностики, автоматизації процесів розгортання і згортання бойових засобів, переведенні на твердотільну елементну базу всієї радіоелектронної апаратури, застосуванні відкритої архітектури електронно-обчислювальних машин, що характерно для сучасних зразків ОВТ та їхніх складових усіх видів збройних сил.

Підвищення вимог щодо стандартизації та уніфікації ОВТ реалізується на етапах розроблення, модернізації та виробництва ОВТ і передбачає розроблення й упровадження нормативних документів і здійснення заходів щодо забезпечення функціонування систем стандартизації, класифікації, кодування та каталогізації військової продукції, систем замовлення, розроблення, виробництва, експлуатації, ремонту й утилізації ОВТ [2, 3].

Зважаючи на розрив військово-технічного співробітництва з РФ та іншими пострадянськими країнами, питання стандартизації продукції військового призначення в Україні стало надзвичайно актуальним. Курс на інтеграцію з Євросоюзом потребує переходу оборонної промисловості на міжнародні (європейські) стандарти, що дасть змогу уніфікувати виробничі процеси та підняти якість продукції оборонного призначення. Це, у свою чергу, підвищить її конкурентоспроможність і дасть можливість переоснащення силових структур держави. Перехід на стандарти НАТО відкриває широкі можливості щодо використання в Україні ОВТ західного виробництва, що особливо актуально нині з наданням Україні міжнародної матеріально-технічної допомоги для відбиття широкомасштабної російської агресії.

Висновки

Підсумовуючи розгляд загальних тенденцій розвитку ЗЗБ, слід зазначити, що в процесі створення нових перспективних зразків в одному більш-менш технічно складному виробі реалізується ціла низка згаданих вище тенденцій, взаємозв'язок яких розглянутий під час аналізу кожної конкретної тенденції. При створенні відносно простих зразків ОВТ, призначених для забезпечення бойових дій, подібний перелік реалізованих тенденцій, звичайно, менший. Зазначені тенденції розвитку ЗЗБ є основними і стосуються всього озброєння та військової техніки збройних сил на світовому рівні. Водночас кожна держава, виходячи зі своїх воєнно-політичних цілей, економічного становища, стану збройних сил, їхнього оснащення та інших факторів, визначає на заданий проміжок часу пріоритетні напрями розвитку ОВТ власних збройних сил.

Урахування розглянутих загальних тенденцій розвитку ОВТ при середньостроковому, а тим більше довгостроковому плануванні їхнього розвитку в Україні дасть змогу на державному рівні зменшити ризики при прийнятті рішень військово-політичним керівництвом під час розробки програм та інших документів щодо розвитку ОВТ.

Урахування сучасних загальних тенденцій розвитку ОВТ на рівні розробників та виробників ОВТ в Україні також дасть їм можливість краще орієнтуватися у нагальних потребах усіх складових Сил оборони держави та прискорити їхнє створення, зокрема за рахунок ініціативних проєктів.

Перелік літератури

1. Горбулін В. П. Забезпечення оборони та безпеки України: актуальні проблеми і шляхи їх вирішення / В. П. Горбулін // Вісник НАН України. – 2019. – № 9. – С. 3–18.
2. Чепков І. Б. Загальні тенденції розвитку озброєння та військової техніки / І. Б. Чепков, П. І. Нор // Озброєння та військова техніка. – 2014. – № 1 (1). – С. 4–13.
3. Нор П. І. Науковий твір «Загальні тенденції розвитку озброєння та військової техніки»: свідоцтво про реєстрацію авторського права на твір № 60828 від 27 липня 2015 р. / П. І. Нор, І. Б. Чепков, О. Д. Мельник; ЦНДІ ОВТ ЗС України. – [К.], 2015. – 30 с.
4. Нор П. І. Основні світові тенденції розвитку озброєння та військової техніки та їх взаємозв'язок з сучасними формами і способами ведення збройної боротьби / П. І. Нор, О. Д. Мельник, В. А. Єфіменко // Зб. наук. праць ЦНДІ ОВТ ЗСУ. – 2006. – Вип. 16. – С. 90–99.
5. Василенко О. В. Основні світові тенденції розвитку озброєння та військової техніки для ведення війн у майбутньому / О. В. Василенко // Наука і оборона. – 2009. – № 4. – С. 18–22.
6. Нор П. І. Основні тенденції розвитку форм і способів ведення збройної боротьби [Електронний ресурс] / П. І. Нор, І. В. Борохвостов, О. І. Соломицький // Наука і оборона. – 2023. – № 1. – С. 20–27. – Режим доступу: <https://doi.org/10.33099/2618-1614-2023-21-1-20-27>.
7. Нор П. І. Основні тенденції розвитку форм і способів ведення збройної боротьби / П. І. Нор, І. В. Борохвостов, О. Л. Глушкевич // Зб. наук. праць ЦНДІ ОВТ ЗСУ. – Вип. 2 (89). – С. 329–342.
8. «Кинджали»: коли та скільки гіперзвукових ракет Росія застосувала проти України [Електронний ресурс] // Слово і Діло. – Режим доступу: <https://www.slovoidilo.ua/2023/03/10/infografika/bezpeka/kyndzhaly-koly-ta-skilky-hiperzvukovykh-raket-rosiya-zastosuvala-proty-ukrayiny>.
9. Hannenko Y. International military assistance to Ukraine [Електронний ресурс] / Y. Hannenko, L. K. Levy II // Зб. наук. праць ЦВСД НУОУ. – 2024. – Т. 1, № 3 (82). – С. 58–64. – Режим доступу: <https://doi.org/10.33099/2304-2745/2024-3-82/58-64>.
10. Олександр Корнієнко: Американська високоточна зброя й українська хоробрість на полі бою зруйнувала не один міф щодо російської армії [Електронний ресурс] / Пресслужба Апарату Верховної Ради України // Верховна Рада України. – Режим доступу: <https://www.rada.gov.ua/news/Tor-novyna/236738.html>.
11. Куфрик Б. Роботизовані системи на передовій: що вони вміють і як допомагають нашим військовим [Електронний ресурс] / Б. Куфрик // Експрес. – Режим доступу: <https://expres.online/spetstema-2/robotizovani-sistemi-na-peredoviy-shcho-voni-vmiyut-i-yak-dopomagayut-nashim-viyskovim>.
12. Рефагі І. 10 найдосконаліших військових роботів у світі: що вони вміють і як виглядають (фото, відео) [Електронний ресурс] / І. Рефагі // Фокус. – Режим доступу: <https://focus.ua/uk/digital/614551-10-najdoskonalih-viyskovih-robotiv-u-sviti-sho-voni-vmiyut-i-yak-viglyadayut-foto-video>.
13. Білецька А. В. Перспективні напрямки розвитку засобів та техніки радіоелектронної боротьби / А. В. Білецька, С. Д. Зібін, В. В. Твердохлібов // Озброєння та військова техніка. – 2022. – № 4 (36). – С. 68–78.
14. Попов А. О. Загальні тенденції розвитку засобів радіоелектронної боротьби / А. О. Попов, В. В. Твердохлібов // Озброєння та військова техніка. – 2014. – № 4 (4). – С. 4–11.
15. Харченко О. В. Глибока модернізація та переозброєння авіації Збройних Сил України – вимога часу / О. В. Харченко, С. В. Пащенко // Наука і оборона. – 2015. – № 1. – С. 40–47.
16. Зброя на нетрадиційних принципах дії (стан, тенденції, принципи дії та захист від неї): монографія / О. П. Ковтуненко, В. В. Богучарський, В. І. Слюсар, П. М. Федоров; ЦНДІ ОВТ ЗС України. – Полтава: ПІВЗ, 2006. – 248 с.

DOI 10.33099/2618-1614-2025-28-1-36-46

УДК 355.4

В. В. Машталір,*доктор історичних наук, професор,
Національний університет оборони України,***Ю. А. Гусак,***доктор військових наук, професор,
Національний університет оборони України*

Розвиток понятійного апарату з питань кібероборони та підходи до створення кіберсил в Україні

Проведений аналіз понятійного апарату з питань кібербезпеки та кібероборони, який застосовується в законодавчих та нормативних документах. На підставі основних положень воєнного мистецтва запропоновано систему понять у сфері кібероборони, зокрема таких, як агресія в кіберпросторі, кіберборотьба, кібернаступ та кібероборона, кібероперація, кіберудар тощо, та надано їхні визначення. Здійснений аналіз кіберсил провідних країн НАТО. Визначено, що кіберсили провідних країн НАТО можуть мати два варіанти організації: перший варіант передбачає входження кіберсил до складу національних збройних сил та взаємодію їх із цивільними кіберпідрозділами (США, Німеччина), а другий – об'єднання в окремій національній структурі військових та цивільних кіберпідрозділів (Велика Британія, Франція). Запропоновані напрями розвитку теоретичних засад створення системи кібероборони України, реалізація яких дасть можливість формувати кіберсили, подібні за складом, організацією, завданнями і функціями до кіберсил країн – членів НАТО, реалізувати єдину стратегію кібероборони в Міністерстві оборони України та Збройних Силах України, здійснювати управління силами кібероборони в умовах правового режиму воєнного стану (особливого періоду).

Ключові слова: кібероборона, кіберпростір, система кібероборони, суб'єкти кібероборони, кібервійська, кібербезпека, кіберзахист, кіберсистема, кібератака, кібернаступ, кібероперація.

© В. В. Машталір, Ю. А. Гусак, 2025

Постановка проблеми. Розвиток сучасних кібертехнологій призвів до виникнення нових ризиків і загроз у сфері національної безпеки та оборони України, які здійснюються через та в кіберпросторі. Ці ризики та загрози створили виклики для України у сфері кібербезпеки (рис. 1) [1]. У зв'язку із цим відбувається трансформація поглядів на питання кібероборони та розробляються теоретичні засади кібероборони з урахуванням розвитку інформаційних технологій та прогнозуються можливі зміни у формах, способах і технологіях ведення війн.

Мілітаризація кіберпростору та розвиток кіберзброї ведуть до невпинного нарощування арсеналу кіберзброї наступального призначення та створюють кіберзагрози кібербезпеці України.

Загрози через кіберпростір впливають на всі базові сфери: політичну, воєнну, економічну, енергетичну, інфраструктурну тощо, та мають деструктивний вплив на національну безпеку та оборону загалом.

Загрозами кібербезпеці України є [1]: невпинне нарощування арсеналу кіберзброї наступального призначення; кіберзлочинність; кібершпиунство; кібертероризм (рис. 2).

Однією з найнебезпечніших кіберзагроз є застосування кіберзброї наступального призначення для проведення кібердиверсій або спеціальних інформаційних операцій.

У сучасному світі кібероборона як складова кібербезпеки має низку проблемних питань, які потребують негайного вирішення. У зв'язку із цим у розвинених країнах світу цьому питанню приділяють велику увагу. Ці питання розглядалися на таких важливих заходах НАТО, як [2]:

- саміт НАТО в Празі (2002) – уперше кіберзахист включений до політичного порядку денного Альянсу;
- саміт НАТО в Ризі (2006) – підтверджена необхідність додаткового захисту інформаційно-комунікаційних систем країн – членів НАТО;
- саміт НАТО в Лісабоні (2010) – прийнята Стратегічна концепція, в якій уперше було визнано, що кібератаки можуть загрожувати національній та євроатлантичній безпеці та стабільності;
- саміт НАТО в Чикаго (2012) – кіберзахист включений до процесу оборонного планування НАТО і визначені заходи централізованого захисту всіх мереж НАТО, для реалізації яких у липні 2012 р. у рамках реформи агенцій НАТО створене Агентство зв'язку та інформації НАТО;
- саміт НАТО у Вельсі (2014) – схвалена нова політика кіберзахисту, в якій кіберзахист визнаний частиною основного завдання НАТО щодо колективної оборони, що означає, що кібератака може бути підставою для застосування статті 5 установчого договору НАТО;

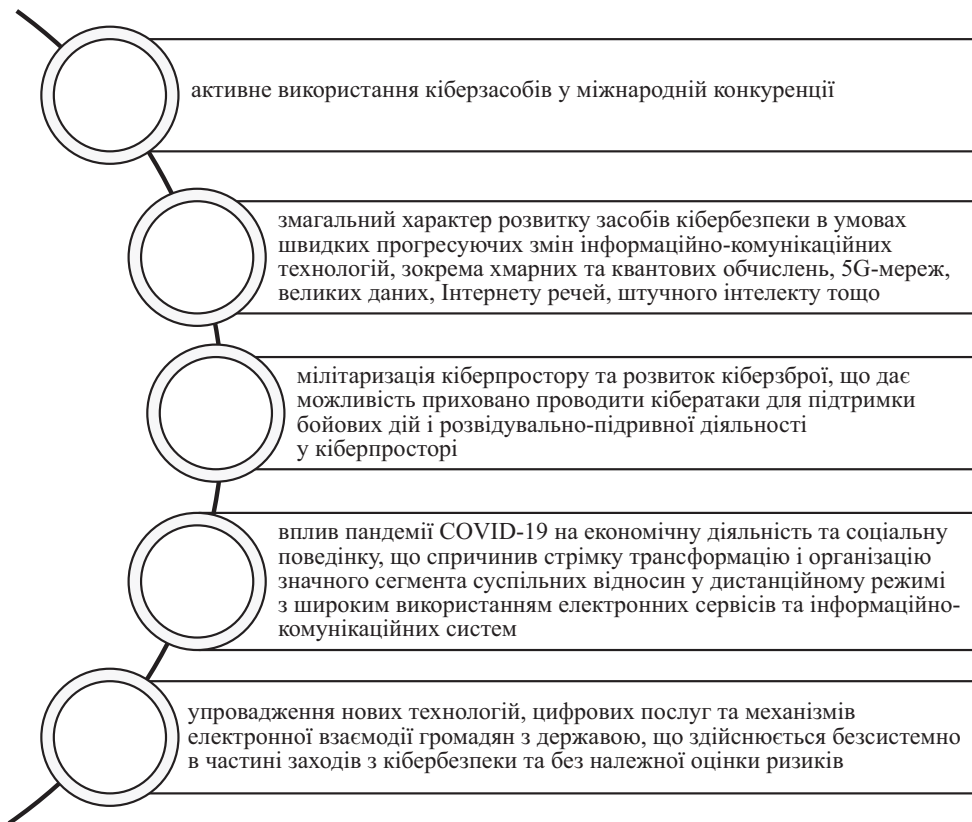


Рис. 1. Виклики для України у сфері кібербезпеки

<p>Кіберзброя наступального призначення</p> <ul style="list-style-type: none"> • кібератаки на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія); • отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності; • проведення спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності
<p>Кіберзлочинність</p> <ul style="list-style-type: none"> • використання кіберпростору для вчинення злочинів проти основ національної безпеки України; • кримінальні правопорушення, пов'язані з легалізацією доходів, одержаних злочинним шляхом
<p>Кібершпигунство</p> <ul style="list-style-type: none"> • викрадення в політичних, економічних або військових цілях чутливої інформації; • здійсненням розвідувально-підривної діяльності
<p>Кібертероризм</p> <ul style="list-style-type: none"> • використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності

Рис. 2. Загрози кібербезпеці України

- саміт НАТО у Варшаві (2016) – кіберпростір визнаний сферою операцій, у якій НАТО має захищатися;

- саміт НАТО в Брюсселі (2018) – прийняте рішення про створення Оперативного центру в кіберпросторі, який має забезпечувати ситуаційну обізнаність і координувати оперативну діяльність НАТО в кіберпросторі та через нього;

- саміт НАТО в Брюсселі (2021) – схвалена Всеосяжна політика кіберзахисту для підтримки трьох основних завдань НАТО: активно стримувати, захищатися і протидіяти повному спектру кіберзагроз у будь-який час (у мирний час, під час криз та конфліктів) – на політичному, військовому і технічному рівнях;

- саміт НАТО у Вільнюсі (2023) – схвалена нова концепція посилення внеску кіберзахисту в загальну систему стримування та оборони НАТО для покращення спільної обізнаності НАТО про ситуацію та кіберстійкість;

- саміт НАТО у Вашингтоні (2024) – прийняте рішення про створення Центру інтегрованого кіберзахисту НАТО для посилення захисту мереж, ситуаційної обізнаності та використання кіберпростору для проведення кібероперацій.

На проведених заходах увага була зосереджена на необхідності своєчасного виявлення, запобігання, нейтралізації та ліквідації кіберзагроз, а також створення кібероборони.

Крім того, щорічно НАТО проводить низку значущих конференцій з питань кібербезпеки та оборони. Основними подіями стали:

1. Міжнародні конференції з кіберконфліктів (CyCon), які щорічно організуються НАТО Cooperative Cyber Defence Centre of Excellence (CCDCOE) у Таллінні (Естонія). Темі CyCon охоплюють дослідження з технічних, стратегічних та правових аспектів кібероборони. Наприклад, на конференції CyCon у 2019 р. «Silent Battle» досліджувалися питання вразливостей, відповідальності та ситуаційної обізнаності в кіберпросторі, а на конференції CyCon у 2024 р. «Over the Horizon» були визначені перспективні виклики в кіберпросторі та заходи щодо реагування на них [3].

2. Щорічні навчання «Cyber Coalition», на яких відпрацьовуються форми та способи спільного реагування на кіберзагрози. Наприклад, у 2023 р. участь взяли 35 країн, включно з Україною [4].

3. Конференції з кібербезпеки в морській галузі, організовані НАТО Maritime Interdiction Operational Training Center (NMIOTC). На цих конференціях досліджуються питання захисту критичної морської інфраструктури та безпеки в цифровому середовищі. Наприклад, 8-ма Конференція з кібербезпеки в морській галузі відбулась у вересні 2024 р. [5].

4. Міжнародні навчання Locked Shields 2024 з кіберзахисту, в яких українські експерти співпрацювали з фахівцями з понад 40 країн для вдосконалення своїх навичок та посилення міжнародної кіберстійкості [6].

Ці заходи демонструють зусилля НАТО щодо вдосконалення колективної кібероборони та забезпечення безпеки своїх членів і партнерів у цифровому світі.

В Україні спільно з країнами НАТО активно проводяться дослідження з кібероборони, в яких беруть участь провідні науковці, організації та центри. Так, у роботі [7] опубліковане дослідження, проведене під егідою НАТО CCDCOE, щодо національного управління кібербезпекою в Україні. У звіті розглядається роль правової бази в розвитку кібербезпеки в Україні, що є основою для розробки міжнародних стратегій кібероборони.

У Національному кластері кібербезпеки України (NCSCC) активно вивчається та здійснюється обмін досвідом кіберзахисту та кібероборони в Україні з НАТО та ЄС [8].

Крім того, НАТО підтримує співпрацю українських дослідників через такі програми, які сприяють інноваціям у сфері кібербезпеки, як DIANA (Акселератор оборонних інновацій) та інвестиційний фонд НАТО. Це включає участь українських дослідників у спільних хакатонах і проєктах, таких як програма BRAVE1 у партнерстві з урядом України.

Ці зусилля свідчать про активну інтеграцію українських та міжнародних експертів для дослідження проблем реагування на виклики у сфері кібероборони, а також проблем розвитку правової бази та організаційних засад кібероборони. Разом з тим, проблемні питання, пов'язані з розвитком понятійного апарату та теоретичних засад кібероборони, системно не розглядалися. У зв'язку із цим актуальним є питання аналізу стану теоретичних засад кібероборони України та визначення перспектив їхнього розвитку.

Мета статті полягає в аналізі та розвитку понятійного апарату з питань кібероборони в Україні та формування пропозицій щодо створення кіберсил в Україні з урахуванням досвіду провідних країн НАТО.

Викладення основного матеріалу дослідження. Питання розроблення теоретичних засад кібероборони держави стало особливо актуальним у 2016 р., коли в березні була прийнята Стратегія кібербезпеки України [9] (далі – Стратегія-2016), у котрій дане поняття кібероборони, під якою розуміються заходи з підготовки держави до відбиття воєнної агресії в кіберпросторі, а Міністерство оборони України та Генеральний штаб Збройних Сил України визначені головними суб'єктами з кібероборони.

Подальший розвиток теоретичних засад кібероборони держави відбувся у 2017 р., коли в жовтні був прийнятий Закон України «Про основні засади забезпечення кібербезпеки України» [10] (далі – Закон про

Кібербезпека

– захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі (пункт 5 статті 1)

Кіберзахист

– сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем (пункт 7 статті 1)

Кібероборона

– сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії (пункт 10 статті 1)

Рис. 3. Система нових понять у сфері кібербезпеки

кібербезпеку), у якому вперше законодавчо визначені такі терміни, як кібербезпека, кіберзахист та кібероборона (рис. 3).

Аналіз цих понять показує, що,

- по-перше, кібербезпека є властивістю держави захищати інтереси як людини (громадянина, суспільства), так і держави під час використання кіберпростору;
- по-друге, кіберзахист та кібероборона є сукупністю заходів у різних сферах інтересів людини (громадянина, суспільства) та держави, які здійснюються в кіберпросторі;
- по-третє, кібербезпека, кіберзахист та кібероборона тісно пов'язані між собою в кіберпросторі, при цьому кіберзахист і кібероборона – це сукупність різних заходів, спрямованих на забезпечення різних складових кібербезпеки;
- по-четверте, в понятті кібероборони розширено та деталізовано сукупність заходів з різних сфер людської діяльності, які здійснюються в кіберпросторі.

Принципово важливим є те, що статтю 3 Закону України «Про оборону України» доповнено новим абзацом про те, що підготовка держави до оборони має охоплювати кібероборону (активний кіберзахист) для захисту суверенітету держави, запобігання збройному конфлікту та відсічі збройній агресії [11].

Модель взаємозв'язків складових кібербезпеки, побудована за результатами стислого аналізу Стратегії-2016 та Закону про кібербезпеку, свідчить про те, що кібербезпека, кіберзахист і кібероборона є значною мірою різними за змістом, інтересами та заходами в кіберпросторі України (рис. 4).

З моделі взаємозв'язків складових кібербезпеки видно, що в широкому розумінні кібероборона здійснюється в інтересах держави шляхом виявлення, запобігання та нейтралізації реальних і прогнозованих загроз у кіберпросторі та спрямована на захист суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсічі збройній агресії.

Указом Президента України № 447/2021 «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» від 26 серпня 2021 року була затверджена нова редакція Стратегії кібербезпеки України. Принципово важливим у цьому документі стало те, що першою стратегічною ціллю у формуванні потенціалу стримування визначено дієву кібероборону, для досягнення якої Україна має створити і забезпечити розвиток підрозділів з повноваженнями ведення збройного протистояння в кіберпросторі, сформувати модель функціонування та застосування кібервійськ, а також забезпечити ефективну взаємодію під час здійснення заходів з кібероборони [1].

У Стратегії кібербезпеки України система кібероборони держави є складовою національної системи кібербезпеки та має будуватися на засадах стримування, кіберстійкості та взаємодії. При цьому стратегічною ціллю створення нової національної системи кібербезпеки України є створення дієвої кібероборони (ціль С.1, Стратегія кібербезпеки України).

Ієрархія формування нової якості Національної системи кібербезпеки, яка охоплює виклики та загрози кібербезпеці України, стратегічні цілі та засади

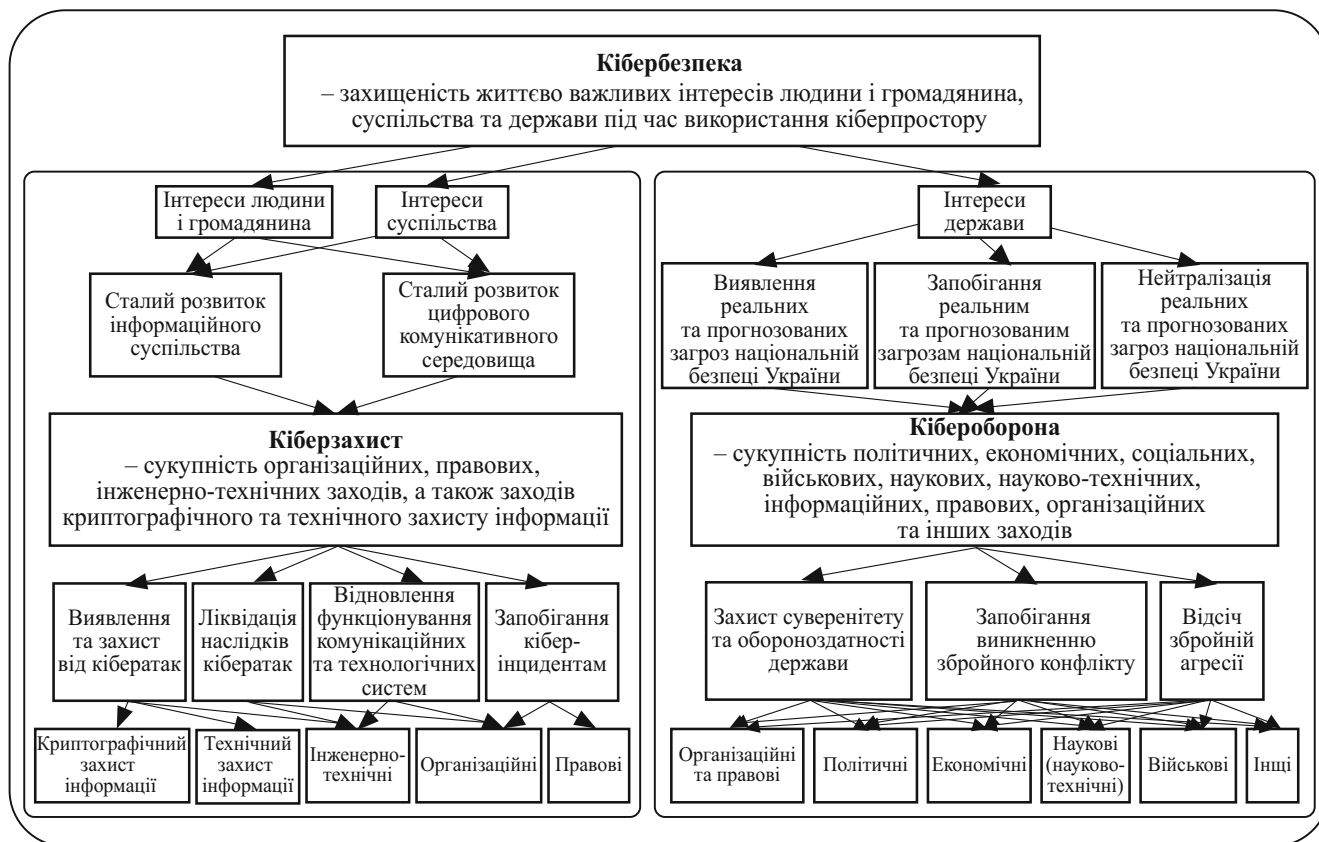


Рис. 4. Модель взаємозв'язків складових кібербезпеки

створення, а також суб'єкти забезпечення кібербезпеки наведена на *рисунку 5*. Аналіз рисунку показує, що в умовах мілітаризації кіберпростору та розвитку кіберзброї дієва кібероборона має передусім захищати від застосування кіберзброї, а також протидіяти кібершпигунству і кібертероризму. При цьому основними суб'єктами кібероборони є Міністерство оборони України, Генеральний штаб Збройних Сил України та Державна служба спеціального зв'язку та захисту інформації України.

Виходячи з основних положень воєнної науки, спираючись на визначення понять з кібероборони, наведені в законах України та нормативно-правових документах, дамо визначення основних категорій та понять з питань кібероборони.

Як відомо, кібероборона передбачає кібердії оборонного характеру, спрямовані на відсіч воєнній (збройній) агресії в кіберпросторі. Тому під агресією в кіберпросторі розумітимемо пряме або непряме застосування кіберпідрозділами іноземних держав кіберозброєння в кіберпросторі іншої держави. У результаті агресії в кіберпросторі між державами може виникнути таке явище, як війна у кіберпросторі, тобто кібервійна.

Специфічним змістом кібервійни є кіберборотьба, сутність якої полягає в організованому застосуванні

кібервійськ та кіберпідрозділів розвідувальних і спеціальних служб у кіберпросторі для відсічі агресії в кіберпросторі. Оскільки агресія в кіберпросторі здійснюється приховано без оголошення загального стану війни між державами, то має місце конфлікт у кіберпросторі, або кіберконфлікт.

Кіберконфлікт є різновидом кіберборотьби, яка полягає в організованому застосуванні кібервійськ для досягнення визначених цілей у кіберпросторі. Характер, способи та масштаби кіберборотьби залежать від розвитку кіберозброєння та відбуваються відповідно до законів війни. Так, зміни у способах кіберборотьби відбуваються стрибками залежно від кількості нового кіберозброєння. Накопичення кількісних змін приводить до якісних змін. У процесі розвитку засобів та способів кіберборотьби виникають протиріччя між ними, оскільки засоби кіберозброєння розвиваються швидше, ніж способи та форми кіберборотьби. А це врешті-решт призводить до появи нових досконаліших форм і способів кіберборотьби.

Протиріччя, які виникають під час ведення дій у кіберпросторі, спричинені впливом різних засобів кіберозброєння, які застосовують сторони кіберконфлікту (або кібервійни). Такі дії в кіберпросторі можуть призвести до порушення управління військами. Подолання

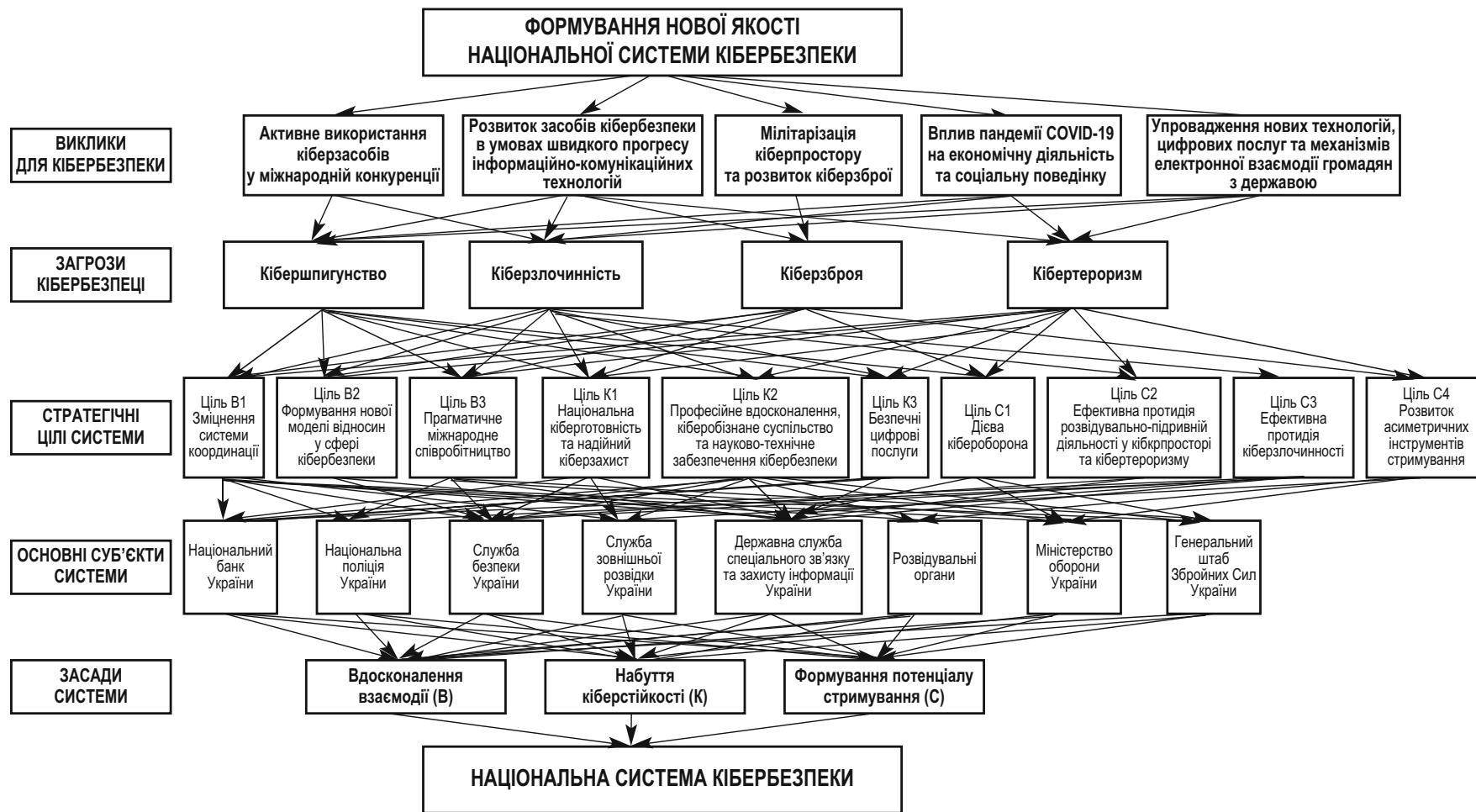


Рис. 5. Ієрархія формування Національної системи кібербезпеки

або зменшення негативних наслідків таких дій противника залежить від якості кіберозброєння та організації кіберборотьби, а також розвитку теоретичних засад кібероборони.

Бойові дії в кіберпросторі – це організоване застосування кіберсил та кіберзасобів з метою нанесення втрат і протидії противнику в кіберпросторі. При цьому під кіберсилами розуміють кіберпідрозділи військових формувань (кібервійська) та кіберпідрозділи розвідувальних і спеціальних служб, а під кіберзасобами – кіберозброєння.

Бойові дії в кіберпросторі можуть бути оборонними, наступальними чи агресивними. У разі агресивних дій у кіберпросторі ураженню піддаються також цивільні та невійськові об'єкти критичної інфраструктури.

На сучасному етапі основними формами дій у кіберпросторі є кібероперація та кіберудар, а способами дій у кіберпросторі – кібернаступ та кібероборона. Під кібернаступом розуміються наступальні дії в кіберпросторі, а під кіберобороною – оборонні дії в кіберпросторі.

Кібероперація – це сукупність узгоджених та взаємопов'язаних за ціллю, місцем та часом впливу кіберударів, які проводяться за єдиним задумом та планом для вирішення завдань у кіберпросторі. Кіберудар – це короточасний вплив на кіберпростір противника із застосуванням кіберозброєння. При цьому кібератака є вирішальним етапом кіберудару.

Кібернаступ проводиться з метою нанесення втрат противнику в кіберпросторі та здійснюється в рамках наступальних дій сил оборони у взаємодії з підрозділами розвідувальних і спеціальних служб. Кібернаступ може проводитися кібервійськами самостійно.

Кібернаступ має дві фази: підготовки та ведення.

Підготовка кібернаступу охоплює: прийняття рішення та планування кібернаступу; постановку завдань кібервійськам та організація взаємодії; групування кіберсил та кіберзасобів; усебічне забезпечення дій у кіберпросторі.

Ведення кібернаступу охоплює нанесення кіберударів по об'єктах кіберпростору противника із застосуванням наявного кіберозброєння.

Кібероборона здійснюється кібервійськами з метою відбиття кібернаступу противника та захисту об'єктів кіберпростору. При цьому кібероборона має свою побудову, яка охоплює: угруповання кіберсил та кіберзасобів, систему кіберзахисту, систему нанесення кіберударів.

Кібероборона, як і кібернаступ, має дві фази: підготовки та ведення.

Підготовка кібероборони охоплює: постановку завдань кібервійськам та планування кібероборони; побудову кібероборони; організація взаємодії; підготовку кібервійськ до дій та всебічне забезпечення оборонних дій у кіберпросторі.

Ведення кібероборони охоплює нанесення кіберударів по об'єктах кіберпростору противника із застосуванням наявного кіберозброєння та відновлення об'єктів кіберпростору, які зазнали ураження.

У провідних країнах світу основою системи кібероборони є новий вид збройних сил – кіберсили (кібервійська) (табл. 1).

Кіберсили НАТО складаються з окремих ключових елементів, інтегрованих у загальну структуру оборони Альянсу. Основні складові кіберсил НАТО розкриті нижче.

1. Головним центром для координації зусиль у сфері кібербезпеки є Центр кібероперацій (Cyber Operations Center, CyOC), основна місія якого полягає в захисті цифрових мереж НАТО від кібератак, забезпеченні безперебійної роботи військових і цивільних функцій [12].

2. Центр передового досвіду у сфері кіберзахисту (CCDCOE) (м. Таллін, Естонія), який займається навчанням, дослідженнями та аналізом стратегій у сфері кіберзахисту. Центр організує щорічні кібернавчання, такі як «Locked Shields» і «Crossed Swords», які є найбільшими у світі [13].

Кіберсили НАТО є комплексною мережею організацій, яка охоплює як військові структури, так і партнерства з приватними й академічними установами, спрямовані на забезпечення колективного кіберзахисту Альянсу та партнерів.

Кіберсили збройних сил країн НАТО об'єднують військових та цивільних фахівців з проведення наступальних чи оборонних дій у кіберпросторі. При цьому вони мають різні системи організації, управління, комплектування та підготовки. Коротко розглянемо їх.

США. Кіберсили США [14] організовані під керівництвом U.S. Cyber Command (USCYBERCOM), який відповідає за оборону в кіберпросторі, підтримку військових операцій і національні інтереси в глобальній мережі, та кіберпідрозділ Cyber National Mission Force (CNMF), котрий проводить кібероперації як частину місії із захисту США, включно з міжнародними операціями «hunt forward» для протидії кіберзагрозам у країнах НАТО.

Основні складові кіберсил США містять п'ять ключових команд і 133 кіберпідрозділи. Команди входять до складу: 16-ї повітряної армії (16th Air Force) для кібероперацій у повітряній сфері; армійського кіберкомандування (Army Cyber Command) для підтримки сухопутних операцій; морського кіберкомандування (Fleet Cyber Command) для забезпечення кібероперацій на морі та морської кіберкоманди (Marine Corps Cyberspace Command) для забезпечення кіберзавдань корпусу морської піхоти.

Велика Британія (UK Cyber Forces). UK Cyber Forces складаються з декількох організацій і підрозділів, що працюють у взаємодії для захисту національних

Таблиця 1

Склад кіберсил провідних країн НАТО

Країна та рік утворення	Основний орган управління та основні складові кіберсил	Призначення складових кіберсил
Кіберсили США	1. U.S. Cyber Command (USCYBERCOM)	
	1.1. Cyber Mission Force (CMF) охоплює 133 кіберкоманди, зокрема:	• основна структура для проведення кібероперацій
	13 національних кіберкоманд (Cyber National Mission Teams)	• виконують незалежні операції для кіберзахисту США, ідентифікуючи кіберзагрози та захищаючи від кібератак
	27 бойових кіберкоманд (Cyber Combat Mission Teams)	• здійснюють підтримку бойових дій
	68 команд з кіберзахисту (Cyber Protection Teams)	• здійснюють захист мереж міністерства оборони США
	25 команд з кіберпідтримки (Cyber Support Teams)	• здійснюють інформаційно-аналітичне забезпечення інших підрозділів
	1.2. Cyber National Mission Force (CNMF)	• проводить кібероперації як частину місії із захисту США та протидії кіберзагрозам у країнах НАТО
Кіберсили Великої Британії (2020)	1. Національний центр кібербезпеки (National Cyber Security Centre, NCSC)	
	1.1. Міністерство оборони (MoD)	• забезпечує стратегічну підтримку операцій NCF; • інтегрує кібернетичні та електромагнітні операції з іншими військовими доменами
	1.2. Центр урядового зв'язку (GCHQ)	• фокусується на розвідувальній діяльності
Кіберсили Німеччини (2017)	1. Служба кібер- та інформаційного простору (Cyber- und Informationsraum, CIR)	
	1.1. Центральне командування CIR	• зосереджене на створенні єдиної оперативної команди для координації як внутрішніх, так і зовнішніх операцій Німеччини в кіберпросторі
	1.2. Підрозділи кіберзахисту (Cyber Defense Units)	• безпосередній захист IT-інфраструктури міністерства оборони, реагування на кіберзагрози та відновлення роботи після атак; • технічний моніторинг, виявлення та аналіз загроз
	1.3. Розвідувальні підрозділи (Cyber Intelligence)	• моніторинг кіберпростору, збирання розвідувальної інформації про загрози
	1.4. Центр військової IT-компетенції (Bundeswehr IT Center of Excellence)	• підготовка та навчання кадрів, дослідження нових технологій і підтримка впровадження сучасних IT-рішень у кіберзахисті
	1.5. Підрозділи інформаційних операцій	• інформаційна безпека та протидія дезінформації, особливо у військових контекстах; • підтримка операцій в інформаційному полі та розвиток стратегій інформаційного впливу
	1.6. Підрозділи інтеграції з НАТО з питань кібероборони	• активна співпраця з іншими країнами НАТО, зокрема в рамках Спільного центру передового досвіду з кібероборони (NATO CCDCOE) в Естонії
Кіберсили Франції	1. Командування COMCYBER (Cyber Defense Command)	• здійснення захисту інформаційних систем для запобігання, виявлення та протидії кібератакам; • захист військових інформаційних систем; • розробка, планування та проведення оборонних та наступальних військових операцій, операцій з впливу в кіберпросторі; • оперативна підготовка збройних сил у кіберпросторі через національні чи міжнародні тренування та навчання; • узгодженість моделі кіберзахисту та її загальна координація (кадрова політика, технічні потреби, розробка доктрини); • розвиток та управління резервом оперативного та цивільного кіберзахисту

Країна та рік утворення	Основний орган управління та основні складові кіберсил	Призначення складових кіберсил
	1.1. Штаб кіберзахисту (EM-CYBER)	<ul style="list-style-type: none"> • проведення операцій з кіберзахисту: командування кіберзахисту розробляє, планує та проводить військові операції з кіберзахисту і відповідає за оборону та захист інформаційних систем міністерства збройних сил, за винятком систем Генерального директорату зовнішньої безпеки (DGSE) і Директорату розвідки та оборонної безпеки (DRSD); • формує Стратегію кіберзахисту: командування кіберзахисту координує внески збройних сил і спільних організацій у національну та міжнародну політику кіберзахисту, зокрема для розробки та реалізації планів співпраці; це також забезпечує узгодженість моделі кіберзахисту міністерства та її загальну координацію; • розвиток спроможності: командування кіберзахисту сприяє розробці кадрової політики кіберзахисту, координації визначення конкретних технічних потреб кіберзахисту і розвитку та управління резервом кіберзахисту
	1.2. Армійська групи кіберзахисту (GCA)	<ul style="list-style-type: none"> • консолідація континууму між кіберзахистом та обороною шляхом сприяння синергії між цими сферами і передача досвіду між окремими підрозділами; • управління інформацією, людськими ресурсами (набір – цивільні, діючі військові та резервні, навчання, канцелярія) та кіберзахистом
	1.2.1. Центр аналізу кіберзагроз (CALID)	<ul style="list-style-type: none"> • координує військову кібероборону, відповідає за організацію як оборонних, так і наступальних операцій у кіберпросторі, забезпечуючи захист військових систем і підтримку стратегічних місій, технічний аналіз кіберзагроз, координацію оборонних заходів і впровадженням нових технологій
	1.2.2. Центр аудиту безпеки інформаційних систем (CASSI)	<ul style="list-style-type: none"> • національний центр, аудиторська місія якого охоплює дві сфери: безпеку інформаційних систем (ISS) і компрометацію паразитних сигналів (SPC)
	1.2.3. Об'єднаний головний узгоджувальний центр (CHPI)	<ul style="list-style-type: none"> • забезпечення безпеки інформаційних систем Міністерства Збройних Сил України протягом терміну їх експлуатації
	1.2.4. Центр оперативної підготовки кіберзахисту (C2PO)	<ul style="list-style-type: none"> • оперативна підготовка кібервинищувачів, спеціальне навчання кіберспеціалістів

інтересів у кіберпросторі, забезпечення обороноздатності та реалізації наступальних кібероперацій. Основними компонентами кіберсил є Національні кіберсили (National Cyber Force, NCF), створені 2020 р., які об'єднують підрозділи Міністерства оборони (MoD) та Центру урядового зв'язку (GCHQ) [15].

Національний центр кібербезпеки (National Cyber Security Centre, NCSC) орієнтований на захист критичної інфраструктури, підвищення стійкості до кіберзагроз та співпрацю з приватним сектором. Він забезпечує регіональну підтримку через надання стратегічних консультацій і допомогу у відбитті кібератак.

Німеччина. Кіберсили Німеччини є частиною Бундесверу та представлені Службою кібер- та інформаційного простору (Cyber- und Informationsraum, CIR), створеної 2017 р. для захисту цифрових інфраструк-

тур, боротьби з кіберзагрозами, забезпечення інформаційної безпеки та управління розвіданими. Головним органом управління є Центральне управління CIR, зосереджене на єдиному оперативному управлінні як внутрішніми, так і зовнішніми операціями Німеччини в кіберпросторі.

Нині розглядається питання щодо трансформації кіберсил у новий четвертий вид збройних сил Німеччини, поряд із сухопутними військами, військово-морськими та військово-повітряними силами.

Франція. Кіберсили Франції складаються з декількох ключових компонентів, що діють під егідою збройних сил. Їхньою основною метою є захист національної безпеки в кіберпросторі, розробка наступальних та оборонних кіберзасобів, а також міжнародне співробітництво у сфері кібероборони. Кіберсили Франції

складаються з [16]: головного органу COMCYBER (Cyber Defense Command), який координує кібероборону та відповідає за організацію як оборонних, так і наступальних операцій у кіберпросторі, забезпечуючи захист військових систем і підтримку стратегічних місій. Для виконання своїх місій COMCYBER має дві структури:

- Штаб кіберзахисту (EM-CYBER);
- Армійську групу кіберзахисту (GCA).

EM-CYBER розробляє, планує та проводить військові операції кіберзахисту, формує стратегію кіберзахисту та розвиває спроможності з кібероборони та кіберзахисту.

GCA призначена для консолідацію континууму між кіберзахистом та обороною шляхом сприяння синергії між цими сферами і передачі досвіду. GCA об'єднує чотири технічні центри COMCYBER:

- центр аналізу оборонної комп'ютерної війни (CALID);
- центр аудиту безпеки інформаційних систем (CASSI);
- спільний головний центр акредитації (CHPI);
- центр підготовки до кібероперацій (C2PO).

COMCYBER взаємодіє з Національним агентством з безпеки інформаційних систем (ANSSI), яке здійснює захист критичної інфраструктури Франції, а також сприяє кібербезпеці в державному і приватному секторах. ANSSI також виконує роль консультанта для оборонних сил у сфері захисту інформаційних систем.

Аналіз *таблиці 1* показує, що кіберсили провідних країн НАТО мають два варіанти організації. Перший варіант передбачає входження кіберсил у склад національних збройних сил та взаємодію їх із цивільними кіберпідрозділами (США, Німеччина). Другий варіант – об'єднання в окремій національній структурі військових та цивільних кіберпідрозділів (Велика Британія, Франція). При цьому незалежно від варіанта організації кожна країна НАТО зберігає відповідальність за національний кіберзахист, але водночас здійснює обмін даними, координацію навчань і розробку спільних стратегій кібероборони.

Україна. Кіберсили України поки перебувають на етапі створення [17]. Відповідно до урядових планів, кіберсили України мають бути окремим родом військ у складі Збройних Сил України. До складу кіберсил мають входити як оперативні підрозділи для негайного реагування, так і аналітичні структури для розробки довгострокових стратегій кібероборони. Крім того, передбачається тісна співпраця з національними та міжнародними організаціями, що займаються питаннями кібербезпеки, зокрема в рамках НАТО. Їхніми основними завданнями стане забезпечення кіберзахисту військових інформаційних систем, відбиття кібератак,

проведення наступальних кібероперацій та моніторинг кіберпростору. Це відповідає світовим тенденціям, де кіберсили стали важливим елементом військових структур багатьох країн, таких як США та Німеччина, які вже мають розвинені кіберкомандування для реалізації подібних функцій.

Висновки, пропозиції та рекомендації

Аналіз законів України, в яких викладені основні поняття з питань кібероборони, показує, що кібероборона є критично важливим елементом кібербезпеки та національної безпеки України загалом, оскільки розвиток сучасних кібертехнологій створює нові загрози для політичної, економічної та військової сфер. Основними загрозами є кіберзброя наступального призначення, кібершпигунство, кібертероризм та кіберзлочинність. При цьому модель кібероборони потребує більшого інтегрування з військовими та цивільними компонентами.

Аналіз досвіду країн НАТО у формуванні кіберсил показує, що існують два підходи: інтеграція кіберсил у збройні сили (США, Німеччина) або створення окремих національних структур, які об'єднують військові та цивільні кіберпідрозділи (Велика Британія, Франція). Тому, виходячи із цього досвіду, доцільно інтегрувати кібероборону в багаторівневу систему кібербезпеки України. При цьому розробка теоретичних засад і законодавчих актів має стати основою для створення дієвих кібервійськ. Для цього необхідно:

- сформулювати окремий рід військ у складі Збройних Сил України, який міститиме оперативні та аналітичні підрозділи;
- розробити нові законодавчі акти або доповнити існуючі для регулювання діяльності кібероборони, враховуючи міжнародний досвід;
- посилити співпрацю з НАТО, зокрема в рамках програм, які підтримують обмін даними, навчання та спільну розробку кіберзасобів;
- розвивати програми підготовки кадрів з кібербезпеки та залучати новітні технології, зокрема штучний інтелект, для підвищення ефективності кібероборони;
- створити єдиний координаційний орган, який відповідатиме за управління всіма аспектами кібероборони;
- зосередити увагу на розробці форм та способів ведення кібероперацій, наприклад таких, як кібероборона, кіберудар, кібернаступ та управління конфліктами в кіберпросторі;
- забезпечити фінансування для розробки нових кіберзасобів і підтримки дослідницьких програм у сфері кібербезпеки;
- упровадити систему моніторингу та аналізу кіберзагроз у реальному часі для своєчасного реагування.

Перелік літератури

1. Стратегія кібербезпеки України [Електронний ресурс] : затверджена Указом Президента України № 447/2021 від 26 серпня 2021 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/447/2021#n7>.
2. Cyber defence [Електронний ресурс] // НАТО. – Режим доступу : https://www.nato.int/cps/en/natohq/topics_78170.htm.
3. International Conference on Cyber Conflict – CyCon [Електронний ресурс] // CCDCOE. – Режим доступу : <https://ccdcoe.org/cycon>.
4. Cyber Coalition: NATO's Flagship Cyber Exercise [Електронний ресурс] // NATO Allied Command Transformation. – Режим доступу : <https://www.act.nato.int/activities/cyber-coalition>.
5. Cyber Security Conference [Електронний ресурс] // NMIOTC – NATO Maritime Interdiction Operational Training Centre – Greece. – Режим доступу : <https://nmiotc.nato.int/transformation/conferences/cyber-security-conference>.
6. Locked Shields 2024 Sets the Stage for Advancing Global Cyber Defence [Електронний ресурс] // CCDCOE. – Режим доступу : <https://ccdcoe.org/news/2024/locked-shields-2024-sets-the-stage-for-advancing-global-cyber-defence>.
7. New Report on National Cybersecurity Governance: Ukraine [Електронний ресурс] // CCDCOE. – Режим доступу : <https://ccdcoe.org/news/2024/new-report-on-national-cybersecurity-governance-ukraine>.
8. Зміцнюючи національну кібербезпеку [Електронний ресурс] // Національний кластер кібербезпеки. – Режим доступу : <https://cybersecuritycluster.org.ua>.
9. Стратегія кібербезпеки України [Електронний ресурс] : затверджена Указом Президента України № 96/2016 від 15 березня 2016 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/96/2016/ed20160315#Text>.
10. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України № 2163-VIII від 5 жовтня 2017 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
11. Про оборону України [Електронний ресурс] : Закон України № 1932-XII від 6 грудня 1991 р. // Верховна Рада України. Законодавство України. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/1932-12#Text>.
12. NATO Cyber Operation Centre [Електронний ресурс] // NATO Rapid Deployable Corps Italy. – Режим доступу : <https://nrdc-ita.nato.int/operations/allied-reaction-force/nato-cyber-operation-centre>.
13. Exercises [Електронний ресурс] // CCDCOE. – Режим доступу : <https://ccdcoe.org/exercises/>.
14. Lonergan E. United States Cyber Force: A Defense Imperative [Електронний ресурс] / E. Lonergan, M. Montgomery // FDD. – Режим доступу : <https://www.fdd.org/analysis/2024/03/25/united-states-cyber-force>.
15. The National Cyber Force: Directions and Implications for UK – Analysis [Електронний ресурс] / D. Steed ; Elcano Royal Institute // Eurasia Review. – Режим доступу : <https://www.eurasiareview.com/12022021-the-national-cyber-force-directions-and-implications-for-uk-analysis>.
16. Le commandement de la cyberdéfense (COMCYBER) [Електронний ресурс] // Ministère des Armées. Commandement de la cyberdéfense. – Режим доступу : <https://www.defense.gouv.fr/comcyber/commandement-cyberdefense-comcyber>.
17. Проект Закону України про Кіберсили Збройних Сил України [Електронний ресурс] : № 12349 від 19 грудня 2024 р. // Верховна Рада України. Законопроекти. – Режим доступу : <https://itd.rada.gov.ua/billinfo/Bills/Card/45453>.

DOI 10.33099/2618-1614-2025-28-1-47-53

УДК 355.433

М. В. Коваль,*доктор військових наук,
Національний університет оборони України,***В. В. Машталір,***доктор історичних наук, професор,
Національний університет оборони України,***О. М. Загорка,***доктор військових наук, професор,
Національний університет оборони України*

Оцінювання результатів війни на виснаження: методичні положення

Стратегія виснаження в сучасній збройній боротьбі є основною концепцією досягнення цілей війни. Результати війни на виснаження залежать насамперед від воєнних потенціалів протидіючих сторін, які поділяються на воєнно-економічні, духовні, воєнно-політичні, військові науково-технічні, бойові потенціали (складові). У статті для оцінювання результатів війни запропонована методика, яка ґрунтується на врахуванні співвідношень факторів, що впливають на складові воєнних потенціалів сторін. У методиці оцінювання результатів війни здійснюється шляхом порівняння (ранжирування) категорій оцінки, наприклад перемога, поразка тощо, які задаються особою, котра приймає рішення. Для ранжирування (визначення пріоритетів) категорій оцінки результатів війни застосовується метод аналізу ієрархій, у якому використовується чотирирівнева ієрархія розв'язання задачі: мета – складові воєнного потенціалу – фактори – категорії (альтернативи). Методика дає змогу визначити пріоритети категорій оцінки результатів війни на виснаження на поточний час і прогнозований період залежно від обставин, що складаються, для прийняття органами державного і військового управління відповідних рішень.

Ключові слова: війна на виснаження, категорії оцінки результатів, воєнний потенціал, пріоритети, метод аналізу ієрархій.

© М. В. Коваль, В. В. Машталір, О. М. Загорка, 2025

Військово-політичним керівництвом держави під час війни здійснюється аналіз її характеру й оцінюються можливі результати. За результатами оцінювання приймаються найважливіші стратегічні рішення, від яких залежить цілісність території країни, її незалежність, авторитет на міжнародному рівні та найголовніше – життя людей.

Залежно від обставин, що складаються, а також потрібних термінів прийняття рішень, оцінювання результатів війни може здійснюватись як на поточний час, так і на прогнозований період війни.

У воєнній стратегії під час аналізу характеру війн зазвичай розглядають дві стратегічні концепції: стратегію руйнування (розпорошення) і стратегію виснаження. У статті [1] відзначається, що в сучасній війні перемога за допомогою стратегії руйнування практично неможлива через стійкість держав і суспільств, а також їхніх збройних сил (ЗС). Будь-яка війна, найімовірніше, завершиться як війна на виснаження, де сукупні цивільні та військові ресурси держави та її союзників урешті-решт визначають результат. До того ж незмірно підвищується роль економіки як бази ведення сучасної війни.

Стратегія виснаження спрямована на послідовне знищення воєнного потенціалу противника, від якого залежить результат війни. На воєнний потенціал впливають багато факторів (економічних, політичних, духовних, науково-технічних, бойових), урахування яких під час оцінювання результатів війни на виснаження потребує дослідження.

У праці [2] наведений опис воєнного конфлікту на якісному (вербальному) рівні відповідно до моделі змінювання воєнних потенціалів сторін під час війни. Війна протилежною стороною вважається програною за умови такого збитку, який становить її воєнний потенціал нижче можливого для продовження війни. Проте кількісне визначення такого критерію залишається відкритим.

Крім того, кількісне оцінювання в абсолютних одиницях воєнного потенціалу утруднене, а в більшості випадків неможливе, тому в роботі [3] пропонується оцінювати рівень воєнного потенціалу відносно противника за лінгвістичними змінними, які вважаються альтернативами. Для визначення пріоритетів рівнів воєнного потенціалу використовується метод аналізу ієрархій (МАІ) [4]. Це дало змогу в статті [3] визначити ймовірність відбиття агресії з використанням логічної функції [5]. Зазначений показник характеризує можливість держави щодо відбиття агресії, але не дає чіткого розуміння про можливі результати війни на виснаження, які можна вважати альтернативами.

Війна на виснаження докладно викладена в теорії та практиці воєнної стратегії, тому як явище добре

зрозуміла емпірично. Проте оцінювання результатів такої війни є достатньо складною важко формалізованою задачею, яка потребує розв'язання.

Метою статті є розроблення методики оцінювання результатів війни на виснаження.

Починаючи війну, агресор, як правило, матиме перевагу у воєнному потенціалі. За такої умови на початок війни може застосовуватися стратегія руйнування, яка передбачає швидку військову перемогу за допомогою проведення блискавичних вирішальних операцій для досягнення цілей війни. У сучасній війні, як зазначалося раніше, досягнення цілей війни за допомогою застосування стратегії руйнування є проблематичним, тому стратегія руйнування в подальшому може перетворюватися на стратегію виснаження.

Стратегія виснаження полягає у знищенні всього потенціалу противника для ведення війни до такої міри, за якої він був би не здатний чинити опір. Це може включати підлив виробництва промисловості, зокрема знищення об'єктів оборонно-промислового комплексу, ресурсів, логістики, критичної інфраструктури, виснаження ЗС, підлив народної волі до опору тощо. Отже, виснаження – це стратегічне послаблення здатності противника вести війну не лише шляхом завдання втрат військам, а й шляхом послаблення економіки, підливу політичної волі, протидії допомоги союзників (партнерів). Стратегічне виснаження відбувається в усіх сферах суспільства, а також у ЗС, як накопичений результат втрат, руйнувань та порушень поставок і стратегічних комунікацій, знищення резервів тощо [1]. У війні на виснаження значна роль належить стійкості економіки, зокрема оборонної промисловості та інфраструктури забезпечення життєдіяльності країни.

Порівняно з війною, в якій використовується стратегія руйнування, війна на виснаження має деякі особливості. До основних з них належать:

- більша тривалість війни, що спричиняє збільшення втрат воєнного потенціалу держави (особового складу ЗС, озброєння та військової техніки, об'єктів економіки тощо), а також збільшення витрат на ведення війни;
- операції (бої) мають обмежений (частковий) характер, вирішальне значення має накопичення втрат воєнного потенціалу, зокрема втрат ЗС, а також послідовне захоплення території країни;
- разом з проведенням військових операцій (боїв) здійснюється систематичне завдання ударів з повітря, в основному балістичними, крилатими ракетами та безпілотними літальними апаратами, з метою знищення військових об'єктів, об'єктів промисловості, інфраструктури, зокрема енергетики на всій території країни;
- на окремих ділянках фронту війна може мати позиційний характер;

- урахування тривалості війни, під час її ведення може здійснюватися постачання озброєння союзниками (партнерами), а також можуть застосовуватися санкції щодо послаблення воєнно-економічного потенціалу агресора, заходи політичного тиску на рівні світових безпекових організацій;

- здійснення безперервного інформаційного впливу на ЗС, населення країни щодо даремності опору, переконачування поточних результатів війни;

- під час війни може здійснюватися продовження переведення економіки країни на воєнні рейки, зокрема переміщення і створення нових підприємств.

З аналізу сутності та особливостей війни на виснаження випливає, що її результат залежить від стану воєнного потенціалу держави і наявності збережених об'єктів критичної інфраструктури на момент оцінювання.

У роботах [2, 3] та інших публікаціях воєнний потенціал держави поділяють на такі складові:

- воєнно-економічний потенціал;
- духовний потенціал;
- воєнно-політичний потенціал;
- військовий науково-технічний потенціал;
- бойовий потенціал.

На кожен складову воєнного потенціалу впливає сукупність факторів, які залежать від обстановки, що складається, та умов ведення війни. Подібна сукупність факторів урахувалася під час визначення ймовірності відбиття агресії [3]. Проте реалії війни, що триває, потребують їх уточнення (корегування), а також під час оцінювання результатів війни на виснаження мають урахувати нові фактори.

Ураховуючи труднощі в кількісному оцінюванні збитку воєнного потенціалу, пропонується критерій програшу у війні, як це наведено в роботі [2], не використовувати, а здійснювати порівняння можливих результатів війни, тобто визначати їхні пріоритети.

Для оцінювання результатів війни пропонується використовувати z категорій $R_k (k = 1, z)$, які зумовлюються наслідками, що проявилися на момент оцінювання. За сутністю такі категорії є категоріями якості. Як приклад, категоріями оцінювання результатів війни на виснаження можна вважати: перемогу (R_1); часткову перемогу (R_2); незмінність положення (R_3); часткову поразку (R_4); поразку (R_5). Під час їх порівняння, тобто визначення пріоритетів, категорії розглядаються як альтернативи.

Є очевидним, що пріоритети категорій оцінки результатів війни залежать від співвідношення воєнних потенціалів протиборчих сторін, що визначається співвідношеннями складових їхніх потенціалів і врешті-решт співвідношеннями факторів, що впливають на ці складові. Тому під час оцінювання результатів війни

на виснаження розглядається n складових воєнного потенціалу $C_i (i = \overline{1, n})$ та для кожної складової m_i факторів $F_{ji} (j = \overline{1, m_i})$, тобто задача стає ієрархічною.

Ураховуючи невизначеність впливу співвідношень факторів протидіючих сторін на оцінювання результатів війни, доцільно для порівняння категорій R_k використовувати МАІ [4].

Модель визначення пріоритетів (ранжирування) категорій оцінки результатів війни на підставі використання МАІ має ієрархічну структуру: мета розв'язання задачі; складові воєнного потенціалу C_i ; фактори, що впливають на складові воєнного потенціалу F_{ji} ; категорії оцінки R_k . Таким чином будується чотирирівнева ієрархія розв'язання задачі (рис. 1). Залежно від обстановки, що складається, категорії оцінки результатів війни та фактори, що впливають на складові воєнного потенціалу, можуть змінюватися й доповнюватися.

Відповідно до процедури МАІ [4, 6] експертами здійснюється попарне порівняння ваг множини елементів кожного рівня ієрархії відносно елемента, який прилягає зверху до даного рівня ієрархії. Використовується дев'ятибальна шкала [4]. Отже, на кожному рівні ієрархії складаються матриці попарних порівнянь, з яких визначаються пріоритети елементів ієрархії.

Одержані пріоритети елементів ієрархії використовуються для визначення пріоритетів категорій оцінювання результатів війни.

Відповідно до моделі ранжирування категорій оцінювання результатів війни (див. рис. 1) на другому рівні ієрархії, як і в роботі [3], експерти складають одну квадратну обернено-симетричну матрицю попарних порівнянь складових воєнного потенціалу (5x5). Експерти визначають, яка складова має найбільший вплив на категорії оцінки результатів війни. З матриці визначаються пріоритети $b_i (i = \overline{1, n})$ складових воєнного потенціалу.

На третьому рівні ієрархії складаються п'ять матриць попарних порівнянь факторів, що впливають на складові воєнного потенціалу (7x7), (7x7), (6x6), (5x5), (8x8). Експерти визначають, який фактор чинить найбільший вплив на відповідну складову воєнного потенціалу. З матриць визначаються пріоритети f_{ji} впливу факторів $F_{ji} (i = \overline{1, n}, j = \overline{1, m_i})$ на складові воєнного потенціалу.

На четвертому рівні ієрархії для кожного фактора F_{ji} (усього тридцять три фактори) складається матриця (5x5). Експерти визначають, на яку категорію оцінки результатів війни найбільше впливає фактор. Під час попарного порівняння експерти враховують співвідношення факторів між протидіючими сторонами. З матриць визначаються пріоритети r_{jik} k -ї категорії, на яку

найбільше впливає j -й фактор i -ї складової воєнного потенціалу. Таким чином, вихідними даними для складання матриць четвертого рівня ієрархії є кількісне співвідношення факторів $l_{ji} = \frac{F_{ji}^H}{F_{ji}^n}$ складових нашого воєнного потенціалу F_{ji}^H і противника F_{ji}^n .

Як приклад розглянемо складання експертами матриць попарних порівнянь категорій оцінки результатів війни стосовно кожного фактора F_{ji} (четвертий рівень ієрархії). Експерти здійснюють оцінювання у вигляді відношень ω_k/ω_μ k -ї та μ -ї категорії. Вигляд матриці попарних порівнянь категорій показаний у таблиці 1.

Таблиця 1

Матриця попарних порівнянь категорій

Категорії	Категорії					
	R_1	R_2	...	R_μ	...	R_z
R_1	1	$\frac{\omega_1}{\omega_2}$...	$\frac{\omega_1}{\omega_\mu}$...	$\frac{\omega_1}{\omega_z}$
R_2	$\frac{\omega_2}{\omega_1}$	1	...	$\frac{\omega_2}{\omega_\mu}$...	$\frac{\omega_2}{\omega_z}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
R_k	$\frac{\omega_k}{\omega_1}$	$\frac{\omega_k}{\omega_2}$...	1	...	$\frac{\omega_k}{\omega_z}$
⋮	⋮	⋮	⋮	⋮	⋮	⋮
R_z	$\frac{\omega_z}{\omega_1}$	$\frac{\omega_z}{\omega_2}$...	$\frac{\omega_z}{\omega_\mu}$...	1

Компоненти власного вектора матриці визначаються за формулою [4]

$$a_k = \sqrt[z]{\frac{\omega_k \cdot \omega_k \cdot \dots \cdot \omega_k}{\omega_1 \cdot \omega_2 \cdot \dots \cdot \omega_\mu \cdot \omega_z}}, \quad k = \mu = \overline{1, z} \quad (1)$$

Ураховуючи індекси факторів, пріоритети категорій стосовно кожного фактора

$$r_{jik} = \frac{a_{jik}}{\sum_{k=1}^z a_{jik}} \quad (2)$$

Аналогічно визначаються пріоритети на другому і третьому рівнях ієрархії (див. рис. 1).

Пріоритети категорії $R_k (k = \overline{1, z})$ оцінки результатів війни визначаються за формулою

$$\Pi(R_k) = \sum_{i=1}^n b_i \sum_{j=1}^{m_i} f_{ji} r_{jik} \quad (3)$$

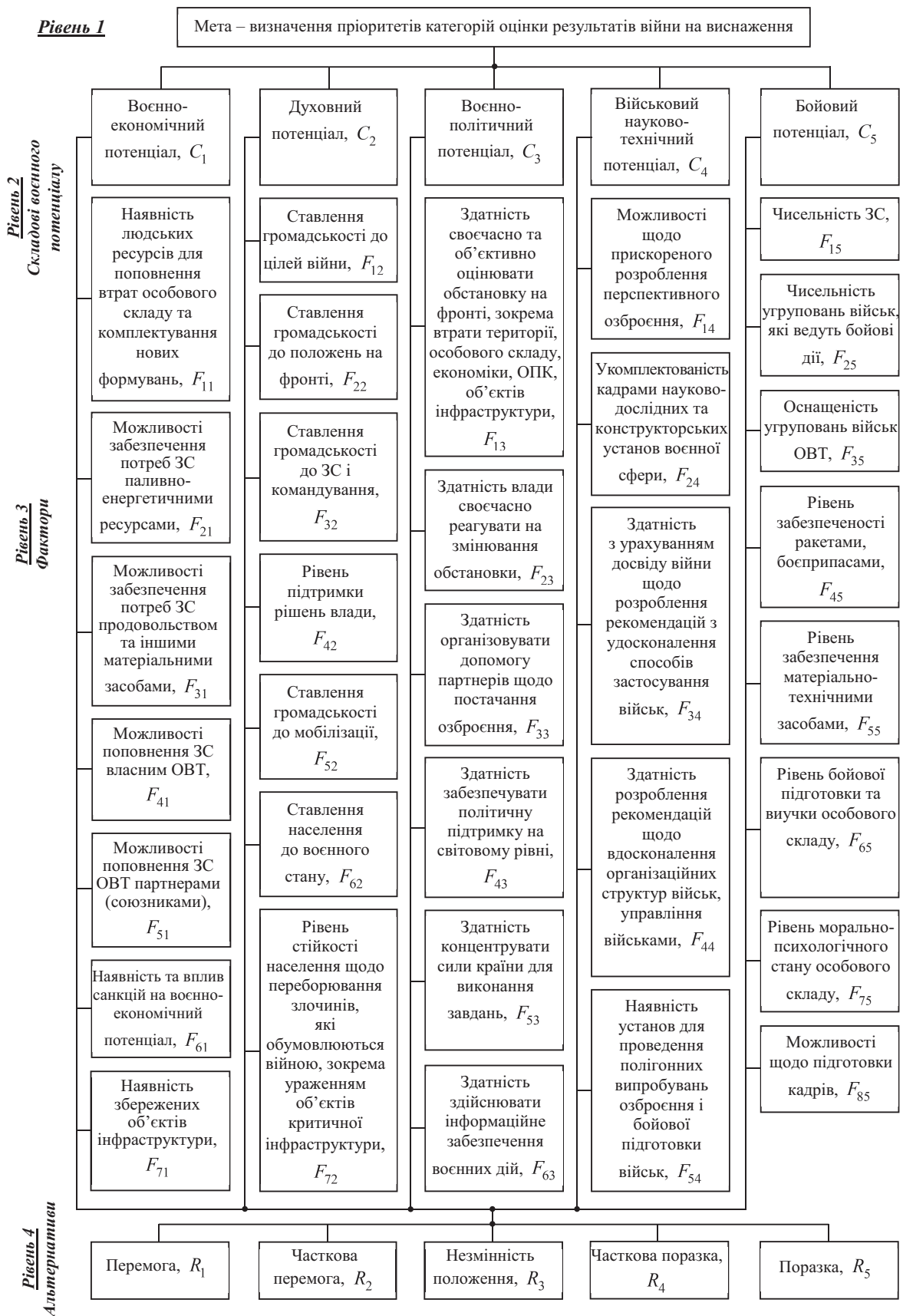


Рис. 1. Побудова моделі ранжирування категорій оцінки результатів війни на виснаження

Розгорнуті залежності для визначення категорій оцінки результатів війни відповідно до моделі ранжирування на *рисунку 1* мають вигляд:

$$\begin{aligned}
 \Pi(R_1) = & b_1(f_{11} \cdot r_{111} + f_{21} \cdot r_{211} + f_{31} \cdot r_{311} + f_{41} \cdot r_{411} + \\
 & + f_{51} \cdot r_{511} + f_{61} \cdot r_{611} + f_{71} \cdot r_{711}) + \\
 & + b_2(f_{12} \cdot r_{121} + f_{22} \cdot r_{221} + f_{32} \cdot r_{321} + f_{42} \cdot r_{421} + \\
 & + f_{52} \cdot r_{521} + f_{62} \cdot r_{621} + f_{72} \cdot r_{721}) + \\
 & + b_3(f_{13} \cdot r_{131} + f_{23} \cdot r_{231} + f_{33} \cdot r_{331} + f_{43} \cdot r_{431} + \\
 & + f_{53} \cdot r_{531} + f_{63} \cdot r_{631}) + \\
 & + b_4(f_{14} \cdot r_{141} + f_{24} \cdot r_{241} + f_{34} \cdot r_{341} + f_{44} \cdot r_{441} + \\
 & + f_{54} \cdot r_{541}) + \\
 & + b_5(f_{15} \cdot r_{151} + f_{25} \cdot r_{251} + f_{35} \cdot r_{351} + f_{45} \cdot r_{451} + \\
 & + f_{55} \cdot r_{551} + f_{65} \cdot r_{651} + f_{75} \cdot r_{751} + f_{85} \cdot r_{851}); \\
 & \dots \\
 & \dots \\
 & \dots \\
 \Pi(R_5) = & b_1(f_{11} \cdot r_{115} + f_{21} \cdot r_{215} + f_{31} \cdot r_{315} + f_{41} \cdot r_{415} + \\
 & + f_{51} \cdot r_{515} + f_{61} \cdot r_{615} + f_{71} \cdot r_{715}) + \\
 & + b_2(f_{12} \cdot r_{125} + f_{22} \cdot r_{225} + f_{32} \cdot r_{325} + f_{42} \cdot r_{425} + \\
 & + f_{52} \cdot r_{525} + f_{62} \cdot r_{625} + f_{72} \cdot r_{725}) + \\
 & + b_3(f_{13} \cdot r_{135} + f_{23} \cdot r_{235} + f_{33} \cdot r_{335} + f_{43} \cdot r_{435} + \\
 & + f_{53} \cdot r_{535} + f_{63} \cdot r_{635}) + \\
 & + b_4(f_{14} \cdot r_{145} + f_{24} \cdot r_{245} + f_{34} \cdot r_{345} + f_{44} \cdot r_{445} + \\
 & + f_{54} \cdot r_{545}) + \\
 & + b_5(f_{15} \cdot r_{155} + f_{25} \cdot r_{255} + f_{35} \cdot r_{355} + f_{45} \cdot r_{455} + \\
 & + f_{55} \cdot r_{555} + f_{65} \cdot r_{655} + f_{75} \cdot r_{755} + f_{85} \cdot r_{855}).
 \end{aligned}
 \tag{4}$$

Структурну схему методики оцінювання результатів війни на виснаження, яку розроблено з ураху-

ванням матеріалів конференції [7], наведено на *рисунку 2*.

Наведена методика може застосовуватися для оцінювання результатів війни на поточний час і на прогнозований період її ведення. Основною умовою застосування методики є здатність експертів визначити співвідношення факторів протиборчих сторін, що впливають на їхні військові потенціали. Застосування співвідношень цих факторів під час оцінювання результатів війни визначає новизну методики. Вірогідність оцінки результатів війни залежить від кваліфікації експертів.

Розглянемо ілюстративний приклад застосування методики. Припустимо, що на момент оцінювання результатів війни на виснаження агресором уже захоплена частина території країни, яка зазнала нападу. Агресор має перевагу у військовому потенціалі. У такому разі перемогою для країни, що зазнала агресії, можна вважати звільнення території, а поразкою – неможливість цього здійснити. Потрібно визначити пріоритети категорій $R_k (k = 1, z)$ оцінки результатів війни на виснаження відповідно до моделі, наведеної на *рисунку 1*.

Співвідношення факторів протиборчих сторін l_{ji} , що впливають на складові їхніх військових потенціалів, наведені в *таблиці 2*.

Пріоритети впливу складових військового потенціалу на результати війни становлять:

$$\begin{aligned}
 b_1 = 0,25; b_2 = 0,18; b_3 = 0,21; \\
 b_4 = 0,13; b_5 = 0,23.
 \end{aligned}$$

Пріоритети f_{ji} впливу факторів F_{ji} на складові військового потенціалу наведені в *таблиці 3*.



Рис. 2. Структурна схема методики оцінювання результатів війни на виснаження

Таблиця 2

Співвідношення факторів протиборчих сторін, що впливають на складові їхніх воєнних потенціалів

Номер фактора, j	Номер складової воєнного потенціалу, i				
	1	2	3	4	5
1	1,0/3,0	3,0/1,0	1,0/1,0	1,0/3,0	1,0/3,0
2	1,0/2,0	2,0/1,0	1,0/1,0	1,0/5,0	1,0/1,5
3	1,0/1,0	1,5/1,0	5,0/1,0	1,0/1,0	1,0/2,0
4	1,0/5,0	1,0/1,0	4,0/1,0	1,0/1,0	1,0/3,0
5	4,0/1,0	2,0/1,0	2,0/1,0	1,0/3,0	1,0/1,0
6	1,0/6,0	1,8/1,0	1,0/1,0	–	1,0/1,0
7	1,0/3,0	3,5/1,0	–	–	2,0/1,0
8	–	–	–	–	1,0/1,0

Таблиця 3

Пріоритети впливу факторів на складові воєнного потенціалу

Номер фактора, j	Номер складової воєнного потенціалу, i				
	1	2	3	4	5
1	0,26	0,18	0,15	0,32	0,11
2	0,09	0,16	0,17	0,11	0,13
3	0,12	0,12	0,20	0,22	0,17
4	0,20	0,08	0,24	0,19	0,14
5	0,19	0,22	0,14	0,16	0,08
6	0,06	0,09	0,10	–	0,12
7	0,08	0,15	–	–	0,15
8	–	–	–	–	0,10

У таблиці 4, як приклад, наведено матрицю попарних порівнянь категорій оцінки результатів війни та їхні пріоритети для фактора F_{11} (див. рис. 1) воєнно-економічної складової воєнного потенціалу.

Таблиця 4

Матриця попарних порівнянь категорій оцінки результатів війни для фактора F_{11}

Категорії	R_1	R_2	R_3	R_4	R_5	Компоненти власного вектора	Пріоритети
R_1	1	2/3	3/5	1/7	1/9	0,361	0,053
R_2	3/2	1	1/2	2/5	2/7	0,614	0,090
R_3	5/3	2/1	1	1/3	1/5	0,738	0,109
R_4	7/1	5/2	3/1	1	1/2	1,922	0,283
R_5	9/1	7/2	5/1	2/1	1	3,160	0,465

ВУ = 3,5%

Відповідно до [4] визначено узгодженість матриці. Відношення узгодженості (ВУ) дорівнює 3,5% за допустимих 10%.

Одержані експертами пріоритети категорій оцінки результатів війни для всіх факторів складових воєнного потенціалу наведені в таблиці 5.

Таблиця 5

Пріоритети категорій оцінки результатів війни для факторів складових воєнного потенціалу

Категорії оцінки, R_k	Воєнно-економічний потенціал, C_1						
	r_{11k}	r_{21k}	r_{31k}	r_{41k}	r_{51k}	r_{61k}	r_{71k}
R_1	0,05	0,12	0,11	0,08	0,11	0,17	0,07
R_2	0,09	0,15	0,18	0,14	0,22	0,19	0,14
R_3	0,11	0,18	0,41	0,18	0,38	0,34	0,19
R_4	0,28	0,22	0,20	0,24	0,20	0,16	0,22
R_5	0,47	0,33	0,10	0,36	0,09	0,14	0,38

Продовження таблиці 5

Категорії оцінки, R_k	Духовний потенціал, C_2						
	r_{12k}	r_{22k}	r_{32k}	r_{42k}	r_{52k}	r_{62k}	r_{72k}
R_1	0,36	0,15	0,10	0,18	0,13	0,09	0,28
R_2	0,23	0,18	0,22	0,22	0,17	0,21	0,19
R_3	0,18	0,33	0,28	0,30	0,28	0,34	0,31
R_4	0,13	0,19	0,21	0,21	0,20	0,26	0,15
R_5	0,10	0,15	0,19	0,09	0,22	0,10	0,07

Продовження таблиці 5

Категорії оцінки, R_k	Воєнно-політичний потенціал, C_3					
	r_{13k}	r_{23k}	r_{33k}	r_{43k}	r_{53k}	r_{63k}
R_1	0,18	0,18	0,38	0,18	0,15	0,21
R_2	0,22	0,22	0,21	0,35	0,31	0,25
R_3	0,20	0,24	0,19	0,21	0,38	0,20
R_4	0,23	0,19	0,14	0,18	0,11	0,18
R_5	0,17	0,17	0,08	0,08	0,05	0,16

Продовження таблиці 5

Категорії оцінки, R_k	Військовий науково-технічний потенціал, C_4				
	r_{14k}	r_{24k}	r_{34k}	r_{44k}	r_{54k}
R_1	0,07	0,09	0,21	0,18	0,10
R_2	0,18	0,18	0,23	0,23	0,15
R_3	0,24	0,28	0,19	0,19	0,21
R_4	0,31	0,30	0,20	0,21	0,34
R_5	0,20	0,15	0,17	0,19	0,20

Закінчення таблиці 5

Категорії оцінки, R_k	Бойовий потенціал, C_4							
	r_{15k}	r_{25k}	r_{35k}	r_{45k}	r_{55k}	r_{65k}	r_{75k}	r_{85k}
R_1	0,06	0,07	0,08	0,02	0,15	0,17	0,21	0,19
R_2	0,08	0,10	0,15	0,09	0,20	0,22	0,33	0,21
R_3	0,18	0,21	0,21	0,23	0,28	0,23	0,28	0,18
R_4	0,32	0,34	0,35	0,42	0,21	0,18	0,12	0,22
R_5	0,36	0,28	0,21	0,24	0,16	0,20	0,06	0,20

У таблиці 6 наведені пріоритети категорій оцінки результатів війни на виснаження та їхні складові відносно прийнятої структури воєнного потенціалу.

Таблиця 6

Пріоритети категорій оцінки результатів війни на виснаження та їх складові

Категорії оцінки, R_k	Пріоритети категорій, $\Pi(R_k)$	Воєнно-економічний потенціал	Духовний потенціал	Воєнно-політичний потенціал	Військовий науково-технічний потенціал	Бойовий потенціал
R_1	0,145	0,022	0,035	0,046	0,017	0,025
R_2	0,200	0,037	0,036	0,055	0,026	0,046
R_3	0,240	0,059	0,051	0,049	0,029	0,052
R_4	0,225	0,058	0,033	0,036	0,035	0,063
R_5	0,190	0,072	0,024	0,023	0,023	0,048

Відповідно до співвідношень факторів, які впливають на складові воєнних потенціалів протидіючих сторін (див. *табл. 2*), найбільший пріоритет має категорія R_3 (незмінність положення у війні на виснаження) $\Pi(R_3) = 0,240$, що характеризує можливість продовження збройної боротьби. Проте достатньо високий пріоритет має категорія R_4 (часткова поразка) $\Pi(R_4) = 0,225$, що можна вважати як неможливість звільнення деякої частини території, що захоплена агресором. Найменший пріоритет одержала категорія R_1 (перемога) $\Pi(R_1) = 0,145$, що за умовою прикладу свідчить про неможливість повного звільнення захопленої агресором території через недостатність воєнно-

економічного і бойового потенціалів (див. *табл. 6*) для ведення війни на виснаження.

Висновки. Розроблено методику оцінювання результатів війни на виснаження. Порівняння категорій оцінки результатів війни пропонується здійснювати на підставі врахування співвідношень факторів, що впливають на складові воєнного потенціалу протидіючих сторін. Для ранжирування категорій оцінки результатів війни застосовується МАІ, використовується чотирирівнева ієрархія розв'язання задачі: мета – складові воєнного потенціалу – фактори – альтернативи (категорії).

Методика може застосовуватися органами державного і воєнного управління під час аналізу перебігу війни і прийняття відповідних рішень. Порядок застосування методики показано на прикладі.

Перелік літератури

1. *Ydstebø P.* Strategy and operations in a war of exhaustion [Електронний ресурс] / P. Ydstebø // 36. наук. пр. Центру воєнно-стратегічних досліджень Національного університету оборони України. – 2023. – № 3 (79). – С. 74–83. – Режим доступу : <https://doi.org/10.33099/2304-2745/2023-3-79/74-83>.
2. *Кириченко І. О.* Війна і математика: елементи теорії складних бойових систем / І. О. Кириченко, Ю. В. Наливайко. – Харків : Академія ВВ МВС України, 2012. – 260 с.
3. Передбачення можливостей держави щодо відбиття збройної агресії [Електронний ресурс] / М. В. Коваль, В. В. Коваль, П. В. Щипанський, О. М. Загорка // Наука і оборона. – 2023. – № 3. – С. 25–32. – Режим доступу : <https://doi.org/10.33099/2618-1614-2023-22-3-25-32>.
4. *Саати Т.* Аналитическое планирование: организация систем / Т. Саати, К. Кернс ; пер. с англ. Р. Г. Вачнадзе. – М. : Радио и связь, 1991. – 224 с.
5. *Шкідченко В. П.* Елементи теорії воєнної безпеки : монографія / В. П. Шкідченко, В. Д. Кохно ; Національний ін-т стратегічних досліджень. – К. : БФ «Миротворець», 2001. – 194 с.
6. *Самохвалов Ю. А.* Экспертное оценивание: методический аспект / Ю. А. Самохвалов, Е. М. Науменко. – К. : ДУІКТ, 2007. – 263 с.
7. *Загорка О. М.* Методичний підхід до оцінювання результатів війни на виснаження / О. М. Загорка, Н. М. Андриянова, І. О. Загорка // Державна політика у сфері оборони. Зміст, проблеми, пріоритети та перспективи : зб. матеріалів ІV наук.-практ. конф. Центру воєн.-стратегіч. досл. Нац. ун-ту оборони України, 27 листопада 2024 р., м. Київ / Нац. ун-т оборони України. – К. : НУОУ, 2024. – С. 125–127.

DOI 10.33099/2618-1614-2025-28-1-54-62

УДК 355.4

М. С. Кармазіна,*доктор політичних наук, професор,
Воєнна академія імені Євгенія Березняка,***І. В. Аблазов,***кандидат політичних наук, професор,
Воєнна академія імені Євгенія Березняка*

Концепт «гібридна війна»: аналіз наукового дискурсу

З використанням методів історичної ретроспекції, порівняння, *real time* та інших досліджується трансформація рефлексій дослідників над сутністю та природою війни. Обстоюється думка, що зі зламу ХХ–ХХІ століть і до сьогодення війни гібридної ери в науковому дискурсі посіли одне із чільних місць та осмислюються в контексті тотальної, необмеженої, асиметричної чи, зрештою, гібридної війни тощо. Нині дається взнаки потужний дослідницький інтерес до процесу кристалізації самого поняття гібридна війна, його складових та особливостей розвитку. Дослідники зосереджують увагу на досвіді та уроках російської гібридної війни проти України, країн Заходу, відзначаючи, що гібридність залишатиметься своєрідним воєнним трендом у найближчі не лише роки, а й десятиліття, а отже, має підлягати ретельному аналізу.

Ключові слова: гібридна війна, тотальна війна, необмежена війна, асиметричні конфлікти, російська гібридна агресія проти України.

Злам XIX–XX століть став часом своєрідного возвеличення в Європі (передовсім на полях битв Першої світової війни) ідей Карла фон Клаузевіца, ретельно відрефлексованих у низці його ранніх праць («1806», «Принципи війни», «Сповідь», «1812»¹) і, врешті-решт, ґрунтовно представлених у трьох томах трактату «Про війну» (що побачив світ у Берліні в 1832–1834 рр.). Сутність підходу фон Клаузевіца концентрувалась у широковідомій «трийці»: війна – це «захоплююча трійця, яка складається з первинного насильства, ненависті та ворожнечі, які слід розглядати як сліпу природну силу, випадковості та ймовірності, у яких вільно блукає творчий дух... як інструмент політики, що підпорядковує його чистому розуму». Цю «трийцю», на думку американського професора стратегії Крістофера Бассфорда, найкраще відтворює формула «жорстка емоція – випадок – раціональний розрахунок» (а не популярне тлумачення «уряд – армія – населення»).

Ідея війни як постійної ескалації насилля була по-своєму розвинена і концептуалізована одним «з найвидатніших і мерзенних німців» (у термінах Джея Локенора) Еріхом Людендорфом² у праці «Тотальна війна» (1935), яка і захопила мислення нацистів: відбулася не лише мобілізація людей і ресурсів задля військових зусиль, а й ступінь обмежень, як засвідчила Друга світова війна, нацистами був мінімізований. Надалі ідеєю Е. Людендорфа послуговувалися неодноразово: приміром, війну у В'єтнамі (1954–1975) комуністичне керівництво Північного В'єтнаму витлумачувало як *тотальну*. А Ірано-Іракська війна (1980–1988), за спостереженням аналітиків, була близькою до *тотальної*. Однак великі держави, усвідомлюючи загрози ядерного конфлікту (в контексті «холодної війни»), демонстрували прагнення нових обмежень (зокрема ядерної зброї).

Коли ж минуле століття добігало кінця і світ наважився сподіватися на закінчення «холодної війни», американська «Газета морської піхоти» (у жовтні 1989 р.) ніби надіслала сигнал «Не розслаблятися: ситуація ускладнюється!», опублікувавши нині широко відому статтю «Зміна обличчя війни: до четвертого покоління» [1], авторами якої були військові офіцери Вільям С. Лінд, Кіт Найтенгейл, Джон Ф. Шмітт, Джозеф В. Саттон та Гері І. Вілсон. Акцентувавши, що головним завданням «солдата мирного часу» є «ефективно підготуватися до наступної війни», та відзначивши, що це складне завдання повсякчас стає дедалі складнішим,

¹ Ці праці були видрукувані після смерті К. фон Клаузевіца (1780–1831).

² Еріх Людендорф – військовий стратег, учасник невдалого нацистського перевороту в Мюнхені (1925), спрямованого на повалення Веймарської республіки; був нацистським депутатом у Рейхстазі (1924–1928) та претендентом на пост президента.

вони не лише обґрунтували власну періодизацію «покоління» сучасних війн, відштовхнувшись від 1648 р. (часу, позначеного завершенням Тридцятилітньої війни і, відповідно, точкою відліку Вестфальського миру) та назвавши катализаторами змін технології та ідеї, а й поставили запитання: «Чи не настав час для появи війн четвертого покоління?».

Попри те, що підходи В. Лінда та його колег зазнали критики (приміром, у працях Томаса Х. Хамса, який у 2004 р., по-своєму ламаючи лінійний підхід у сприйнятті процесів розгортання війн, схилився до думки, що від часу Мао Цзедуна асиметричні конфлікти у ХХ ст. і були уособленням війн четвертого покоління), вони все ж продовжують розвиватися. Тож на різного рівня аналітичних майданчиках мова заходить про війни *п'ятого*, а то й *шостого* покоління. Кожне наступне «покоління війни» представлене новими акторами (особами, групами), ідеями, тактиками і стратегіями.

Водночас інші дослідники, осмислюючи на зламі ХХ–ХХІ століть феномен сучасної війни, рефлексували над ним, приміром, у контексті постмодерну: ізраїльський дослідник Мартін ван Кревельд (тримаючи в умі згадану вище приписувану фон Клаузевицу формулу «уряд – армія – населення»), у 1991 р. визначав постмодерний тип війн як «нетринітарні». Елвін та Гайді Тоффлери також не були схильними до спрощення ситуації та запропонували зацікавленим інтелектуалам обмірковувати *війну третьої хвилі* (характерної для «цивілізації комп'ютера», що розвивалася, відповідно, після попередніх «цивілізації мотики» і згодом «цивілізації конвеєра»), про що свідчило оприлюднене ними дослідження «Війна та антивійна. Вживання на зорі ХХ століття» (1993). Взявши епіграфом до праці відомий вислів Троцького: «Можете не цікавитися війною, але тоді війна зацікавиться вами», подружжя Тоффлерів не тільки спрогнозувало наступне збільшення кількості війн, а й наголосило важливість «стратегії знань» у процесі їх розгортання, як і зазначило, що переваги під час них матимуть постіндустріальні держави зі значним високотехнологічним потенціалом (який охоплюватиме супутники спостереження, бойових роботів, безпілотні бойові літаки тощо). Крім того, особливістю війн мало стати, як прозорливо стверджували Тоффлери, посилення загроз, пов'язаних із тероризмом, застосуванням біологічної, хімічної зброї та «суперчумами».

Ще один тогочасний погляд на війну (який у жодному разі не можна проігнорувати) був представлений Мері Калдор у її праці «Нові та старі війни: організоване насильство в глобальну еру» (1999), а його своєрідний акцент зводився до того, що в «нових війнах», як усвідомила авторка, уже брали участь «мережі державних і недержавних акторів, а найбільше насильство спрямовувалося проти цивільного населення» [2, р. vi].

Утім, прикметною особливістю реалій ХХІ століття став новий і дедалі гучніший акцент, що розширював/розширює політичний лексикон нинішнього століття, додаючи до нього такі поняття, як *гібридна ера*, *гібридні загрози*, *гібридні конфлікти* і, зрештою, *гібридна війна*. Наслідком рефлексій стала постійна поява десятків нових дефініцій, які віддзеркалюють численні спроби дослідників з досить відмінних сфер (не лише полемологів, а й політологів, юристів тощо) адекватно розкрити сутність найрізноманітніших *гібридних явищ*, визначити їхні цілі, проаналізувати особливості трансформації та механізми розгортання, конкретні засоби та інструменти впровадження (у тому чи іншому середовищі, серед членів якоїсь зі спільнот, чи ж таргет-груп), як і особливості синтезу *гібридного* з *традиційним* тощо. Попри це, зважаючи на постійну мінливість безпекового середовища, як і невпинну мімікрію *гібридності* у надскладних процесах сучасності (пов'язаних насамперед як з російською агресією проти України, котру окремі прогнозисти трактують як старт третьої світової війни, так і, приміром, з розвитком штучного інтелекту, квантової фізики і – ширше – квантового мислення) на тлі примноження війн на планеті (на початок 2024 р. у світі велося 59 війн – найбільше за останні майже 50 років [3]) з яскраво вираженим *гібридним характером*, *гібридність* як така та, безумовно, *гібридні війни* залишаються одним з найактуальніших явищ нинішніх і майбутніх міжнародних та внутрідержавних реалій, що підлягають постійному моніторингу й аналізу. З урахуванням цього, **метою** нашого дослідження є рефлексії щодо процесу концептуалізації поняття *гібридна війна* (з використанням методу *наукової ретроспекції*) в процесі аналізу «наповнення» контексту парасолькового поняття *війна* (за допомогою методів *розрізнення* та *обґрунтування дефініцій*) вітчизняними та зарубіжними дослідниками (чому посприяє метод *порівняння*) у попередній час, як і в теперішній (що по-своєму забезпечує використання методу *real time*).

Результати аналізу публікацій, передусім вітчизняних дослідників дають підстави твердити, що щонайменше з 2006 р. українські науковці вдавалися не лише до аналізу тенденцій розвитку озброєння та військової техніки, а й їхнього взаємозв'язку із «сучасними формами і способами ведення збройної боротьби» [4; 5], рефлексували над питанням імовірних форм війн і збройних конфліктів майбутнього [6], осмислювали специфіку збройної боротьби у війнах четвертого-шостого покоління [7]. Крім того, дослідники, найперше Володимир Горбулін [8, с. 19, 20], заговорили про загрози «перманентної політичної нестабільності» у світі та їхні причини, про такі явища, як «хвилі дестабілізації», «інформаційні та дипломатичні війни». Мова заходила і про нових недержавних акторів («всесвітне

ісламське терористичне підпілля») та про ліквідацію державної монополії на насильство, про перенесення епіцентрів протистояння на «периферію» і, зрештою, про «новітні формули конфліктів» та сутність, закони, причини «нової війни» [8, с. 20–23]. Учений звертав увагу на факт втрати кордонами між окремими країнами «традиційного значення» (вони «стають проникливими»), що так чи інакше ставало «викликом світовій стабільності»; передбачив розгортання сценарію «спіраль страху» (безконтрольне поширення зброї масового знищення, глобальний економічний колапс, крах сучасних міжнародних інститутів і міжнародної системи) та посилення ролі «силової політики» [9, с. 32, 41, 43].

Показово, що аналізуючи варіанти політики Росії після розгляду (у 2009 р.) російським законодавчим органом законопроекту, що дозволив використовувати підрозділи збройних сил за кордоном, В. Горбулін зауважив, що «відтепер провокація російської сторони на території України і застосування військової сили може відбутися в будь-який момент», що Україна підійшла до точки біфуркації: її подальший розвиток «може з рівною імовірністю піти в кількох, абсолютно різних і в тому числі протилежних напрямках» під тиском «оформлених викликів і загроз», серед яких «активна робота Росії на дипломатичному, економічному, інформаційному та соціальному рівнях» на тлі певної інфантильності політичної еліти України, яка не розуміла рівня загроз та демонструвала «васальні настрої» щодо Росії, «неспроможність, наслідком якої стала зовнішньополітична анемія» [10, с. 49, 50, 53, 52]. Висновок В. Горбуліна: «Вже років із десять Україна розвивається за хибною парадигмою» [10, с. 55]. За таких обставин війна, загроза війни була «ідеальним механізмом маніпуляції», «чудово сконструйований важіль впливу Росії на Україну» [10, с. 54].

Фактично у період 2006–2014 рр. у дослідженнях В. Горбуліна (самостійних чи у співпраці з Валентином Бадраком чи Олександром Литвиненком) у процесі аналізу політики та геополітики держав світу, але, найперше, Росії, аналізувалися цілі, ознаки, засоби/інструменти та наслідки того явища, визначення якому вчений дав у 2014 р., опублікувавши статтю «Гібридна війна як ключовий інструмент російської геостратегії реваншу» [11].

Водночас осмислювати гібридну війну в Україні як «нову реальність» намагався Михайло Требін [12]. У 2015 р. про посилення зацікавленості проблематикою гібридної війни свідчила поява публікацій Є. Магди [13–15], у яких аналізувалися сутність, природа, структура феномена, як і статті В. Власюка та Я. Кармана [16], присвяченої вивченню поняття «гібридна війна» в контексті міжнародного права. З позицій соціології російську гібридну війну проти України досліджував Ігор Рущенко [17]. У 2017 р. світ поба-

чили фундаментальні праці за редакцією В. Горбуліна «Світова гібридна війна: український фронт» [18], дослідження Олександра Власюка та Сергія Кононенка «Кремлівська агресія проти України: український фронт» [19], праця колективу авторів Донецького національного університету імені Василя Стуса «Гібридна війна: in verbo et in praxi» [20], які віддзеркалювали в чомусь схожі, а в чомусь і ні кути зору дослідників на проблематику *гібридності*.

Крім того, дослідники аналізували гібридну війну як «дискурсивний конструкт» [21], концентрували увагу на онтології [22], аналізі сутності, структурі феномена [23–26], збройній агресії «гібридного типу» [27]. Досліджували корупцію як фактор «системної (гібридної) війни» [28]. Значна увага приділялась історичним кореням безпосередньо гібридної війни Росії проти України [29–33].

Після повномасштабного вторгнення Росії в Україну в центрі дослідницької уваги опинилися такі питання, як інструментарій гібридної війни [34], особливості війни в медіа-просторі [35; 36]. Дослідники аналізували когнітивну війну як складову гібридної [37] чи гібридну війну як різновид асиметричних дій [38].

Характерною особливістю багатьох як вищезгаданих публікацій, так і інших, є, по-перше, не просте зростання інтересу до *гібридності*, а (що кидається у вічі) постійне ускладнення кута зору на проблематику. По-друге, публікації вітчизняних дослідників свідчать не лише про увагу до суто теоретичного аналізу гібридної війни, а й до її осягнення безпосередньо крізь призму російської агресії проти України. По-третє, має місце спроба досліджувати одні й ті самі процеси, явища, особливості російської війни проти України як у контексті, власне, *гібридної війни*, так і «тотальної» (див.: [39; 40]) чи війни «п'ятого покоління» (див.: [41]).

Аналіз зарубіжних досліджень засвідчив, що поняття *гібридна війна* вперше зустрічаємо наприкінці ХХ ст. – у 1995 р. у праці Томаса Р. Мокайтиса «Гібридна війна: індонезійське протистояння» [42], у якій автор аналізував дії «слабшого» («повстанців») проти «сильнішого» (британців у «постімперську добу»). У ширшому контексті поняття вперше обґрунтовував у 2005–2007 рр. підполковник Корпусу морської піхоти США і військовий теоретик Френк Г. Хоффман у низці досліджень, проведених як у співавторстві (зокрема із Джеймсом Меттісом, див.: [43]), так і самостійно: у статті «Складна іррегулярна війна: наступна революція у військовій справі» [44], а потім і в книзі «Конфлікт у ХХІ столітті: зростання гібридних війн» (Потомаський інститут політичних досліджень) [45]. Показовим при цьому було зізнання самого Ф. Г. Хоффмана в тому, що він запозичив поняття з дисертації Роберта Г. Волкера і, таким чином, відбулося свого роду *повторне введення терміна* (поняття) в науковий, політичний

та інші дискурси, зміст якого Ф. Г. Хоффман визначив як «поєднання смертоносності державного конфлікту з фанатичним і тривалим запалом нерегулярної війни» [45, р. 28].

Осмислюючи світ після завершення «холодної війни», Ф. Г. Хоффман заговорив про одночасне (комбіноване) використання противником кількох типів війн заради досягнення намічених цілей та застеріг від застарілої та спрощеної класифікації конфліктів на «великий традиційний» та «малий чи нерегулярний». Крім того, Ф. Г. Хоффман наголосив, що готовність (зокрема США) до участі лише в окремих видах конфліктів, а не в усьому їхньому спектрі, може стати в майбутньому таким собі «рецептом поразки».

Таке зауваження було небезпідставним, якщо взяти до уваги книгу двох стратегів-полковників Національно-визвольної армії Китаю Цяо Лян і Ван Сянсуї «Необмежена війна», видрукувану в КНР ще в лютому 1999 р. (переклад англійською з'явився вже у 2002 р.; див. скорочену версію монографії у відкритому доступі: [46]), у якій, по-перше, прямо вказувалося на США як на ворога КНР та інших країн, що розвиваються, а по-друге, *необмежена війна* пропонувалась як адекватний інструмент і своєрідна тактика задля компенсації власної військової неповноцінності таких (*слабких*) країн у боротьбі зі США під час майбутньої високотехнологічної війни. З погляду Цяо Лян і Ван Сянсуї, *необмежена війна* – це військові і невійськові заходи для ударів по США, це докорінне стирання відмінностей у ролях солдата і цивільного. Серед інструментів *необмеженої війни* – політичний та економічний тиск, хакерські атаки на веб-сайти, напади на фінансові установи, тероризм, екологічна війна, торговельна і фінансова війни, вбивства, використання медіа (наприклад через створення фондів), сприяння соціальному розбрату в суспільствах, ведення бойових дій у містах тощо. Тобто поле бою – все суспільство.

Першим правилом *необмеженої війни* було проголошено відсутність правил і заборон (як стверджував Цяо Лян в одному з інтерв'ю).

Китайський погляд на *необмежену* чи (за західними стандартами) *гібридну війну* – це не лише кардинальний відхід від уявлень про традиційну війну та демонстрація власного китайського стратегічного мислення (що є вражаючим своєрідним продовженням «мистецтва», чи «технологій війни», запропонованих Сунь Цзи ще у VI–V ст. до н. е.): це насамперед здатність заглянути в майбутнє (зокрема кібер-майбутнє) і виробити специфічні стратегії та тактики як для *сучасної війни*, так і *війни майбутнього*, сутність яких і була сконцентрована в понятті *необмежена війна*. Крім того, це усвідомлення та відкрита демонстрація переваг Китаю (ще слабкої наприкінці XX століття держави), *породжених слабкістю*. Це – *потужна стратегія слабких*.

Але *слабких* до певного часу, оскільки стає очевидним, що їхня *необмежена війна*, що розпочиналася на теоретичному рівні наприкінці минулого століття, у процесі відстоювання власних інтересів продовжує набирати обертів *щоденно і повсякчас*.

Говорячи про свої переваги, китайці розвивають ідеї, сконцентровані у твердженні: *сильні* держави не зможуть скористатися вседозволеністю у війні/боротьбі проти *слабких*, оскільки вони діють у межах установлених міжнародних правил, порушення яких тягне за собою деградацію довіри з боку країн світу, а *слабкі* актори на міжнародній арені можуть порушувати встановлені правила з неймовірною легкістю та користуватися всілякими лазівками у протистоянні із *сильними*.

Тож, усвідомлюючи роль правил-пасток, у які потрапили демократичні країни Заходу, китайці культивують ідею вседозволеності *слабких*. *Необмежена війна* по-китайськи – вседозволеність у використанні як збройної, так і незбройної сили, військової та не-військової, летальної та нелетальної. *Необмежена війна* – це безліч майданчиків, на яких відбуваються чи відбуватимуться в майбутньому «битви».

Інтерес викликають оцінки та висновки щодо роботи Цяо Лян і Ван Сянсуї, зроблені (у 2016 р.) американським генерал-лейтенантом у відставці Девідом Барно та науковицею доктором Норою Бенсахель, які зводилися до того, що:

- Цяо Лян і Ван Сянсуї своїми судженнями щонайменше на півтора десятиліття випередили час;
- праця «*Необмежена війна*» була явною відповіддю на «панівну західну військову ортодоксальність того часу», про що говорила датована 17 січня 1999 р. передмова до книги, і що, як відзначили самі Цяо Лян і Ван Сянсуї, було восьмою річницею початку війни в Перській затоці 1991 р.;
- у багатьох відношеннях аргументи Цяо Лян і Ван Сянсуї спростовували «багато уроків Заходу, витягнутих із цього конфлікту, і, зокрема, той, що війни можуть бути короткими, гострими та проводитися за допомогою високотехнологічної зброї, яка використовується з приголомшливою точністю, щоб розбити збройні сили ворога за години чи дні».

Вочевидь, актуальність «короткої та гострої війни» по-американськи (з погляду китайців), як і рашистських планів «взяти Київ за три дні» (як стало очевидним тут у нас, в Україні), втрачається. Трендом серед форм війни в XXI ст. стає китайський винахід – *необмежена війна*.

Водночас Натан П. Фраєр [47] (один з двох робочих стратегів, відповідальних за концептуальну розробку оборонної стратегії США у 2005 р.), розмірковуючи над американською концепцією «чотирьох викликів» (традиційних, нерегулярних, катастрофічних та руйнівних), які й були закріплені у «Стратегії національної

оборони США» (2005), запропонував (у 2007 р.) концепцію *гібридної норми*, згідно з якою противник буде варіативно використовувати згадані вище чотири виклики-архетипи, керуючись у кожен конкретний момент особливостями обстановки та наявними ресурсами.

Особливо цінною в той час стала публікація ізраїльського дослідника Девіда Джонсона (2010) [48], у якій він аналізував практику (досвід та уроки) боротьби Армії оборони Ізраїлю (ЦАХАЛ) з «гібридними опонентами» в Лівані та Газі – Хезболлою та ХАМАС, та, будучи переконаним, що ізраїльський досвід обов'язково знадобиться армії США та об'єднаним силам у майбутньому, виклав власний погляд на «військовий потенціал для гібридної війни». Д. Джонсон зауважив, що для успішних дій проти противників з такими можливостями, як Хезболла та ХАМАС, важливими є загальновійськовий вогонь та маневреність (оскільки «ці гібридні противники здатні створити якісний виклик, який потребує спільного вогню та маневру на нижчих рівнях»), «точність і протистояння», які є «критичними, але недостатніми, щоб упоратися з противниками гібридної війни» (особливо, якщо вони діють «серед народу»), «чутлива та адекватна підтримка з повітря, артилерії та безпілотних літальних апаратів є критично важливими компонентами загальновійськової боротьби проти гібридних противників», як і «добре відпрацьована здатність до інтеграції». Такі «можливості» Д. Джонсон назвав «передумовою успіху». Крім того, дослідник твердив, що «важкі сили на основі танків і бойових машин піхоти є ключовими елементами будь-якої сили, яка боротиметься з гібридними ворогами», хоч і з мінімальною підготовкою та організацією, але сучасним озброєнням (на зразок протитанкових ракетних комплексів і протиракетних зенітних ракетних комплексів). «Легкі та середні сили» можуть, на думку Д. Девідсона, доповнювати «важкі сили» (особливо в місті та в іншій «складній місцевості»), забезпечуючи «живучість, смертоносність або мобільність, властиві важким силам», та зменшуючи оперативні ризики і зводячи до мінімуму «дружні втрати».

З того часу західні дослідники провели не одну дискусію щодо природи, цілей, акторів, інструментів новітніх війн. І якщо одні дослідники оперували поняттям «покоління війни», то інші розглядали особливості новітніх війн крізь призму їхньої *гібридності*. Помітним внеском у дослідження проблематики в період 2005–2015 рр. стала підготовлена у 2012 р. (у Коледжі командування та генерального штабу армії США) магістерська (!) робота Томаса Б'єррегора «Гібридна війна: військова революція чи революція у військових справах?», у якій автор дійшов висновку, що гібридна війна не є ані «військовою революцією», ані «революцією у військових справах» (про що писали деякі практики), але чимось іншим.

Того самого 2012 р. спробу осмислення війни у XXI ст. здійснили понад сорок науковців, представників урядів та збройних сил з багатьох країн світу в «Оксфордському довіднику з війни» (редакторами якого були Джуліан Ліндлі-Френч та Ів Бойер). Серед розміщених у десяти розділах довідника сорока чотирьох текстів (присвячених таким проблемам, як основні причини війни, її моральні та правові аспекти, теорії щодо практик війни, стратегії ведення війни та окремо незахідні способи ведення війни) особливий інтерес викликає дослідження Роба де Вейка «Гібридний конфлікт і мінливий характер акторів» [49], у якому було фактично підсумовано (на той час) дебати щодо гібридних війн на Заході. Р. де Вейк констатував, з-поміж іншого, що прогрес технологій однозначно сприяв розвитку воєнного мистецтва, ефективності як звичайних, так і нерегулярних бойових сил. Однак асиметричні відповіді (недержавних акторів) по-своєму дещо компенсували технологічні переваги. І поки «слабкі актори» виявляють здатність протистояти сильнішим, гібридна війна залишатиметься своєрідною нормою.

Своїм шляхом пішов Макс Манварінг (полковник армії США у відставці, професор військової стратегії у Військовому коледжі армії США, очільник кафедри досліджень імені генерала Дугласа Макауртура), зосередивши увагу на сучасній *асиметричній війні* [50], тим самим не лише продовживши тематику, розроблювану в роботі «Незручні війни знову» (2006), а й, таким чином, завершивши трилогію, розпочату працями «Повстанці, тероризм і злочинність: тіні минулого та провісники майбутнього» (2008) та «Банди, псевдовійськові та інші сучасні найманці: нова динаміка в незручних війнах» (2010). Автор у багатомірній (складній, як заявив у назві книжки М. Манварінг) парадигмі ґрунтовно проаналізував конфлікти/повстання, які відбувались у світі в другій половині XX ст. (в Алжирі в 1954–1962 рр., у Сальвадорі в 1954–1962 рр., відродження «Сяючого шляху» в Перу, «троянських коней різного кольору» – діяльність Аль-Каїди в Іспанії, збройних формувань на Кубі, Гаїті та в Бразилії, крім того, російську молодіжну групу «Наші»³, політику у Гватемалі щодо боротьби з наркотиками та бандами),

³ «Наші», «нашисти», «Путін-югенд», «покоління Путіна» неофіційні назви російського молодіжного руху «Молодіжний демократичний антифашистський рух “Наші”», що постав у 2005 р. на базі переформатованої всеросійської молодіжної організації «Идущие вместе», створеної у 2000 р. Виникнення «нашистів» пов'язують з ініціативою В. Путіна, В. Суркова, С. Маркова та ін. У 2012–2013 рр. «нашисти» переживали кризу, яка призвела до фактичного припинення їхньої діяльності (формально – лише у 2019 р.). Нині в Росії та в тимчасово окупованих рашистами українських регіонах діє цілий спектр пропагандистських, мілітарних молодіжних утворень, більшість із яких керується Федеральним агентством у справах молоді («Росмолодежь», створена у 2008 р.).

а також не оминув проблематику асиметричних кібер-, інфо- та біологічних війн. М. Манварінг показав, що «невеликі війни та повстання» принципово відрізняються від «традиційних війн», що у ХХІ ст. стираються відмінності між повстанцями, злочинністю, тероризмом, підривною діяльністю, ополченцями, найманцями, бандами і війною, яка вже не ведеться виключно військовими професіоналами: в архітектурі сучасних конфліктів та війн свою нішу займають і хакери, і фінансисти, і медіа-експерти чи інженери програмного забезпечення та ін.

Один з ключових висновків М. Манварінга зводився до того, що яку б термінологію ми не використовували для позначення зазначених деструктивних явищ (*необмежені війни*, повстання, революції), війни майбутнього будуть *загальними* як за масштабом, так і за часом. Крім того, він запропонував свій «план» боротьби із цими явищами та обґрунтував «уроки виживання» для лідерів та організацій, для військових і цивільних, які працюють у сфері безпеки, зауваживши необхідність «поєднання зусиль» (чи координації) військових, поліцейських, політиків, дипломатів із зусиллями в економіці при врахуванні, до того ж, психологічних та етичних аспектів. Координація та співпраця всіх гілок влади, знання лідерами всього, що відбувається в суспільстві, повинні перебувати, на думку М. Манварінга, в основі стратегій ведення *асиметричної війни* (насамперед з повстанцями та терористами).

Утім, впадає в око твердження М. Манварінга про те, що мета війни «дедалі частіше полягає не в тому, щоб убивати людей чи захоплювати територію, а в тому, щоб підірвати здатність і волю противника використовувати звичайну військову силу, незалежно від того, наскільки вона переважає» [50, р. 133]: у контексті найбільшої війни на планеті (після Другої світової) як наслідку російської агресії проти України ідея саме «вбивати і захоплювати» залишається пріоритетною для рашистів і тим самим суперечить висновку М. Манварінга.

Помітною в шерезі праць, присвячених гібридним війнам та зокрема їхньому розумінню США та НАТО, стало франкомовне дослідження Елі Тененбаума «Пастка гібридної війни» (2015) [51], у якому автор, аналізуючи власне «пастки», зауважив, з-поміж іншого, що в рефлексіях новітніх форм війни не варто обмежуватися нинішнім століттям, але слід занурюватись у попереднє – двадцяте. Тим самим, можна твердити, Е. Тененбаум по-своєму додав елемент до алгоритму вивчення природи гібридної війни.

Вартими уваги є і підходи Рода Торнтонна в публікації (2015) «Зміна природи сучасної війни» [52], у якій він указав на необхідність для країн НАТО бути готовими не лише до «нерегулярних війн» малими

добре оснащеними арміями (що цілком ефективно в боротьбі з терористичними організаціями на зразок Аль-Каїди, Талібану чи ІДІЛ), а й до війн проти держав як безпосередньо на полі бою, так і під час пропагандистських війн, використовуючи, зокрема, інформацію, як це робила Росія, захоплюючи український Крим. І чого не брало до уваги НАТО, – розроблюючи свої стратегії.

Зрештою, своєрідним підсумком вивчення сучасних процесів розгортання *гібридних війн* з початку ХХІ ст. і до початку повномасштабної агресії Росії проти України стала колективна праця 2021 р. за назвою «Ведення війни в ХХІ столітті» за редакцією Роба Джонсона, Мартіна Кітцена та Тіма Свейса. Особливий інтерес у ній викликає розділ, підготовлений Робом Джонсоном [53], у якому містяться міркування щодо розвитку *гібридної війни* впродовж двадцяти років перед тим та військових практик протидії насиллю, контргібридних операцій.

У період після 24 лютого 2022 р., як свідчить аналіз наукового дискурсу за допомогою метода *real time*, у західному науковому дискурсі чільна увага приділяється аналізу уроків та досвіду протидії російській *гібридній війні* проти України та країн Заходу (див., наприклад, «найсвіжіші» праці: [54 56]). Автори рефлексують над проблематикою в контексті *асиметричних, нерегулярних* дій і процесів.

Висновки. Викладене дає підстави твердити, що війни *гібридної ери* в науковому дискурсі посіли одне із чільних місць. Зі зламу ХХ–ХХІ ст. і до сьогоднішня досить потужний дослідницький інтерес виявлявся та виявляється як до витоків самого поняття *гібридна війна*, так і до його природи та особливостей розвитку. Має місце певне різночитання (а, отже, і пояснення) дослідниками (зокрема, Заходу, України чи Китаю) воєнних явищ сучасності не лише в контексті гібридної, а й *необмеженої, асиметричної, тотальної* тощо війни. Крім того, проаналізований масив праць засвідчує неабияку зосередженість аналітиків на досвіді та уроках російської гібридної війни проти України, що, безсумнівно, становитиме своєрідний дослідницький тренд у найближчі не тільки роки, а й десятиліття.

Перелік літератури

1. The Changing Face of War: Into the Fourth Generation [Електронний ресурс] / W. S. Lind, K. Nightengale, J. F. Schmitt et al. // Marine Corps Gazette. – 1989. – Р. 22–26. – Режим доступу : https://www.academia.edu/7964013/The_Changing_Face_of_War_Into_the_Fourth_Generation.
2. Kaldor M. New and Old Wars: Organized Violence in a Global Era / M. Kaldor. – 3rd edition. – Cambridge : Polity Press, 2012. – XII, 268 p.

3. *Прус М.* На початок 2024 у світі велося 59 активних воєн – найбільше за пів століття [Електронний ресурс] / М. Прус // *Голос Америки*. – Режим доступу : <https://www.holosameryky.com/a/skilky-voien-u-sviti/7814944.html>.
4. *Нор П. І.* Основні світові тенденції розвитку озброєння та військової техніки та їх взаємозв'язок з сучасними формами і способами ведення збройної боротьби / П. І. Нор, О. Д. Мельник, В. А. Єфіменко // *Зб. наук. праць ЦНДІ ОВТ ЗСУ*. – 2006. – Вип. 16. – С. 90–99.
5. *Василенко О. В.* Взаємозв'язок світових тенденцій розвитку озброєння та військової техніки і форм та способів ведення збройної боротьби / О. В. Василенко, П. І. Нор, В. А. Єфіменко // *Стратегічна панорама*. – 2009. – № 4. – С. 119–127.
6. *Галака О. М.* Основні тенденції розвитку та ймовірні форми воєн і збройних конфліктів майбутнього // О. М. Галака, О. А. Ільшов, Ю. М. Павлюк // *Наука і оборона*. – 2007. – № 4. – С. 10–15.
7. *Ільшов О. А.* Тенденції розвитку збройної боротьби у війнах четвертого-шостого поколінь / О. А. Ільшов // *Наука і оборона*. – 2009. – № 3. – С. 43–48.
8. *Горбулін В.* Український фронт «четвертої світової війни» / В. Горбулін // *Хроніки передбачень: 2006–2017* / В. Горбулін. – Харків, 2017. – С. 19–30.
9. *Горбулін В.* Безпека 2010 / В. Горбулін // *Хроніки передбачень: 2006–2017* / В. Горбулін. – Харків, 2017. – С. 31–48.
10. *Горбулін В.* Конкістадор у панцирі залізім / В. Горбулін, В. Бадрак // *Хроніки передбачень: 2006–2017* / В. Горбулін. – Харків, 2017. – С. 49–56.
11. *Горбулін В. П.* «Гібридна війна» як ключовий інструмент російської геостратегії реваншу / В. П. Горбулін // *Стратегічні пріоритети*. – 2014. – № 4. – С. 5–12.
12. *Требін М. П.* «Гібридна» війна як нова українська реальність [Електронний ресурс] / М. П. Требін // *Український соціум*. – 2014. – № 3 (50). – С. 113–127. – Режим доступу : <https://doi.org/10.15407/socium.2014.03.113>.
13. *Магда Є.* Гібридна війна: вижити і перемогти / Є. Магда. – Харків : Віват, 2015. – 302 с.
14. *Магда Є.* Гібридна війна: сутність та структура феномену [Електронний ресурс] / Є. Магда // *Academia*. – Режим доступу : https://www.academia.edu/42584031/ГІБРИДНА_ВІЙНА_СУТНІСТЬ_ТА_СТРУКТУРА_ФЕНОМЕНУ.
15. *Магда Є.* Гібридна війна: питання і відповіді [Електронний ресурс] / Є. Магда // *DM Media Sapiens*. – Режим доступу : <https://ms.detector.media/media-analitika/post/13805/2015-07-27-gibrydna-viyna-pytannya-i-vidpovidi>.
16. *Власюк В. В.* Деякі основи поняття «гібридна війна» в міжнародному праві [Електронний ресурс] / В. В. Власюк, Я. В. Карман // *Право і громадянське суспільство*. – Режим доступу : <http://lcslaw.knu.ua/index.php/item/207-deyaki>.
17. *Рущенко І. П.* Російсько-українська гібридна війна: погляд соціолога : монографія / І. П. Рущенко. – Харків : Павленко О. Г., 2015. – 266 с.
18. *Світова гібридна війна: український фронт* [Електронний ресурс] : монографія / за заг. ред. В. П. Горбуліна ; Національний інститут стратегічних досліджень. – К. : НІСД, 2017. – 496 с. – Режим доступу : <https://niss.gov.ua/publikacii/monografii/svitova-gibridna-viyna-ukrainskiy-front-monografiya>.
19. *Власюк О. С.* Кремлівська агресія проти України: роздуми в контексті війни [Електронний ресурс] : монографія / О. С. Власюк, С. В. Кононенко ; Національний інститут стратегічних досліджень. – К. : НІСД, 2017. – 304 с. – Режим доступу : http://lib.rada.gov.ua/static/about/text/niss_Kreml-agressin_druk-d7e5f.pdf.
20. *Гібридна війна: in verbo et in praxi* [Електронний ресурс] : монографія / Донецький національний університет імені Василя Стуса ; під. заг. ред. проф. Р. О. Додонова. – Вінниця : Нілан-ЛТД, 2017. – 412 с. – Режим доступу : <https://jmonographs.donnu.edu.ua/issue/view/94>.
21. *Яворська Г. М.* Гібридна війна як дискурсивний конструкт [Електронний ресурс] / Г. М. Яворська // *Стратегічні пріоритети. Серія «Політика»*. – 2016. – № 4 (41). – С. 41–48. – Режим доступу : http://nbuv.gov.ua/UJRN/sppol_2016_4_7.
22. *Парахонський Б. О.* Онтологія гібридної війни: гра прихованих смислів [Електронний ресурс] / Б. О. Парахонський, Г. М. Яворська // *Стратегічна панорама*. – 2017. – № 1. – С. 7–16. – Режим доступу : http://nbuv.gov.ua/UJRN/Strp_2017_1_4.
23. *Комарчук О.* Гібридна війна: сутність та структура феномену [Електронний ресурс] / О. Комарчук // *Міжнародні відносини, суспільні комунікації та регіональні студії*. – 2018. – № 1 (3). – С. 48–54. – Режим доступу : <https://doi.org/10.29038/2524-2679-2018-01-48-54>.
24. *Комарчук О.* Загальна характеристика рис гібридної війни / О. Комарчук // *Науковий вісник Східноєвроп. нац. ун-ту ім. Лесі Українки. Серія «Міжнародні відносини»*. – 2016. – № 11 (336). – С. 45–51.
25. *Морозов О. М.* Визначення та складові системної (гібридної) війни / О. М. Морозов // *Антропологія*. – 2017. – № 2. – С. 3–9.
26. *Гібридні війни. Компоненти та особливості* [Електронний ресурс] / Ю. М. Лисецький, О. О. Старовойтенко, Ю. В. Семенюк, Д. Г. Павленко // *Вчені*

записки Таврійського нац-го ун-ту ім. В. І. Вернадсько-го. Серія: Публічне управління та адміністрування. – 2021. – Т. 32 (71), № 5. – С. 63–70. – Режим доступу : <https://doi.org/10.32838/TNU-2663-6468/2021.5/11>.

27. Лобко М. М. Об'єднана операція як основна форма відсічі збройній агресії «гібридного» типу [Електронний ресурс] / М. М. Лобко // Наука і оборона. – 2021. – № 2. – С. 24–33. – Режим доступу : <https://doi.org/10.33099/2618-1614-2021-15-2-24-33>.

28. Леун О. І. Корупція як фактор системної (гібридної) війни [Електронний ресурс] / О. І. Леун // Наука Онлайн. – Режим доступу : <https://nauka-online.com/publications/jurisprudence/2019/8/koruptsiya-yak-faktor-sistemnoyi-gibridnoyi-vijni>.

29. «Братня» навала. Війни Росії проти України XII–XXI ст. / В. Брехуненко, В. Ковальчук, М. Ковальчук, В. Корнієнко ; [за заг. ред. В. Брехуненка] ; Ін-т укр. археографії та джерелознавства ім. М. С. Грушевського НАН України. – Київ : Брехуненко Н. А., 2016. – 246, [1] с.

30. Головченко В. Гібридна війна Росії проти України: історико-політичне дослідження / В. Головченко, М. Дорошко. – К. : Ніка-Центр, 2016. – 184 с.

31. Левченко О. В. Еволюція гібридної війни Російської Федерації проти України [Електронний ресурс] / О. В. Левченко // Наука і оборона. – 2017. – № 2. – С. 11–16. – Режим доступу : <https://doi.org/10.33099/2618-1614-2017-0-2-11-16>.

32. Сегеда С. П. Гібридна війна Росії проти України: історичний вимір [Електронний ресурс] / С. П. Сегеда, В. П. Шевчук // Наука і оборона. – 2019. – № 1. – С. 31–35. – Режим доступу : <https://doi.org/10.33099/2618-1614-2019-6-1-31-35>.

33. Лемеха С. Острів Коса Тузла: як росія почала гібридну війну проти України 20 років тому [Електронний ресурс] / С. Лемеха // АрміяInform. – Режим доступу : <https://armyinform.com.ua/2023/09/28/ostriv-kosa-tuzla-yak-rosiya-pochala-gibrydnu-vijnu-proti-ukrayiny-20-rokiv-tomu>.

34. Жовтенко Т. Гібридна війна: анатомія інструментарію й перемоги [Електронний ресурс] / Т. Жовтенко // Фонд «Демократичні ініціативи» ім. Ілька Кучеріва. – Режим доступу : <https://dif.org.ua/article/gibridna-vijna-anatomiya-instrumentariyu-y-peremogi>.

35. Зятьєв С. Гібридна війна в медіа-просторі: українське «меню» сильніше за кремлівську брехню [Електронний ресурс] / С. Зятьєв // АрміяInform. – Режим доступу : <https://armyinform.com.ua/2023/10/04/gibrydna-vijna-v-media-prostori-ukrayinske-menyu-sylnishe-za-kremlivsku-brehyu>.

36. Гібридна війна Росії проти України. Як перемогти на інформаційному фронті [Електронний ресурс] : аналітичний посібник / Центр стратегічних кому-

нікацій та інформативної безпеки, Центр демократії та верховенства права // Google Диск. – Режим доступу : <https://drive.google.com/file/d/1AEUYRLeYOx7kBbNpJL1XzwHXstCNJaJW/view?pli=1>.

37. Шемаєв В. М. Когнітивна війна як складова сучасної гібридної війни [Електронний ресурс] / В. М. Шемаєв, Л. В. Єрьоміна // Юридичний науковий електронний журнал. – 2024. – № 7. – С. 300–304. – Режим доступу : <https://doi.org/10.32782/2524-0374/2024-7/73>.

38. Дерев'яно І. П. Гібридна війна як різновид асиметричних дій [Електронний ресурс] / І. П. Дерев'яно // Міжнародні відносини: теоретико-практичні аспекти. – 2023. – № 11. – С. 6–16. – Режим доступу : <https://doi.org/10.31866/2616-745X.11.2023.278396>.

39. Литвиненко О. Тотальна війна по-путінські: «гібридна» війна РФ проти України [Електронний ресурс] / О. Литвиненко // «Гібридна» війна Росії – виклик і загроза для Європи / Центр Разумкова. – Київ, 2016. – С. 45–48. – Режим доступу : https://razumkov.org.ua/images/Material_Conference/2016_12_14/GIBRID-WAR-FINAL-1-1.pdf.

40. Дацюк С. Про тотальну війну [Електронний ресурс] / С. Дацюк // Українська правда. – Режим доступу : <https://blogs.pravda.com.ua/authors/datsuk/6329f5f30ed76>.

41. Середін А. Війна в Україні як війна п'ятого покоління: чому ця війна не переросте у Третю світову [Електронний ресурс] / А. Середін // Політична теологія. – Режим доступу : <https://politteonline.com/materialy/vijna-v-ukrayini-yak-vijna-pyatogo-pokolinnya-chomu-czya-vijna-ne-pereroste-u-tretyu-svitovu>.

42. Mockaitis T. R. A hybrid war: the Indonesian Confrontation / T. R. Mockaitis // British counter-insurgency in the post-imperial era / T. R. Mockaitis. – Manchester, UK, 1995. – P. 14–44.

43. Mattis J. N. Future Warfare: The Rise of Hybrid Wars / J. N. Mattis, F. G. Hoffman // Proceedings. – 2005. – Vol. 131, No 11 (1233). – P. 18–19.

44. Hoffman F. G. Complex Irregular Warfare: The Next Revolution in Military Affairs [Електронний ресурс] / F. G. Hoffman // Orbis. – 2006. – Vol. 50, No 3. – P. 395–411. – Режим доступу : <https://doi.org/10.1016/j.orbis.2006.04.002>.

45. Hoffman F. G. Conflict in the 21st century: the rise of hybrid wars [Електронний ресурс] / F. G. Hoffman ; Potomac Institute for Policy Studies // Potomac Institute for Policy Studies. – Режим доступу : https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

46. Q. Liang. Unrestricted Warfare / Q. Liang, W. Xiangsui. – Beijing : PLA Literature and Arts Publishing House, 1999. – 228 p.

47. *Freier N. P.* Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context [Електронний ресурс] / N. P. Freier // US Army War College Press. – Режим доступу : <https://press.armywarcollege.edu/monographs/680>.
48. *Johnson D. E.* Military Capabilities for Hybrid War. Insights from the Israel Defense Forces in Lebanon and Gaza [Електронний ресурс] / D. E. Johnson // RAND. – Режим доступу : https://www.rand.org/pubs/occasional_papers/OP285.html.
49. *De Wijk R.* Hybrid Conflict and the Changing Nature of Actors [Електронний ресурс] / R. De Wijk // The Oxford Handbook of War / edited by Y. Boyer, J. Lindley-French. – Oxford, 2012. – P. 358–372. – Режим доступу : <https://doi.org/10.1093/oxfordhb/9780199562930.013.0025>.
50. *Manwaring M. G.* The Complexity of Modern Asymmetric Warfare / M. G. Manwaring. – Norman, OK : University of Oklahoma Press, 2012. – XVI, 208 p.
51. *Tenenbaum E.* Le piège de la guerre hybride [Електронний ресурс] / E. Tenenbaum // IFRI. – (Focus Stratégique / IFRI ; 2015, No 63). – Режим доступу : <https://www.ifri.org/fr/etudes/le-piege-de-la-guerre-hybride>.
52. *Thornton R.* The Changing Nature of Modern Warfare [Електронний ресурс] / R. Thornton // RUSI Journal. – 2015. – Vol. 160, issue 4. – P. 40–48. – Режим доступу : <https://doi.org/10.1080/03071847.2015.1079047>.
53. *Johnson R.* Hybrid warfare and counter-coercion [Електронний ресурс] / R. Johnson // The Conduct of War in the 21st Century. Kinetic, Connected and Synthetic / edited by R. Johnson, M. Kitzen, T. Sweijs. – London, 2021. – P. 45–57. – Режим доступу : <https://www.taylorfrancis.com/chapters/edit/10.4324/9781003054269-5/hybrid-warfare-counter-coercion-rob-johnson>.
54. *DeBenedictis K.* Russian ‘Hybrid Warfare’ and the Annexation of Crimea: The Modern Application of Soviet Political Warfare / K. DeBenedictis. – London : I.B. Tauris, 2022. – XVI, 262 p.
55. *McInnis M.* Russia and China look at the future of warfare [Електронний ресурс] / M. McInnis // ISW. – Режим доступу : <https://www.understandingwar.org/backgrounder/russia-and-china-look-future-war>.
56. *Bilal A.* Russia’s hybrid war against the West [Електронний ресурс] / A. Bilal // NATO Review. – Режим доступу : <https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html>.

P. M. Steshenko, Candidate of Technical Sciences, Senior Researcher, State Research Institute of Aviation,

P. B. Volotivskiy, Candidate of Military Sciences, Senior Researcher, State Research Institute of Aviation,

O. A. Zhevtiuk, Candidate of Technical Sciences, Senior Researcher, State Research Institute of Aviation

Creation of a special UAV-interceptor to counter UAVs of the «Shahed» type is an urgent task of the state

Among the unmanned aerial vehicles (UAVs) of the Russian Armed Forces, which are focused on performing most of the tasks of the so-called «special military operation» (SVO), currently the most widespread are unmanned aerial systems (UASs) with UAVs that solve the tasks of detecting and striking troops and ground objects. Countering these UAVs has become one of the main tasks of the Ukrainian air defence, on a par with missile defence. The experience of the Armed Forces of Ukraine in combating enemy UAVs indicates the almost absence of perfect specialized systems and means designed exclusively for countering UAVs.

Therefore, the finding of methods and means of countering enemy UAVs is becoming an even more urgent task for the defence forces of Ukraine. Among the effective means of countering UAVs, UAV interceptors are currently being considered. It is believed that the development of unmanned interceptors is becoming one of the main areas of development of unmanned aerial systems. Now it is time to move from the idea of the need to create an appropriate type of special UAV interceptors to its practical implementation. After all, unmanned equipment will become the main weapon system in the near future.

Key words: air defence, anti-drone defence, aircraft weapons, unmanned aerial vehicle-interceptor, method of application of an unmanned aerial vehicle-interceptor.

A. K. Pavlikovskiy, Candidate of Military Sciences, Associate Professor, National Defence University of Ukraine,

V. O. Tiutiunnyk, Candidate of Technical Sciences, Senior Researcher, Ivan Kozhedub Kharkiv National Air Force University,

V. A. Tkachenko, Candidate of Military Sciences, Senior Researcher, Central Research Institute of the Armed Forces of Ukraine,

N. I. Tkachenko, National Defence University of Ukraine

Increasing the effectiveness of countering the massive employment of strike unmanned aerial vehicles

In the process of the armed aggression against Ukraine, the Russian Federation resorts to the massive employment

of single-use strike unmanned aerial vehicles of the «Shahed-136/131» type, which fly over the territory of Ukraine at low and extremely low altitudes at a distance of up to 1,500 km, to inflict fire damage on civilian and military infrastructure facilities. The mass nature and relatively low cost of their production and employment make it irrational to use anti-aircraft missile systems to combat them due to the significant cost of anti-aircraft guided missiles. There is a need to find new ways to counter the massive employment of single-use strike unmanned aerial vehicles of the «Shahed-136/131» type that are less expensive than using anti-aircraft missile systems.

The article analyses the weaknesses of single-use strike unmanned aerial vehicles of the «Shahed-136/131» type and substantiates the possibility and conditions of using artillery (small arms) weapons to destroy them. It is shown that a rational way to use artillery (small arms) weapons to solve this problem is the actions of mobile fire groups from ambushes, which are promptly organized on the flight routes of strike unmanned aerial vehicles based on the notifications about an air enemy. The requirements for the organization of the fire system, reconnaissance system and aiming means of mobile fire groups armed with anti-aircraft guns or large-calibre machine guns are determined.

Key words: anti-aircraft gun, probability of hit, mobile fire group, air defence, rational composition of means, small arms, strike unmanned aerial vehicles.

V. A. Tymoshenko, Doctor of Juridical Sciences, Professor, National Defence University of Ukraine,

V. P. Otroshchenko, Armed Forces of Ukraine,

S. V. Dromov, Candidate of Juridical Sciences, Armed Forces of Ukraine

Legislative and regulative problems of awarding military personnel rewards for the destruction and capture of enemy equipment

The publication highlights the results of a study of the legislative and regulative problems of the mechanism for awarding military personnel rewards for the destruction and capture of enemy equipment. The specified mechanism is considered as one of the elements of the institution of motivation of the military personnel of the security and defence forces of Ukraine, which can be used to influence the process of forming a military personnel's interest in the military profession and awareness of its social significance.

The authors analysed the provisions of legislative acts and regulations that regulate the issues of awarding military personnel rewards for the destruction and capture of enemy equipment. Conclusions were drawn about

the imperfection of the provisions of the specified legislative acts and regulations and the existence of inconsistency between them.

The authors believe that when forming state policy in this area there is no systematic approach and proper scientific substantiation. Ways are proposed to improve the legislation of Ukraine that regulates the issues of awarding military personnel with rewards for the destruction and capture of enemy equipment.

Key words: national security, state sovereignty, independence, territorial integrity, Armed Forces of Ukraine, legislation and legal regulation, Constitution of Ukraine, motivation for military service, additional reward for military personnel, destruction of enemy equipment, damage of enemy equipment, capture of enemy equipment, martial law, combat operations journal.

I. B. Chepkov, Doctor of Technical Sciences, Professor, Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine,

V. M. Mozharovskyi, Doctor of Military Sciences, Professor, Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine,

P. I. Nor, Candidate of Technical Sciences, Senior Researcher, Central Research Institute of Armaments and Military Equipment of the Armed Forces of Ukraine

Modern general trends in the development of means of warfare

The analysis and systematization of the currently promising global trends in the development of means of warfare have been carried out in order to identify the trends common for the development of all services and branches of the armed forces. The development of armaments and military equipment of the majority of the developed countries of the world and the experience of their application during wars and military conflicts of recent decades, including the Russia-Ukraine war, have been analysed.

Key words: armed conflicts, means of warfare, armaments and military equipment, development trends, combat means, strike means.

V. V. Mashtalir, Doctor of Historical Science, Professor, National Defence University of Ukraine,

Yu. A. Husak, Doctor of Military Sciences, Professor, National Defence University of Ukraine

Development of the set of concepts on cyber defence and approaches to the creation of cyber forces in Ukraine

The increased attention to solving the tasks of cyber defence of the state is due to the development of cyber technologies and the formation of cyberspace as a separate sphere of struggle between states. In the modern world, cyber defence as a component of cybersecurity has a large number of problematic issues that require immediate resolution. In this regard, it is shown that in developed countries of the world this issue is given great attention and a list of important NATO events dedicated to these issues is given. An analysis of the set of concepts on cybersecurity and cyber defence, which is used in legislative and regulatory documents, is conducted. Based on the basic provisions of the art of war, a system of concepts in the field of cyber defence is proposed, for example, such as aggression in cyberspace, cyber combat, cyber attack and cyber defence, cyber operation, cyber strike, etc., and their definitions are provided. An analysis of the cyber forces of the leading NATO countries has been conducted, which indicates that the cyber forces of the leading NATO countries can have two organizational options: the first option involves the inclusion of cyber forces in the national armed forces and their interaction with civilian cyber units (USA, Germany), and the second option is the integration of military and civilian cyber units in a separate national structure (Great Britain, France). At the same time, regardless of the organizational option, each NATO country retains responsibility for national cyber defence, but at the same time carries out data exchange, coordination of exercises and development of joint cyber defence strategies. The areas for the development of the theoretical foundations of the creation of the cyber defence system of Ukraine are proposed, the implementation of which will make it possible to form cyber forces that are similar in composition, organization, tasks and functions to the cyber forces of NATO member states, to implement a unified cyber defence strategy in the Ministry of Defence of Ukraine and the Armed Forces of Ukraine, to manage cyber defence forces under martial law (special period).

Key words: cyber defence, cyberspace, cyber defence system, cyber defence entities, cyber troops, cybersecurity, cyber defence, cyber system, cyberattack, cyber offensive, cyber operation.

M. V. Koval, Doctor of Military Science, National Defence University of Ukraine,

V. V. Mashtalir, Doctor of Historical Science, Professor, National Defence University of Ukraine,

O. M. Zahorka, Doctor of Military Science, Professor, National Defence University of Ukraine

Assessment of the results of a war of attrition: methodological provisions

The strategy of attrition in modern warfare is the main concept of achieving the goals of war. The results of a war of attrition depend primarily on the military potentials of the opposing sides, which are composed of military-economic, spiritual, military-political, military scientific and technological, combat potentials (components).

The article proposes a methodology for assessing the results of war, which is based on taking into account the ratio of factors that influence the components of the military potentials of the parties. In the methodology, the assessment of the results of war is carried out by comparing (ranking) the categories of assessment, for example, victory, defeat, etc., which are set by the decision-maker.

For ranking (prioritizing) the categories of assessment of the results of war, the analytic hierarchy process is used, which uses a four-level hierarchy of problem solving: goal – components of military potential – factors – categories (alternatives).

The methodology allows you to determine the priorities of the categories of assessment of the results of the war of attrition for the current time and the forecasted period, depending on the circumstances, for the adoption of appropriate decisions by state and military authorities.

Key words: war of attrition; categories of assessment of results; military potential; priorities; analytic hierarchy process.

M. S. Karmazina, Doctor of Political Science, Professor, Yevhenii Berezniak Military Academy,

I. V. Ablazov, Candidate of Political Science, Professor, Yevhenii Berezniak Military Academy

The concept of «hybrid warfare»: an analysis of scientific discourse

Using methods of historical retrospection, comparison, real time, etc. the transformation of researchers' reflections on the essence and nature of war is investigated. There is an opinion that from the turn of the XX–XXI centuries and until now, the war of the hybrid era has occupied one of the prominent places in the scientific discourse and is interpreted in the context of total, unlimited, asymmetric or, ultimately, hybrid war, etc. Currently, there is a strong research interest in the process of crystallization of the very concept of hybrid war, its components, and development features. The researchers focus on the experience and lessons of the Russian hybrid war against Ukraine and the countries of the West, noting that hybridity will remain a kind of military trend in the coming years and decades, and therefore should be subject to careful analysis.

Key words: hybrid warfare, total warfare, unlimited warfare, asymmetric conflicts, Russian hybrid aggression against Ukraine.

Основні вимоги до оформлення статей, які подаються до журналу «Наука і оборона»

Журнал приймає для опублікування статті українською або англійською мовами. Анотації статей подаються українською та англійською мовами.

Журнал «Наука і оборона» включений до категорії «Б» наукових фахових видань України (наказ Міністерства освіти і науки України № 409 від 17 березня 2020 р.).

Спеціальності, за якими видання публікує наукові праці:

253 – Військове управління (за видами збройних сил);

254 – Забезпечення військ (сил);

255 – озброєння та військова техніка;

256 – Національна безпека (за окремими сферами забезпечення і видами діяльності);

263 – Цивільна безпека.

Подані авторами статті повинні за змістом відповідати тематиці журналу та вимогам щодо опублікування наукових статей. Передусім приймаються матеріали, в яких викладені результати наукових досліджень, спрямованих на розв'язання проблем, що мають важливе оборонне значення, статті, які містять нові теоретичні ідеї, принципи, концепції, моделі, спрямовані на пояснення певних явищ і процесів у галузі національної безпеки і оборони та прогнозування їх розвитку. Також приймаються до опублікування статті практичного змісту, які висвітлюють актуальні питання національної безпеки і оборони, науково-методичні та оглядові статті, інформаційні повідомлення про наукові новини і події.

Рукопис статті повинен бути підготовлений з використанням комп'ютера і подається до редакції в електронному вигляді. Для цього автори можуть скористатися своїми обліковими записами, попередньо зареєструвавшись на сайті журналу (<http://nio.nuou.org.ua>), або надіслати статтю на електронну пошту редакції журналу (nio2017@ukr.net).

Загальний обсяг рукопису разом з графічними матеріалами не повинен перевищувати 20 сторінок у форматі паперу А4. Поля сторінок, мм: зліва – 30, справа – 10, зверху та знизу – 20. Сторінки мають бути пронумеровані.

Основний текст статті друкується шрифтом Times New Roman чорного кольору прямого накреслення через півтора міжрядкові інтервали кеглем 14. Допускається авторські акценти виділяти напівжирним шрифтом або курсивом.

На першій сторінці рукопису розміщуються індекс УДК, назва статті, анотація, перелік ключових слів і далі текст статті. Обсяг анотації – у межах 120–150 слів, включаючи ключові слова.

У кінці статті наводиться перелік джерел, на які є посилання у тексті статті. Бібліографічні описи джерел у переліку оформлюються згідно з ГОСТ 7.1:2006. Нумерація джерел – відповідно до порядку появи їх у тексті статті.

Рисунки, таблиці, формули, посилання оформлюються відповідно до ДСТУ 3008:2015.

Ілюстрації, виконані в окремих графічних редакторах, подаються як у середині тексту, так і в окремих файлах, створених цими редакторами.

Для забезпечення гарантій сліпого рецензування відомості про авторів у файлі статті не наводяться. У разі подання статті на сайті журналу ці відомості необхідно занести у відповідні поля форми подання. Якщо стаття надсилається до редакції електронною поштою, їх необхідно розмістити в окремому файлі. Відомості про авторів надаються за формою: прізвище, ім'я та по батькові, науковий ступінь та вчене звання, найменування посади та місце роботи, військове звання, почесні звання, ідентифікатор ORCID, інформація для зворотного зв'язку (телефонні номери, адреса електронної пошти).

Про журнал «Наука і оборона»

Науково-теоретичне та науково-практичне видання «Наука і оборона» було започатковане з огляду на загальну потребу суспільства, державних діячів, політиків, учених, військових – усіх, хто опікується питаннями національної безпеки та оборони і професійно працює в цій сфері, – у друкованому засобі масової інформації, на сторінках якого обговорювалися б актуальні проблеми воєнної політики й реформування оборонної галузі держави та публікувалися б результати наукових досліджень з питань воєнної безпеки України, з воєнно-теоретичних і військово-технічних питань.

Часопис видається на громадських засадах. Найміцнішою його опорою в нелегкий час становлення були читачі та автори. Редакційна колегія сподівається на Вашу подальшу, шановні друзі, підтримку діяльності журналу «Наука і оборона», яка має на меті:

- сприяння створенню необхідного науково-теоретичного підґрунтя для постановки та розв'язання завдань військового будівництва шляхом опублікування

інформації щодо результатів основних напрямів наукових досліджень, які стосуються оборонної сфери;

- сприяння обговоренню нагальних питань реформування оборонної сфери всіма, хто опікується питаннями національної безпеки та оборони і професійно працює в цій галузі;

- поширення воєнно-наукових знань;
- сприяння підвищенню професійного рівня військовослужбовців Збройних Сил України та інших військових формувань, утворених згідно із чинним законодавством України.

Статті до друку відбираються з урахуванням результатів рецензування членами редакційної колегії або зовнішніми фахівцями. Передусім приймаються матеріали, в яких на підставі виконаних авторами досліджень розв'язано проблему, що має важливе оборонне значення.

Видання розповсюджується за передплатою.

Редакційна колегія може мати точку зору, відмінну від поглядів авторів.

**Видання розповсюджується за передплатою.
Передплата здійснюється у поштових відділеннях.
Передплатний індекс 74303.**

**Поточні та попередні номери журналу можна замовити у видавництві за адресою:
stylos.publish@gmail.com**

Електронні версії попередніх випусків журналу «Наука і оборона» можна знайти на веб-сторінці журналу: <http://nio.nuou.org.ua>, а також на сайті Національної бібліотеки України ім. В. І. Вернадського: www.nbuv.gov.ua

Усі права застережені.
Переклад і передрук – лише за згодою авторів і редакції.
Адреса редакції:
03049 Київ, проспект Повітряних Сил, 28.
Тел.: (044) 271-08-91, (067) 790-23-22, (066) 362-79-50.
E-mail: nio2017@ukr.net.
<http://nio.nuou.org.ua>.
Ідентифікатор медіа R30-01599.

© Національний університет оборони України, 2025

Підп. до друку 26.03.2025 р.
Формат 60x90/8. Папір офс. Друк офсет.
Ум. друк. арк. 8,5. Обл.-вид. арк. 9,6.

Видавничий дім «Стилос».
04080, Київ, вул. Оленівська, 8, к. 2.
Тел.: (050) 331-85-03.
E-mail: stylos.publish@gmail.com.
<http://www.stylos.com.ua>.

Свідоцтво про внесення до Державного реєстру суб'єктів видавничої справи України ДК № 1465 від 13.08.2003 р.