ISSN 2304-2699

Збірник наукових праць
Центру воєнно-стратегічних досліджень
Національного університету оборони України

№ 2(78), 2023

УДК 355:623 (08)

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

Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України.
2023. № 2(78).

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

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

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

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

Рекомендовано до друку рішенням Вченої ради Національного університету оборони України (протокол № 11 від 25.09.2023)

Головний редактор: ЗАГОРКА Олексій Миколайович, доктор військових наук, професор
Редакційна колегія:
БОГДАНОВИЧ Володимир Юрійович, доктор технічних наук, професор;
БИЧЕНКОВ Василь Васильович, доктор технічних наук, ст. наук. співробітник;
БОЧАРНІКОВ Віктор Павлович, доктор технічних наук, професор;
ГАВЛІЧЕК Петро, кандидат технічних наук, професор (Польща);
ГАЛАГАН Віктор Іванович, кандидат військових наук, доцент (науковий редактор);
КАРПЕНКО Микола Іванович, доктор юридичних наук, доцент;
КІРПІЧНІКОВ Юрій Анатолійович, кандидат технічних наук;
КОРЕЦЬКИЙ Андрій Анатолійович, кандидат військових наук, ст. наук. співробітник;
КОСЕВЦОВ В'ячеслав Олександрович, доктор військових наук, професор;
КОТЛЯРЕНКО Олександр Петрович, кандидат юридичних наук;
ЛОБКО Михайло Миколайович, кандидат військових наук, доцент;
МАЙСТРЕНКО Олександр Васильович, доктор військових наук, старший дослідник;
МАРКО Іван Юрійович, доктор економних наук, професор;
МЕДВІДЬ Людмила Петрівна, кандидат юридичних наук, доцент;
МОСОВ Сергій Петрович, доктор військових наук, професор;
НІЛЛСОН Ніклас, PhD (Military), assistant professor (Швеція);
ПАВЛІКОВСЬКИЙ Анатолій Казимирович, кандидат військових наук, доцент;
ПРИПОЛОВА Людмила Іванівна, кандидат юридичних наук, старший дослідник;
РИБИДАЙЛО Анатолій Анатолійович, кандидат технічних наук, ст. наук. співроб. (відп. редактор);
РУСНАК Юрій Іванович, кандидат юридичних наук;
РОСЕТ Том, PhD, Associate Professor;
СЕМОН Богдан Йосипович, доктор технічних наук, професор;
СНІЦАРЕНКО Петро Миколайович, доктор технічних наук, ст. наук. співробітник;
ТЕЛЕЛИМ Василь Максимович, доктор військових наук, професор;
ТИМОШЕНКО Радіон Іванович, доктор військових наук, ст. наук. співробітник;
ТКАЧ Іван Миколайович, доктор економічних наук, доцент;
ТОПОЛЬНІЦЬКИЙ Віталій Володимирович, кандидат юридичних наук;
ФАТТЕРЛІ Росс, PhD (War Studies) adjunct professor (Канада);
ФРОЛОВ Валерій Семенович, кандидат військових наук, ст. наук. співробітник;
ШЕВЧЕНКО Віктор Леонідович, доктор технічних наук, професор;
ШОПІНА Ірина Миколаївна, доктор юридичних наук, професор;
ЩИПАНСЬКИЙ Павло Володимирович, кандидат військових наук, професор

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

Редакція може не поділяти думку авторів.
Автори відповідають за достовірність поданих матеріалів.
Посилання на збірник у разі використання його матеріалів попереджує плагіат.
© ЦВСД НУО України, 2023

CONTENT

ЗМІСТ

УДК 339.96+355.45 (477) DOI: https://doi.org/10.33099/2304-2745/2023-2-78/6-19

Кириленко В. І., доктор економічних наук, професор[1] (0000-0002-4950-0378)
Шевченко М. М., кандидат філософських наук, доцент[2] (0000-0002-1139-1970)
Лепіхов А. В.[3] (0000-0003-0745-8113)
Храпач Г. С.[4] (0000-0002-1089-1535)

[1] – Київський національний економічний університет імені Вадима Гетьмана, Київ;
[2] – Управління забезпечення реагування на кризові ситуації при МО України, Київ;
[3] – Центр безпекових досліджень Національного інституту стратегічних досліджень, Київ;
[4] – Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Проблеми забезпечення національної безпеки від загроз геоекономічних війн: теоретичний і практичний досвід США та Японії – уроки для України

Резюме. Розглянуто перспективні теорії науковців США щодо впливу гострої геоекономічної конкуренції могутніх держав світу на посилення воєнно-стратегічної нестабільності, зростання міжнародної конфліктності та загроз державному суверенітету менш розвинених країн. Досліджено стратегії США та Японії щодо протидії загрозам геоекономічних війн. Здійснено огляд перспективних науково-дослідницьких здобутків України у сфері забезпечення економічної безпеки. Запропоновано підходи до проєктування нової удосконаленої моделі системи забезпечення економічної безпеки України, з урахуванням сучасного розвитку стратегічного безпекового середовища.

Ключові слова: глобалізація; геоекономіка; міждержавна взаємозалежність; геополітичне протиборство; геоекономічні війни; зовнішньоекономічне примушення; економічна безпека; національна безпека.

Постановка проблеми. Стратегічним курсом у сфері забезпечення економічної безпеки України, поміж іншого, передбачено виконання таких основних завдань:

“забезпечення стійкості від зовнішніх і внутрішніх викликів та загроз національним економічним інтересам держави та інтересам її громадян”;

“гарантування національної економічної незалежності та здатності до захисту національних економічних інтересів…”.

Ці пріоритети визначено у розділі 3 пункту 18 Стратегії економічної безпеки України на період до 2025 року від 11.08.2021 [1]. Ці пріоритетні завдання актуалізуються у розрізі геоекономічних проблем, а саме:

Україна володіє потужним економічним потенціалом і природними ресурсами. Їх значущість для міжнародної економіки у майбутньому лише посилюватиметься з урахуванням наявних загроз для розвитку і безпеки людства [2], тому Україна знаходиться на перетині національних інтересів провідних держав світу, які є центрами світової економіки. Економічно могутні держави знову і знову перебувають у гострій конкуренції на глобальному ринку, яка часто набирає форм геополітичного протиборства економічними засобами тиску (геоекономічної війни) [3]. Могутні держави реалізують геостратегії комплексного досягнення геоекономічних, геополітичних, воєнно-політичних та інших цілей. Використовуються технології гібридних загроз, політика санкцій. Посилюються небезпеки збройних конфліктів, які заподіюють міжнародні кризи та загрожують суверенності менш розвинених країн [4].

Прикладом є збройна агресія Російської Федерації (РФ) проти України. Воєнний конфлікт супроводжується геополітичним протиборством РФ з державами НАТО та ЄС фінансово-економічними, воєнно-політичними та іншими засобами. Стратегічним цілям держав-суперників характерний певний рівень антагоністичності. Вони тісно пов’язані з геополітичним майбутнім України як однієї із ключових геоекономічних ланок у Центральній Європі та у воєнно-стратегічному просторі Європейської системи безпеки [5, 6]. Через наслідки воєнного конфлікту національна економічна система України в кризовому стані. Перспективи виходу з війни та відновлення України залежить від посиленої допомоги міжнародних фінансових організацій і держав-партнерів. Водночас відбувається суттєве збільшення зовнішнього державного боргу при знижені боргової стійкості України. Зросла її макроекономічна

нестабільність. Знищується збройним шляхом економічна інфраструктура України. Критично скоротилося промислове виробництво. Блокується або обмежується експорт української продукції. Вельми зріс імпорт іноземних товарів до Української держави тощо [7].

За таких умов, нинішня система забезпечення економічної безпеки України (СЗЕБ) стала суттєво вразливою та потребує досконалої оптимізації до сучасних і майбутніх змін стратегічного безпекового середовища.

Ці обставини визначають зв'язок з важливими науковими завданнями:

1) аналіз іноземних і вітчизняних наукових теорій та досвіду щодо забезпечення національної безпеки від загроз геоекономічних війн;

2) удосконалення наявних та напрацювання нових форм і методів забезпечення економічної безпеки України від геоекономічних та інших деструктивних впливів.

Аналіз останніх досліджень і публікацій. Дослідження геоекономічної конкуренції, спричинених цим тригерів міжнародної конфліктності та загроз національній безпеці, зокрема і в економічній сфері, здійснювали вітчизняні [3, 4, 7, 17–24] та іноземні дослідники [2, 5, 8–14]. Науковці вивчали: явища – "геополітичне протиборство", "геоекономіка", "геоекономічна війна", "міждержавна взаємозалежність в епоху глобальної економіки", а також механізми забезпечення економічної безпеки тощо.

Однак на сьогодні існує ще обмаль наукових праць, у яких би вивчався перспективний теоретичний і практичний досвід провідних держав світу щодо протидії іноземним стратегіям геополітичного протиборства економічними засобами тиску. Також недостатньо розглядалася проблема методичного забезпечення державної політики національної безпеки України з питань запобігання та реагування на зовнішньоекономічні загрози та наслідки геоекономічних війн.

Водночас аналізуючи наукові досягнення та практичний досвід іноземних держав у сфері забезпечення економічної безпеки доцільно констатувати, що найбільш перспективними є науково-теоретичні дослідження та підходи до застосування здобутих знань у державно-управлінській практиці, які реалізуються в США та Японії. Зазначені держави мають високорозвинені економіки та є центрами світового економічного розвитку. Це досягнуто не лише завдяки новітнім технологіям та інноваціям, але й стратегічному партнерству між зазначеними країнами, тісному міжнародному співробітництву з іншими державами, накопиченій базі знань і досвіду у сфері забезпечення економічної безпеки, розвиненим спроможностям здійснювати вплив на розвиток стратегічного безпекового середовища. Зокрема, авторами проаналізовано деякі перспективні дослідження науковців США за проблематикою протидії загрозам геоекономічних війн [8–14], розглянуто окремі нормативно-правові акти США у сфері захисту економічних інтересів [15], а також чинну стратегію національної безпеки Японії у контексті аналізу цілей і завдань щодо реагування на виклики гострої геоекономічної конкуренції [16]. З'ясовано, що у даних державах приділяється значна увага науці з проблем економічної безпеки, удосконаленню форм і методів посилення готовності, запобігання та реагування на зовнішньоекономічні загрози національній безпеці, які виникають унаслідок геоекономічних війн на міжнародній арені. Для України знання й досвід США та Японії у сфері забезпечення економічної безпеки є вельми корисними у контексті обрання та розбудови (на основі перспективних наукових теорій та світових практик) перспективної національної моделі СЗЕБ України, яка має ефективно протидіяти сучасним економічним та іншим загрозам стратегічного безпекового середовища.

Мета статті полягає в:

аналізі теорії та практики щодо захисту національних інтересів від загроз геоекономічних війн, які проводилися у цілях зміцнення національної безпеки США та Японії;

аналізі сучасних науково-дослідницьких здобутків України щодо забезпечення національної безпеки, насамперед, в економічній сфері;

оцінюванні перспективності досвіду США та Японії, а також вітчизняних наукових досягнень у сфері забезпечення економічної безпеки для їх застосування з метою удосконалення СЗЕБ України.

Вирішення завдань дослідження потребує використання: системно-діяльнісного підходу, що ґрунтується на принципах проблематизації, структуризації і

дивергенції; кібернетичного підходу, який стосується досліджень розвитку організаційних і управлінських спроможностей держави; інституціонального підходу; проблемно-структурного та програмно-середовищного методів; методу порівняльного аналізу для вивчення першоджерел з досліджуваної теми, а також для вивчення зарубіжного досвіду науково-методичного забезпечення розроблення політики національної безпеки та її складової економічної безпеки; методу структурно-функціонального моделювання.

Виклад основного матеріалу. Дослідники США (Д. В. Дрезнер, Г. Фаррелл, А. Л. Нюман) [8–11] у 2019–2021 рр. розробили теорію міждержавної взаємозалежності, як явища глобалізації. Вивчався вплив цього явища на розвиток глобальних торгово-економічних, фінансових та інформаційних мереж, а також на зростання міжнародної конфліктності через геоекономічні війни. Досліджувалися методи зовнішньоекономічного примушення з боку одних держав стосовно інших країн, а також наслідки геополітичного протиборства економічними засобами тиску для конкуруючих держав.

Результати їх досліджень дають змогу констатувати, що глобалізація посилює інтеграційну взаємозалежність держав у світовому розвитку. Наслідком інтеграції є утворення глобальних і регіональних мереж міждержавного співробітництва на чолі з державами, так званими центрами сили – дослідники зосереджують увагу на США, Китаї, Великій Британії, провідних державах ЄС, а також РФ. Вони є центрами світової економіки, які розвивають між собою економічне співробітництво, але одночасно перебувають в умовах конкуренції, яка може посилювати конфліктні суперечності. У найгострішій невоєнній формі – це має прояв у вигляді геополітичного протиборства із застосуванням економічних засобів, а також іншого інструментарію гібридної війни.

Термін "держава-центр сили" чітко не визначається дослідниками. Проте вони характеризують його як – держава, яка завдяки національній могутності здатна істотно впливати на світовий або регіональний порядок співіснування менш розвинених країн. Така держава є ключовим співзасновником однієї із світових мереж міждержавного співробітництва, зокрема, комплексно у сферах виробництва та постачання ресурсів і технологій, товарів і послуг, а також логістики, інформаційних та фінансових мереж та ін. Зазначені могутні держави реалізують зовнішню політику спрямовану на:

1. Зміцнення спроможностей та розширення підконтрольних державі-центру сили глобальних і регіональних мереж міждержавного співробітництва, шляхом політики "м'якої сили". Нарощування геоекономічного впливу на менш розвинені країни та розвитку економічного співробітництва з ними для отримання спільної вигоди. Посилення залежності менш розвинених країн від національної могутності держави-центра сили.

2. Здобуття стратегічних переваг над іншими могутніми державами-конкурентами (центрами сили). Реалізація стратегій стримування держав-суперників в економічному, технологічному, воєнному та іншому розвитку, їх впливу на міжнародній арені, з одночасним продовженням співробітництва з ними у вигідних сферах співпраці [8–11].

Дослідження Г. Фаррелла та А. Л. Ньюмана свідчать, що держави-центри сили з метою централізації управління над мережами міждержавного співробітництва, комплексно застосовують такі методи [10].

Метод "Ефект панoптікона" *(англ. panopticon effect)* – збір розвідувальних даних стосовно фінансово-економічних та інших уразливостей менш розвинених країн з метою використання цієї інформації для посилення їх залежності від держави-центра сили. Використовується фактор залежності менш розвинених країн від глобальних інформаційних і фінансово-банківських систем, які контролюються державою-центром сили, завдяки чому остання спроможна отримати доступ до необхідних відомостей з урядових та інших інформаційно-аналітичних баз даних менш розвиненої країни.

Метод "Ефект уразливих точок" *(англ. chokepoint effect)* – здійснення державою-центром сили санкційного та іншого тиску на ключові вразливості менш розвинених країн, реалізуючи тим самим стратегію економічного примушення. Метод застосовується тоді, коли уряд менш розвиненої країни незгоден із зовнішньою політикою держави-центра сили, що спричиняє розбалансування інтересів та гострі суперечності. Зокрема, вводяться квоти та обмеження на постачання критично важливих товарів і ресурсів. Обмежується доступ до

послуг глобальних міжбанківських та інших фінансових систем, а також інформаційно-телекомунікаційних мереж. Практикується відмова у передаванні новітніх технологій. Створюються "боргові пастки", шляхом надання позик менш розвиненим країнам у спосіб, який ігнорує їх боргову стійкість. Може здійснюватися арешт іноземних активів країни. Запроваджуються тарифні бар'єри для експорту продукції на зовнішні економічно-торгівельні ринки тощо [10].

Дослідження Д. В. Дрезнера вказують на парадоксальне явище, яке виникає під час застосування цих методів, а саме, методи можуть ефективно застосовуватися проти менш розвинених країн. Водночас, виникає протилежний ефект якщо їх використовують один проти одного відносно рівні за національною могутністю держави-центри сили. Ефект посилюється у разі їх значної міждержавної взаємозалежності у фінансовій, економічній, технологічній та інших сферах [11].

Зокрема, держави-центри сили послідовно запроваджують санкції один проти одного та отримують рівнозначний спротив у відповідь у перебігу геоекономічної війни. Посилюється міждержавна криза, за якої політика санкцій наносить шкоду обом конкуруючим державам-центрам сили. Поглиблення кризи збільшує витрати, гальмує розвиток національних економік, не дає змоги здобути стратегічних переваг і спричиняє гостру міждержавну конфліктність. Це приводить геоекономічну війну у глухий кут і потребує перезавантаження зовнішньоекономічних та інших міждержавних відносин шляхом пошуку компромісів. У протилежному випадку зростає ймовірність загострення воєнно-політичної обстановки та виникнення збройного конфлікту, що спричинятиме руйнівні наслідки державам-центрам сили та її союзникам. Менш розвинені країни можуть стати жертвами перерозподілу державами-центрами сили геополітичного, геоекономічного та воєнно-політичного впливу на міжнародній арені із застосуванням ними військових та гібридних методів протиборства [11].

Підтвердженням є дослідження, які проводили науковці США, а саме: Т. Г. Манкен [12], Р. Д. Блеквілл, Дж. Харріс [13], С. Кук [14]. Вони вивчали стратегії міждержавного протиборства, зокрема щодо застосування інструментарію економічного тиску для досягнення геополітичних та воєнно-політичних цілей. Також розглядалися стратегії використання військової сили, спецслужб для досягнення геоекономічних цілей. Їх дослідження свідчать, що провідні держави світу часто реалізують комплекс стратегій-конкуренції, цілеспрямованих на: досягнення стратегічних переваг; забезпечення стратегічного стримування держави-суперника; примушення його до збільшення витрат або виснаження противника; спонукання уряду конкуруючої країни до політики, яка спричинить поразку; підрив політичної та економічної систем держави-суперника, змушуючи її уряд йти на поступки для уникнення політичного розпаду. Це регулярно супроводжується проявами гібридних загроз, таких як демонстрація воєнної сили, тероризм, кібератаки, диверсії, інформаційно-психологічні операції, дестабілізація суспільно-політичної ситуації, конфлікти низької інтенсивності, блокування поставок критично важливих ресурсів, товарів і послуг, а також часто перебуває на порозі початку відкритої війни [12–14].

Науково-теоретичні дослідження на кшталт [8–14], а також висновки та рекомендації дослідників враховуються урядами США та Японії під час розроблення національної політики забезпечення економічної безпеки з метою зниження ризиків і загроз від геоекономічних війн та ефективного реагування на їх наслідки.

Досвід США. Адміністрацією президента США затверджено виконавче Розпорядження "Про забезпечення стійкості та безпеки ланцюгів постачання критично важливих ресурсів, товарів, послуг та технологій до США" від 24.02.2021 *(англ. – Executive Order on America's Supply Chains)* [15]. Вимоги документа зорієнтовані на комплексний захист національної економіки США від геоекономічних та інших загроз, які через каскадний ефект можуть спричинити кризові наслідки для сталого розвитку та безпеки і оборони.

Згідно з цим розпорядженням, урядом цієї держави реалізується стратегія, яка комплексно спрямована на забезпечення економічної безпеки та стійкості США до геоекономічних та інших загроз на випадок кризових ситуацій, а також проведено низку реформ. Стратегічними цілями є такі: підвищення ефективності управління ризиками; покращення конкурентоздатності країни; запобігання монополіям та корупції; створення альтернативних ланцюгів поставок та їх диверсифікація; розвиток імпорту-

заміщення; підвищення контролю за іноземними активами; нарощування внутрішнього виробництва критично важливих товарів і послуг; зміцнення виробничої бази; формування надлишкових резервів критично-важливих ресурсів і товарів; удосконалення функції держави щодо фінансування національної політики США стосовно забезпечення внутрішнього виробництва та безперервності постачання важливих ресурсів, товарів і послуг; розвитку науково-дослідницької діяльності, перспективних інновацій і технологій щодо виробництва дефіцитної продукції; зміцнення надійності інформаційно-цифрових мереж, забезпечення їх кібербезпеки; розширення та підвищення стійкості транспортної логістики; розвиток робочих місць та підготовка висококваліфікованих фахівців міжнародного рівня; підтримка середнього бізнесу; сприяння економічному зростанню недостатньо розвинених районів країни; посилення міжнародного співробітництва з країнами-союзниками для спільного забезпечення стійких поставок та колективної безпеки; зміцнення спроможностей щодо реагування на міжнародні кризи та ін. [15].

Досвід Японії. В абз. (vi) пп. 5 п. 2 розділу IV Стратегії національної безпеки Японії від 16.12.2022 щодо стратегічних підходів у сфері забезпечення економічної безпеки визначено: *"Японія сприятиме ефективним зусиллям проти економічного примусу з боку іноземних держав"*. Також в абз. 1 пп. 6 п. 2 розділу IV цієї стратегії стосовно пріоритетів зовнішньої політики Японії за напрямом розвитку та зміцнення міжнародного економічного порядку, зазначено: *"...Японія посилить національні зусилля щодо протидії недобросовісній торговій практиці та економічному примусу, у тому числі шляхом реалізації заходів зі зміцнення міжнародних норм у співпраці зі своїм союзником та країнами-однодумцями"* [16]. До того ж у цій стратегії ключовим союзником визначено США. Для реалізації цих стратегічних підходів, стратегією визначено пріоритетні завдання державної політики Японії щодо комплексного забезпечення економічної безпеки:

1. Зміцнювання відкритого і стабільного міжнародного економічного порядку, запобігаючи невійськовому тиску з боку окремих держав, які здійснюють його з метою перешкоджання прийняттю іншими країнами незалежних зовнішньополітичних рішень, а також їх національному економічному розвитку.

2. Всеохоплююче сприяння зміцненню міжнародної торговельної системи, основою якої є Світова організація торгівлі *(англ. World Trade Organization, WTO)*. Запровадження ініціатив щодо удосконалення її інституційних, правових і організаційних механізмів щодо протидії недобросовісній конкуренції та загрозам від зовнішньоекономічного примушення.

3. Розвиток вільного і справедливого економічного порядку, сталого економічного зростання в Індо-Тихоокеанському регіоні.

4. Посилення взаємовигідного співробітництва з питань вдосконалення міжнародних норм, правил та стандартів щодо здійснення справедливим способом фінансування країн, які розвиваються. Це стосується викорінення негативної практики економічно потужних держав щодо цілеспрямованого створення ними "боргових пасток" для країн, які розвиваються через непрозорі форми фінансової допомоги, що спричиняє зростання зовнішнього державного боргу слабких держав в умовах їх низької боргової стійкості. [16].

5. Удосконалення системи постійного моніторингу, стратегічного аналізу і прогнозування, оцінювання ризиків, ідентифікації загроз, аналізу та оцінки вразливостей, а також спроможностей, планування у сфері забезпечення економічної безпеки Японії.

6. Удосконалення правових норм Закону Японії "Про сприяння економічній безпеці" від 11.05.2022 № 43 *(англ. Act No. 43, 2022; the "Economic Security Promotion Act")* та інших організаційних та правових засад у цій сфері, здійснення державного нагляду за неухильним дотриманням їх вимог.

7. Забезпечення диверсифікації, стабільності і безперервності постачання критично важливих ресурсів, товарів і послуг до Японії. Зниження надмірної залежності від поставок з іноземних держав, особливо, з якими у Японії нестабільні відносини, а також країн, які намагаються узалежнити Японську державу від своїх ресурсів, товарів і послуг. Удосконалюватимуться механізми фінансування цієї національної політики Японії.

8. Здійснення періодичного перегляду та удосконалення державних процедур закупівлі, зокрема тих, які проводяться місцевими префектурами. Посилення ревізійних

перевірок у сфері функціонування критично важливої інфраструктури економіки Японії.

9. Підвищення інформаційної безпеки національної економічної системи Японії. Посилення режиму доступу до конфіденційних відомостей (у тому числі комерційної таємниці) та порядку обміну інформацією обмеженого доступу. Забезпечення безпеки та надійності інформаційно-телекомунікаційних послуг та технологій, а також урядових, економічних, фінансових та інших інформаційно-аналітичних систем збору та обробки даних. Проведення аудиту системи забезпечення інформаційної безпеки Японії.

10. Удосконалення процедур експортного контролю, нагляду за іноземними активами та інвестиціями тощо.

11. Розвиток науки у сфері забезпечення економічної безпеки та інше [16].

Результати дослідження актуальних загроз економічній безпеці України в умовах воєнного стану [7], а також розглянутих іноземних теорій і практики дають змогу констатувати таке [8–16].

Нині функціонуюча СЗЕБ України неспроможна забезпечити ефективну захищеність національної економічної системи України від економічних загроз в умовах воєнного стану. Також СЗЕБ України є малоефективною в обставинах гострого геополітичного протиборства могутніх держав світу та застосування ними воєнно-політичних, фінансово-економічних, енергетичних, інформаційних та інших невійськових засобів тиску. У майбутньому проблема посилюватиметься впливом чинника технологічного та інноваційного світового прогресу. З одного боку, прогрес сприятиме розвитку глобального світового господарства та національної економіки країн світу. Разом з тим, ймовірно з'являтимуться нові форми та методи геоекономічних війн, виникатимуть більш універсальні гібридні загрози національній безпеці в умовах гострої геоекономічної конкуренції та міжнародної конфліктності. Можна спрогнозувати, що СЗЕБ країн світу будуть поступово трансформуватися у нові більш стійкі та гнучкі моделі, а також адаптуватися до майбутніх реалій стратегічного безпекового середовища на сонові удосконалених підходів до розвитку даних систем. У зв'язку з цим, СЗЕБ України має бути якісно реформована та оптимізована в організаційно-управлінському та інших аспектах її функціонування з метою підвищення рівня ефективності цієї системи щодо протидії сучасним та майбутнім економічним та іншим загрозам.

Отже перед українським науковим і експертним середовищем актуалізуються завдання щодо проєктування та конструювання нової удосконаленої моделі системи забезпечення економічної безпеки України. Розглядаючи наукові дослідження вітчизняних науковців [17–22], можна дійти висновку, що зміст проєктування СЗЕБ має передбачати визначення місії, цілей, функцій та завдань цієї нової системи, а також розроблення удосконалених механізмів забезпечення економічної безпеки та стійкості. Сутність конструювання СЗЕБ, як етапу процесу проєктування, полягає у впровадженні проєкту в соціально-економічну матерію відповідно до вимог місії та завдань вказаної системи. Його зміст полягає в політико-правовому, структурно-функціональному, просторовому, часовому, організаційному, операційно-діяльнісному конструюванні.

Новій моделі СЗЕБ має володіти властивістю гомеостазу, яке досліджував вітчизняний науковець А. Качинський, зокрема: високий рівень динамічної стійкості СЗЕБ до зовнішніх і внутрішніх загроз; її здатність підтримувати стабільність і безперервність свого функціонування в умовах впливу загроз; опірність і протидія СЗЕБ намаганням зовнішніх чинників змінити її сталі внутрішні характеристики [23].

При науковому обґрунтуванні вибору моделей нової СЗЕБ України необхідно застосовувати кібернетичний підхід. Доцільно звернути увагу на науковий закон "*необхідної різноманітності*" (англ. The Law of Requisite Variety – сформулював британський дослідник Вільям Росс Ешбі), який стосується досліджень розвитку організаційних і управлінських спроможностей держави [24]. Цей закон, відповідно до тематики наукової статті, можна інтерпретувати таким чином – для забезпечення ефективного державного управління у сфері національної економіки в умовах чинення із зовні економічних та інших гібридних загроз рівень розвиненості структури СЗЕБ, її функцій, інструментарію, сил та засобів має бути за своєю різноманітністю рівнозначним рівню розвиненості таких властивостей в організаційно-управлінських системах держав, які створюють ці загрози або мати перевагу над ними.

Аналізуючи перспективні наукові доробки дослідників України [17, 18, 20, 22]

можна констатувати, що найбільш доцільним є застосування методології побудови та використання *комплементарної моделі* СЗЕБ. А саме, ця комплементарна організаційно-управлінська модель СЗЕБ України має структурно складатися з комплексу другорядних функціональних моделей щодо розроблення, прийняття та реалізації управлінських рішень, які мають цілісно забезпечувати економічну безпеку на національному, регіональному, обласному та місцевому рівнях, а також у рамках міжнародного та міждержавного співробітництва (Табл. 1).

Комплементарна модель СЗЕБ України сприятиме результативному вирішенню таких організаційно-управлінських завдань: вивчення стану захищеності національної економічної системи України від зовнішніх та внутрішніх загроз економічній безпеці України; обґрунтування необхідного рівня економічної безпеки, адекватного визначеному рівню загроз і небезпек, а також тенденціям розвитку безпекового середовища; синтез раціональної структури та оцінки ефективності функціонування СЗЕБ; обґрунтування комплексних заходів щодо підвищення ефективності СЗЕБ; обґрунтування вимог до суб'єктів СЗЕБ щодо забезпечення економічної безпеки; обґрунтування рекомендацій щодо участі та посилення міжнародного та регіонального співробітництва у сфері забезпечення економічної безпеки, вибору напрямів міждержавної співпраці у цій сфері тощо [18].

Таблиця 1

Комплементарна організаційно-управлінська модель СЗЕБ

Другорядні моделі	Функціональні напрями діяльності другорядних моделей комплементарної моделі СЗЕБ
I	Формування СЗЕБ України, яка структурно включає в себе: діюче законодавство, що регулює забезпечення економічної безпеки; національні інтереси України у сфері економічної безпеки; складові економічної безпеки згідно із законодавством; загрози економічній безпеці; система порогових індикаторів; організаційні структури гарантування економічної безпеки
II	Розроблення державної політики, в рамках якої визначаються пріоритетні напрями і завдання у сфері забезпечення економічної безпеки України
III	Реалізація державної політики у сфері забезпечення економічної безпеки України
IV	Аналіз та оцінювання результативності та ефективності державної політики у сфері забезпечення економічної безпеки України на проміжних етапах її реалізації та за кінцевим результатом досягнення цілей
V	Коригування державної політики у сфері забезпечення економічної безпеки України

На підставі огляду наукових досліджень, які проведені в Україні [18, 22], визначено основні функції та завдання, які має виконувати комплементарна модель СЗЕБ України (Табл. 2).

Таблиця 2

Функції та основні завдання системи забезпечення національної економічної безпеки України (варіант)

Функції	Основні завдання
Цілепокладання	Концептуалізація національних інтересів в економічній сфері
	Своєчасне прийняття та контроль виконання державно-управлінських рішень у сфері забезпечення економічної безпеки, і внесення коректив за результатами їх реалізації
Цілевизначення	Формування національних цілей забезпечення економічної безпеки
Цілереалізації	Захист недоторканості національних цілей забезпечення економічної безпеки, їх носіїв та гаранта протягом усього періоду їх юридичної дієвості
	Збереження смислу національних цілей забезпечення економічної безпеки в рішеннях, які приймаються на всіх рівнях управління і в галузях права протягом усього періоду їх юридичної дієвості
	Визначення форм взаємодії між суб'єктами забезпечення національної економічної безпеки
	Визначення концептуальних засад формування системи забезпечення економічної безпеки з урахуванням контексту політичного режиму держави, домінуючої парадигми національної безпеки, зовнішньополітичного курсу держави, економічного укладу країни
	Визначення форм взаємодії між різними підсистемами системи забезпечення економічної безпеки
	Визначення форм взаємодії між різними підсистемами системи національної економічної безпеки та міжнародними системами безпеки
	Відбір і композиційна побудова впливу на систему міжнародних економічних відносин на кожному етапі досягнення цілей економічної політики держави
Організаційно-управлінська	Організація функціонування системи забезпечення економічної безпеки в цілому; прийняття державно-управлінських рішень; відповідальність за прийняті рішення
Прогностична	Моніторинг процесів, що відбуваються в усіх складових сфери економічної безпеки;

Функції	Основні завдання
	прогнозування змін, що стануться в них, та загроз життєво важливим національним інтересам в економічній сфері
	Спостереження за сучасними тенденціями геополітичного протиборства та геоекономічної конкуренції та прогнозування новітній форм геоекономічних війн
	Виявлення зовнішніх небезпек, загроз економічного характеру та дестабілізаційних чинників
	Виявлення внутрішніх небезпек, загроз економічного характеру та дестабілізаційних чинників
	Виявлення внутрішніх небезпек, загроз зниження рівня ефективності функціонування системи забезпечення економічної безпеки
	Оцінювання загроз національним інтересам економічного характеру
	Виявлення причин виникнення загроз економічній безпеці та прогнозування наслідків їх прояву
Основоположна (фундаментальна)	Гарантування економічного суверенітету, розвиток економічної могутності, підвищення конкурентоспроможності, економічне зростання, зростання добробуту або якості життя
	Використання можливостей Ради безпеки ООН, НАТО, ЄС, СОТ та інших міжнародних інститутів в питаннях забезпечення економічної безпеки
	Вжиття заходів щодо запобігання економічному конфлікту
	Боротьба з організованими злочинними угрупованнями, в тому числі міжнародними, які намагаються діяти через державний кордон України та виключну (морську) економічну зону України
	Вжиття заходів щодо стримування розв'язання економічного конфлікту та недопущення його переростання в геоекономічну війну
	Проведення інформаційних і фінансових операцій для запобігання економічному конфлікту та стримування його
	Переведення національної економіки, окремих її галузей або підприємств, у тому числі транспортних, і комунікацій на функціонування в умовах особливого періоду
Програмно-теоретична	Розроблення концепцій, стратегій і програм у сфері суспільного розвитку та національної економічної безпеки
	Планування і вжиття конкретних заходів щодо протидії та нейтралізації загроз економічного характеру національним інтересам
	Створення та удосконалення нормативної бази для ефективного функціонування системи забезпечення економічної безпеки
	Удосконалення організаційної структури системи забезпечення економічної безпеки
	Розроблення науково обґрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень для захисту національних інтересів України у економічній сфері
Планово-аналітична	Прискорення реформування органів державної влади та служб, що опікуються забезпеченням економічної безпеки для забезпечення максимальної ефективності виконання ними завдань за призначенням
	Спільне проведення планових та оперативних заходів у межах міжнародних організацій і договорів у галузі економічної безпеки
	Участь у дво- та багатосторонньому співробітництві в галузі економічної безпеки, якщо це відповідає національним інтересам України
	Забезпечення соціального захисту населення країни
	Розвиток вітчизняної науки, формування науково-технічної й технологічної бази
	Посилення контролю за станом воєнно-економічної безпеки
	Комплексне кадрове, фінансове, матеріальне, технічне, інформаційне та інше забезпечення діяльності складових (структурних елементів) системи забезпечення економічної безпеки для виконання завдань за призначенням
	Підготовка сил і засобів системи забезпечення економічної безпеки до застосування їх за призначенням
Інтеграційна	Виконання міжнародних договорів України в економічній сфері
	Поглиблення економічного партнерства та співробітництва з НАТО та ЄС; участь у міжнародному розподілу праці
	Розвиток транскордонного співробітництва із суміжними державами
Координаційна	Оцінка рівня економічної безпеки, досягнутого системою забезпечення економічної безпеки на цей час
	Надання допомоги органам публічної влади щодо соціального захисту населення під час економічних криз та ліквідації їх наслідків
Ідеологічна	Інформаційно-пропагандистське супроводження державної політики національної безпеки
	Поширення комплексу ідей, поглядів, над довготривалих програм суспільного розвитку та забезпечення економічної безпеки
	Формування економічної культури та культури безпеки
Партисипаторна	Соціалізація громадян країни, з метою їх активної участі в забезпеченні економічної безпеки
	Залучення громадянського суспільства до прийняття політичних рішень у сфері забезпечення економічної безпеки
Моніторингу та контролю	Встановлення доцільної взаємодії між структурними компонентами системи забезпечення економічної безпеки в процесі її функціонування за допомогою передавання інформації

Розбудова СЗЕБ має здійснюватися на основі сучасних наукових досягнень, новітніх інновацій та перспективного практичного досвіду. Система має бути креативного типу та діяти на випередження з метою забезпечення стійкості та ефективного реагування на загрози економічній безпеці, передусім, на стадії тенденцій до їх виникнення. СЗЕБ повинна мати гнучкі підсистеми стратегічного аналізу, прогнозування, планування, організації та управління, зокрема: здатними завчасно адаптуватися до змін безпекового середовища, визначати пріоритети і забезпечувати якісний розвиток спроможностей, а також ефективну протидію загрозам економічній безпеці на будь-якому етапі їх реалізації при різноманітності варіантів їх прояву [22]. Державна політика у сфері забезпечення економічної безпеки України повинна реалізовуватися у поєднанні із зміцненням національної могутності та економічної стійкості України, а також бути взаємно доповненою із реалізацією державної політики в інших сферах національної безпеки України [17, 20].

Функціонування нової системи СЗЕБ України має ґрунтуватися на *принципах*: міжнародного права та співробітництва; участі у міжнародних системах і механізмах забезпечення глобальної та регіональної економічної безпеки; пріоритетності національних інтересів; верховенства права та законності; гнучкості зовнішньої і внутрішньої економічної політики; управління ризиками; публічного та адаптивного управління; пріоритетності законних прав, свобод і інтересів фізичних та юридичних осіб; державно-приватного партнерства; координації та взаємодії; врахування теоретичних економічних законів і закономірностей; відкритості та прозорості тощо.

З проведеного аналізу наукових досліджень Ю. Сурміна [21] та інших вітчизняних науковців [17–20, 22–24] можна констатувати, що структура проєктної діяльності у сфері забезпечення економічної безпеки України має містити п’ять етапів (рис. 1).

Рис. 1. Порядок проєктування СЗЕБ

При цьому, в рамках системно-діяльнісного підходу на етапі формулювання задуму проєкту та створення концепції проєктування СЗЕБ (*3 етап*) варто враховувати:

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

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

цивілізаційний, геополітичний та геоекономічний коди держави;

інтегральний показник національної могутності держави;

панівний тип комунікації в суспільстві та тип політичного режиму;

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

наукові закони геоекономіки, геополітики, війни;

закономірності геоекономічного і геополітичного протиборства, збройної та інформаційної боротьби;

закономірності криз у міжнародних, економічних і соціальних системах;

сучасні тренди розвитку світової цивілізації;

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

зміни організаційно-функціональних форм публічного управління;

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

результати пошукового та нормативного прогнозування у сфері міжнародної та національної безпеки, зокрема стосовно сучасних трендів розвитку загроз геополітичного, геоекономічного, воєнно-політичного та іншого характеру;

наявну модель національної економічної системи України, її вади та недоліки, а також проблеми забезпечення економічної стійкості, які спричиняють уразливості.

На *4 етапі* проєктування СЗЕБ структурно має включати в себе структурно-функціональне моделювання процесу забезпечення економічної безпеки, просторове, часове, оперативно-діяльнісне, інституційне, організаційне проєктування вказаної системи. Воно передбачає визначення місії, функцій та завдань СЗЕБ, а також механізмів забезпечення економічної безпеки. До того ж, у межах інституціонального підходу необхідно враховувати закономірності розвитку тріад "культура – інститути – економіка", "економіка – політика – війна", "економіка – інститути – організації", "організація – ресурси – час". Це дасть змогу виявити перспективні моделі СЗЕБ, що узгоджуватиметься зі станом і перспективами геоекономічного, геополітичного, суспільно-політичного й соціально-економічного розвитку України та суспільства.

Під час конструювання нової моделі СЗЕБ (*5 етап*) слід враховувати вимоги щодо виконання наведених нижче завдань системи національної безпеки.

1. *Політико-правове конструювання*:

удосконалення національного законодавства щодо розвитку системи забезпечення національної безпеки та її складової СЗЕБ, готовності сектору безпеки і оборони, а також інших органів державної влади відповідної компетентності, приватного бізнес-сектору до реагування на гібридні та інші загрози геополітичного, геоекономічного, воєнно-політичного та іншого характеру;

розроблення та впровадження системоутворюючого закону про СЗЕБ України;

активна участь держави у процесах удосконалення міжнародного права у сфері протидії зовнішнім загрозам економічного, фінансового та іншого гібридного характеру;

законодавче забезпечення стратегічного планування у сферах національної безпеки України з урахуванням принципів сталого розвитку та національної стійкості, зокрема в економічній, фінансовій, продовольчій, енергетичній та інших сферах;

розвиток єдиної нормативно-правової бази у сфері планування, підвищення готовності та реагування на економічні та інші загрози для скоординованих дій державних органів, бізнес-сектору, політикуму, суспільства та ін.

2. *Структурно-функціональне конструювання* – створення нових та удосконалення вже наявних елементів, структур, підсистем, механізмів забезпечення економічної безпеки та встановлення зв'язків між ними:

розвиток єдиної системи стратегічного планування та її методологічної основи, яка комплексно об'єднуватиме сфери сталого розвитку та національної безпеки;

створення державного органу координації і міжвідомчої взаємодії у сфері забезпечення економічної безпеки України, структури його допоміжних органів, розроблення правових і організаційних механізмів, повноважень і відповідальності щодо його функціонування, а також співробітництва з приватним бізнес-сектором національної економіки, а також співпраці на міжнародному рівні;

розвиток національної мережі уповноважених державних органів і науково-експертних установ з питань стратегічного аналізу і прогнозування, планування у сфері забезпечення економічної безпеки України;

удосконалення діяльності уповноважених державних органів з питань державних закупівель, експортного контролю, нагляду за іноземними активами та інвестиціями тощо;

розвиток ефективної взаємодії державних органів, бізнесу, громадянського суспільства, мережі наукових та аналітичних установ тощо з питань готовності, запобігання та реагування на загрози економічній безпеці, а також подолання їх наслідків.

3. *Просторове та часове конструювання* – створення нових елементів, структур, підсистем, механізмів забезпечення економічної безпеки на національному, регіональному, обласному, місцевому рівнях, а також на рівнях міжнародного та міждержавного співробітництва, які мають діяти на постійній або тимчасовій основі залежно від місії, цілей, завдань, профільної компетенції, повноважень та відповідальності:

зміцнення спроможностей суб'єктів забезпечення економічної безпеки щодо розвитку готовності та реагування на економічні та інші загрози національній безпеці.

4. *Організаційне конструювання* – формування алгоритмів функціонування СЗЕБ, а також підготовки відповідних фахівців:

запровадження повного циклу забезпечення економічної безпеки (моніторинг, аналіз і прогнозування, оцінювання ризиків, ідентифікація загроз, виявлення вразливостей, забезпечення готовності, планування, запобігання, реагування, відновлення тощо) та ефективного функціонування єдиного механізму координації цієї діяльності;

удосконалення кризового менеджменту та управління ризиками у сфері економіки;

якісний розподіл відповідальності та повноважень державних органів за визначеними напрямами забезпечення економічної безпеки;

забезпечення безперервності критично важливих функцій держави у сфері економічного розвиту та безпеки;

забезпечення безпеки та безперервності постачання із зовні до України критично важливих ресурсів, товарів, послуг та технологій, диверсифікації ланцюгів поставок;

забезпечення безпеки та стабільності поставок експорту української продукції на зовнішні ринки товарів і послуг;

забезпечення ефективного запобігання та реагування на геоекономічні загрози та їх наслідки, пов'язані із зовнішньоекономічним примушенням, політикою санкцій, створенням "боргових пасток" для України тощо, а також нейтралізації або пом'якшення цих наслідків;

зміцнення готовності та нарощування спроможностей для ефективного реагування на загрози безпеці та стійкості критичної економічної інфраструктури України;

активізація розвідувальної діяльності, спрямованої на викриття можливих планів, намірів та підготовки держав-конкурентів до геоекономічних війн, геополітичного протиборства із застосуванням ними нових форм їх проведення на шкоду національній безпеці України;

розвиток надійних і постійно діючих двосторонніх каналів комунікацій держави з міжнародними партнерами, національним та іноземним бізнесом, мережею аналітично-експертних та наукових установ, громадянським суспільством тощо;

проведення підготовки (теоретичної, практичної) усіх наявних сил на національному, регіональному та місцевому рівнях України щодо розвитку готовності, запобігання та реагування на загрози економічній безпеці України.

5. *Операційне-діяльнісне конструювання* – удосконалення наявних та розроблення нових правил і принципів діяльності у сфері забезпечення економічної безпеки: запровадження єдиних стандартів і рекомендацій (інструкцій) з питань забезпечення економічної безпеки України та ін.

У процесі планування цілей, завдань і заходів щодо проєктування та функціонування нової СЗЕБ України, доцільно використовувати перспективні іноземні практики, зокрема досвід США та Японії щодо розроблення і реалізації стратегій, програм і планів з питань забезпечення економічної безпеки, який розкритий у цій статті.

Висновки. Результати дослідження іноземних теорій та практичного досвіду США і Японії, які розглянуті у зазначеній науковій статті свідчать про таке:

1. У майбутньому держави центри-сили застосовуватимуть стратегії зовнішньоекономічного примушення, передусім, проти менш розвинених країн з метою посилення на них впливу. Зазначене здійснюватиметься у відкритій формі відповідної зовнішньої політики або у рамках стратегій непрямих дій та комплексу гібридних загроз. Невиключно поєднання цих підходів, а також застосування воєнної сили.

2. Менш розвинені країни адаптуватимуться до складної міжнародної обстановки. Такі держави все активніше

ініціюватимуть удосконалення міжнародного права та організаційних механізмів щодо їх захисту від загроз геоекономічних війн. Вони шукатимуть ефективні моделі забезпечення сталого розвитку і національної безпеки від зовнішньоекономічних та інших загроз, віддаючи перевагу універсальним підходам. Вбачається, що ці підходи можуть комбінувати такі напрями зовнішньої політики:

продовжувати стратегічне партнерство з обраною державою-центром сили та інтеграцію до глобальної мережі міждержавного співробітництва, за умови якісного збалансування спільних колективних інтересів щодо сталого розвитку та безпеки;

розвивати тісні економічні відносини одразу з декількома державами-центрами сили з метою диверсифікації джерел постачання критичних ресурсів, товарів і послуг, а також для зниження залежності від глобальних монополій;

об'єднуватися у міждержавні регіональні союзи менш розвинених країн, яким характерні подібні загрози національній безпеці від зовнішньоекономічного та іншого примушення (при цьому, такі регіональні союзи можуть стати геоекономічним зв'язком у системі міжнародних відносин та у глобальному світовому господарстві на основі збалансування національних, корпоративних та інших інтересів стосовно цього геополітичного простору);

3. Практичний досвід США та Японії свідчить, що ці країни активно реалізують державну політику щодо удосконалення своїх СЗЕБ до сучасних геоекономічних та інших загроз національній безпеці. Цей досвід є корисним. Його доцільно використовувати під час планування цілей, завдань і заходів забезпечення економічної безпеки України.

4. Україна має врахувати тенденції світового розвитку та почати проєктування нової удосконаленої моделі СЗЕБ, що сприятиме перетворенню України із зони конфліктів у зону компромісного розвитку, при забезпеченні динамічної рівноваги та стійкості держави у системі міжнародних відносин та в глобальному світовому господарстві.

5. Найбільш доцільним є застосування методології розбудови комплементарної організаційно-управлінської моделі СЗЕБ України. Комплементарна модель СЗЕБ України має структурно складається з комплексу п'яти ключових другорядних моделей за напрямами функціонування цієї системи щодо розроблення, прийняття та реалізації управлінських рішень. Ці другорядні моделі (як складові комплементарної моделі СЗЕБ України) мають цілісно забезпечувати економічну безпеку на національному, регіональному, обласному та місцевому рівнях, а також у рамках міжнародного та міждержавного співробітництва. Вони мають бути комплексно зорієнтовані на: формування та розвиток СЗЕБ України; розроблення та реалізацію державної політики у сфері забезпечення економічної безпеки; аналіз та оцінювання результативності та ефективності цієї державної політики на проміжних етапах її реалізації та за кінцевим результатом досягнення цілей; а також на її корегування, у разі потреби.

6. Комплементарна модель СЗЕБ України передбачає, що ця система має виконувати такі функції: цілепокладання, цілевизначення, цілереалізації, організаційно-управлінську, прогностичну, основоположну (фундаментальну), програмно-теоретичну, планово-аналітичну, інтеграційну, координаційну, ідеологічну, партисипаторну, моніторингу та контролю.

7. Визначено, що проєктну діяльність у сфері забезпечення економічної безпеки України в умовах динамічного безпекового середовища доцільно проводити у п'ять етапів.

Перспективним **напрямом подальших досліджень** вбачається розроблення методики проєктування системи забезпечення економічної безпеки України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про рішення Ради національної безпеки і оборони України від 11 серпня 2021 року "Про Стратегію економічної безпеки України на період до 2025 року" : Указ Президента України від 11.08.2021 р. № 347/2021. URL: https://www.president.gov.ua/documents/3472021-39613 (дата звернення: 18.05.2023).
2. World stumbling into a new era of risk, concludes SIPRI report / Stockholm International Peace Research Institute (SIPRI). 2022. 23 May. URL: https://www.sipri.org/media/press-release/2022/ world-stumbling-new-era-risk-concludes-sipri-report (дата звернення: 18.05.2023).
3. Чернятевич Я. В. Економічна війна. Енциклопедія державного управління : у 8 т. / Нац. акад. держ. упр. при Президентові України ; наук.-ред. колегія : Ю. В. Ковбасюк (голова) та ін. Київ : НАДУ, 2011. Т. 3 : Історія державного управління / наук.-ред. колегія : А. М. Михненко

(співголова), М. М. Білинська (співголова) та ін. 2011. С. 93–94.
4. Абрамов В. І., Зюзя О. В. Удосконалена базова модель міждержавного протиборства з урахуванням сучасних тенденцій російсько-української війни // Державне управління: удосконалення та розвиток. 2022. № 5. URL: http://www.dy.nayka.com.ua/?op=1&z=2679 (дата звернення: 19.05.2023).
5. Philippe Gros, Stéphane Delory, Vincent Tourret. Stratégies russes et guerre en Ukraine: état des lieux // The Fondation pour la recherche stratégique. 2022. 1 Mars. URL: https://www.frstrategie.org/publications/notes/strategies-russesguerre-ukraine-etat-lieux-2022 (дата звернення: 19.05.2023).
6. Шевченко М. М., Зозуля О. С., Лепіхов А. В., Храпач Г. С. Російсько-українська війна: особливості реалізації загроз державному суверенітету України та перспективи виходу з війни // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2022. № 2 (75). С. 6–15.
7. Актуальні виклики та загрози економічній безпеці України в умовах воєнного стану : Експерт-аналіт доп. НІСД від 31.05.2023 р. URL: https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/aktualni-vyklyky-ta-zahrozy-ekonomichniy-bezpetsi-ukrayiny-v (дата звернення: 19.05.2023).
8. Daniel W. Drezner, Henry Farrell, Abraham L. Newman. The Uses and Abuses of Weaponized Interdependence. March 2, 2021. URL: https://www.brookings.edu/book/the-uses-and-abuses-of-weaponized-interdependence/ (дата звернення: 19.05.2023).
9. Daniel W. Drezner. The uses and abuses of weaponized interdependence in 2021 // Washingtonpost. 02.03.2021. URL: https://www.washingtonpost.com/outlook/2021/03/02/uses-abuses-weaponized-interdependence-2021/?utm_campaign=wp_opinions&utm_medium=social&utm_source=twitter (дата звернення: 20.05.2023).
10. Farrell H., Abraham L. Newman Weaponized Interdependence: How Global Economic Networks Shape State Coercion. July 01, 2019. URL: https://direct.mit.edu/isec/article-abstract/44/1/42/12237/Weaponized-Interdependence-How-Global-Economic?redirectedFrom=fulltext (дата звернення: 20.05.2023).
11. Daniel W. Drezner. The Sanctions Paradox: Economic Statecraft and International Relations (Cambridge Studies in International Relations, Series Number 65). September 13, 1999. URL: https://www.amazon.com/gp/product/0521644151?ie=UTF8&tag=thewaspos09-20&camp=1789&linkCode=xm2&creativeASIN=0521644151 (дата звернення: 20.05.2023).
12. Thomas G. Mahnken. Cost-Imposing Strategies: A Brief Primer. November 18, 2014. URL: https://www.cnas.org/publications/reports/cost-imposing-strategies-a-brief-primer (дата звернення: 20.05.2023).
13. Blackwill, Robert D., Harris, Jennifer. War By Other Means: Geoeconomics and Statecraft. 2016. URL: https://www.jstor.org/stable/j.ctt1c84cr7 (дата звернення: 21.05.2023).
14. Cynthia Cook. Destruction, Subversion, and the Long War // CSIS. May 3, 2022. URL: https://www.csis.org/analysis/destruction-subversion-and-long-war (дата звернення: 21.05.2023).
15. Joseph R. Biden Jr. Executive Order on America's Supply Chains // The White House. February 24, 2021. URL: https://www.whitehouse.gov/briefing-room/ presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/ (дата звернення: 21.05.2023).
16. National Security Strategy of Japan. Japan Ministry of Defense. December 16, 2022. URL: https://worldjpn.net/documents/texts/JPSC/20221216.O1E.html (дата звернення: 21.05.2023).
17. Кириленко В. І., Шевченко М.М. Методологія побудови та використання комплементарної моделі національної економічної безпеки // Науковий вісник Дипломатичної академії України. Випуск 22. Зовнішня політика і дипломатія: традиції, тренди, досвід. Частина ІІІ. Серія "Економічні науки". 2015. С. 40–50.
18. Кириленко В. І. Інноваційна складова економічної безпеки // Науково-інформаційний вісник Академії національної безпеки. 2014. № 2. С. 60–68. URL: http://nbuv.gov.ua/UJRN/nivanb_2014_2_10 (дата звернення: 21.05.2023).
19. Лепіхов А. В., Храпач Г. С. Проєктна діяльність у сфері забезпечення національної стійкості: сутність, зміст, структура // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2021. № 1 (71). С. 18–26.
20. Семенченко А. І. Методологія стратегічного планування у сфері державного управління забезпеченням національної безпеки України : монографія. Київ : НАДУ, 2008. 428 с.
21. Сурмин Ю. П. Социальное проектирование в кризисном обществе: методологический аспект // Вісник НАДУ. 2014. № 3. С. 5–17.
22. Шевченко М. М., Зозуля О. С. Системи забезпечення національної безпеки адаптивного та креативного типів: порівняльний аналіз // Інвестиції: практика та досвід. 2015. № 16. С. 125–129. URL: http://www.investplan.com.ua/pdf/16_2015/28.pdf (дата звернення: 21.05.2023).
23. Качинський А. Б. Індикатори національної безпеки: визначення та застосування їх граничних значень // Стратегічні пріоритети. 2013. Вип. № 4. С.200–201.
24. Шевченко М. М., Лепіхов А. В., Храпач Г. С. Теоретичні підходи та практична цінність прикладних досліджень міждержавної конфліктності в інтересах національної безпеки: Британський досвід – уроки для України // Збірник наукових праць Центру воєнно-

стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2022. №1 (74). С.12–21.

Стаття надійшла до редакційної колегії 20.06.2023

Problems of ensuring national security from the threats of geo-economic wars: theoretical and practical experience of the USA and Japan – lessons for Ukraine

Annotation

Ukraine is located at the intersection of national interests of the world's leading countries, which are the centers of the world economy. Economically powerful states are again and again in fierce competition in the global market, which often takes the form of geopolitical confrontation with economic means of pressure (geo-economic wars). The existing system of ensuring the economic security of Ukraine ("SEESU") has become significantly vulnerable and needs to be thoroughly optimized for current and future changes in the strategic security environment and the development of new forms and methods of ensuring Ukraine's economic security from geo-economic and other destructive influences.

The article considers the promising theories of US researchers on the impact of the sharp geo-economic competition of the world's powerful states on the growth of military and strategic instability, international conflict and threats to the state sovereignty of less developed countries. The strategies of the United States and Japan to counteract the threats of geo-economic wars are studied. An overview of Ukraine's promising research achievements in the field of economic security is provided.

Approaches to the design of a new improved model of the system of ensuring economic security of Ukraine, taking into account the current development of the strategic security environment (SSE), are proposed. The complementary model of Ukraine's SEESU envisages that this system should perform the following functions: goal setting, goal determination, goal realization, organizational and managerial, prognostic, fundamental, programmatic and theoretical, planning and analytical, integration, coordination, ideological, participatory, and monitoring and control. The stages of project activities in the field of ensuring the economic security of Ukraine in a dynamic security environment are defined.

Keywords: globalization; geo-economic; interstate interdependence; geopolitical confrontation; geo-economic wars; foreign economic enforcement; economic security; national security.

УДК 355.354 DOI: https://doi.org/10.33099/2304-2745/2023-2-78/20-26

Загорка О. М., доктор військових наук, професор[1] (0000-0003-1131-0904)
Дейнега О. В., доктор військових наук, професор[2] (0000-0002-2371-3252)

[1] – Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ;
[2] – Центральний науково-дослідний інститут Збройних Сил України, Київ

Аналіз застосування нестратегічних балістичних ракет у локальних війнах і збройних конфліктах та боротьби з ними

Резюме. У статті аналізується досвід бойового застосування нестратегічних балістичних ракет у локальних війнах і конфліктах кінця XX – початку XXI століть. Узагальнюються форми і способи їх застосування та наводяться дані стосовно досвіду боротьби з цим типом засобів повітряного нападу.

Ключові слова: аеробалістична ракета; бойове застосування; зенітний ракетний комплекс (система); нестратегічна балістична ракета; протиракетний комплекс; ефективність протиракетної оборони.

Постановка проблеми. У всіх війнах і конфліктах останніх десятиліть протиборчі сторони намагались насамперед застосовувати такі засоби повітряного нападу (ЗПН), за допомогою яких можна було більш успішно виконувати завдання щодо придушення системи протиповітряної оборони (ППО), дезорганізації системи управління, ураження військ і важливих об'єктів. Значна роль у виконанні цих завдань поряд зі стратегічними крилатими ракетами (КР) належить нестратегічним балістичним ракетам (НБР), які є найбільш складними та найменш уразливими цілями для системи ППО.

Застосування НБР дає змогу стороні, що наступає, досягати успіху у виконанні завдань без втрат пілотованої авіації в умовах наявності у противника сил ППО. Узагальнення досвіду бойового застосування НБР, а також боротьби з ними дасть змогу обґрунтовано розробляти рекомендації щодо організації прикриття військ та об'єктів від ракетних ударів. Таке узагальнення може бути корисним і під час обґрунтування рекомендацій щодо удосконалення структури і складу протиповітряної компоненти Повітряних Сил Збройних Сил України. Отже питання, що розглядається у статті, є актуальним.

Аналіз останніх досліджень і публікацій. Застосуванню НБР та боротьбі з ними присвячено низку публікацій [1–5], у яких, здебільшого, наводяться дані щодо застосування НБР у деяких війнах і конфліктах. Водночас практично відсутні публікації, у яких би узагальнювався досвід застосування балістичних ракет у війнах і конфліктах різної інтенсивності з аналізом масштабу їх застосування та боротьби з ними.

Метою статті є узагальнення досвіду застосування НБР у чисельних війнах і конфліктах різної інтенсивності з кількісно-якісним аналізом масштабу їх використання. При цьому проаналізувати ефективність боротьби з даними типами ЗПН, як найбільш складними цілями для засобів ППО.

Виклад основного матеріалу. Появу балістичних ракет часто пов'язують з німецькими ракетами "Фау-2", які застосовувались фашистською Німеччиною у другій світовій війні.

З червня 1944 року по березень 1945 року було здійснено понад чотири тисячі бойових пусків "Фау-2" по містах Англії та Бельгії [6]. Однак ефективність їх застосування оцінюється неоднозначно. Збитки (як матеріальні, так і людські), що наносилися, були меншими, ніж очікувалося. Німцям не вдалося досягти масованих ракетних ударів, хоча щомісячна кількість "Фау-2", які запускались по території Англії, зростала і в 1945 році досягла 220-230 ракет. Ефективних засобів боротьби з "Фау-2" у повітрі на той час у англійців (як і у світі) не було.

Тим часом німецькі БР ("Фау-2") стали ефективним засобом відволікання крупних сил авіації союзників, а їх застосування мало великий морально-психологічний ефект на війська та населення. Англо-американська авіація у боротьбі з ракетною зброєю німців здійснила близько 70 тис. літако-вильотів та скинули на об'єкти, пов'язані з виробництвом та застосуванням ракет, близько 120 тис. т бомб. Втрати військово-повітряних сил союзників склали близько 500 бойових літаків і 3 тис. льотчиків. При цьому ракетна промисловість і частини ракетної зброї німців не понесли суттєвих втрат [6]. Слід зазначити, що й у подальшому боротьба з БР, які у післявоєнний період отримали широкий розвиток у світі, і досі практично для усіх

країн залишається важливою невирішеною проблемою. Проведений аналіз показав, що наявність на озброєнні армій багатьох країн світу НБР призвело до їх широкого бойового застосування в багатьох регіональних і навіть внутрішніх конфліктах (Табл. 1).

Таблиця 1

Бойове застосування нестратегічних балістичних та аеробалістичних ракет у війнах і конфліктах

Війни та конфлікти, де застосовувались балістичні ракети	Роки	Країни, які застосовували БР	Типи балістичних ракет, що застосовувались
Арабо-ізраїльські війни	***1973***	Єгипет	Вперше застосовані оперативно-тактичні ракети (ОТР) “Скад” та тактичні ракети (ТР) “Луна-М” (витрачені майже всі ракети)
		Сирія	ТР “Луна-М” (близько 24 ракетних ударів)
	1982	Ізраїль	ТР “Зєєв”
Війна в Афганістані	***1979-1989***	СРСР	ОТР Р-300 (понад 2000 ракет)
Громадянські та міжкланові війни у Ємені	***з 1983***	Північний Ємен	ОТР “Скад”, ТР “Луна-М”
		Південний Ємен	ТР “Точка-У” (близько 35 ракет)
Ірано-іракська війна 1980-1988 рр.	***до 1983***	Ірак	ТР “Луна-М”, ОТР “Скад”
	1987-1988	Ірак	ОТР “Скад” (близько 76 ракетних ударів)
		Іран	ОТР “Скад”, ТР “Огхаб”, ‘Іран-130” (понад 200 ракетних ударів)
Війни у зоні Перської затоки	***1991***	Ірак	ОТР “Скад”, “Аль-Хусейн”, ТР “Луна-М” (133 ракетних ударів по об’єктах Ізраїлю, Саудівської Аравії та Бахрейну)
		США	Вперше був застосований ракетний комплекс (РК) АТАКМС (30 ракет ATACMS (Block 1))
	2003	Ірак	ОТР “Скад”, ТР “Аль-Самуд-2” (15 ракет по об’єктах Кувейту)
		США	ОТР АТАКМС (близько 400 ракет)
Війна у Боснії	***1995***		ТР “Луна-М”
Антитерористична операція у Чечні	1995-1996	Росія	ОТР Р-300 (близько 250 ракет), ТР “Точка”, “Точка-У”
	1999-2000		ТР “Точка-У” (декілька сотен ракет)
Російсько-грузинська війна	***2008 (8-12 серпня)***	Росія	ТР “Точка-У” (близько 15 ракет) вперше були застосовані ОТР “Іскандер-М” (2 ракети)
Російсько-українська війна (АТО та ООС)	***2014-2021***	Україна	ТР “Точка-У”
		Росія	ТР “Точка-У”
Вірмено-азербайджанський конфлікт	***2020***	Вірменія	ОТР “Іскандер-Э”, ОТР Р-300 (10-15 ракет), ТР “Точка-У”
		Азербайджан	ОТР “Лора”
Громадянська війна в Сирії	***2015-2016***	Росія	ОТР “Іскандер-М”
		Іран	ОТР “Фатех-110” та вперше застосовані ОТР “Золфагар” (6 ракет)
Російсько-українська війна	***2022***	Україна	ТР “Точка-У”
		Росія	ОТР “Іскандер-М”, ТР “Точка-У”, вперше була застосована аеробалістична ракета Х-47 авіаційного комплексу “Кинджал”

Особливо слід зазначити, що застосування НБР у війнах і конфлікта 70–90-х років минулого століття не носило масованого характеру. Зазвичай під час застосування НБР завдавалися поодинокі або групові удари по визначених цілях або районах. До того ж ракетні удари завдавалися практично без протидії засобів ППО, бо зенітні ракетні комплекси (ЗРК), які знаходилися на озброєнні армій конфліктуючих сторін, практично були не здатні боротися з цілями такого класу. Винятком можна вважати лише війни в зоні Перської затоки та російсько-українську війну.

Так у війні 1991 року бойове застосування оперативно-тактичних ракет (ОТР) збройні сили Іраку розпочали практично з початком операції “Буря в пустелі”. Ракетні удари наносилися по містах Тель-Авів, Єрусалим (Ізраїль), авіабазі (Дахран) та командному пункту багатонаціональних сил (Ер-Ріяд) на території Саудівської Аравії, військово-морській базі (Манама) та території Бахрейну. За перший тиждень бойових дій було застосовано більше 60 ОТР, у подальшому темп знизився до 1-4 за добу. Проте масованого застосування ОТР в ракетних ударах іракцям досягти не вдалося. Лише в деякі дні застосовувалося до 10-20 ОТР. Усього іракцям вдалося здійснити 133 пуски ОТР (61 – по Саудівської Аравії, 51 – по Ізраїлю та 21 – по Бахрейну) [7].

Для боротьби з пусковими установками

(ПУ) та ракетами "Скад" США створили комплексну систему, подібну тактичній системі протиракетної оборони (ПРО) на театрі воєнних дій. При цьому, за даними західних фахівців, американськими ЗРК "Петріот", які входили до цієї системи, було перехоплено майже 35 % іракських ОТР [4]. Безрезультативними виявилися спроби авіації багатонаціональних сил боротися з іракськими ракетними комплексами (РК), хоча для цього виділялися значні сили (до 30 % льотного ресурсу авіації союзників щодобово). Із 30 стаціонарних іракських ПУ було знищено 8, а із 43 мобільних ПУ, які активно застосовувались, були виявлені та обстріляні авіацією тільки 8. Причиною цьому можна вважати високу мобільність РК, які після пусків ракет або змінювали позиції, або переміщувалися в укриття та сховища природного характеру.

Хоча ефективність ударів ОТР була низькою, слабка протидія їм відіграла деморалізуючу роль на війська і особливо на цивільне населення міст Ізраїлю. Лише до 30 % запущених іракських ОТР досягли цілей, частина ракет з технічних причин сходили з траєкторій, а ті, що були перехоплені американськими ЗРК "Петріот" (за наявності підривів бойових частин зенітних керованих ракет) практично не "збивалися з траєкторії" і, як правило, падали в точку прицілювання (з незначними промахами).

Необхідно зазначити той факт, що в цій війні БР застосовувались і з боку США. Так вперше було здійснено бойове застосування ракетного комплексу АТАКМС (реактивна система залпового вогню MLRS з тактичними ракетами ATACMS). Ракетні комплекси АТАКМС досить ефективно застосовувались з території Саудівської Аравії по об'єктах ППО та службах тилу іракської армії. Так, за різними даними, американцями було застосовано від 30 [8] до 76 [9] ракет ATACMS (Block 1) з дальністю стрільби 100 км при залученні 18 ПУ. При цьому було завдане ураження 65 об'єктам. Однак інтенсивність використання комплексу була низькою (дольова участь комплексу у вогневому ураженні противника оцінювалась як 2-2,5 % [9]).

У війні 2003 року масштаб застосування іракських НБР був значно меншим порівняно з 1991 роком. Так, відмічалися лише поодинокі ракетні удари. З 15 запущених по території Кувейту ракет були перехоплені шість (достовірні дані щодо знищення іракських ракет ЗРК "Петріот", які були модернізовані після війни 1991 року по програмі ПАК-2, відсутні). Ракетні удари по території Ізраїлю у війні 2003 року не завдавались.

Водночас система захисту Ізраїлю від БР стрімко розвивалась і на початку XXI століття набула статусу національної багатоешелонованої протиракетної (від усіх типів ракет) оборони. Вона довела свою ефективність бойового застосування, особливо комплексами "Залізний купол" під час перехоплень некерованих ракет (аналогічних ракетам від систем залпового вогню типу "Град"). Так, під час антитерористичної операції "Хмарний стовп", яка проводилася у секторі Газа з 14 по 21 листопада 2012 року зареєстровано до 87 % перехоплень системою "Залізний купол" ракет, які загрожували житловим районам. З 1506 ракет, що були випущені по Ізраїлю, більшість (майже 875 – 58 %) підірвались на відкритій місцевості поза населених пунктів, 58 ракет – у міських кварталах (3,8 %). ЗРК "Залізний купол" перехопили 421 ракету, до того ж по цілях, що являли собою загрозу населенню, була випущена 501 ракета-перехоплювач. Під час операції "Непорушна скеля", що проводилась в секторі Газа з 7 липня по 26 серпня 2014 року, з 3360 випущених бойовиками ракет ЗРК "Залізний купол" було знищено 584 [10]. Загалом слід зазначити, що за даними Організації ПРО Ізраїлю (IMDO) за 10 років функціонування до січня 2021 року, комплексами "Залізний купол" сумарно було перехоплено близько 2400 ракет. За даними розробника системи (компанія Rafael Defence Systems) ця цифра становить 2500 ракет, а ефективність системи сягнула 90 % [11].

Крім того, в засобах масової інформації були повідомлення про факти перехоплення вогневими засобами системи ПРО Ізраїлю таких ЗПН: іранської ОТР (можливо "Фатех-110" або "Золфагар"), запущеної з території Сирії; сирійської зенітної керованої ракети ЗРК С-200; двох ТР "Точка-У" (перехоплені протиракетним комплексом "Праща Давида" у липні 2018 року).

Щодо російсько-української війни, то за досвідом її ведення сформувалася певна тактика завдання російською авіацією ВКС, РВіА СВ, а також надводними кораблями, підводними човнами та береговими мобільними ракетними комплексами ВМФ комбінованих ударів балістичними, аеробалістичними та крилатими ракетами.

Під час завдання комбінованих ракетних ударів використовувались такі носії балістичних та аеробалістичних ракет:

нестратегічних БР наземного базування – оперативно-тактичний РК "Іскандер-М" та

тактичний РК “Точка-У”;

аеробалістичних ракет повітряного базування Х-47 – авіаційний (на базі літаків МіГ-31К) комплекс “Кинжал”;

зенітних керованих ракет (політ яких під час стрільби по наземних цілях здійснюється практично по балістичних траєкторіях) – пускові установки ЗРК С-300П та С-400.

У російсько-українській війні, АТО та ООС (2014–2021) з обох сторін застосовувались ракетні комплекси “Точка-У” (з дальністю стрільби до 120 км), а з початком повномасштабної російської агресії у 2022 році росією активно застосовується і РК “Іскандер-М” з ОТР 9М723. Крім того слід зазначити, що в російсько-українській війні у 2022 році вперше в бойових умовах були застосовані: аеробалістичні ракети Х-47 авіаційного (на базі літаків МіГ-31К) комплексу “Кинжал” (з дальністю пуску до 2000 км); зенітні керовані ракети ЗРК С-300П та С-400 для стрільби по наземних цілях.

За даними різних відкритих джерел інформації (в тому числі і офіційних) лише за 10 місяців війни противником було застосовано до 120 балістичних ракет РК “Іскандер” та до 70 балістичних ракет РК “Точка-У”.

Для забезпечення протиракетної оборони (ПРО) об’єктів застосуванню НБР доцільно протиставити адекватні заходи, які повинні мати комплексних характер щодо їх виявлення системою розвідки, оповіщення про їх застосування, знищення активними засобами ППО (ПРО), а також протидії їхньому ефективному використанню. Комплексний характер такої боротьби має полягати у [12]:

а) створенні глибоко ешелонованої системи виявлення та оповіщення про НБР, яка б забезпечувала безперервне ведення розвідки носіїв НБР усіма силами і засобами, які є в наявності, виявлення НБР і спостереження за ними на траєкторіях польоту тощо;

б) забезпеченні неперервного управління за єдиним планом силами і засобами в процесі боротьби з НБР, сутність якого полягає:

у визначенні можливих напрямків ударів НБР по військах та об’єктах;

централізованому оповіщенні військ та об’єктів про пуски НБР;

визначенні можливих секторів удару НБР та точок падіння їх головних частин;

виданні цілевказівок по НБР на пункти управління ППО тощо;

в) забезпеченні неперервного вогневого впливу на носії та самі НБР на траєкторіях польоту, сутність якого полягає в знищенні ПУ БР у позиційних районах, вогневому ураженні НБР на траєкторіях їх польоту активними засобами наземної ППО (ПРО), а також використанні нетрадиційних засобів та способів;

г) використанні забезпечуючих дій щодо зниження ефективності ударів НБР, сутність яких полягає в: постановці перешкод системам супутникової навігації, використанні інфрачервоних (ІЧ) загороджень для перешкоджання роботи оптико-електронних та тепловізійних систем кінцевого наведення, а також в здійсненні заходів щодо створення обманних об’єктів та викривлення контурів об’єктів удару, застосування аерозольних утворень, димів для прикриття об’єктів тощо.

Комплексне застосування наявних сил і засобів має забезпечувати неперервну дію на носії НБР, самі НБР у польоті, і тим самим ефективну боротьбу з ними. Водночас необхідно зазначити, що жодна з перелічених умов забезпечення комплексної боротьби з НБР у війнах та конфліктах кінця ХХ – початку ХХІ ст. у повному обсязі практично не виконувалася. З одного боку це зумовлене відсутністю потрібної кількості сил і засобів для забезпечення комплексної боротьби з НБР (об’єктивні фактори), а з іншого – недостатнім урахуванням принципів застосування БР під час організації прикриття об’єктів від їх ударів (суб’єктивні фактори).

Сутність комплексного характеру боротьби з НБР показана на рис. 1 [12].

З рис. 1 випливає, що для організації і ведення комплексної боротьби з НБР у повному обсязі необхідно застосовувати достатньо велику кількість різнорідних сил і засобів, які можуть перебувати на озброєнні армій тільки розвинених країн, у тому числі засобів космічної розвідки, бомбардувальників середньої і великої дальності, літаків далекого радіолокаційного виявлення й управління, надводних кораблів, підводних човнів та інших засобів. За досвідом останніх війн для оборони об’єктів протиборчі сторони застосовували як ударну авіацію та РВ і А (для дії по ПУ БР на стаціонарних позиціях та в позиційних районах), так і наземні засоби ППО (ПРО), тобто вели боротьбу з НБР на землі та у повітрі.

Щодо боротьби з НБР у повітрі, то для забезпечення ефективної протиракетної оборони військ та об’єктів у складі угруповань ППО (ПРО) необхідно мати як універсальні ЗРК (ЗРС), так і спеціалізовані протиракетні комплекси (ПРК). Основні характеристики наземних універсальних ЗРК (ЗРС) та спеціалізованих ПРК, які є на озброєнні зарубіжних країн і характеризують здатність боротися з НБР, наведені в Табл. 2.

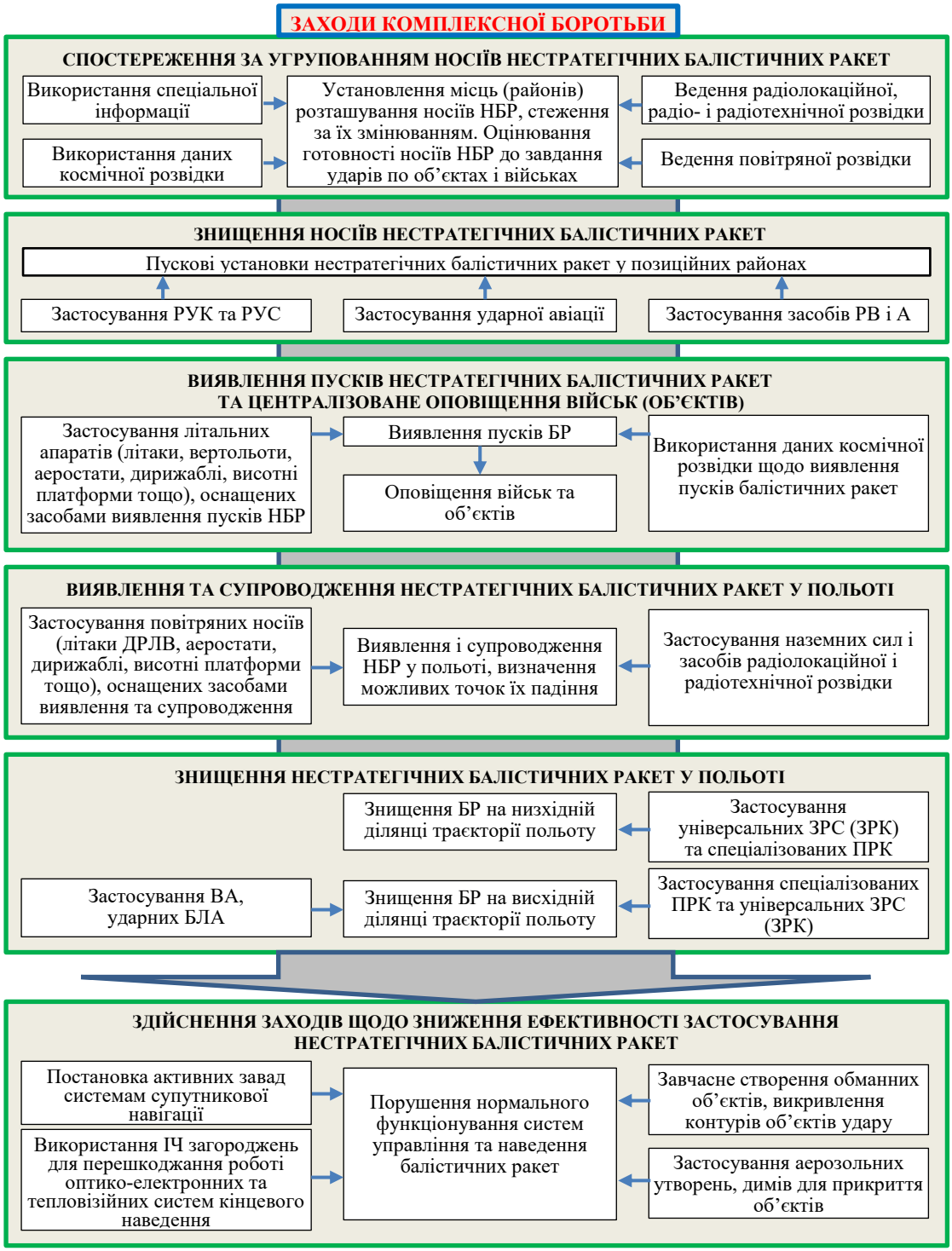


Рис. 1. До пояснення сутності комплексної боротьби з НБР за умови використання засобів, заснованих на традиційних фізичних принципах дії

Слід зазначити, що рис. 1 та Табл. 2 пояснюють сутність комплексного характеру боротьби з НБР лише за умови використання засобів, заснованих на традиційних фізичних принципах дії. Водночас вже є реальністю використання нових фізичних принципів у системах і засобах виявлення та ураження балістичних ракет [13–14].

Висновки

1. Нестратегічні балістичні ракети в майбутніх війнах і конфліктах залишатимуться важливим засобом нанесення перших ракетних ударів по важливих об'єктах системи ППО, військового та державного управління.

2. На початковому етапі війни під час повітряної (повітряно-наступальної) операції слід очікувати декілька масованих ракетно-авіаційних ударів у першому ешелоні яких поряд з КР можуть застосовуватись НБР для прориву системи ППО та дезорганізації системи управління.

Таблиця 2

Основні характеристики наземних універсальних ЗРК (ЗРС) та спеціалізованих ПРК, які характеризують здатність боротися з нестратегічними балістичними ракетами

Найменування зенітного ракетного комплексу, системи (тип ЗКР (ПР))	Основні характеристики комплексу (системи)			
	Типи БР, що уражаються	Максимальна дальність старту / швидкість БР, що уражаються, км / м/с	Максимальна дальність / висота перехоплення БР, км	Маса ЗКР (ПР), кг
Універсальні зенітні ракетні комплекси (системи)				
ЗРК "Петріот ПАК-2" (MIM-104 C/D)	ТБР, ОТБР	600* / 2200	20 / до 12	906
ЗРК "Петріот ПАК-3" (ПР "ERINT")	ТБР, ОТБР	1000 / 3000	40 / до 20	316
ЗРС С-300ПТ-1, ПС (5В55Р)	ТБР	200 / 1300	35 / до 25	1665
ЗРС С-300ПМ, ПМУ1 (48Н6)	ТБР, ОТБР	250* / 2800	40 / до 25	1900
ЗРС С-300ПМУ2 (48Н6Е2)	ТБР, ОТБР	250* / 2800	40 / до 25	1900
ЗРС С-400 (9М96/9М96Е2)	ТБР, ОТБР, БРСД	3500 / 4800	40/60* / 20/30	333/420
ЗРК С-350 (9М96/9М96Е2)	ТБР, ОТБР	3000* / 1000	30 / до 25	333/420
ЗРС С-300В1 (9М83)	ТБР	200 / 1200	40 / до 25	2290
ЗРС С-300В (9М82/9М83)	ТБР, ОТБР	1100 / 3200	40 / до 25	4500/ 2290
ЗРС С-300ВМ (9М82М/9М83М)	ТБР, ОТБР, БРСД	2500 / 4500	40 / до 30	4500/ 2290
ЗРК "Бук-М1-2, -М2" (9М317)	ТБР	150 / 1200	20 / до 16	715
ЗРК "Бук-М3" (9М317М)	ТБР, ОТБР	200* / 3000	30 / до 16	581
ЗРС С-500 (режим ПСО) (9М96/9М96Е2)	ТБР, ОТБР, БРСД	3500 / 5-7 М	60* / 35*	333/420
ЗРК МЕАДС (ПР "ERINT")	ТБР, ОТБР	1000 / 3000*	40 / до 20	316
ЗРК САМП-Т ("Астер-30")	ТБР, ОТБР	600 / 1000	35 / до 25	445
ЗРК ІРІС-Т (IRIS-T SLM)	ТБР	200* / 1000*	40 / до 20	87
Спеціалізовані протиракетні комплекси				
ПРК "Праща Давида" (ПР "Станер")	ТБР, ОТБР	300 / 700	40 / до 15	180
ПРК "Залізний купол" (ПР "Тамир")	ТБР	70 / ·	17 / до 10	90
ПРК "Хец-3" (ПР "Ерроу-3")	ТБР, ОТБР, БРСД	2500 / 4500	250 / до 100	1300
ПРК "Хец-2" (ПР "Ерроу-2")	ТБР, ОТБР, БРСД	3000 / 3000	150 / 50 – 60	1350
ПРК ТХААД	ТБР, ОТБР, БРСД	3500 / 4000*	200 / 40-150	900
ПРК "Іджис Ешор" (ПР "Стандарт СМ-3")	ТБР, ОТБР, БРСД	3000 / 3000	700 / до 500	1500
ПРК С-500 (режим ПРО) (ПР 77Н6-Н)	БРСД, МБР	3500 / 5-7 М	·/ 200	·

Примітка: * – оціночні значення

3. Застосуванню НБР в ударах необхідно протиставити адекватні заходи, які повинні мати комплексний характер щодо їх виявлення системою розвідки, оповіщення про їх застосування, знищення активними засобами системи ППО (ПРО), а також протидії їхньому ефективному використанню.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Боевое применение ракет в войне в районе Персидского залива // Авиационная и ракетная техника. 1992. № 9. С. 15–22.
2. Загорка О. М., Дейнега О. В. Зарубіжний досвід створення нестратегічних системи протиракетної оборони (ПРО на ТВД) // Наука і техніка Повітряних Сил Збройних Сил України. 2010. № 1 (3). С. 28–37.
3. Загорка А., Дейнега А. Анализ развития ЗРК для противоракетной обороны объектов и войск // Арсенал XXI века. 1999. № 2. С.16–18.
4. Дрожжин А., Алтухов Е. Воздушные войны в Ираке и Югославии. Москва : ООО "Восточный горизонт", 2002. 80 с.
5. Российские тактические ракетно-артиллерийские системы "Луна-М" // Иностранная печать об экономическом, научно-техническом и военном потенциале государств-участников СНГ и технических средствах его выявления. Серия: Вооруженные силы и военно-промышленный потенциал. Москва : ВИНИТИ, 1997. С. 20–29.
6. Порицкий Л. ФАУ (оружие возмездия) и противовоздушная оборона Англии // Зеркало недели. 2000. 15 янв. (№ 1–2).
7. Краснов А. Боевое применение крылатых ракет воздушного базирования // Зарубежное военное обозрение. 2001. № 2. С. 30–35.
8. Растопшин М. Зарубежные реактивные системы залпового огня // Техника и вооружение вчера, сегодня, завтра. 2003. № 3. С. 10–15.
9. Овчинніков В. О., Філіпенко Ю. Г. Огляд застосування ракетних військ та тенденції розвитку принципів їх бойового застосування //

Наука і техніка Повітряних Сил Збройних Сил України : наук.-техн. журнал. 2010. № 1 (3). С. 230–236.
10. Новиков В., Голубчиков С. Праща под куполом. Израиль начинает строить пятый рубеж противоракетной обороны // Военно-промышленный курьер. 2016. 23 листоп. № 45 (660). URL: http://vpk-news/ru/articles/33793 (дата звернення: 14.11.2018).
11. Штайнер У., Гункель Е. Щит Израиля: как работает система ПВО "Железный купол". 14.05.2021. // URL: https: //www.dw.com.>kak-rabotaet…(дата звернення: 14.11.2018).
12. Загорка О. М., Дейнега О. В. Комплексна боротьба з крилатими та балістичними ракетами // Наука і техніка Повітряних Сил Збройних Сил України : наук.-техн. журнал. 2015. № 1 (18). С. 6–11.
13. Романченко І. С., Загорка О. М., Бутенко С. Г., Дейнега О. В. Теорія і практика боротьби з малорозмірними низьколітними цілями (оцінка можливостей, тенденції розвитку засобів протиповітряної оборони) : монографія. Житомир: Полісся, 2011. 344 с.
14. Класифікація зброї на нетрадиційних принципах дії : методич. посіб. Київ : ЦНДІ ОВТ ЗС України, 2004. 52 с.

Стаття надійшла до редакційної колегії 18.08.2023

Analysis of the use of non-strategic ballistic missiles in local wars and armed conflicts and the fight against them

Annotation

The article analyzes the experience of combat use of non-strategic ballistic missiles in local wars and conflicts of the late twentieth and early twenty-first centuries. Non-strategic ballistic missiles used in local wars and conflicts include: tactical ballistic missiles: "Luna-M", "Zeev", "Tochka-U", "Oghab", "Al-Samud-2", "Iran-130", etc., operational and tactical ballistic missiles: R-300, "Scud", "Al-Hussein", ATACMS, "Iskander-M, -E", "Lora", etc., as well as airborne ballistic missiles of the "Kinzhal" aviation complex.

The article summarizes the forms and methods of use of non-strategic ballistic missiles in the most significant wars (conflicts) and provides data on the experience of combating this type of air attack.

It is noted that in order to combat non-strategic ballistic missiles, the world has created many universal (for use in organizing both anti-aircraft and missile defense) anti-aircraft missile systems (complexes) and several specialized (for organizing missile defense) missile systems that can be used in organizing missile defense of civilian and military facilities. The following ground-based air defense systems are considered to be the main universal ones: Russian - S-300P and S-300V, S-350 "Vityaz", S-400 "Triumph", S-500 "Prometheus" (air defense mode) and "Buk" air defense systems (starting with the M1-2 modification); American – systems of the "'Patriot" family (starting with the PAK-2 modification); Israeli – systems "David's Sling", "Iron Dome"; German – systems IRIS-T; jointly produced (Germany, Italy, France) – systems SAMP-T. Specialized ground-based air defense systems include the American THAAD and Aegis Ashore systems with Standard SM-3 missiles, the Israeli Hetz with Arrow missiles, and the Russian S-500 (missile defense mode).

Keywords: aeroballistic missile; combat use; anti-aircraft missile system (system); non-strategic ballistic missile; anti-missile system; missile defense effectiveness.

УДК 355/359.07 DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/27-34

Зубков В. П. (0000-0003-1616-2795)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Механізм впливу на інформаційні системи противника як складова інформаційного забезпечення сил оборони України

Резюме. У статті аналізується сутність інформаційно-технічного впливу на інформаційні системи противника як складової інформаційного забезпечення сил оборони України. За результатами аналізу пропонуються механізм реалізації інформаційно-технічного впливу як інструмента інформаційної зброї та підходи до подальшого його вдосконалення.

Ключові слова: інформаційне забезпечення; інформаційна зброя; інформаційно-технічний вплив.

Постановка проблеми. У XXI столітті глобалізація та стрімкий розвиток інформаційної сфери дають істотне підґрунтя для поширення нових інформаційних загроз, які потребують негайного реагування. Бурхливе втілення інформаційних технологій сучасності супроводжується активним виникненням таких загроз, а також відповідного їм *інформаційного впливу*, під яким розуміється "… організоване цілеспрямоване втручання у свідомість (підсвідомість) чи фізичний стан цільової аудиторії та/або в процес функціонування технічних об'єктів інформаційної інфраструктури шляхом застосування інформаційних засобів і технологій" [1].

Розвиток інформаційних технологій у воєнній сфері призводить до посилення інформаційного протиборства, зокрема за рахунок тотальної інформатизації засобів збройної боротьби, яка дала змогу об'єднати пункти управління, засоби розвідки, озброєння, зв'язку, навігації в єдине інформаційно-мережеве середовище у рамках мережецентричної війни [2–4]. Водночас таке середовище стає більш вразливим від засобів інформаційного протиборства, зокрема проявів інформаційного впливу [5].

Концепція мережецентричних воєн виводить на новий рівень сферу ведення військового протиборства – *інформаційний простір*, під яким розуміється інформаційне середовище, у якому відбуваються інформаційні процеси та інформаційні відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації, інформаційних продуктів та інформаційних ресурсів [1]. У цьому просторі актуальне значення набуває новий вид озброєння – *інформаційна зброя*, одним з інструментів якої є інформаційно-технічний вплив (ІТВ) на інформаційні системи противника як складова інформаційного забезпечення сил оборони України [6, 7]. У таких умовах потребує більшої конкретизації сутність механізму реалізації інформаційно-технічного впливу на інформаційні системи противника.

Особливої актуальності це питання набуває у зв'язку з повномасштабною збройною агресією Російської Федерації проти України, коли інформаційна складова постала щонайважливішим елементом забезпечення ефективного спротиву.

Аналіз останніх публікацій. Стан інформаційного забезпечення у воєнній сфері неодноразово висвітлювався в наукових публікаціях. Цій темі присвячено низку робіт [6–15]. Так, у [9] стверджується, що "інформаційна зброя, як правило, не спрямована на досягнення втрат у живій силі супротивника. Вона не знищує фізично й не руйнує людські, матеріально-технічні та інші ресурси, а лише підриває основи дії механізмів організації управління". З таким твердженням можна лише частково погодитися. У воєнному плані виведення з ладу системи управління розглядатиметься як важлива умова завдання противнику поразки. Адже порушення алгоритмів управління будь-якої системи в сучасних умовах неминуче призведе до погіршення її стану. Крім того, важливим способом ведення боротьби з противником із застосуванням інформаційної зброї вважатиметься віддалене ураження економічного (енергетичного) потенціалу будь-якої держави шляхом виведення з ладу засобів автоматизації управлінських процесів [5].

У деяких працях головна увага приділяється, в основному, термінологічним визначенням. Зокрема, в [13] автори, формулюючи аспекти інформаційної війни, дають загальне визначення ІТВ як "впливу на інформаційну інфраструктуру об'єкта для забезпечення реалізації необхідних змін у її

роботі (зупинку роботи, несанкціонований виток інформації, програмування на певні помилки, зниження швидкості опрацювання інформації тощо)". Водночас роль, сутність, питання організації та оцінювання ІТВ на інформаційні системи противника в цих наукових працях не розкриваються.

З огляду на це, існує проблемне питання визначення механізму реалізації негативного ІТВ на інформаційні системи противника, що потребує більш детального наукового опрацювання.

Метою статті є обґрунтування системно-цільового підходу до визначення механізму реалізації ІТВ на інформаційні системи противника як складової інформаційного забезпечення сил оборони.

Виклад основного матеріалу. Сутність системно-цільового підходу до визначення механізму реалізації ІТВ на інформаційні системи противника полягає в застосуванні цілісної системи, що складається з відносно відокремлених взаємодіючих і взаємопов'язаних між собою елементів (підсистем), вивчення всієї сукупності параметрів і показників функціонування такої системи в динаміці з постійною орієнтацією діяльності на кінцеві результати, коли цілепокладання та цілереалізація ІТВ здійснюється покроково в кожному елементі з урахуванням специфіки їх функціонування.

Загалом, системно-цільовий підхід може бути реалізований у загальних межах теорії кібернетичного управління [14, 15], при якому будь-яку функцію в системі управління неможливо реалізувати без належного інформаційного забезпечення цього процесу. Інформаційний вплив здійснюється виключно за допомогою елементів інформаційної інфраструктури та наявних інформаційних ресурсів, під якими розуміються дані та знання, відмінною і невід'ємною характеристикою яких є їх прагматична цінність, що визначається практичними потребами в інтересах вирішення певних завдань [1].

Будь-який інформаційний простір формується за наявності необхідних інформаційних ресурсів із застосуванням відповідної інформаційної інфраструктури. *Інформаційна інфраструктура* – це сукупність інформаційних систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування.

Засоби, що здійснюють деструктивну дію в інформаційному просторі, об'єднані в новий клас зброї – інформаційну зброю. Нині до інформаційної зброї відносять широкий клас прийомів і способів інформаційного впливу на противника – від дезінформації і пропаганди до засобів радіоелектронної боротьби та дій у кіберпросторі. *Інформаційна зброя* – це сукупність способів, прийомів, засобів і технологій інформаційного впливу, призначених для нанесення збитку (ураження) елементам інформаційної інфраструктури протилежної сторони під час ведення інформаційної боротьби шляхом:

придушення елементів інформаційної інфраструктури державного та військового управління;

електромагнітного впливу на елементи інформаційних та телекомунікаційних систем;

доступу до інформаційних ресурсів з подальшою деформацією (спотворенням), знищенням або витоку інформації;

інформаційно-психологічного впливу на військовослужбовців та громадянське населення.

Інформаційній зброї притаманні такі *якісні характеристики* [5]:

універсальність (застосування не залежить від кліматичних та географічних умов, часу доби, сезонів року тощо);

прихованість – не потрібно проводити мобілізацію, створювати великі угруповання військ;

непомітність;

раптовість застосування;

економічна ефективність (розроблення інформаційної зброї та її застосування потребує істотно менших витрат у порівнянні з іншими видами зброї);

масштабність застосування (вирішення завдань не тільки тактичного, але й можливо стратегічного рівня);

наявність ефекту "ланцюгової реакції" (вплив інформаційної зброї на окремий елемент інформаційної системи, інформаційного ресурсу може призвести до виведення з ладу інших елементів системи, а можливо і системи в цілому);

складність здійснення контролю за створенням та випробуванням інформаційної зброї (факти розроблення і застосування можна надійно приховати від розвідки противника).

Відповідно до сфери свого застосування інформаційна зброя поділяється на

інформаційно-технічну зброю та інформаційно-психологічну зброю.

Інформаційно-психологічна зброя – вид інформаційної зброї як сукупність засобів, форм, способів і прийомів прихованого маніпулювання інформацією в інформаційному просторі протиборчої сторони для ураження індивідуальної і масової свідомості (підсвідомості), зокрема через друковані, електронні та аудіовізуальні засоби масової інформації [5].

Зосередимо увагу на розгляді інформаційно-технічної зброї, особливістю функціонування якої є її орієнтованість на поразку апаратно-програмних засобів систем передачі, зберігання та обробки інформації противника, що функціонують в інформаційному просторі електронних інформаційних ресурсів (кіберпросторі).

Інформаційно-технічна зброя – сукупність спеціально організованої інформації, інформаційних технологій, способів і засобів, які дають змогу цілеспрямовано змінювати (знищувати, спотворювати), копіювати, блокувати інформацію, долати системи захисту, обмежувати допуск санкціонованих користувачів, порушувати функціонування систем обробки інформації, здійснювати дезінформацію, дезорганізацію роботи технічних засобів комп'ютерних систем та інформаційно-обчислювальних мереж, а також інших інфраструктур забезпечення функціонування систем управління.

Інформаційно-технічна зброя включає технічні та програмні засоби, що забезпечують несанкціонований доступ до баз даних, порушення штатного режиму функціонування апаратно-програмних засобів, а також виведення з ладу ключових елементів інформаційної інфраструктури. Застосування інформаційно-технічної зброї спрямоване на зрив виконання цільових завдань із застосуванням інформаційної системи. Приклади деяких видів інформаційно-технічної зброї, що ґрунтуються на різних технологіях, наведено у Табл. 1.

Таблиця 1

Види інформаційно-технічної зброї, що ґрунтуються на різних технологіях

Вид інформаційно-технічної зброї	Засоби, що використовуються	Тип технології
Засоби впливу на компоненти радіоелектронного обладнання та системи їх енергозабезпечення	Засоби силового радіоелектронного придушення; надпотужні генератори НВЧ-випромінювання (гіротрони, магнетрони та ін.); вибухомагнітні генератори (ВМГ), вибухові магнітогідродинамічні генератори (МГД-генератори); засоби силового впливу через електромережу; засоби виведення з ладу електромереж	На основі енергетичної дії
	Програмні засоби виведення з ладу обладнання (резонанс головок жорстких дисків, випалювання моніторів та ін.); програмні засоби стирання пам'яті, що перезаписується; програмні засоби впливу на системи безперебійного живлення	На основі інформаційних технологій
Засоби впливу на інформаційні ресурси та апаратно-програмні засоби АСУ	Засоби подолання систем захисту інформації; засоби проникнення в інформаційні системи противника; засоби маскування джерел отримання інформації; засоби виведення з ладу інформаційної системи; засоби прихованої часткової зміни алгоритму функціонування програмного забезпечення; засоби збору даних, що циркулюють в інформаційних системах противника; засоби доставки та впровадження певних алгоритмів у конкретне місце інформаційної системи; засоби впливу на системи охорони об'єктів	На основі інформаційних технологій
Засоби впливу на процес передачі інформації	Засоби радіоелектронної боротьби; станції перешкод радіозв'язку (у тому числі з елементами штучного інтелекту); передавачі перешкод одноразового використання, що закидаються	На основі енергетичного впливу
	Засоби впливу на протоколи передачі даних систем зв'язку та передачі даних; засоби впливу на алгоритми адресації та маршрутизації; засоби перехоплення та порушення проходження інформації в технічних каналах її передачі; засоби виклику перевантаження системи хибними запитами на встановлення зв'язку	На основі інформаційних технологій

Застосування інформаційно-технічної зброї реалізується шляхом ІТВ на відповідні об'єкти.

ІТВ на інформаційні системи противника – це цілеспрямоване втручання в процес функціонування технічних об'єктів інформаційної інфраструктури противника з

метою порушення їх роботи або виведення з ладу шляхом застосування засобів і технологій радіоелектронного впливу та кіберзброї [1]. Такий вплив – основний вражаючий фактор інформаційно-технічної зброї, що є дією або на інформаційний ресурс, або на інформаційну систему, або на засоби отримання, передачі, обробки, зберігання та відтворення інформації в її складі, з метою викликати певні деструктивні структурні та/або функціональні зміни [5].

ІТВ можуть бути поодинокі або групові. ІТВ також класифікують за характером вражаючих властивостей [5, 6]:

вибіркові впливи – на визначений певний ресурс в інформаційно-обчислювальній мережі;

комплексні впливи – на всю інформаційно-телекомунікаційну інфраструктуру.

За способом реалізації ІТВ можуть бути поділені на алгоритмічні; програмні; апаратні; фізичні: електромагнітні (радіоелектронні; оптико-електронні; оптичні; електричні); акустичні; гідроакустичні; радіаційні; хімічні; біологічні; на основі інших фізичних принципів [5].

ІТВ різних видів можуть застосовуватися спільно. Крім того, деякі види інформаційно-технічних впливів одночасно несуть у собі риси кількох видів.

До *алгоритмічного ІТВ* відноситься дія на алгоритми використання засобів (програмного, апаратного, фізичного) для здійснення несанкціонованого впливу на інформаційні ресурси. Прикладом алгоритмічного впливу є DoS-атака (Denial of Service – відмова в обслуговуванні). Сутність такого впливу полягає в тому, що на систему, що атакується, посилаються з високою інтенсивністю коректні запити на використання її інформаційних ресурсів. Це призводить до того, що можливості інформаційної системи обслуговування таких запитів швидко вичерпуються, і вона відмовляє в обслуговуванні всім своїм користувачам.

До *програмного ІТВ* належить дія на програмне забезпечення з метою несанкціонованого впливу на інформаційні системи противника, їх інформаційні ресурси. До такого ІТВ можна віднести засоби організації віддалених мережевих атак, комп'ютерні віруси, програмні закладки, нейтралізатори тестових програм та програм аналізу коду.

До *апаратного ІТВ* можуть бути віднесені дії на засоби, які вбудовані в інформаційну систему або несанкціоновано впроваджені до неї, а також на санкціоновані апаратні засоби, які дають змогу у процесі своєї роботи здійснювати несанкціонований вплив на інформаційні ресурси системи. До найпоширенішого типу апаратного інформаційно-технічного впливу належить дія на апаратні закладки.

До *фізичного ІТВ* можуть бути віднесені дії стосовно добування інформації шляхом доступу до інфраструктури інформаційного простору, аналізу фізичних полів, що генеруються об'єктами цієї інфраструктури, а також засоби радіоелектронного та вогневого ураження її фізичних елементів. Здійснювати фізичний інформаційно-технічний вплив можливо через: засоби технічної розвідки; засоби радіоелектронного придушення; засоби оптико-електронного придушення; засоби ураження електромагнітним випромінюванням (генератори електромагнітних імпульсів, генератори НВЧ-випромінювання, генератори лазерного випромінювання та ін.); засоби ураження силовими електромагнітними впливами (генератори електричного струму надвисокої напруги); засоби виведення з ладу елементної бази радіоелектронних систем. Інформаційно-технічний вплив на інформаційні системи противника може бути реалізований шляхом:

віддаленої мережевої атаки – це руйнівний або дестабілізуючий ІТВ, що здійснюється по каналах зв'язку віддаленим щодо атакованої системи суб'єктом і характерний для структурно- та просторово-розподілених інформаційних систем;

використання комп'ютерних "вірусів" – приховані програми, що застосовуються для деструктивної зміни програмного забезпечення комп'ютерів та комп'ютерних мереж;

поширення фальшивої (недостовірної) інформації в комп'ютерних мережах;

обмеження або заборони доступу до інформаційного ресурсу легальним користувачам комп'ютерних мереж;

радіоелектронного придушення радіотехнічних засобів (зв'язку, спостереження, навігації, радіо, телебачення тощо).

Деструктивний ІТВ має бути спрямований на такі об'єкти в інформаційній інфраструктурі противника, як: інформаційно-телекомунікаційні мережі (мережі та засоби зв'язку, електронні засоби масової інформації,

електронні архіви (сховища) та банки даних, засоби автоматизації систем управління військами (силами) та зброєю, радіоелектронні засоби і системи управління, навігації, спостереження тощо, а також на інформацію (інформаційний ресурс), що циркулює в таких об'єктах у реальному часі.

Проведений аналіз дає змогу орієнтовно визначити такі *основні напрями* ІТВ на процес функціонування інформаційних об'єктів противника:

порушення встановленого порядку інформаційного обміну, несанкціонований доступ (або обмеження будь-якого доступу) до інформаційних ресурсів противника, збір, отримання, використання та розповсюдження інформації (дезінформація, приховування або спотворення інформації);

порушення ефективності функціонування інформаційних засобів противника, цілеспрямоване розповсюдження комп'ютерних "вірусів" і спеціальних програм перехоплення інформації у комп'ютерних мережах, поширення недостовірної інформації, радіоелектронне ураження (придушення) тощо, спотворення (знищення) інформаційного ресурсу, зокрема програмного забезпечення;

спрямований (відкритий і прихований) негативний ІТВ в інформаційному просторі противника з метою масового розповсюдження по інформаційних каналах противника дезінформації для введення в оману та коригування намірів осіб, які приймають рішення;

створення перешкод для розроблення та впровадження інформаційних технологій противника.

Сутністю деструктивного ІТВ на інформаційні системи противника є: пошук, добування (одержання), збір, оброблення, накопичення, збереження і використання інформації, планування та здійснення вражаючого (придушуючого) впливу, аналіз наслідків цього впливу з можливістю його корекції.

Модель функціонування механізму реалізації ІТВ на інформаційні системи противника базується на кібернетичній схемі як послідовності часткових функцій загального процесу управління – таких, як збір інформації про інформаційну систему противника, аналіз зібраної інформації, виявлення вразливостей інформаційної системи противника, прийняття рішення щодо застосування ІТВ на противника з використанням цих вразливостей, здійснення ІТВ виконавчими силами і засобами інформаційної інфраструктури, оцінку результатів ІТВ та уточнення подальших завдань (рис.1).

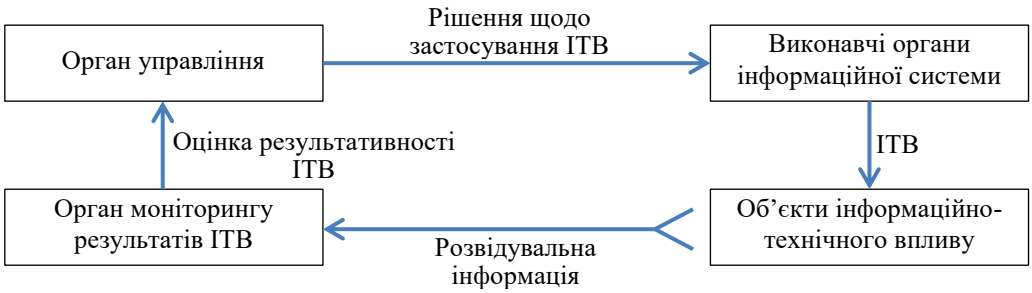


Рис. 1. Кібернетична модель механізму реалізації інформаційно-технічного впливу на інформаційні системи противника

Управляти механізмом реалізації ІТВ на інформаційні системи противника відповідно до теорії управління [14, 15] означає виконання декількох етапів.

1-й етап процесу управління механізмом ІТВ на інформаційні системи противника є найбільш складним утворенням логічної послідовності окремих часткових функцій, коли *орган управління* на підставі збору та аналізу розвідувальної інформації про об'єкти інформаційної системи противника, виявлення їх уразливостей приймає рішення щодо застосування ІТВ на конкретні об'єкти такої системи противника. З цією метою визначають:

наявність потенційних загроз з боку об'єктів інформаційної системи противника;

ступені важливості об'єктів інформаційної системи противника;

рівень вразливості об'єктів інформаційної системи противника;

визначення першочергових об'єктів інформаційної системи противника, порядку та послідовності здійснення на них впливу;

вибір засобів і способів реалізації ІТВ на визначені об'єкти інформаційної системи противника;

час початку та закінчення ІТВ на визначені об'єкти інформаційної системи противника;

заходи прикриття здійснення ІТВ на об'єкти інформаційної системи противника;

завдання виконавчому (им) органу (ам) щодо підготовки та здійснення ІТВ на визначені об'єкти інформаційної системи противника.

2-й етап процесу управління механізмом ІТВ на інформаційні системи противника здійснюється *виконавчим органом* та спрямований на реалізацію заходів ІТВ на конкретні об'єкти інформаційної системи противника. Відповідно до завдань, визначених органом управління, *виконавчий орган* готує та здійснює відповідний вид ІТВ на такі об'єкти інформаційної системи противника з використанням існуючої інформаційної інфраструктури, виходячи з можливостей засобів ІТВ, що є у наявності. При цьому:

усвідомлюються (за необхідністю – уточнюються) завдання, визначені органом управління щодо впливу на об'єкти інформаційної системи противника з урахуванням існуючої інформаційної інфраструктури;

проводиться оцінка можливостей власних сил та засобів ІТВ, а також противника відповідно до отриманих завдань;

здійснюється вибір способів реалізації ІТВ за характером вражаючих властивостей для виконання завдань з максимальною ефективністю;

здійснюється розподіл наявних засобів ІТВ по завданнях, визначених органом управління;

визначається порядок виконання завдань щодо ІТВ на об'єкти противника з урахуванням можливостей власних засобів інформаційної інфраструктури та противної сторони;

здійснюється постановка завдань безпосереднім виконавцям ІТВ.

3-й етап процесу управління (*контроль результатів ІТВ*) виконується *органом моніторингу*, який здійснює постійний контроль за результативністю впливу на визначені об'єкти інформаційної системи противника. Сутність виконання 3-го етапу полягає в оцінці результатів змін інформаційної активності об'єктів інформаційної системи противника та надання об'єктивної інформації про їх стан до органу управління.

4-й етап – *орган управління* на підставі даних, отриманих від органу моніторингу щодо результатів змін рівня функціонування об'єктів інформаційної системи противника, по яких було здійснено ІТВ, приймає *рішення про результати ІТВ* та робить висновок щодо необхідності подальшого впливу.

Запропонований 4-етапний механізм організації ІТВ на інформаційні системи противника дозволяє реалізувати адаптивну систему управління впливом. Зазначені етапи виконуються циклічно, оскільки залежно від ситуації можуть змінюватися загрози, з'являтися нові інформаційні ресурси або змінюватися порядок їх використання, а також можуть змінюватися технології та методи впливу на інформаційні системи. Такий підхід потребує постійного контролю та (за необхідності) удосконалення методів впливу на інформаційні системи противника.

На підставі зазначеного можна сформувати деякі рекомендації щодо визначення напрямів поліпшення інформаційного забезпечення сил оборони, зокрема його складової – ІТВ на інформаційні системи противника, пов'язаного з удосконаленням методів та способів:

добування необхідних даних щодо інформаційних систем противника з використанням усіх можливих джерел;

отримання розвідувальної інформації шляхом перехоплення та розшифровування інформаційних потоків, що передаються каналами зв'язку противника, а також за рахунок побічних випромінювань;

здійснення доступу до інформаційних ресурсів противника з подальшим добуванням інформації та її перекручуванням;

формування та масове поширення по інформаційних каналах противника або глобальних мережах дезінформації для впливу на оцінки, наміри осіб ворога, які приймають рішення;

ведення радіоелектронної боротьби (радіоелектронного ураження або придушення радіоелектронних засобів противника);

вогневого ураження (у воєнний час) елементів інформаційної інфраструктури державного та військового управління противника.

Таким чином, для вирішення завдання адекватної протидії у гібридній агресії проти Україні із застосуванням системно-цільового підходу передбачає створення та впровадження системи забезпечення інформаційної безпеки сил оборони, зокрема її складової – підсистеми ІТВ як складової інформаційного забезпечення сил оборони України, яка діє превентивно для рішучого нівелювання переваги технологічно більш розвиненого противника. Водночас, для

комплексного вирішення проблем захисту національного інформаційного простору потрібні спільні зусилля як з боку органів влади, усіх складових сектору безпеки і оборони, так і громадських організацій, бізнесових структур.

Висновки

1. У світовому інформаційному просторі перманентно зростає рівень інформаційного протиборства як один з головних напрямів реалізації інформаційної політики сучасних міжнародних відносин. Збільшується кількість та складність інформаційних загроз. Унаслідок бурхливого втілення інформаційних технологій набирає актуальності інформаційна зброя, одним з інструментів якої є ІТВ на інформаційні системи противника як складова інформаційного забезпечення сил оборони України.

2. Системно-цільовий підхід до визначення механізму реалізації ІТВ на інформаційні системи противника передбачає виконання послідовності етапів: аналіз потенційних загроз на підставі збору розвідувальної інформації про об'єкти інформаційної системи противника; прийняття рішення щодо застосування ІТВ; підготовку та здійснення ІТВ на призначені об'єкти інформаційної системи противника; контроль за результативністю впливу на визначені об'єкти противника, по яких було здійснено ІТВ; прийняття рішення про результати ІТВ та висновок щодо подальших управлінських дій.

3. Роль ІТВ на інформаційні системи (об'єкти) противника як складової інформаційного забезпечення сил оборони України полягає в організації та проведенні комплексу акцій та атак, якими реалізується деструктивне електронне втручання в інформаційні ресурси противника та процес функціонування об'єктів його інформаційної інфраструктури з метою виведення їх з ладу або порушення сталого режиму функціонування.

Перспектива подальших досліджень. Метою подальшого дослідження є визначення комплексу заходів ІТВ на інформаційні об'єкти противника як складової інформаційного забезпечення сил оборони України, що повинні бути органічно пов'язані із заходами безпеки власної інформації (інформаційно-технічним захистом). Зазначені завдання можуть бути вирішені із застосуванням системно-цільового підходу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ВСТ 01.004.004–2014(01). Інформаційна безпека держави у воєнній сфері. Терміни та визначення. [Чинний від 2014-02-27] . Київ, 2014. (Військовий стандарт).

2. Ільяшов О. А. Тенденції розвитку збройної боротьби у війнах четвертого – шостого поколінь // Наука і оборона. 2009. № 3. С.43–48.

3. Макаренко С. И., Иванов М. С. Сетецентрическая война – принципы, технологии, примеры и перспективы. Санкт-Петербург : Наукоемкие технологии, 2018. 898 с.

4. Воєнна доктрина США "Joint Vision 2020". URL: http:// Joint Vision 2020.pdf (дата звернення: 07.08.2023).

5. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры // Системы управления, связи и безопасности. № 3. 2016. URL: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (дата звернення: 08.08.2023).

6. Саричев Ю. О. Аналіз підходів щодо визначення сучасної ролі та місця інформаційного забезпечення в системі державного управління // Вісник НАДУ при Президентові України. 2016. Вип. 3 (82). С.138–143.

7. Сніцаренко П. М., Саричев Ю. О., Ткаченко В. А. Комплексна система протидії негативному інформаційно-психологічному впливу на особовий склад Збройних Сил України // Наука і оборона. 2018. № 2. С. 40–45.

8. Саричев Ю. О. Теоретичний підхід до інформаційного забезпечення в системі державного управління у воєнній сфері // Вісник НАДУ при Президентові України. Серія "Державне управління" 2016. Вип. 4 (83). С. 153–160.

9. Горбулін В. П., Качинський А. Б. Засади національної безпеки України : підручник. Київ : Інтертехнологія, 2009. 272 с.

10. Смалько О. А. Захист інформаційних ресурсів : монографія. Кам'янець-Подільський : ПП Буйницький, 2011. 704 с.

11. Сніцаренко П. М. Організаційні основи державної системи забезпечення інформаційної безпеки України у воєнній сфері // Інформаційна безпека людини, суспільства, держави. 2012. № 2 (9). С. 46–52.

12. Теоретичні основи управління угрупованням військ (сил) у сучасних умовах збройної боротьби : монографія / О. М. Загорка, А. К. Павліковський, А. А. Корецький, С. О. Кириченко, І. О. Загорка ; за заг. ред. І. С. Руснака. Київ : НУОУ, 2020. 248 с.

13. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України // Політичний менеджмент. 2008. № 4. С.136–140. URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/ostroukhov_do_problemy.pdf (дата звернення: 09.08.2023).

14. Винер Н. Кибернетика или управление и связь в животном и машине. Москва : Сов. Радио, 1968. 328 с.

15. Глушков В. М. Кибернетика. Вопросы теории и практики. Москва : Наука, 1986. 488 с.

Стаття надійшла до редакційної колегії 08.09.2023

Mechanism of influence on enemy information systems as a component of information support for the Ukrainian defense forces

Annotation

The development of information technologies in the military sphere leads to the intensification of information confrontation, in particular due to the total informatization of armed struggle, which has made it possible to combine control points, intelligence, weapons, communications, navigation into a single information and network environment within the framework of network-centric warfare. The concept of network-centered warfare brings to a new level the sphere of military confrontation - the information space, which means the information environment in which information processes take place. In this space, a new type of weapon – information weapons – is gaining importance, one of the tools of which is information and technical influence (ITI) on enemy information systems as a component of information support for the Ukrainian defense forces. In such circumstances, the essence of the mechanism of realization of information and technical influence on the enemy's information systems needs to be more specified. This issue is especially relevant in connection with the full-scale armed aggression of the Russian Federation against Ukraine, when the information component has become a crucial element of ensuring effective resistance.

The model of functioning of the mechanism of implementation of ITI on enemy information systems is based on a cybernetic scheme as a sequence of partial functions of the general management process. A 4-stage mechanism for organizing ITE on adversary information systems is proposed, which allows to implement an adaptive impact management system. The stages are carried out cyclically, since, depending on the situation, threats may change, new information resources may appear or the order of their use may change, and technologies and methods of influence on information systems may change. Such an approach requires constant monitoring and (if necessary) improvement of methods of influencing the enemy's information systems.

Keywords: information support; information weapons; information and technical influence.

УДК 004.77, 355.1, 355.4 DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/35-43

Прокопенко О. С., доктор філософії (0000-0002-5482-0317)
Федорієнко В. А., кандидат технічних наук (0000-0002-0921-3390)
Кульчицький О. С. (0000-0002-4901-0192)

Навчально-науковий центр стратегічних комунікацій у сфері забезпечення національної безпеки та оборони Національного університету оборони України, Київ

Підхід щодо виявлення і аналізу інформаційних загроз національній безпеці України у системі стратегічних комунікацій

Резюме. Розглянуті певні питання побудови системи управління стратегічними комунікаціями і запропоновано методичний підхід щодо своєчасного виявлення, аналізу та оцінювання інформаційних загроз національній безпеці України.

Ключові слова: стратегічні комунікації; інформаційний простір; наратив; інформаційна загроза; негативний інформаційний вплив; моніторинг інформаційного простору.

Постановка проблеми. Умови існуючого сьогодення характеризуються стадією становлення глобального інформаційного простору, революційною ознакою якого є використання інформації як засобу досягнення бажаної мети. Це досягається завдяки активізації процесів розвитку інформаційних технологій, для задоволення комунікаційних потреб у політичній, економічній, військовій, соціальній та інших сферах діяльності людства. Водночас, інформаційна відкритість світу об'єктивно сприяє проведенню інформаційних атак (операцій), що у даному контексті характеризує інформацію як зброю. Викладення інформації у необхідний на користь організатора інформаційної пропаганди спосіб, дозволяє формувати у суспільстві потрібну точку зору, громадську думку, хід взаємодоповнюючих логічних думок, тощо.

В умовах повномасштабної війни з Російською Федерацією (РФ) особливо актуальним постає питання інформаційної безпеки – одного з ключових чинників національної безпеки України. З 2014 року Україна стикається з безпрецедентним обсягом інформаційних атак, спрямованих на підрив державності, демократії, суверенітету та територіальної цілісності України. Найбільш значущими видами інформаційних загроз для України, яку поширюють Російські державні ЗМІ, проросійськи налаштовані агенти впливу через соціальні мережі і інші комунікативні канали, є спотворення інформації у вигляді відкритої пропаганди, інформаційного тероризму та дезінформації. При цьому, ціллю формування негативного образу, висвітлення у світовому сприйнятті України, як нестабільної, корумпованої та неспроможної до реформ держави. Негативний інформаційно-психологічний вплив спрямований на психологічну деморалізацію українського населення, посилення соціально-політичної поляризації, поглиблення розбрату між Україною та її західними партнерами.

Існуючі виклики і загрози національній безпеці України, обумовлюють необхідність проведення комплексу ефективних заходів для реалізації державних стратегічних наративів, а також своєчасної інформаційної протидії, нейтралізації деструктивного інформаційного впливу і підвищення інформаційної безпеки особистості, суспільства і держави.

Довідка. *Стратегічний наратив* – основоположна ідея, що відображає та визначає базові принципи існування та розвитку держави (її інституції), характер і спрямованість внутрішніх і зовнішніх взаємовідносин, на основі якої формуються напрямки реалізації державної (відомчої) політики [1].

З огляду на вищезазначене, значна роль в інформаційній протидії противнику належить оцінюванню інформаційного простору у системі стратегічних комунікацій, основу якого становить моніторинг. Застосування у моніторингу інформаційного простору сучасних теоретичних підходів та інформаційних технологій дозволить суттєво покращити виявлення та аналіз інформаційних загроз національній безпеці України.

Аналіз останніх досліджень і публікацій. Аналіз зарубіжних та вітчизняних джерел, відносно теорії і практики використання технологій моніторингу інформаційного простору, методів оцінювання інформаційного простору для виявлення інформаційних загроз, а також проведення досліджень у окремих галузях моніторингу,

як, наприклад, розвідка на основі відкритих джерел (Open Source Intelligence, OSINT), показує невпинність зростання інтересу до цієї галузі знань.

Проблематику інформаційних воєн, інформаційної безпеки у теорії комунікацій і моніторингу інформаційного простору досліджували вітчизняні вчені роботах [2-14].

Методологічні основи інформаційної безпеки, розгляд інформаційних воєн, як джерела загроз національній безпеці держави і воєнно-теоретичних аспектів інформаційної боротьбі висвітлено у роботах [2–6].

Класифікація і оцінка інформаційних загроз, негативного інформаційно-психологічного впливу, питань виявлення інформаційних операцій на основі аналізу інформаційного простору за результатами моніторингу, досліджено у роботах [7–11].

Питання, пов'язані з удосконаленням системи стратегічних комунікацій для забезпечення інформаційної безпеки України у воєнній сфері, обґрунтуванням умов функціонування системи стратегічних комунікацій, а також фактори, що створюють перешкоди на шляху створення нових комунікативних можливостей досліджено у роботах [12–14].

Аналіз наведених вище джерел надає змістовне уявлення загальнотеоретичних положень щодо підвищення ефективності і вирішення спектру завдань для забезпечення інформаційної безпеки держави у воєнній сфері, ефективного функціонування системи стратегічних комунікацій Міністерства оборони і Збройних Сил України. Проте, запропоновані теоретичні підходи щодо класифікації і оцінки інформаційних загроз за результатами моніторингу інформаційного простору не враховують специфіки їх використання у системі стратегічних комунікацій в умовах широкомасштабного вторгнення і розгорнутої інформаційної війни РФ проти України. Недостатньо уваги приділено класифікації інформаційних загроз національній безпеці України за у системі стратегічних комунікацій, зокрема, виявлення ворожих наративів РФ проти України. Водночас, потребує доопрацювання підходів до визначення успішності реалізації заходів протидії негативному інформаційно-психологічному впливу противника, а також до застосування сучасних інформаційних технологій і передових методів обробки текстового інформаційного контенту для підвищення обґрунтованості та оперативності прийняття рішень.

Мета статті – методичний підхід до моніторингу інформаційного простору для своєчасного виявлення і аналізу інформаційних загроз національній безпеці держави у системі стратегічних комунікацій на основі використання сучасних інформаційних технологій.

Виклад основного матеріалу. Головним завданням стратегічних комунікацій (СК) є скоординоване і належне використання комунікативних можливостей держави: публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави. [1]

Виходячи з вищевикладеного, складовими частинами (елементами) стратегічних комунікацій є: ініціатор комунікацій, адресат або цільова аудиторія, подання інформації та зворотний зв'язок із цільовою аудиторією. Розглядаючи управління стратегічними комунікаціями, як складну систему, можна виділити її наступні складові елементи наведені на схемі (Рис. 1).

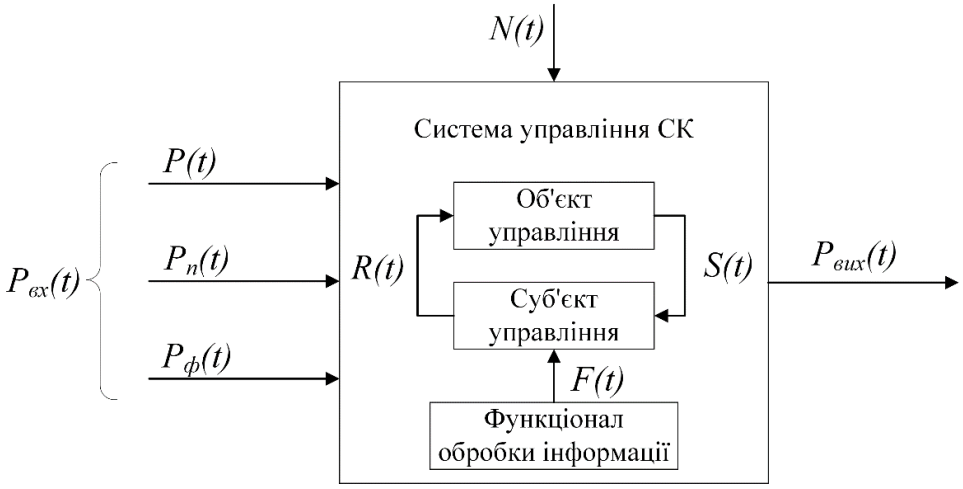


Рис. 1. Узагальнена схема управління стратегічними комунікаціями

Об'єктом управління (ОУ) або об'єктом інформаційного впливу може виступати особистість, певна цільова аудиторія, суспільство або держава.

Цільова аудиторія – це група людей, об'єднаних загальними ознаками. Це можуть бути представники однієї статі, віку, професії, соціального статусу, тощо.

Суб'єкт управління (СУ) – керівний склад Міністерства оборони і Генерального штабу Збройних Сил України, органи військового управління Міністерства оборони і Генерального штабу Збройних Сил України, а також організаційні структури, що здійснюють функції контролю реалізації заходів інформаційної політики.

Інформаційна політика (ІП) – це сукупність основних напрямів і способів діяльності по одержанню, використанню, поширенню та зберіганню інформації [15].

До вхідних інформаційних потоків системи управління СК, які здійснюють вплив на конкретний час – t, можна виокремити наступні:

$P(t)$ – інформаційні ресурси (текстовий, аудіо і відео інформаційний контент), що знаходиться у інформаційному просторі, джерелами якого можуть виступати веб сторінки глобальної мережі Інтернет, соціальні мережі, блогосфера, телебачення і радіо, тощо;

$P_n(t)$ – державна інформаційна політика, інформаційна політика Міністерства оборони України – сукупність інформації, яка визначає концептуальні засади, склад, структуру та стратегію розвитку СУ, у відповідності до імовірних сценаріїв застосування ОУ;

$P_ф(t)$ – фінансові потоки – інформація про рух грошових коштів, направлених на утримання і розвиток системи управління СК (програмно-технічне забезпечення).

Вхідний інформаційний потік на систему управління СК – $P_{вх}(t)$, можна відобразити у вигляді кортежу:

$$P_{вх}(t) = \langle P, P_n, P_ф, t \rangle. \quad (1)$$

Одночасно, на систему управління СК здійснюється негативний (деструктивний) інформаційно-психологічний вплив противника – $N(t)$, у вигляді проведення спеціальних інформаційно-психологічних заходів, акцій, операцій, кампаній, спрямованих на дестабілізацію реалізації заходів державної інформаційної політики.

Негативний інформаційно-психологічний вплив (ІПВ) – це, насамперед, маніпулятивні впливи на особистість, її емоційно-вольову сферу, на групову і масову свідомість, інструмент психологічного тиску з метою явного чи прихованого спонукання індивідуальних і соціальних суб'єктів до дій на шкоду власним інтересам на користь окремих осіб, груп чи організацій, що здійснюють ці впливи [3–6].

Контроль реалізації заходів ІП (ступінь реалізації комунікативних можливостей), а також наслідки негативного ІПВ $N(t)$, де суб'єктом управління аналізується стан ОУ – $S(t)$.

Вплив СУ на ОУ здійснюється шляхом реалізації (коригування) заходів ІП, а також заходів протидії негативному ІПВ – $R(t)$.

Вихідний потік системи управління СК – $P_{вих}(t)$, утворюється за рахунок обробки вхідних та внутрішніх інформаційних потоків функціоналом системи – F:

$$P_{вих}(t) = \langle P_{вх}, N, S, R, F, t \rangle. \quad (2)$$

Під функціоналом – F, системи управління СК, розуміють стійку впорядковану сукупність функцій (операцій) щодо вироблення і реалізації інформаційних, організаційних і розпорядчих заходів СУ, за результатами моніторингу інформаційного простору:

$$F = \{f_1, f_2, \dots, f_\mu\} \mid \mu \in \mathbb{N}, \quad (3)$$

де μ – індекс кількості виконуваних функцій;

$\mathbb{N}$ – натуральний ряд чисел.

Моніторинг інформаційного простору [16] – постійне спостереження за подіями та комунікаційними процесами в інформаційному просторі, збір та класифікація відповідної інформації для її подальшого аналізу, відслідковування основних тенденцій в інформаційному просторі, своєчасного виявлення інформаційних загроз та організації ефективної інформаційно-комунікаційної діяльності.

Функціонал системи управління СК включає:

- функції обліку і контролю поточного стану ОУ – добування, структурування, зберігання, пошук і тиражування даних;
- функції аналізу – аналіз стану реалізації заходів державної ІП, ІП Міністерства оборони України, виявлення в інформаційному просторі негативного ІПВ противника, ступінь його прояву, можливі наслідки, масштабність та джерела поширення;
- функції прогнозування – виявлення тенденцій розвитку державних та ворожих наративів, формування на основі статистичних даних прогнозних моделей щодо визначення

значущості ворожої пропаганди за відповідними наративами: акція, спеціальна операція, кампанія;

- функції планування, організації і регулювання – вироблення інформаційних впливів по утриманню ОУ в існуючому стані або для його переведення в новий стан (вироблення управлінських рішень, заходи, та порядок їх реалізації у загальній системі управління).

Пріоритетними цілями та завданнями системи управління СК становить скоординоване і належне використання комунікативних можливостей, спрямованих на просування цілей держави. В свою чергу, спроможність у досягненні цілей управління на контрольну дату t визначаються показниками ефективності СК – $E(t)$, які входять до області значень відображення вихідного потоку параметрів у вигляді: $f_e: P_{\text{вих}} \to E$, отже:

$$E(t) = f_e(P_{\text{вих}}, t) = f_e(\langle P_{\text{вх}}, N, S, R, F \rangle, t). \quad (4)$$

Показники ефективності управління доцільно розглядати за складовими: організаційної, економічної та соціальної ефективності, які належать множині E, та представляють об'єднання попарно непересічних множин у вигляді:

$$E = \{E_o, E_e, E_s\}, \text{де: } E_o \cap E_e \cap E_s = \emptyset. \quad (5)$$

Організаційна ефективність E_o, включає показники, які визначають спроможність СУ:

- своєчасно реалізовувати комунікативні можливості до конкретної цільової аудиторії через конкретні канали комунікації;
- проводити якісний моніторинг інформаційного простору з метою встановлення стану реалізації заходів ІП, просування державних наративів, їх сприйняття суспільством;
- своєчасно виявляти, класифікувати і типізувати інформаційні загрози і ступінь їх прояву;
- реалізовувати заходи протидії і нейтралізації негативного інформаційного впливу.

Економічна ефективність E_e, включає показники, які визначають: поточні та прогнозні витрати на утримання СУ, а також забезпечення СУ всіма видами для гарантованого виконання функцій і завдань за призначенням.

Соціальна ефективність E_s, характеризується показниками, які відображають:

- посилення єдності, патріотизму, бойового духу, рівня мотивації, ступеню реалізації особистих потреб та вподобань ОУ;
- посилення віри у ОУ в обраному курсі держави, воєнно-політичного керівництва і складових сектору безпеки і оборони;
- формування у ОУ реального бачення перебігу подій зовнішньої і внутрішньої політики держави;
- формування у ОУ національної ідеї, культурних і духовних цінностей; зменшення рівня злочинності і корупційних проявів.

Складові ефективності системи управління СК мають притаманний кожній групі набір показників для їх розрахунку.

Наприклад, реалізація заходів протидії і нейтралізації негативного ІПВ противника за конкретною темою (наратив або складова частина наративу) (Табл. 1), що входить до групи показників організаційної ефективності приймає наступний вигляд:

$$E_{o_{ij}}(t) = N_{\text{н}_{ij}}(t) / N_{\text{в}_{ij}}(t), \quad (6)$$

де $N_{\text{н}_{ij}}$ – кількість нейтралізованих інформаційних загроз;

$N_{\text{в}_{ij}}$ – кількість виявлених інформаційних загроз;

i – індекс показника організаційної ефективності, де $i \in I$;

I – множина показників організаційної ефективності;

j – індекс теми, за яким класифіковано інформаційну загрозу, де $j \in J$;

J – множина тем;

t – контрольна дата.

Кожна тема, наведена у Табл. 1, на конкретний момент часу t може набирати свою гостроту, в залежності від цілей проведення інформаційної акції (операції) противника. Зазначене спостерігається за кількістю повідомлень по кожній темі, кількістю залучених до цього каналів розповсюдження інформації, тональності і інформаційного забарвлення повідомлень. Отже, окрема тема на момент часу t – матиме відповідний ваговий коефіцієнт, який визначається методом експертного оцінювання.

З цією метою, проводиться опитування групи з K експертів, де кожен залучений ε-*й* експерт, на основі особистої думки, виставляє чисельне значення рангу для кожної j-*ї* теми на момент часу t. Найбільш важливій темі виставляється 1-*й* ранг, найменш важливій – значення рангу дорівнюватиме J. Таким чином, кожним ε-*м* експертом упорядковується важливість тем присвоєним значенням відповідного рангу.

Таблиця 1

Приклад класифікації текстового контенту з ознаками негативного ІПВ за темами

Назва кейса (процесу)	Назва теми
ДІЇ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ УКРАЇНИ	Інформаційна політика Офісу Президента України
	Порушення свободи слова в Україні
	Залежність України від Західних країн
	Внутрішні протиріччя органів державної влади
	Корупція, махінації в органах державної влади
ІНФОРМАЦІЙНА ПОЛІТИКА ЗАХІДНИХ КРАЇН	Західні країни використовують Україну в своїх інтересах
	Західні країни "втомилися" від війни в Україні
	Західні режисери війни в Україні
	Скорочення військової, фінансової, гуманітарної допомоги Україні
КРИЗА В УКРАЇНІ	Енергетичний сектор
	Обстріли і руйнування цивільної і промислової інфраструктури
	Демографічна криза (внутрішньо-переміщені особи, виїзд з України)
	Екологічні проблеми
	Економічна криза
ПРОБЛЕМИ ЗБРОЙНИХ СИЛ УКРАЇНИ	Великі втрати особового складу в ЗС України
	Нехватка боєприпасів. Великі втрати озброєння і військової техніки
	Мобілізація через великі втрати особового складу
	Українська влада посилає бійців на смерть
	Невдалий контрнаступ ЗС України
	Некомпетентність, неправомірні дії (бездіяльність), тяжка хвороба (поранення) керівних посадових осіб Міністерства оборони і ЗС України
ПЕРЕГОВОРНИЙ ПРОЦЕС	Переговорний процес з Західними країнами і міжнародними організаціями
	Переговори з РФ не відбудуться. Небажання української влади вести переговори з РФ.
	Намагання РФ залучити Україну до переговорів для найшвидшого закінчення війни
ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА РОСІЙСЬКОЇ ФЕДЕРАЦІЇ	Успіхи збройних сил РФ у "СВО"
	Залякування населення України тактичною ядерною зброєю, ударами крилатих і балістичних ракет по енергетичній інфраструктурі, центрах прийняття рішень, тощо
	Плани збройних сил РФ по захопленню території України, країн Європи, застосування ядерної зброї по центрах прийняття рішень Великобританії і США
	Велич і бойовий потенціал збройних сил РФ ("другої армії Світу")

Враховуючи, що між присвоєним кожній темі рангом і важливістю теми існує лінійна залежність, для подальших розрахунків вагових коефіцієнтів, необхідно провести процедуру масштабування, із визначенням коефіцієнта важливості *j-ї* теми, наданої *ε-м* експертом [17, 18]:

$$V_{j\varepsilon}(t) = 1 - \frac{R_{j\varepsilon}(t)-1}{J}, \quad (7)$$

де ε – індекс експерта, де $\varepsilon \in K$;

$R_{j\varepsilon}(t)$ – ранг *j-ї* теми, виставлений *-м* експертом, на момент часу *t*, де $R_{j\varepsilon} \in \mathbb{N}$;

$V_{j\varepsilon}(t)$ – коефіцієнт важливості *j-ї* теми, на момент часу *t*, на основі експертної думки *ε-го* експерта, де $V_{j\varepsilon}(t) = \overrightarrow{0,1}$;

$\mathbb{N}$ – натуральний ряд чисел.

В результаті проведеної процедури масштабування, формується матриця коефіцієнтів важливості розмірністю $j \times \varepsilon$, отриманої на основі експертної думки *ε-го* експерта, для кожної *j-ї* теми, на момент часу *t*.

Для приведення отриманих абсолютних значень показників у безрозмірне значення без втрати їх вагомості, проводиться процедура нормування. Дана процедура необхідна для оцінки зваженості кожної *j-ї* теми серед множини тем J.

Нормування матриці коефіцієнтів важливості здійснюється наступним чином:

$$\varphi_{j\varepsilon}(t) = \frac{V_{j\varepsilon}(t)}{\sum_{j=1}^{J} V_{j\varepsilon}(t)}, \quad (8)$$

де $\varphi_{j\varepsilon}(t)$ – нормоване значення *j-ї* теми, на момент часу *t*, на основі експертної думки *-го* експерта.

В результаті проведеної процедури, формується матриця нормованих значень показників розмірністю $j \times \varepsilon$, де $\sum_{j=1}^{J} \varphi_{j\varepsilon}(t) = 1$.

Вагові коефіцієнти кожної *j-ї* теми на момент часу (t) становитимуть:

$$\varphi_j(t) = \frac{1}{K}\sum_{\varepsilon=1}^{K} \varphi_{j\varepsilon}(t), \quad (9)$$

де $\varphi_j(t)$ – ваговий коефіцієнт j-*ї* теми.

Отже, загальне значення i-*го* показника організаційної ефективності для всієї множини тем J, на конкретний час t, прийматиме вигляд:

$$E_{o_i}(t) = \prod_{j=1}^{J} E_{o_{ij}}{}^{\varphi_j}(t). \quad (10)$$

Аналогічним шляхом розраховуються вагові коефіцієнти для кожного показника організаційної ефективності, де загальне значення показників організаційної ефективності $E_o(t)$ прийматиме вигляд:

$$E_o(t) = \prod_{i=1}^{I} E_{o_i}{}^{\eta_i}(t) \times 100\%, \quad (11)$$

де η_i – ваговий коефіцієнт i-*го* показника організаційної ефективності E_{o_i}.

Результати управління вважаються позитивними при підвищенні показника організаційної ефективності, де:

$$E_o^*(t_\delta) > E_o(t_{\delta-1}) \mid \delta \in \mathbb{N},$$

де δ - індекс кількості циклів управління;

$\mathbb{N}$ - натуральний ряд чисел.

Розрахунки ефективності реалізації заходів протидії і нейтралізації негативного ІПВ противника, за наведеним вище прикладом були апробовані у табличному процесорі MS Excel. В якості вхідних даних, було використано значення присвоєних рангів десяти актуальним темам, оцінених шістьма експертами, а також кількість виявлених і нейтралізованих інформаційних загроз по кожній конкретній темі на момент часу *t*.

Ознаки негативного ІПВ виявляються на основі аналізу контенту інформації, отриманої шляхом моніторингу інформаційного простору, який здійснюється за певними етапами:

1) підготовчий;
2) добування даних;
3) класифікація і типізація даних;
4) аналіз даних;
5) прийняття рішень.

На Рис. 2 висвітлено структурно-логічну схему моніторингу інформаційного простору, з метою виявлення негативного ІПВ та адекватного реагування на загрози.

На *першому* етапі, визначається цілі і завдання, які повинен вирішити моніторинг. При цьому враховується охоплення (масштабність) виконання завдань: географічні, соціальні, політичні, на які цільові аудиторії слід зосереджувати увагу, тощо. Визначаються обмеження досліджень (тематика досліджень) і обираються перелік інформаційних ресурсів, які підлягатимуть моніторингу: веб-сторінки, Telegram, Facebook, Instagram, Twitter, тощо. Отже, всі ключові особливості і завдання, які виконувались за аналізом попереднього моніторингу, можуть уточнятись для проведення наступного. Підставою для цього можуть слугувати нові ключові події в Україні і світі, посилення негативного ІПВ противника по окремим темам, поява нових ворожих наративів, тощо.

На *другому* етапі, визначаються правила обробки даних. Визначаються шляхи отримання даних з інформаційних ресурсів, наприклад, яка саме технологія парсингу даних, наприклад, web scraping, web crawling, буде використовуватись і яким чином її налаштовувати під кожен окремий інформаційний ресурс. Також, визначаються способи структуризації даних: у текстових файлах, пласких таблицях, датафреймах, реляційних або нереляційних базах даних. Як правило, структурована інформація розміщується у реляційних базах даних, яка містить основні типові поля: дата і час повідомлення, заголовок, автор повідомлення, текст повідомлення, хештеги, посилання на джерело повідомлення, посилання (лінки) на інші джерела, які присутні в основному тексті повідомлення, тощо. Таким чином, структуризація даних надає первинні представлення (кількісні показники) для проведення подальшого аналізу.

Парсинг –це метод швидкої обробки інформації, точніше синтаксичний аналіз даних, розміщених на веб-сторінках. Він використовується для оперативного опрацювання великої кількості текстів, цифр, зображень [19].

Третій етап є найбільш відповідальним, в ході якого виконується класифікація (відповідність) повідомлень за певними темами (Табл. 1), а також встановлюється тональність і семантика текстів повідомлень (типізація даних).

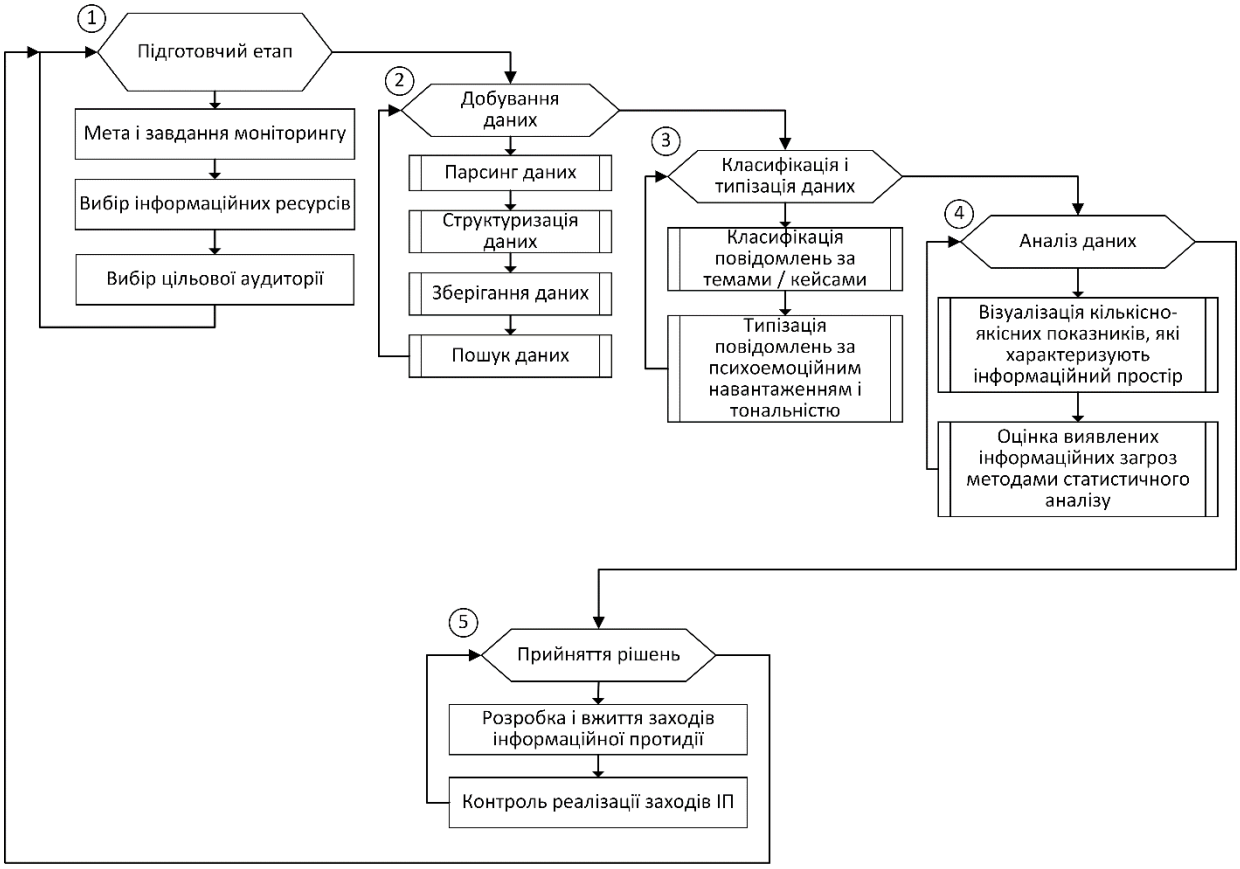


Рис. 2. Структурно-логічна схема моніторингу інформаційного простору

На сьогоднішній день, дана процедура виконується шляхом використання технологій машинного навчання (Machine Learning). Існує багато сервісів, призначених для аналізу семантики та структури текстового контенту, наприклад Gensim, FastText, SpaCy, TextRazor, Aylien та інші, які можуть бути використані для аналізу соціальних мереж, веб-сторінок та інших джерел інформації. Зазначене здійснюється на основі глибокого аналізу текстових даних для вилучення зв'язків, типізованих залежностей між словами та синонімами, створюючи своєрідні контекстно-семантичні конструкції. Наприклад, функції тематичного моделювання Gensim, на основі байєсівської моделі тематичного моделювання (Hierarchical Dirichlet Process), здійснює автоматизоване розпізнавання тематики текстового контенту. А на основі ймовірнісної моделі тематичного моделювання (Latent Dirichlet Allocation) – визначити кількість тематик та їх ключові слова. Інструментарій для збору та аналізу даних з соціальних мереж, які дозволяють відслідковувати обговорення певної теми в соціальних мережах. Такі інструменти, як: Social Mention, Netvibes та Hootsuite, можуть використовуватися для моніторингу репутації, виявлення інформаційних загроз та аналізу тенденцій у громадській думці. Наведені вище бібліотеки побудовані на базі платформи з відкритим кодом NLTK (Natural Language Toolkit) [20] для роботи з природними мовами. Вона надає доступ до корпусів текстів та лексичних ресурсів, а також має набір інструментів для обробки текстів, що допомагає вирішувати завдання, пов'язані з обробкою природних мов.

Якість отриманих показників значно підвищується, якщо для їх верифікації залучати широке кола експертів. Проте, зазначена процедура є найбільш трудомісткою і потребує витрати більшої кількості часу.

На *четвертому* етапі, проводиться аналіз кількісно-якісних показників, отриманих на попередніх двох етапах. З цією метою розробляються інтерактивні інформаційні панелі, на яких здійснюється їх візуалізація у вигляді графіків, діаграм, зведених таблиць, тощо. Зазначене, значно спрощує сприйняття інформації, дозволяє проводити аналіз тональності повідомлень і їх кількості за визначеними темами, проводити часові зрізи інформації.

Додатково досліджуються зміни інформаційного простору за визначений період на основі побудови статистичних моделей регресійного та кореляційного аналізу. Це дає змогу швидко оцінити критичні зони розвитку певної теми в ретроспективі, ступінь активності певних джерел. Кореляція при цьому можлива між

втратами противника, санкціями проти РФ, негативним інформаційним впливом противника тощо.

На основі отриманих статистичних моделей, формуються прогнозні аналітичні моделі можливого розвитку зміни інформаційного простору. Виявляються тренди розвитку певних тем та їх майбутня поведінка (за період до 30 діб). Використовуючи методи дослідження функції за ретроспективний період, існує можливість визначити початок інформаційних акцій (операцій) противника. Це сприяє підтримці прийняття обґрунтованих рішень і раціональному розподілу ресурсів залучених до протидії негативному ІПВ.

На *п'ятому* етапі, проводиться розробка і вжиття заходів щодо протидії негативному ІПВ, уточнення цілей і завдань моніторингу і контроль стану реалізації ІП.

Кожен описаний вище етап включає виконання ряду процедур, деталізувати які в рамках написання однієї статті неможливо. Водночас, систематизація знань про методи і способи, які використовують при моніторингу інформаційного простору, вказують на певну послідовність дій щодо комплексного уявлення цього процесу.

Висновок. Розглянуті у статті питання визначення показників ефективності системи управління стратегічними комунікаціями і запропонований методичний підхід щодо своєчасного виявлення, аналізу та оцінювання інформаційних загроз національній безпеці України, надає комплексне представлення щодо інформаційного супроводження діяльності уряду, державних інституцій і публічних осіб через комунікативні можливості держави. Інформаційна обізнаність цільової аудиторії про правильно обраний курс держави, державну інформаційну політику, інформаційну політику МО України забезпечує більш стійке просування стратегічних цілей держави. Ці функції набирають особливої актуальності під час розгорнутої проти України широкомасштабної збройної агресії, де крім проведення активних бойових дій, розгорнуто інформаційну війну. Зазначене вимагає застосування дієвих механізмів щодо виявлення, аналізу і прогнозування інформаційних загроз у інформаційному просторі.

Запропонований підхід щодо класифікації інформаційних загроз національній безпеці України у системи стратегічних комунікацій, визначення ефективності реалізації заходів інформаційної протидії і удосконалення процесу виявлення негативного ІПВ, може стати концептом для розроблення інформаційно-аналітичної системи моніторингу інформаційного простору, з подальшим її використанням в інформаційно-аналітичному забезпеченні органів військового управління, підрозділів Збройних Сил і Міністерства оборони України, на які покладаються зазначені функції. Це дозволить підвищити обґрунтованість рішень і ефективність вжиття заходів для протидії негативному інформаційно-психологічному впливу противника.

Подальші дослідження доцільно зосередити на деталізації етапів моніторингу інформаційного простору, методах на основі штучного інтелекту, які використовуються для класифікації і оцінювання інформаційних загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про затвердження Концепції стратегічних комунікацій Міністерства оборони України та Збройних Сил України. Наказ Міністерства оборони України від 22.11.2017 № 612. – URL: https://zakon.rada.gov.ua/rada/show/v0612322-17#Text (дата звернення: 21.08.2023).
2. Почепцов Г. Г. Информационные войны. Киев: Ваклер, 2000. – 576 с.
3. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти): Монографія. Київ: НАОУ, 2003. – 320 с.
4. Жарков Я. М., Дзюба М. Т., Замаруєва І. В. Інформаційна безпека особистості, суспільства, держави: Підручник. Київ: Видавничо-поліграфічний центр "Київський університет", 2008. – 274 с.
5. Курбан О. В. Інформаційні війни у соціальних он-лайн-мережах : Монографія. Київ : ун-т ім. Б. Грінченка, 2017. – 392 с.
6. Інформаційна безпека держави у воєнній сфері: Навч. посібник / [.О. Кацалап, С.А. Микусь, О.В. Войтко та ін.]. Київ: НУОУ ім. І. Черняховського, 2020. − 304 с.
7. Додонов А.Г. Распознавание информационных операций/ А.Г. Додонов, Д.В. Ландэ, В.В. Цыганок, О.В. Андрейчук, С.В. Каденко, А.Н. Грайворонская. Київ : ООО «Инжиниринг», 2017. – 282 с.
8. Сніцаренко П. М., Кацалап В. О. Методика оцінювання психологічного впливу. *Сучасні інформаційні технології у сфері безпеки та оборони.* Київ : НУОУ ім. І. Черняховського, 2018. № 3(33). – С. 113–118.
9. Сніцаренко П. М. Грицюк В. В. Аналіз стану виявлення та оцінювання негативного інформаційного впливу на особовий склад Збройних Сил України в системі протидії такому впливу. *Збірник наукових праць Центру воєнно-стратегічних досліджень.* Київ : НУОУ ім. І. Черняховського, 2019. № 2(66). – С. 52–61.
10. Кацалап В. О., Кирпічніков О. Д., Саунін Р. Д. Методичний підхід до оцінювання рівня інформаційно-психологічного впливу противника в інтересах інформаційної операції .Збройних Сил України. *Збірник наукових праць Центру воєнно-*

стратегічних досліджень. Київ : НУОУ ім. І. Черняховського, 2022. № 3(76). – С. 24–31.
11. Федоренко Р. М. Контент-моніторинг інформаційного простору як чинник забезпечення інформаційної безпеки держави у воєнній сфері. *Сучасний захист інформації.* Київ, 2015. № 2. – С. 21–25.
12. Вербицька А. М., Савченко В. А., Дзюба Т. М., Кацалап В. О. Система стратегічних комунікацій Міністерства оборони України та Збройних Сил України. *Наука і оборона.* Київ, 2017. №1. – С. 9–12.
13. Войтко О., Кацалап В., Бабій Ю. Обґрунтування елементів комунікативної моделі системи стратегічних комунікацій Сил оборони. *Збірник наукових праць Національної академії Державної прикордонної служби України.* Хмельницький, 2019. № 2(80). – С. 61–72.
14. Войтко О. В. Оцінювання ефективності функціонування системи стратегічних комунікацій Міністерства оборони та Збройних Сил України. *Системи управління, навігації та зв'язку*. Київ, 2018. № 3(49). – С. 97–99.
15. Інформаційна політика. – URL: http://volynstandart.com.ua/information-policy/ (дата звернення: 21.08.2023).
16. Доктрина зі стратегічних комунікацій, затверджена Головнокомандувачем Збройних Сил України від 12.10.2020 року № ВКП 10-00(49).01. Київ, 2020. 32 с.
17. Загорка О. М., Мосов С. П., Сбітнєв А. І., Стужук П. І. Елементи дослідження складних систем військового призначення. Київ : НАОУ, 2005. – 100 с.
18. Денисов А. А., Колесников Д. Н. Теория больших систем управления: Учеб. пособие для вузов. Ленинград: Энергоиздат, 1982. – 288 с.
19. Що таке парсинг і для чого використовується? . – URL: https://dalistrategies.com/ua/shho-take-parsing-i-dlya-chogo-vikoristovuietsya/ (дата звернення: 21.08.2023).
20. Documentation. Natural Language Toolkit. – URL : https://www.nltk.org/ (дата звернення: 14.08.2023).

Стаття надійшла до редакційної колегії 25.08.2023

An approach to the identification and analysis of information threats to the national security of the state in strategic communications management systems

Annotation

The current conditions are characterized by the stage of formation of the global information space, the revolutionary feature of which is the use of information as a means of achieving the desired goal. This is achieved thanks to the activation of information technology development processes to meet communication needs in the political, economic, military, social and other spheres of human activity. At the same time, the information openness of the world objectively contributes to information attacks (operations), which in this context characterizes information as a weapon. Presentation of information in a manner necessary for the benefit of the organizer of information propaganda allows forming the necessary point of view, public opinion, course of complementary logical thoughts, etc. in society.

In the conditions of a full-scale war with the Russian Federation, the issue of information security - one of the key factors of Ukraine's national security - becomes especially relevant. Since 2014, Ukraine has faced an unprecedented volume of information attacks aimed at undermining Ukraine's statehood, democracy, sovereignty, and territorial integrity. The most significant types of information threats to Ukraine, which are spread by Russian state media, pro-Russian agents of influence through social networks and other communication channels, are information distortion in the form of open propaganda, information terrorism and disinformation. The purpose of the mentioned is the formation of a negative image, highlighting in the world perception of Ukraine as an unstable, corrupt and incapable of reforms state. The negative informational and psychological influence is aimed at the psychological demoralization of the Ukrainian population, the strengthening of socio-political polarization, and the deepening of discord between Ukraine and its Western partners.

The existing challenges and threats to the national security of Ukraine necessitate the implementation of a complex of effective measures for the implementation of state strategic narratives, as well as timely informational countermeasures, neutralization of destructive informational influence, and increased informational security of the individual, society, and the state.

In view of the above, the resolution of this issue directly depends on the effectiveness of monitoring the information space and the application of modern approaches to the detection and analysis of information threats in the strategic communications system of the Ministry of Defense and the Armed Forces of Ukraine.

Keywords: strategic communications, information space, narrative, information threat, negative information impact, information impact analysis

УДК 355.45.02 DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/44-49

Фролов В.С., кандидат військових наук, старший науковий співробітник (0000-0003-0105-6439)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Рекомендації щодо побудови, удосконалення та організації застосування системи Територіальної оборони України

Резюме. У статті викладені основні висновки загального аналізу функціонування системи територіальної оборони України в умовах ведення широкомасштабної війни з Російською Федерацією та рекомендації щодо її удосконалення.

Ключові слова: територіальна оборона; національний спротив; Збройні Сили України; широкомасштабна війна**.**

Постановка проблеми. Вторгнення військових угруповань збройних сил Російської Федерації (РФ) в Україну на 4-х стратегічних напрямках одночасно, започаткувало розв'язання широкомасштабної війни з Україною із застосуванням більшої частини угруповань Сухопутних військ, повітряно-космічних сил Росії, угруповання військ Повітрянодесантних військ та Чорноморського флоту у повному складі.

Воєнно-політичне керівництво Росії основними цілями війни визначило "денаціоналізацію" та "демілітаризацію" України, що на практиці означає повну ліквідацію держави та української нації як такої. Протистояти півторамільйонній армії, яка має повну перевагу у повітрі, на морі, в чисельності та озброєнні сухопутних військ та стримати противника тільки угрупованнями регулярних військ (сил) Збройних Сил України, значна частина яких була задіяна у бойових діях в Донецькій та Луганській областях, на перший погляд було не можливо. Провідні військові експерти, воєнно-політичне керівництво НАТО та провідних держав світу не були впевнені, що Сили оборони України у взаємодії з силами територіальної оборони (ТрО), розгромлять угруповання російських військ у боях за оборону Києва, на інших оперативних напрямках та зірвуть досягнення воєнно-політичних цілей, так званої, "спеціальної операції" РФ.

Оцінка результатів організації оборони та ведення бойових дій на усій території України потребує окремого вивчення та глибокого аналізу. Досвід стратегічної оборони держави в умовах раптового нападу "другої" армії світу – чисельність тільки Повітрянодесантних військ і сил спеціального призначення збройних сил РФ перевищують чисельність угруповання усіх Збройних Сил України – увійде в історію світового воєнного мистецтва.

Аналіз останніх досліджень і публікацій. Досвід протистояння широкомасштабному вторгненню агресора на територію України показав, що без чіткої організації системи ТрО протистояти противнику, який має повну військову перевагу, надзвичайно складно.

Основи організації територіальної оборони розроблялись ще з 90-х років – з часів набуття незалежності України та розбудови Збройних Сил України.

Доктор технічних наук, академік Володимир Горбулін, один із провідних фахівців у сфері оборони, у своїй книзі "Як перемогти Росію у війні майбутнього" [1] розглядає територіальну оборону, *по-перше,* як "кадровий резервуар", який у будь-який час здатний швидко поповнити мобілізаційний компонент сил оборони. *По-друге*, автор визначає, що в організації територіальної оборони необхідно передбачити виключну роль місцевих державних адміністрацій у підготовці та забезпечення військ ТрО. *По-третє*, матеріально-технічним забезпеченням індивідуальними засобами ведення бойових дій та автомобілями військові частини ТрО забезпечуються у мирний час. Іншими вогневими засобами, такими, як: ПТРК, мінометами, ПЗРК тощо комплектуються Збройні Сили України за мірою нарощування загроз військової агресії противника. *По-четверте*, система підготовки військ ТрО планується та поводиться із залученням максимально можливої кількості громадян. На думку автора, до завдань ТрО можуть належати ведення бою в населених пунктах, охорона важливих об'єктів, пошук і ліквідація ДРГ, агентури противника тощо.

Перший заступник голови Комітету Верховної Ради України з питань національної

безпеки, оборони та розвідки М. Забродський (2019–2023), розглядає систему територіальної оборони як “Рух опору”, який має бути розгорнутий у тилових районах держави як другий (*резервний*) комплект СВ ЗС України. [2]

Значний вклад у розроблення сучасної системи територіальної оборони внесла група РНБОУ під керівництвом першого заступника секретаря Ради Національної Безпеки і оборони України доктора військових наук М. В. Коваля На основі аналізу проблем існуючої системи ТрО України колектив військових фахівців розробив проєкт Закону України “Про основи національного спротиву”, який прийнято Верховною Радою України та введено в дію.

Разом з тим у дослідженнях авторів, не розглядаються проблеми відповідності варіантів організації Територіальної оборони Конституції та законам України, не розроблялись пропозиції щодо узгодження між собою вимог законів України. Авторами не повністю враховувались конституційні функції центральних органів виконавчої влади, органів місцевого самоуправління, правоохоронних органів, Командування ЗС України та Силами оборони України.

Мета статті – за результатами вивчення нормативно-правових актів України, змісту основних завдань Територіальної оборони та аналізу їх виконання під час російсько-української війни розробити рекомендації щодо удосконалення побудови, організації застосування та управління системою ТрО України.

Виклад основного матеріалу. Досвід ведення широкомасштабної війни з РФ, детальний аналіз практичного функціонування системи територіальної оборони підтверджують необхідність коригування деяких положень з метою удосконалення її побудови та управління.

Насамперед, доцільно чітко визначити мету створення системи ТрО, принципи її побудови та організації ТрО, яких на сьогодні існує декілька варіантів.

По-перше, сили ТрО входять до складу Збройних сил держави як окремий рід військ. Планування застосуванням та управління силами ТрО здійснюється Генеральним штабом на усій території держави без прив’язки їх до зон та районів відповідальності.

По-друге, система ТрО створюється з метою посилення спроможностей збройних сил за рахунок застосування особового складу, який не підлягає мобілізації для збройних сил, залучення цивільних підприємств та техніки, які можуть використовуватись для організації комендантської служби, ремонту (відновлення) військової техніки і озброєння, утримання та захисту бар’єрних дільниць маршрутів, мостів, тунелів тощо. Всебічне забезпечення (крім озброєння та спеціального спорядження) здійснюється за рахунок бюджетів та резервів органів місцевого самоврядування. Часто такий варіант ТрО називають *тотальною* обороною держави.

У деяких державах – членах НАТО, наприклад в Німеччині, територіальна оборона розглядається як система додаткових заходів держави для посилення потенціалу збройних сил оборони. Частини ТрО комплектуються добровольцями, які не можуть використовуватись для поповнення регулярних військ і відносяться до підрозділів Об’єднаних сил забезпечення ЗС. Доброволець не може служити в регулярних частинах збройних сил. Аналогічні системи застосовуються у польських Силах територіальної оборони, Китайської Народної Республіки, на Тайвані тощо [3, 4].

В Україні перший і другий варіанти ТрО об’єднані: Сили ТрО складають окремий рід військ ЗС України, разом з тим, основні завдання ТрО виконуються частинами зон та районів ТрО під загальним керівництвом Командувача Сил ТрО ЗС України.

Відповідно до ст. 1 (пункт15) Закону України “Про основи національного спротиву” [5] Сили територіальної оборони Збройних Сил України – окремий рід сил Збройних Сил України, на який покладається організація, підготовка та виконання завдань територіальної оборони.

Відповідно до вимог ст. 1 (пункт16) цього ж закону, *територіальна оборона* – це система загальнодержавних, воєнних і спеціальних заходів, що здійснюються у мирний час та в особливий період з метою протидії воєнним загрозам, а також для надання допомоги у захисті населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій.

З метою визначення сумісності завдань ТрО та ЗС України проведемо порівняльний аналіз визначених законами України їх функцій та завдань, що показано у Табл. 1.

Законом України “Про основи національного спротиву” визначено, що сили ТрО беруть участь у виконанні 10 завдань, які

зорганізуються та проводяться правоохоронними органами України.

Законом України "Про Збройні Сили України" [6] визначні основні функції ЗС України. Включення Сил ТрО до складу ЗС України, як роду військ, передбачає їх повне підпорядкування Командуванню ЗС України та утримання їх за рахунок бюджету держави, виділеного для ЗС України.

Разом з тим до складу Сил оборони входять військові підрозділи правоохоронних органів, які відповідно до Закону України "Про основи національного спротиву", організують виконання 10 із 13 завдань ТрО, а вся система територіальної оборони лише "бере участь у виконанні цих завдань".

Таблиця 1

Порівняння функцій Збройних Сил України та завдань Територіальної оборони

Основні завдання Територіальної оборони		**Основні функції Збройних Сил України**	
1.	Своєчасне реагування та вжиття заходів щодо оборони території та захисту населення на визначеній місцевості (***ЗСУ, МВС***)	**1.**	ЗСУ забезпечують стримування збройної агресії проти України та відсіч їй, охорону повітряного простору держави та підводного простору у межах територіального моря України у випадках, визначених законом, беруть участь у заходах, спрямованих на боротьбу з тероризмом
2.	Участь у посиленні охорони та захисті державного кордону; МВС (***ДПС, НГУ***)		
3.	Участь у захисті населення, територій від надзвичайних ситуацій, ліквідації наслідків ведення бойових дій (***МВС, ДСНС***)		
4.	Участь у підготовці громадян до національного Спротиву (***МВС, ЗСУ***)	**2.**	З'єднання і військові частини ЗСУ відповідно до закону можуть залучатися до здійснення заходів правового режиму воєнного і надзвичайного стану, заходів із відсічі і стримування збройної агресії РФ у Донецькій та Луганській областях, організації та підтримання дій руху опору, проведення військових інформаційно-психологічних операцій, боротьби з тероризмом, заходів щодо захисту життя громадян та об'єктів державної власності за межами України
5.	Участь у забезпеченні умов для функціонування органів державної влади та військового управління (***МВС, НГУ***)		
6.	Участь в охороні важливих об'єктів, визначених КМУ, та об'єктів, виведення з ладу яких становлять загрозу для життєдіяльності населення (***МВС, НГУ***)		
7.	Забезпечення оперативного розгортання військ (сил) або їх перегрупування (***ЗСУ***)		
8.	Участь у здійсненні заходів щодо заборони або обмеження руху транспортних засобів в межах зон ведення бойових дій (***МВС, Нац. Поліція***)	**3.**	Органи військового управління розвідки та військові частини розвідки ЗСУ, ССО відповідно до закону можуть залучатися до розвідувальних завдань
9.	Участь у забезпеченні заходів громадської безпеки і порядку в населених пунктах (***МВС, Нац. поліція, НГУ***)		
10.	Участь у запровадженні та здійсненні заходів правового режиму воєнного стану (***МВС, Нац. поліція, НГУ***)	**4.**	Органи військового управління забезпечують додержання вимог Конституції України стосовно того, що ЗСУ не можуть бути використані для обмеження прав і свобод громадян або з метою повалення конституційного ладу, усунення органів державної влади чи перешкоджання їх діяльності
11.	Участь у боротьбі з ДРГ, збройними формуваннями противника та або антидержавними збройними формуваннями (***МВС, НГУ, СБУ***)		
12.	Участь в інформаційних заходах, спрямованих на підвищення рівня обороноздатності держави та на протидію інформаційним операціям агресора (***МВС, СБУ***)	**5.**	З'єднання, військові частини і військовослужбовці, у тому числі чергові сили, ЗСУ в мирний час та в особливий період мають право застосовувати і використовувати зброю та бойову техніку відповідно до Конституції та Законів України
13.	Участь у наданні населенню правових послуг у визначеному законами порядку (***МВС, Прокуратура***)		

ЗС України беруть участь в організації виконання таких завдань ТрО:

своєчасне реагування та вжиття заходів щодо оборони території та захисту населення на визначеній місцевості;

забезпечення оперативного розгортання військ (сил) або їх перегрупування;

участь у підготовці громадян до національного спротиву.

Отже, якщо Сили ТрО підпорядковуються Командуванню ЗС України, як рід військ, то вони застосовуються рішенням Командування ЗС України на усій території держави, а зони та райони ТрО залишаються без засобів виконання визначених їм завдань.

Водночас, якщо планування та організацію ТрО покласти на ЗС України, то до функцій ЗС України необхідно додати 10 завдань ТрО та підпорядкувати ЗС України правоохоронні органи держави, які, відповідно до їх призначення, безпосередньо організують виконання завдань ТрО.

Функціонування Сил ТрО, як роду військ ЗС України, регламентується Конституцією, усіма законами України, підзаконними актами та доктринальними документами, відповідно до яких організована діяльність ЗС України.

З проведеного аналізу випливає, що Сили ТрО можуть (повинні) оперативно підпорядковуватись військовому Командуванню ЗС України у межах кордонів ведення військових операцій. На територіях, де військові операції не проводяться, Сили ТрО виконують завдання відповідно до їх призначення.

Сили ТрО можуть (повинні) підпорядковуватись командуванню військових з'єднань, які здійснюють управління угрупованнями військ (сил) ЗС України у межах зон ведення військових операцій. На територіях, де військові операції не проводяться, сили ТрО виконують завдання відповідно до їх призначення.

Досвід ведення війни підтверджує недоцільність призначення керівниками зон та районів ТрО голів місцевих військових державних адміністрацій.

Відповідно до Закону України "Про основи національної безпеки" ст.1 (п.14) [7] керівником зони територіальної оборони є Голова Ради міністрів Автономної Республіки Крим, голова обласної державної адміністрації, голова Київської, Севастопольської міської державної адміністрації (керівник відповідної військово-цивільної або військової адміністрації у разі її утворення).

Разом з тим, Конституція України (ст.118) [8] чітко визначає, що голови місцевих державних адміністрацій під час виконання своїх повноважень відповідальні перед Президентом України і Кабінетом Міністрів України, підзвітні та підконтрольні органам виконавчої влади вищого рівня, тому місцеві державні адміністрації не можуть підпорядкуватись будь-яким іншим інституціям держави, окрім тих, що визначені Конституцією України.

Зокрема, відповідно до ст. 27 Закону України "Про місцеві державні адміністрації" [9], місцева державна адміністрація в галузі оборонної роботи:

забезпечує виконання законодавства про територіальну оборону, військовий обов'язок посадовими особами і громадянами, підприємствами, установами і організаціями;

здійснює заходи, пов'язані з територіальною обороною, мобілізаційною підготовкою, цивільним захистом на відповідній території.

Отже місцева державна адміністрація *не керує* територіальною обороною, а *забезпечує* виконання заходів у межах визначених Конституцією та законодавством повноважень.

З метою чіткого розподілу функцій управління територіальною обороною, розглянемо визначення "оборона держави".

Закон України "Про оборону України" ст. 1 [10] визначає, що *оборона України* – система політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших *заходів держави* щодо підготовки до збройного захисту та її захист у разі збройної агресії або збройного конфлікту.

Відповідно до ст. 113 Конституції України "*Кабінет Міністрів України* є вищим органом у системі органів виконавчої влади, на який разом із місцевими державними адміністраціями покладається функція виконання заходів держави щодо підготовки до оборони та відсічі агресії".

Отже, в області (районі) з метою більш ефективного державного управління створюються штаби оборони областей (районів), які виконують функції планування, координації та забезпечення управління системою політичних, економічних, соціальних, інформаційних, правових, організаційних та інших заходів держави.

Досвід ведення війни з РФ підтверджує необхідність створення штабів оборони для організації виконання таких основних завдань оборони, як:

евакуація (приймання та розміщення) цивільного населення, підприємств;

вирішення соціальних проблем та медичного забезпечення населення;

участь у забезпеченні сил ТрО, розміщених на території областей і районів тощо.

Штаб оборони області (району) очолює перший заступник голови державної адміністрації. Для протидії воєнним діям противника на території областей і районів створюється система ТрО, основними завданнями якої можуть бути:

своєчасне реагування та вжиття заходів щодо оборони території та захисту населення на визначеній місцевості;

посилення охорони та захисту визначених ділянок державного кордону і військової інфраструктури;

утримання маршрутів та забезпечення пересування і маневру військових угруповань Сил оборони;

виконання бойових завдань у зонах ведення військових операцій за планами військового командування;

підтримання правового режиму воєнного стану на території зон (районів) ТрО у взаємодії з органами місцевого самоуправління;

планування та організація підготовки громадян до національного спротиву;

управління оповіщенням, збором та подачею мобілізаційних ресурсів для Сил оборони в особливий період.

Отже, такий підхід до визначення завдань ТрО, дасть змогу більш чітко визначити роль і місце ТрО в загальній системі оборони держави та усунути наявні протиріччя між вимогами законодавчих актів України щодо оборони держави. Успішність організації діяльності державних адміністрацій, органів місцевого самоуправління та системи ТрО залежить від рівня щільної взаємодії систем державного і військового управління в областях (районах). Змішування систем державного та військового управління призводить до дезорганізації як державного, так і військового управління в областях і зонах ТрО.

Вертикаль системи управління наведена на рис. 1.

Рис. 1. Вертикаль системи управління

У зоні (районі) ТрО штаб ТрО на формується на основі штабу бригади (батальйону) ТрО. У регіональному командуванні безпосереднє управління системою ТрО здійснює заступник командувача регіонального командування з ТрО через підпорядковане йому управління ТрО, якому підпорядковані обласні територіальні центри комплектування.

Слід підкреслити, що структура і чисельність військ ТрО не залежить від чисельності населення в зоні (районі). Основною структурною одиницею системи ТрО є батальйон ТрО. Кількість батальйонів у бригаді ТрО залежить від обсягу завдань ТрО у конкретній зоні ТрО. Більш детальний аналіз та варіанти формування системи ТрО можуть бути продовжені у наступних публікаціях.

Аналіз ведення ТрО в період російсько-української війни, відповідність організації ТрО Конституції та нормативно-правовим актам України дає змогу дійти висновку, що організаційна структура та система управління територіальною обороною України потребує подальшого коригування та реформування деяких її складових. Закони України та інші нормативно-правові акти потребують уточнення та коригування їх вимог між собою.

Висновок. Система ТрО одна із найважливіших складових заходів держави щодо підготовки її до збройного захисту від збройної агресії противника. До її формування залучаються державні структури із системою державного управління та військові структури держави із системою військового управління.

Державне та військове управління суттєво відрізняються одне від одного та не можуть переплітатись, особливо на оперативному та тактичному рівнях. Раціональне функціонування двох систем управління можливе лише у разі чіткого узгодження двох систем управління на рівні Конституції та законів держави.

Подальші дослідження доцільно зосередити на таких аспектах:

виявлення протиріч у вимогах законів України щодо організації ТрО та розроблення рекомендацій щодо їх усунення;

розроблення пропозицій щодо створення оперативно-тактичного рівня управління системою ТрО та коригування усієї вертикалі керівництва системою ТрО держави;

розроблення рекомендацій щодо створення переліку підзаконних актів, на основі яких може бути організована професійна підготовка персоналу для всебічного забезпечення та військового управління системою та силами ТрО.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Горбулін В. Як перемогти Росію у війні майбутнього. 2021. 248 с.
2. Бадрак Д. Територіальна оборона як асиметричний захист від російської загрози. Яка ситуація в Україні? // День. 2020. № 88. URL:

https://day.kyiv.ua/article/podrobytsi/marsh-na-mistsi (дата звернення: 02.08.2023).
3. Раубо Я. Берлін рухається до територіальної оборони. URL: https://www.ukrmilitary.com/2021/04/deutsch-terdef.html (дата звернення: 02.08.2023).
4. Корчагін С. Концепція створення Військ територіальної оборони Респу-0бліки Польща. URL: https://mil.in.ua/uk/articles/kontseptsiya-stvorennya-vijsk-terytorialnoyi-oborony-respubliky-polshha/ (дата звернення: 03.08.2023).
5. Про основи національного спротиву : Закон України // Відомості Верховної Ради. 2021. № 41. Ст. 339.
6. Про Збройні Сили України : Закон України // Відомості Верховної Ради. 1992. № 39. Ст. 108.
7. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII.
8. Конституція України : офіц. текст. : із змінами.
9. Про місцеві державні адміністрації : Закон України // Відомості Верховної Ради України. 1999. № 20-22. Ст. 190.
10. Про оборону України : Закон України // Відомості Верховної Ради України. 1992. № 9. Ст. 106.

Стаття надійшла до редакційної колегії 04.09.2023

Recommendations for building, improving and organizing the use of the Territorial Defense System of Ukraine

Annotation

The invasion of Ukraine by military groups of the Armed Forces of the Russian Federation (RF) on 4 strategic directions simultaneously launched a large-scale war with Ukraine using most of the groups of the Army, the Russian Aerospace Forces, the Airborne Forces and the Black Sea Fleet in its entirety. Leading military experts, the military and political leadership of NATO and the world's leading states were not sure that the Ukrainian Defense Forces, in cooperation with the Territorial Defense Forces (TDF), would defeat the Russian troops in the battles for the defense of Kyiv and other operational areas and disrupt the achievement of the military and political goals of the so-called "special operation" of the Russian Federation. Assessment of the results of the organization of defense and combat operations throughout Ukraine requires a separate study and in-depth analysis.

The purpose of the article is to develop recommendations for improving the construction, organization of use and management of the Territorial Defense system of Ukraine based on the results of studying the legal acts of Ukraine, the content of the main tasks of the Territorial Defense and analysis of their implementation during the Russian-Ukrainian war.

The purpose of creating a TDF system, the principles of its construction and organization of TDF are determined. Firstly, the logistics forces are part of the Armed Forces of the State as a separate branch of the military. Secondly, the logistics system is created to strengthen the capabilities of the armed forces through the use of personnel who are not subject to mobilization for the armed forces.

The analysis of the conduct of territorial defense during the Russian-Ukrainian war, the compliance of the organization of territorial defense with the Constitution and legal acts of Ukraine allows us to conclude that the organizational structure and management system of Ukraine's territorial defense needs further adjustment and reform of some of its components. The laws of Ukraine and other legal acts need to be clarified and their requirements adjusted to each other.

Keywords: territorial defense; national resistance; Armed Forces of Ukraine; large-scale war.

УДК: 355.4 (477) DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/50-55

Остапчук О. П., кандидат історичних наук[1] (0000-0002-0991-0778)
Вавілова Н. В., кандидат історичних наук [2] (0000-0002-0939-7820)

[1] – Науково-дослідний центр гуманітарних проблем Збройних Сил України, Київ;
[2] – Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Міжнародна підтримка України у травні 2022 року

Резюме. У статті розкрито особливості міжнародної підтримки України під час російсько-української війни у травні 2022 року та її вплив на воєнно-політичну обстановку. Висвітлено роль і місце провідних країн та організацій демократичного світу в підтримці України.

Ключові слова: міжнародна підтримка країни; російсько-українська війна; військово-технічна допомога; воєнно-політична обстановка.

Постановка проблеми. Вивчення нового етапу в сучасній російсько-українській війні є надзвичайно актуальною проблемою новітньої історії України у глобальному вимірі. Її наукове опрацювання активно триває і потребує копітких міждисциплінарних досліджень, у яких на цей час беруть участь учені-історики, фахівці зі споріднених чи суміжних галузей знань.

Життєво важливою для України у війні з Росією є міжнародна підтримка – політична, військово-технічна, економічна та гуманітарна. У травні 2022 року демократичний світ визначився з метою війни: завдати Росії такої поразки, внаслідок якої вона протягом 10 років після завершення бойових дій буде не спроможна загрожувати Україні та країнам Заходу. З травня 2022 року міжнародна підтримка України була спрямована на формування у Сил оборони України необхідних спроможностей для досягнення цієї мети.

На сьогодні є актуальними та потребують всебічного дослідження особливості надання та здобута результативність міжнародної підтримки України під час російсько-української війни.

Ці обставини визначають пов'язаність із важливими науковими завданнями:

розкриття особливостей і виявлення значущості міжнародної підтримки України у травні 2022 року;

з'ясування ролі та місця провідних країн та організацій демократичного світу у підтримці України у травні 2022 року.

Аналіз останніх досліджень і публікацій. Поглиблений інтерес до сучасної історії потребує скрупульозного підходу до ретельного відбору й сумлінного аналізу історичних джерел, у тому числі в режимі реального часу з електронних ресурсів. Уже оприлюднено низку аналітичних, інформаційно-аналітичних та науково-публіцистиних праць [1–3].

У зазначених роботах висвітлені такі аспекти щодо міжнародної підтримки України у травні 2022 року:

в аналітичному огляді "Інформаційна оборона: аналітичний огляд ситуації за минулий тиждень (15–22 травня 2022 року) [1] зазначено, що основними напрямами міжнародної підтримки України були: політична підтримка, військова допомога та фінансова підтримка. В огляді розглянуто особливості міжнародної підтримки України за обмежений в часі період та не охоплює весь травень 2022 року;

в інформаційно-аналітичних матеріалах "Воєнно-політична обстановка в ході російсько-української війни (лютий-червень 2022 року)" [2] висвітлено роль і місце найбільш активних міжнародних партнерів які підтримували України в травні, як великихи міжнародних організацій так і окремих країн. У роботі детально не розкриваються особливості і не виявляється значущість міжнародної підтримки України у травні 2022 року.

у воєнно-історичному описі російсько-української війни за травень 2022 року [3] проведено опис основних подій які характеризували воєнно-політичну обстановку в травні 2022 року. Аналітична реконструкція особливостей процесу розгортання, перебігу і впливу міжнародної підтримки України на воєнно-політичну обстановку не висвітлювалися в описі.

Водночас на сьогодні опрелюднено обмаль наукових праць, в яких всебічно досліджено роль і місце провідних країн та організацій демократичного світу у підтримці України, її особливості і вплив на воєнно-політичну обстановку під час російсько-української війни, зокрема у травні 2022 року.

Мета статті полягає в аналітичній реконструкції особливостей процесу розгортання, перебігу і впливу міжнародної підтримки України на воєнно-політичну обстановку під час російсько-української війни у травні 2022 року на основі наведених фактів.

Виклад основного матеріалу. Вирішення завдань дослідження потребує використання таких методів:

аналітичного – для поділу цілого на складові, виокремлення в міжнародній підтримці України процесів розгортання і перебігу міжнародної підтримки, кола її учасників;

синтезу – для визначення особливостей міжнародної підтримки України, добору необхідного фактичного матеріалу;

індукції – для переходу у процесі пізнання від окремого знання до загального, від накопичених у процесі пізнання достовірних окремих фактів до встановлення певних закономірностей історичного процесу, формулювання законів, які сприяють пізнанню окремих явищ, фактів, процесів;

дедукції – для полегшення і прискорення процесу історичного дослідження, забезпечення відображення міжнародної підтримки Україні у травні 2022 року на тлі російсько-української війни.

Україні наодинці було важко подолати противника, адже її військові перспективи на фронті залежали не лише від рівня професійності Командування Збройних Сил України, героїчних зусиль українських військових, а й від обсягів і темпів надання західної військово-технічної допомоги.

Протягом травня 2022 року у важких оборонних боях українські військові продовжували виснажувати противника, знищувати його бронетехніку і позбавляти його війська наступального потенціалу. Одночасне постачання сучасної важкої наступальної техніки та озброєння західних партнерів дало змогу створити для ЗС України вирішальну перевагу на полі бою [1].

Україну активно підтримували Польща, Естонія, Литва, Латвія, Чехія, Словаччина, що безумовно, розуміли якщо Україна зазнає поразки наступними цілями російського агресора будуть саме їх території і люди, тому їх воєнно-політичні інтереси збігалися з воєнно-політичним інтересом України.

22 травня 2022 року Президент України Володимир Зеленський у Києві провів зустріч з Президентом Республіки Польща Анджеєм Дудою, під час якої наголосив, що Польща демонструє історичний рівень підтримки України, наших Збройних Сил та громадян, змушених залишити власні домівки через російське вторгнення [4].

Системну підтримку Україні продовжували надавати і глобальні центри сили: США, Велика Британія, ЄС та НАТО. Так, США пройшли шлях від недопущення поразки України у війні до необхідності забезпечення поразки Росії. Водночас політична еліта США категорично не зацікавлена в територіальній дезінтеграції Росії та розповзанні ядерної зброї по різних регіональних домівках.

Міністр оборони США Ллойд Остін чітко визначив мету війни: завдати Росії такої поразки, внаслідок якої вона протягом 10 років після завершення бойових дій не могтиме загрожувати Україні та країнам Заходу. У США склалася двопартійна та громадська підтримка українського опору російській агресії. За різними опитуваннями близно 70 % американців підтримують надання зброї та іншої допомоги Україні, тому 9 травня 2022 року був підписаний закон про ленд-ліз, 21 травня – закон про військову допомогу у розмірі $40 млрд, проведено координаційні зустрічі у форматі “Рамштайн” [1, 4–8].

В адміністрації Джо Байдена різні групи впливу намагалися обмежити обсяг військової допомоги Україні, наголошуючи на стримуванні ескалації конфлікту та недопущенні застосування тактичної ядерної зброї Росією. Представники частини американської політичної еліти активно намагалися обмежити постачання озброєння в Україну. Промовистим прикладом наслідків такої політики стала певна затримка із постачанням реактивних систем залпового вогню.

Велика Британія на чолі з прем’єр-міністром Борисом Джонсоном, маючи менший арсенал зброї та можливостей для її виробництва, ніж США, перетворилася на своєрідну ідеологиню розвитку військово-технічної допомоги та активну захисницю України. Саме Велика Британія виступила з пропозицією створити новий військово-політичний союз, до складу якого увійшли б Україна, Велика Британія, Польща, можливо, країни Балтії і Туреччина. Про імовірність створення такого союзу як альтернативи ЄС заявляв британський прем’єр Борис Джонсон [9].

Європейський Союз як політико-економічне об’єднання у своїх діях був

згуртованим та займав жорстку антиросійську позицію. Так, 9 травня 2022 року ЄС прийняв від України заповнену другу частину опитувальника, необхідного для отримання статусу кандидата на членство в ЄС. Питання, що порушило єдність, було пов'язане із запровадженням нафтогазового ембарго. Через протидію Угорщини ЄС довго не міг запровадити шостий пакет санкцій проти Росії [10].

У травні в Європі тривала дискусія між групами прихильників політики традиційного умиротворення агресора та жорсткої лінії відновлення повноцінної дії євроатлантичного союзу, що зовсім по-різному детермінує для європейської еліти обриси майбутнього миру та архітектуру його безпеки.

На відміну від більшості інших країн, "стара" Європа у травні ще не змогла остаточно визначитися зі своєю політикою у російсько-українській війні та демонструвала постійні коливання в "генеральній лінії". Особливо помітно це було в Німеччині, коли за особистим розпорядженням німецького канцлера Олафа Шольца зі списку озброєння для передання Україні викреслювали дуже потрібне Україні важке озброєння, а пізніше Шольц заявляв, що Україна має сама, без зовнішнього тиску прийняти рішення про сутність її мирних домовленостей із Росією [11].

Тривала дискусія і навколо членства України у Євросоюзі. Так, 9 травня 2022 року президент Франції Емманюель Макрон зробив украй несподівану заяву: "Потрібні кілька років, а може й десятиліття, щоб Україну прийняли в Європейський Союз". Таку позицію фактично підтримав канцлер Німеччини Олаф Шольц, який наголосив, що заявка України на приєднання до Європейського Союзу не може бути швидко розглянута, незважаючи на масштабне вторгнення Росії [12].

Міністр закордонних справ України Дмитро Кулеба критично відреагував на заяву Олафа Шольца, заявивши про "другосортне ставлення" до Києва з боку деяких країн ЄС. Зрозуміло, що в умовах російсько-української війни наша країна розраховує на підтримку країн-партнерів, а будь-яке штучне зволікання із наданням їй статусу кандидата на вступ до ЄС буде вкрай негативно та болісно сприйматимуть як суспільство, так і політична еліта країни [13].

Президент України Володимир Зеленський наголосив, що, на його думку, ті, хто пропонують Україні такі "альтернативи"– свідомо або несвідомо просувають інтереси Росії [14].

19 травня 2022 року стало відомо, що уряд Італії підготував та передав ООН поетапний план миру для України. Перший етап передбачав припинення вогню та відведення військ від лінії фронту під наглядом ООН. На другому етапі мало відбутися приєднання України до ЄС за умови і гарантій її неприєднання до НАТО. На третьому етапі було заплановано підписання двосторонньої угоди між Україною та Росією щодо Криму та Донбасу, при цьому "спірні території", як їх названо в італійському плані, мали набути повної автономності, але за збереження суверенітету України. На останньому етапі було передбачено підготовку нового багатостороннього договору про мир та безпеку в Європі, який би забезпечував контроль за озброєннями [15].

Зазначені пропозиції не мали підтримки в Україні. Якщо на початку широкомасштабної війни цілком прийнятним було відведення російських військ на лінію розмежування та кордони станом на 23 лютого 2022 року, то після перемоги під Києвом влада і суспільство побачили перспективу завершення війни у відновленні територіальної цілісності країни, повному її звільненні, включно із Кримом. Будь-які інші пропозиції влада України і суспільство розглядали як зраду, не надаваючи їм суспільної легітимації.

Зрозуміло, що країни "старої" Європи не стали беззастережно підтримувати агресора, бо їх не зрозуміли б виборці, що загрожувало їх безхмарному політичному майбутньому. Робити заяви про цілковиту підтримку України та негайне надання їй озброєння, кваліфікувати масове вбивство українського цивільного населення в Бучі як геноцид українського народу і тут же закликати "не заганяти Путіна у глухий кут", "надати можливість зберегти йому обличчя", пропонувати Україні мирну угоду із територіальними поступками, – саме так вибудовували свою політику країни "старої" Європи.

Невизначеність у власній політиці окремих європейських країн, нерозуміння основних засад майбутнього світу, ролі України у майбутній світовій безпековій архітектоніці впливали на європейські перспективи нашої держави.

У межаxx міжнародної коаліції на підтримку України 23 травня 2022 року відбулася друга зустріч міністрів оборони

різних країн у форматі Контактної групи з питань оборони України "Рамштайн". У цій зустрічі взяли участь понад 40 країн, до яких доєдналися Австрія, Боснія і Герцеговина, Колумбія, Ірландія та Косово, що підтверджувало розширення підтримки України у світі. Можливо, не всі країни, які приєдналися до коаліції, мали великі спроможності в оборонній сфері, однак політичний ефект розширення був безсумнівним [16].

Генеральний секретар НАТО Єнс Столтенберг 24 травня 2022 року описав війну Росії проти України як чинник, що ламає світовий порядок, і наголосив, що роль НАТО полягає в запобіганні поширенню конфлікту, а також наданні допомоги Україні. Він чітко дав зрозуміти, що альянс оборонятиме "кожен дюйм території НАТО", на що вказувало велике підсилення колективного стримування й оборони Альянсу, включно з утримуванням 100 тис. особового складу на високому рівні боєготовності [17].

Підтримуючи Україну, країни НАТО також значно посилили свою оборону у східній частині Альянсу. Залучено понад 40 тис. військовослужбовців під безпосереднім командуванням НАТО, сотні кораблів і літаків, а також 8 багатонаціональних бойових груп від Балтійського до Чорного морів [18].

Рішення Фінляндії і Швеції стати членами НАТО демонструє, що "європейська безпека не буде залежати від диктату насильства і залякування", – зазначив Єнс Столтенберг, а також наголосив, що розширення НАТО стало історичним успіхом та поширює свободу і демократію в Європі [19].

27–30 травня 2022 року у столиці Литовської Республіки Вільнюсі відбулося засідання весняної сесії Парламентської Асамблеї НАТО. За його результатами ухвалено декларацію, в якій закликано:

уряди країн – членів Альянсу виконати конкретні подальші кроки, спрямовані на просування України до членства в НАТО та посилення протидії Росії;

наростити постачання важкого озброєння, зокрема систем ППО, ПРО, протикорабельних систем та артилерії, посилити обмін розвідувальною інформацією;

масштабувати руйнівні санкції проти російських олігархів, посадових осіб та їхніх сімей, а також пропагандистів і державних ЗМІ;

поступово відмовитися від імпорту вугілля, газу, нафти та урану з Росії;

вислати з країн НАТО російських дипломатів, які ведуть ворожу діяльність;

створити спеціальний Міжнародний трибунал для розслідування, кримінального переслідування та притягнення до відповідальності винних в агресії проти України.

Акт також передбачав в оновленій Стратегічній концепції НАТО чітко визначити ревізіонізм та агресивні дії Росії як безпосередні та головні загрози євроатлантичній безпеці та посилити східний фланг Альянсу. Це стосувалося й істотного зміцнення військового потенціалу НАТО, зокрема ядерного, для стримування Росії [18].

Туреччина намагалася зайняти нейтральну позицію між Україною та Росією, що дало їй змогу вести активну політику щодо організації можливого переговорного процесу між сторонами та врегулювання виниклих гуманітарних криз.

Продовженням такої політики 30 травня 2022 року стала телефонна розмова Президента Туреччини Реджепа Тайїпа Ердогана з президентом Росії Путіним про можливість проведення у Стамбулі зустріч між представниками Росії, України й ООН.

Як зазначав Президент України Володимир Зеленський, "продовжився діалог з Президентом Туреччини Реджепом Тайїпом Ердоганом, під час якого обговорено створені агресором загрози продовольчій безпеці, шляхи розблокування портів та взаємодію в безпековій сфері. Президенти були одностайні в питанні необхідності відновлення миру [20].

У травні 2022 року в рамках міжнародної підтримки України країнами-партнерами як індивідуально, так і спільно у форматі "Рамштайн-2" були прийняті рішення, які мали значний вплив на хід війни. Так, 9 травня 2022 року президентом США Джо Байденом був підписаний закон про ленд-ліз, 21 травня – закон про військову допомогу у розмірі $40 млрд. Отже, 23 травня 2022 року в форматі "Рамштайн-2" вперше набула певної конкретики воєнно-технічна допомога. Партнери зобов'язалися наростити поставки артилерії 155-мм калібру та посилити берегову оборону України. Зокрема, Італія, Греція, Норвегія та Польща оголосили про передачу критично необхідних артсистем та боєприпасів, також пускових установок Mk 141 для ракет Harpoon і ракет від Данії. Чехія анонсувала передачу гелікоптерів вогневої підтримки, танків та ракетних систем. Такі рішення дали змогу оперативно та системно надавати необхідну воєнно-технічну допомогу

Україні. Ця допомога додала Силам оборони України більшої стійкості в обороні та було започатковане формування наступальних спроможностей. Наявність таких систем як Harpoon посилело берегову оборону України, примусило Росію відмовитися від морської десантної операції, а в поєднанні з артилерією 155-мм калібру пришвидшело звільнення острова Зміїнного.

Висновки. Результати дослідження особливостей міжнародної підтримки України під час російсько-української війни у травні 2022 року, вплив цієї підтримки на воєнно-політичну обстановку, роль і місце провідних країн та організацій демократичного світу в підтримці України, показують:

1. Системну підтримку Україні продовжували надавати глобальні центри сили – США, Велика Британія, ЄС і НАТО. Так, США пройшли довгий шлях від недопущення поразки України у війні до необхідності забезпечення поразки Росії, Велика Британія стала ідеологинею розвитку військово-технічної допомоги та активною захисницею України, Європейський Союз як політико-економічне утворення був згуртованим і дотримувався жорсткої антиросійської позиції.

2. До міжнародної коаліції, що підтримувала Україну, приєдналися ще п’ять країн демократичного світу і зберігалася тенденція до її розширення.

3. Країни “старої” Європи у травні ще не змогли остаточно визначитися зі своєю політикою у російсько-українській війні та демонстрували постійні коливання “генеральної лінії”. Невизначеність у власній політиці окремих європейських країн, нерозуміння основних засад майбутнього світу і ролі України у майбутній світовій безпековій архітектоніці могли впливати на європейські перспективи нашої держави.

4. Міжнародна підтримка та успіхи України на полі бою дали підстави українському суспільству та воєнно-політичному керівництву розширити масштаб воєнно-політичних інтересів: відновити територіальну цілісність України у міжнародно визнаних кордонах.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Жданов І. Інформаційна оборона: аналітичний огляд ситуації за минулий тиждень (15-22 травня 2022 року) // Інтерфакс-Україна. 2022. URL:https://interfax.com.ua/news/blog/834077.html (дата звернення: 01.06.2023).
2. Воєнно-політична обстановка в ході російсько-української війни (лютий – червень 2022 року) : збірник інформаційно-аналітичних матеріалів / О. Остапчук, В. Топальський, С. Черевичний та ін. Київ : НДЦ ГП ЗС України, 2022. 107 с.
3. Воєнно-історичний опис російсько-української війни (травень 2022 року) / В. Залужний, Є. Мойсюк, С. Шаптала та ін. Київ : МО України, ГШ ЗС України, 2022. 130 с.
4. Зеленський В. Виступ Президента України: офіційне інтернет-представництво. 2022. URL: https://www.president.gov.ua/news/ polsha-sogodni-demonstruye-istorichnij-riven-pidtrimki-ukray-75269 (дата звернення: 02.06.2023).
5. Вже 73 % американців підтримують поставки зброї в Україну // Українська правда. 2022. URL: https://www.pravda.com.ua/news/2022/04/27/7342343/ (дата звернення: 02.06.2023).
6. Калініченко О. Як війна в Україні змінює громадську думку в Європі та світі // LB.ua. 2022. URL: https://lb.ua/world/2022/05/11/516489_yak_viyna_ukraini_zminyuie_gromadsku.html (дата звернення: 03.06.2023).
7. Байден підписав законопроєкт про виділення 40 млрд доларів Україні // Слово і Діло. 2022. URL: https://www.slovoidilo.ua/2022/05/21/novyna/ekonomika/bajden-pidpysav-zakonoproyekt-pro-vydilennya-40-mlrd-dolariv-ukrayini (дата звернення: 03.06.2023).
8. Волошин Н. Історичний закон про ленд-ліз для України: що це нам дасть // АрміяInform. 2022. URL: https://armyinform.com.ua/2022/05/10/istorychnyj-zakon-pro-lend-liz-dlya-ukra yiny-shho-cze-nam-dast/ (дата звернення: 03.06.2023).
9. Джонсон запропонував Україні створити альтернативний ЄС альянс // Слово і Діло. 2022. URL: https://www.slovoidilo.ua/2022/05/27/novyna/polityka/dzhonson-zaproponuvav-ukrayini-stvoryty-alternatyvnyj-yes-alyans-corriere-della-sera (дата звернення: 04.06.2023).
10. Капустинська К. Україна передала ЄС повністю заповнений опитувальник про членство // Obozrevatel. 2022. URL: https://news.obozrevatel.com/ukr/economics/analytics-and-forecasts/ukraina-povnistyu-zapovnila-opituvalnik-pro-chlenstvo-v-es-zelenskij (дата звернення: 04.06.2023).
11. Уряд Німеччини викреслив все важке озброєння зі списку військової допомоги Україні // Європейська правда. 2022. URL: https://www.eurointegration.com.ua/news/2022/04/21/7138148/ (дата звернення: 05.06.2023).
12. Ліскович М. 9 травня 2022 року Президент Франції Емманюель Макрон зробив украй несподівану заяву // Укрінформ. 2022. URL: https://www.ukrinform.ua/rubric-ato/3480367-zamist-clenstva-v-es-makron-proponue-dla-ukraini-sos-nezrozumile.html (дата звернення: 05.06.2023).
13. Канцлер Німеччини: короткого шляху до ЄС для України немає // Радіо Свобода. 2022. URL: https://www.radiosvoboda.org/a/news-scholz-ukraina-eu/31858192.html (дата звернення: 05.06.2023).

14. Warspeeches: Росія без підтримки ОДКБ та вже “не проти” розширення НАТО // Українська правда. 2022. URL: https://www.pravda.com.ua/columns/2022/05/23/7347999/ (дата звернення: 05.06.2023).
15. Італія запропонувала ООН мирний план для України // UAZMI. 2022. URL: https://uazmi.org/news/post/0557374fb65f10322c0e0a71883ca244 (дата звернення: 06.06.2023).
16. Рамштайн-2. Міністр оборони США провів віртуальну зустріч щодо України з представниками понад 40 країн // Espreso.tv. 2022. URL: https://espreso.tv/ramshtayn-2-ministr-oboroni-ssha-proviv-virtualnu-zustrich-shchodo-ukraini-z-predstavnikami-ponad-40-krain (дата звернення: 05.06.2023).
17. ПА НАТО ухвалила декларацію про підтримку євроатлантичного курсу України та протидію російській агресії // Верховна Рада України. 2022. URL: https://www.rada.gov.ua/news/Top-novyna/223370.html (дата звернення: 05.06.2023).
18. Брайлян Є., Мосьондз О. Наша підтримка триватиме стільки, скільки буде необхідно, щоб Україна перемогла // АрміяInform. 2022. URL: https://armyinform.com.ua/2022/05/31/nasha-pidtrymka-tryvatyme-stilky-skilky-bude-neobhidno-shhob-ukrayina-peremogla-vineta-klyajne/ (дата звернення: 06.06.2023).
19. Генеральний секретар НАТО в Давосі: “Воля важливіша за вільну торгівлю” // Організація північноатлантичного договору. 2022. URL: https://www.nato.int/cps/uk/natohq/news_195753 (дата звернення: 06.06.2023).
20. Зеленський обговорив з Ердоганом продовольчу безпеку та відновлення миру // Укрінформ. 2022. URL: https://www.ukrinform.ua/rubric-polytics/3496064-zelenskij-obgovoriv-z-erdoganom-prodovolcu-bezpeku-ta-vidnovlenna-miru.html (дата звернення: 06.06.2023).

Стаття надійшла до редакційної колегії 03.07.2023

International support for Ukraine in May 2022

Annotation

In May 2022, the democratic world decided on the goal of the Russian-Ukrainian war: to defeat Russia so that it would not be able to threaten Ukraine and Western countries for 10 years after the end of hostilities. Since May 2022, international support for Ukraine has been aimed at building the necessary capabilities of the Ukrainian Defense Forces to achieve this goal. Today, the specifics of the provision and the effectiveness of international support for Ukraine during the Russian-Ukrainian war are relevant and require a comprehensive study.

The article reveals the peculiarities of international support for Ukraine during the Russian-Ukrainian war in May 2022 and its impact on the military-political situation. The role and place of the leading countries and organizations of the democratic world in supporting Ukraine are highlighted.

Systematic support for Ukraine was provided by global centers of power - the United States, the United Kingdom, the EU, and NATO. Thus, the United States has come a long way from preventing Ukraine's defeat in the war to the need to ensure Russia's defeat, the United Kingdom has become an ideologue of military and technical assistance and an active defender of Ukraine, the European Union as a political and economic entity was united and maintained a tough anti-Russian stance.

In May, the countries of the "old" Europe had not yet been able to finalize their policy toward the Russian-Ukrainian war and demonstrated constant fluctuations in the “general line”. Uncertainty in the policies of individual European countries, lack of understanding of the basic principles of the future world and Ukraine's role in the future global security architecture could affect the European prospects of our country.

International support and Ukraine's successes on the battlefield gave the Ukrainian society and military and political leadership grounds to expand the scope of military and political interests: to restore Ukraine’s territorial integrity within internationally recognized borders.

Keywords: international support for the country; Russian-Ukrainian war; military-technical assistance; military-political situation.

УДК 004.8, 354 DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/56-67

Свєшніков С. В., кандидат технічних наук, старший науковий співробітник (0000-0001-8924-4535)
Бочарніков В. П., доктор технічних наук, професор (0000-0003-4398-5551)
Мазуренко І. М., доктор філософії (0000-0003-2233-7563)
Ковальчук П. А. (0000-0002-9434-444X)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Оцінка ефективності та ризиків виконання оборонних проєктів на основі нечітко-інтегрального числення

Резюме. У статті запропоновано кількісні показники ефективності та ризиків виконання оборонних проєктів, а також алгоритми їх розрахунку на основі поєднання методів сітьового планування та нечітко-інтегрального числення. Це має забезпечити вимірність оборонних проєктів.

Ключові слова: оборонне планування; оборонний проєкт; ефективність; ризик; сітьове планування; нечітко-інтегральне числення.

Постановка проблеми. Російсько-українська війна наочно показала актуальність розвитку Збройних Сил (ЗС) України на основі оборонного планування, яке має забезпечити якісну підготовку ЗС України до оборони України і сприяти їх ефективному застосуванню у подальшому. У кризових фінансово-економічних умовах держава переходить до вирішення завдань оборонного планування на основі проєктного менеджменту, який забезпечує орієнтацію заходів оборонної політики на кінцевий, функціонально завершений результат і, завдяки цьому, сприяє більш ефективному використанню державних коштів. Відповідно до наказу Міністерства оборони України “Про організацію виконання окремих заходів оборонної реформи на середньострокову перспективу” [1], реалізація оборонної реформи має здійснюватися у формі проєктів. Такими проєктами можуть бути “Огляд спроможностей сил оборони” (який розпочато у 2022 році), або Матриця спроможностей сил оборони, яка визначена Стратегічним оборонним бюлетенем України (затверджено Указом Президента України від 17 вересня 2021 року № 473/2021), або майже будь-яке завдання, яке визначено цим бюлетенем.

Життєвий цикл проєкту складається з проєктування, виконання і оцінювання результату.

Зі свого боку, головним завданням проєктного менеджменту є забезпечення вимірності [2] на всьому життєвому циклі проєкту, який складається з етапів планування і виконання плану, під час яких планується і створюється результат. Без цього неможливо говорити ані про кінцеву ефективність виконання проєкту, ані про можливість контролю процесу його виконання.

На сьогодні найбільш поширеним залишається опис проєкту засобами теорії сітьового планування [3], відповідно до якої проєкт представляється у вигляді сукупності окремих робіт. Кожна робота потребує певного часу для виконання і взаємопов’язана з іншими роботами за послідовністю, яка визначається логікою утворення часткових елементів загального результату і логікою витрачання ресурсів. Нині відомо кілька способів формального опису проєкту, наприклад, діаграми Ганта [4], дводольні орієнтовані графи [5] та інші. Головною науковою задачею в рамках теорії сітьового планування є розрахунок загальної тривалості проєкту та резервів часу окремих робіт. Час виконання проєкту розглядається одним з головних підсумовуючих показників.

Залежно від особливостей проєкту, окремі роботи можуть додатково навантажуватись іншими величинами. Тоді розподіл у часі їх суми по роботах або значення іншої функції (що є композицією цих величин, не обов’язково адитивною) може розглядатись як відповідний показник ефективності виконання проєкту. Наприклад, якщо роботи навантажити певними ресурсами і визначити швидкість їх витрачання в ході роботи, можна розглядати графік потрібного забезпечення ресурсами та його характеристики. Інший приклад: навантаження окремих робіт обсягом створюваного результату дає змогу розглянути графік утворення результату проєкту. Варіюючи часом початку робіт (у межах припустимих обмежень), можна

сформулювати оптимізаційну задачу, наприклад, забезпечення рівномірності ресурсних витрат. Подібні задачі є дуже важливими для ефективного проєктного менеджменту.

На практиці будь-який проєкт пов'язаний з великою долею невизначеності, оскільки етап планування проєкту стосується процесів, виконання яких відбуватиметься у майбутньому, де важко передбачити та врахувати усі можливі фактори, що можуть призвести до відхилень від планів та норм. Невизначеність умов виконання проєкту впливає на його результат і природним чином викликає ризики, оцінювання яких є одним з найважливіших завдань проєктного менеджменту. Такий підхід повністю узгоджується з міжнародним визначенням [6] ризиків в теорії ризик-менеджменту, де ризик розглядається як прояв невизначеності. Зауважимо, що невизначеність породжує не лише ризик втрат, а й можливість придбання певного ефекту у разі позитивного збігу обставин.

Крім того, додаткова невизначеність породжується на етапі виконання проєкту через неадитивні залежності обсягу створюваного результату від часткових результатів, створюваних в рамках окремих робіт. Показник обсягу створюваного результату є невід'ємним елементом системи вимірності оборонних проєктів. У цьому показнику має бути врахована синергія поєднання часткових елементів в загальному результаті і застосування тут адитивних методів неминуче викликатиме систематичну похибку.

Отже, у проєктному менеджменті, який здійснюється в умовах невизначеності, існує проблема формування та вимірювання показників, які мають забезпечити вимірність оборонних проєктів на етапах і планування, і виконання. Вони мають враховувати невизначеність кількісної та якісної природи. Кількісні показники можуть бути розраховані за допомогою визначення параметрів робіт на впорядкованих (як правило, числових) множинах і використання арифметичних операцій з нечіткими операндами. Розрахунок якісних показників має здійснюватись іншими методами, орієнтованими на обробку невпорядкованих множин. В обох випадках невизначеність має бути гармонізована з ризиками. Крім того, в проєктному менеджменті вагомою є задача управління портфелем проєктів.

Як бачимо, повне розкриття проблеми в рамках однієї статті потребує значного обсягу. Тому далі розгляд результатів дослідження здійснюється лише стосовно кількісних показників. Розгляд проблеми в інших контекстах буде здійснено в інших публікаціях.

Аналіз останніх досліджень і публікацій. Однією з базових у сфері сітьового планування та управління проєктами є робота [7], яка внесла свою вагому частку у формування загального тренду і принципів у вирішенні задач проєктного менеджменту.

Однією зі сфер, де методи сітьового планування знайшли широке застосування, є сфера енергетики. Зокрема, в роботі [8] надано огляд моделювання невизначеності в переломленні до предметної області планування роботи розподільчих сіток в енергетиці. Робота [9] пропонує сукупність оптимальних сітьових рішень для забезпечення потреб в електроенергії споживачів, розподілених по географічному району. Критерій оптимальності враховує вимогу використання існуючих розподільчих сіток. Робота [10] пропонує гібридний алгоритм для мінімізації функції вартості капітальних вкладень в енергетичні сітки.

Робота [11] зосереджена на спробі кількісного виразу якісних показників ризиків невизначеної природи під час побудови міських електромереж. Також питанням оцінювання ризиків проєктів присвячена робота [12].

Робота [13] розглядає частковий випадок сітьового планування, коли структура графу, який описує виконання проєкту, невизначена повністю, тобто час окремих робіт визначено лише зі впевненістю або ймовірністю.

У роботі [14] автори роблять спробу використання нечітких множин і нечіткої арифметики в методах сітьового планування, зокрема PERT (Project Evaluation and Review Technique) та CPM (Critical Path Method). Автори використовують неінтерактивне віднімання для розрахунку показників робіт: найбільш раннього часу початку, найбільш пізній припустимий час завершення і час простою, а також критичний шлях для різного рівня впевненості.

Зауважимо, що однією з головних проблем нечіткої арифметики є проблема [15] забезпечення еквівалентності зі стандартною арифметикою. Це так звана проблема "нечіткого нуля і нечіткої одиниці". Різні методи намагаються забезпечити цю

еквівалентність різними шляхами. Наприклад, орієнтовані нечіткі числа забезпечують дотримання аксіоматики стандартних арифметичних операцій, проте для завдання таких чисел необхідна додаткова експертна інформація [16]. Одночасно з цим зберігаються інші проблеми нечіткої арифметики, зокрема проблема збереження форми функції належності при множенні нечітких операндів [17]. У разі використання трикутних функцій належності з'являється проблема втрати інформації [18]. Проте найбільш важливою і важкою проблемою [19, 20] нечіткої арифметики є різке збільшення носія результуючого нечіткого числа у випадку багатократних операцій. Ця проблема призводить до вибухового зростання невизначеності і результату, який неможливо раціонально інтерпретувати для прийняття рішення.

Аналіз відомих підходів свідчить, що розвиток проєктного менеджменту в умовах невизначеності кількісних величин сьогодні рухається шляхом механістичного застосування відомих методів опису і обробки нечітких даних до предметної області управління проєктами. Чіткі дані заміняються нечіткими, звичайна арифметика заміняється нечіткою, але якісно нові підходи, які дозволили б комплексно розглянути проблеми проєктного менеджменту в умовах невизначеності в сучасній літературі відсутні або розвинуті слабко. Зокрема, не розкриті питання оцінювання якості. Слабко розкриті питання оцінювання ризиків.

Отже **мета статті** полягає у визначенні складу кількісних показників і ризиків оборонних проєктів, алгоритмів розрахунку цих показників з урахуванням невизначеності процесу виконання робіт проєкту. Вирішення цієї задачі має забезпечити вимірність процесу виконання оборонних проєктів під час їх планування та виконання.

Виклад основного матеріалу. *Методичний підхід до визначення показників проєктів*. Відповідно до Методичних рекомендацій з управління проєктами в Міністерстві оборони України [21], під час виконання оборонних проєктів мають враховуватись:

час виконання проєкту у цілому;

час завершення проєкту і час початку окремих робіт;

ресурси, які витрачаються в процесі виконання робіт, зокрема людські та грошові;

якість виконання окремих робіт і результату проєкту у цілому;

ризики виконання проєкту;

контрольні точки проєкту, де має контролюватись якість виконання створеної частини результату проєкту.

Усі ці величини і категорії можуть бути поєднані на основі наступної логічної моделі. Крім того, ця модель доповнює склад показників.

Проєкт представляється як сукупність окремих робіт, в яких створюється частка результату проєкту. Роботи залежать одна від одної за логікою створення результату проєкту або вивільнення ресурсів, потрібних для її виконання (якщо один і той же ресурс може бути задіяним для різних робіт, наприклад, команда аналітиків). Тобто робота не може розпочатись, якщо не завершено усі попередні роботи. Кожна робота має певний час виконання та, необов'язково, може мати резерв часу для початку виконання. Змінюючи початок виконання роботи в межах резерву, можна обирати більш кращі (за певним критерієм) умови для забезпечення виконання роботи.

У процесі виконання роботи поступово витрачаються певні ресурси і також поступово створюється результат роботи. Ресурси мають подаватись до місця виконання або перед початком роботи, або в процесі роботи. У будь-якому випадку подача ресурсів має здійснюватися не пізніше моменту їх витрачання. Будь-якому результату притаманна якість, яка за міжнародними стандартами [22] визначається як сукупність властивостей продукції або послуги, які надають їм спроможність задовольнити потреби споживача або замовника. У результаті виконання певних робіт поступово створюються системно значимі елементи (частки) результату проєкту. Моменти закінчення цих робіт розглядаються як контрольні точки проєкту, у яких має оцінюватись обсяг і якість часткових результатів. У загальному випадку моменти закінчення кожної роботи можуть розглядатись як контрольні точки.

Залежність загального результату проєкту від його створюваних елементів не є адитивною функцією, оскільки застосування середньозваженої суми розраховуватиме середній відсоток створення часток результату, але не обсяг власне результату. Як приклад, розглянемо процес створення споживчого результату будівництва будинку. У процесі будівництва результат виникає не поступово, а внаслідок стрибка, який з'являється після облаштування фундаменту,

будівництва стін, даху, встановлення вікон і підключення комунікацій. Після виконання всіх цих процедур за рахунок їх синергії виникає споживчий результат – в будинку можна жити, навіть без внутрішнього ремонту. Більш того, приміщення будинку можна продавати. Подібне створення результату притаманне складним системам з синергетичними ефектами.

Таким чином, для забезпечення вимірності проєкту мають бути розглянуті такі показники, розділені на дві групи:

часові і ресурсні показники:

загальний час виконання проєкту, який визначається часовими показниками виконання окремих робіт;

обсяги ресурсів, потрібних для виконання проєкту, які визначаються обсягами ресурсів для виконання окремих робіт та графіками їх витрачання в рамках цих робіт;

показники створюваного результату:

обсяг створюваного результату проєкту як функція від обсягу часткових результатів, досягнутих в контрольних точках проєкту;

якість створюваного результату проєкту як функція від якості часткових результатів, досягнутих в контрольних точках проєкту.

Показники розділено на дві групи, оскільки вони використовуються по-різному. Часові та ресурсні показники проєкту визначаються і розраховуються на етапі планування проєкту. На етапі виконання проєкту вони виступають цілями, які необхідно досягнути, а також обмежень, яких потрібно дотриматись. Показники створюваного результату розраховуються на етапі виконання проєкту. Для їх розрахунку використовуються поточні оцінки обсягу та якості часткових результатів в контрольних точках проєкту, а також залежність загального результату проєкту від його окремих елементів, яка визначається на етапі планування проєкту.

Методичний підхід до представлення оборонних проєктів. Методичною основою для розрахунку перелічених показників служить представлення будь-якого проєкту у вигляді дводольного орієнтованого графу (рис. 1) з однією початковою і однією кінцевою вершинами, що описують початок і кінець проєкту відповідно: $G = (V, E)$, де $V = \{v_i, i = \overline{1,I}\}$ – множина вершин графу, I – кількість вершин, $E = \{e_n(\overrightarrow{v_\iota, v_j}); i, j = \overline{1,I}; i \neq j; n = \overline{1,N}\}$ – множина впорядкованих пар вершин (дуг), N – кількість дуг. Стрілка позначає перехід від v_i до v_j. Вершини графу також називають подіями. Початкова v_1 і кінцева v_I вершини (відповідно, початок і закінчення проєкту) можуть бути фіктивними, тобто граф може бути добудовано за допомогою дуг, які не навантажені будь-якими величинами, у тому числі, часом. Перехід між будь-якими вершинами v_n та v_m може бути описано як шлях $(\overrightarrow{v_n, \dots, v_m})$, у який будь-яка вершина може входити лише один раз (умова ациклічності). У цьому сенсі найкоротшим шляхом є дуга, а власне граф може бути представлений множиною шляхів $G = \{(\overrightarrow{v_1, \dots, v_I})_k, k = \overline{1,K}\}$, де K – кількість шляхів. У загальному випадку різні шляхи можуть перетинатись $(\overrightarrow{v_1, \dots, v_I})_k \cap (\overrightarrow{v_1, \dots, v_I})_l \neq \emptyset, k \neq l$.

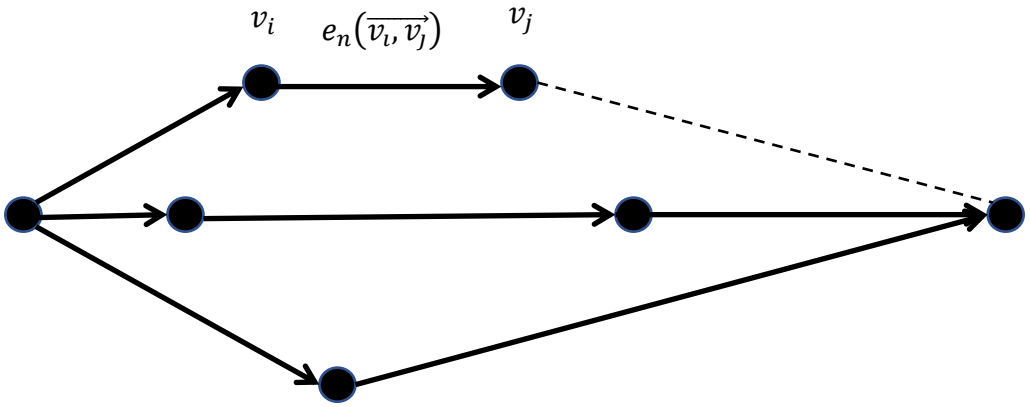


Рис. 1. Приклад дводольного орієнтованого графу

Методичний підхід до врахування невизначеності та оцінки ризиків. Зауважимо, що виходячи з фізичного смислу показників проєктів, ризики розглядаються виключно до часових та ресурсних показників. Ці показники мають кількісну природу. Відповідно до принципу розширення Заде [24], для врахування впливу невизначеності зовнішніх умов на показники робіт проєкту можна використовувати нечіткі числа замість

чітких та нечітку арифметику як аналог стандартної арифметики. Тоді стандартні величини, наприклад, час t, припустимо описати аналогічними за смислом нечіткими величинами: $\tilde{t}$.

Оскільки ризики прямо пов'язані з невизначеністю, а невизначеність показників проєкту описано нечіткими числами, то буде природним описати ризики проєкту характеристиками цих чисел. За смислом ризики проєкту мають відображати можливість і розмір відхилення реальних значень часових та ресурсних показників від планових (цільових) значень внаслідок дії зовнішніх умов, які будуть реалізовані під час виконання проєкту. Але показників ризиків може бути більше.

Наприклад, розглядаємо відхилення часу виконання проєкту від найбільш очікуваного. Чим більше можливі відхилення у бік збільшення часу, тим більше ризик. Навпаки, чим більші можливі відхилення у бік зменшення часу, тим більше стійкість проєкту до можливих несприятливих обставин.

Такий підхід дає змогу гармонізувати розрахунок показників ефективності і оцінювання ризиків. Підхід не потребує розроблення спеціальних алгоритмів для визначення ризиків. Ризики імплементовані в невизначеності значень показників і трансформуються під час їх розрахунків.

Як було показано в огляді літератури, існує багато варіантів опису числової невизначеності. Кожен варіант має свої індивідуальні особливості та недоліки. Але загальною вимогою до нечітких чисел є точний опис невизначеності нечіткої величини, а методів реалізації арифметичних операцій – коректність композиції невизначеності операндів. З огляду на цю вимогу, пропонується використовувати дискретизовані (по носію) нечіткі числа з довільною формою функції належності та алгоритм нечіткої арифметики, заснований на принципі максимуму ентропії. Як показано у спеціальному дослідженні [25], ці методи є найбільш підходящими для вирішення прикладних завдань.

Розглянемо представлення дискретизованих нормальних (одно модальних) нечітких чисел довільної форми та їх характеристики, які є важливими для оцінювання ризиків. Будемо називати нечітким числом $\tilde{R}$ нечітку множину з носієм, визначеним на множині дійсних чисел:

$$\tilde{R} = \{(x, y) \in \mathbb{R} \times [0,1] : y = \mu_{\tilde{R}}(x)\},$$

$$\mu_{\tilde{R}}(x) = \begin{cases} f_{\tilde{R}}(x) & \text{якщо } x \in [a, b), \\ 1 & \text{якщо } x \in [b, c], \\ g_{\tilde{R}}(x) & \text{якщо } x \in (c, d] \\ 0 & \text{у противному випадку,} \end{cases}$$

де $\mu_{\tilde{R}}(x)$ – функція належності, $a, b, c, d \in \mathbb{R}$, $a \le b \le c \le d$, $f_{\tilde{R}}(\cdot)$ – зростаюча справа безперервна функція і $g_{\tilde{R}}(\cdot)$ зростаюча зліва безперервна функція.

Для представлення у комп'ютері нечіткого числа довільної форми використовується дискретизація по осі абсцис, на якій завдано носій нечіткого числа. У цьому випадку, нечітке число представляється множиною пар:

$$\tilde{R} = \left\{ \left(x_i, \mu(x_i)\right),\ i = \overline{1,n},\ x_{i+1} - x_i = \frac{\mathrm{d} - \mathrm{a}}{n-1},\ x_0 = a,\ x_n = d \right\},$$

де n – номер дискети (дискретного сегмента), d, a – нижня та верхня границя носія нечіткого числа.

На сьогодні відомо багато характеристик нечітких чисел, вибір яких залежить від потреб конкретного прикладного дослідження. Достатньо повний огляд цих характеристик надано в роботі [26]. На рис. 2 проілюстровано найбільш розповсюджені характеристики, які використовуються для оцінювання ризиків.

1. Мінімум на α-рівні – дискрета носія нечіткого числа, зліва від якої усі значення функції належності дискет є меншими:

$$x^{\alpha min} = \min\{x_i | \mu(x_i) \ge \alpha \in [0,1], x_i \in R\}.$$

2. Максимум на α-рівні – дискрета носія нечіткого числа, справа від якої усі значення функції належності дискет є меншими:

$$x^{\alpha max} = \max\{x_i | \mu(x_i) \ge \alpha \in [0,1], x_i \in R\}.$$

3. Найбільш очікуване значення нечіткого числа – дискрета носія нечіткого числа, яка має найбільше значення функції належності:

$$x^{MEV} = \left\{ x_i | \mu(x_i) = \max_{j=\overline{1,n}} \mu(x_j), x_i \in R \right\}.$$

4. Центр тяжіння нечіткого числа – дискрета носія нечіткого числа, справа і зліва від якої площі фігур є рівними:

$$x^{CG} = \sum_{i=1}^{j-1} |x_i - x_{i+1}| \cdot \mu(x_i), j = \overline{1,n}, x^{CG} \in R.$$

5. Ризик-функція нечіткого числа:

$$\rho(x_k) = \min_{x_i \ge x_k} \mu(x_k) - \max_{x_i \le x_k} \mu(x_k),\ i, k = \overline{1,n}.$$

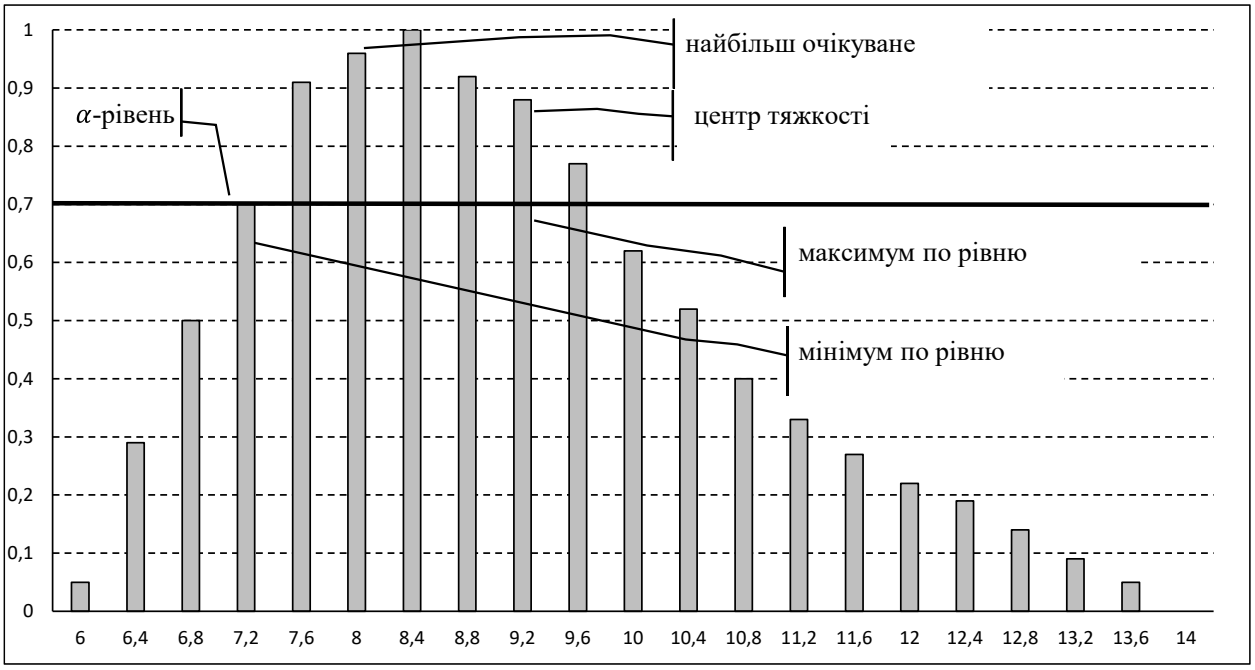


Рис. 2. Характеристики нечітких чисел, які використовуються для оцінювання ризиків

Ризик-функція нечіткого числа $\tilde{R}$ описує можливість того, що реальне значення числової величини виявиться більше значення, яке описує нечітке число $\tilde{R}$. На рис. 3 наведено ризик-функцію нечіткого числа, яке представлене на рис. 2.

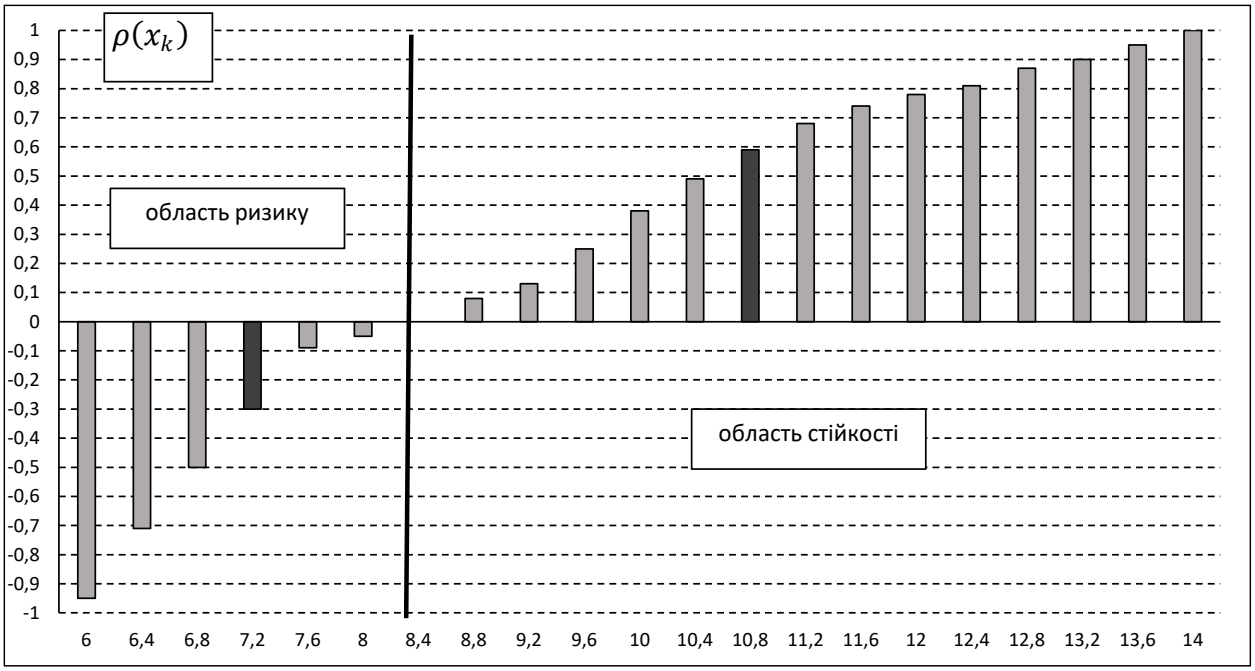


Рис. 3. Ризик-функція нечіткого числа, яке представлене на рис. 2

На рис. 3 показано дві області: область ризику і область акт-ризику (область стійкості). Щоб зрозуміти смисл цих областей, розглянемо приклад використання ризик-функції у практиці. На рис. 3 затемнене дві дискрети нечіткого числа, яке описує витрати певного ресурсу: $(x_k = 7.2;\ \mu(x_k) = -0.3)$ і $(x_i = 10.8;\ \mu(x_i) = 0.6)$. Припустимо, що є зацікавленість у зменшенні витрат. Тоді перша дискрета означає таке. Якщо під час прийняття рішення орієнтуватись на витрати $x_i = 7.2$, то ризик прийняття невірного рішення буде дорівнювати $\mu(x_k) = -0.3$. Друга дискрета означає, що якщо орієнтуватись на витрати $x_k = 10.8$ (тобто передбачимо більше ресурсів, ніж найбільш очікуване значення), то ризик невірного рішення буде відсутній, а можливість правильного рішення дорівнюватиме $\mu(x_k) = 0.6$.

Тобто ризик-функція описує дві онтологічних характеристики кількісного ризику: розмір можливих втрат і події настання в термінах можливості. Використання ризик-функції забезпечує менеджерів додатковими даними для прийняття рішень.

Ця нова характеристика запропонована вперше, оскільки під час оцінювання кількісних ризиків різних проєктів автори зіштовхнулись з такою суперечністю.

З погляду онтології ризиків, розглянуті вище характеристики нечітких чисел $x^{\alpha min}$, $x^{\alpha max}$, x^{MEV} та x^{CG} описують розмір очікуваних втрат, оскільки завдані на множині носія нечіткого числа. Але розмір втрат не є повною характеристикою ризику. Хоча ці характеристики можна ототожнити з ризиками, все ж ризик вимагає додаткового опису в термінах настання втрат, іншими словами, в термінах відношення до дійсності або модальності. Наприклад, в поточних умовах замовник проєкту може втратити \$1.5 млн через зростання цін на ресурси. Це розмір можливих втрат. Але залишається питання, наскільки ця оцінка може бути реалізована на практиці? Отже, оскільки йдеться про оцінку втрат в майбутньому, оцінка ризику має включати не лише розмір втрат, але й оцінку настання цієї події.

Зі свого боку, тут виникають три додаткових питання. По-перше, питання про модальність як відношення до дійсності. По-друге, питання про опис апетиту до ризику. І по-третє, питання про придбання як про категорію, зворотну до категорії ризику.

Питання про модальність як відношення до дійсності. Оскільки будь-яке нечітке число представлене як нормальна функція належності, задана на дискретизованій множини дійсних чисел, то таке нечітке число є нечіткою мірою можливості. Ризик-функція нечіткого числа повністю відповідає цьому твердженню, оскільки розраховується як можливість. Таким чином, запропонована ризик-функція може бути використана для опису не лише розміру очікуваних втрат, але й можливості настання цих втрат.

Питання про опис апетиту до ризику. Описом апетиту до ризику може служити α-рівень, від якого залежать часткові критерії ризику, зокрема $x^{\alpha min}$ та $x^{\alpha max}$. Чим нижче α-рівень, тим більше елементів x_i попаде в діапазон $\left(x^{\alpha max} - x^{\alpha min}\right)$ та, відповідно, тим більше факторів ризику буде враховано в результаті.

Питання про втрати та придбання. Виходячи з міжнародного визначення ризику, фактори невизначеності можливо ототожнити з факторами ризику. В області визначення нечіткого числа завжди існує найбільш очікуване значення, яке ділить число на дві частини. Якщо це число описує показник проєкту, який бажано збільшити, то є справедливими такі міркування. Числа, котрі менше найбільш очікуваного значення (розташовані зліва на шкалі дійсних чисел) є результатом дії факторів ризику, оскільки вони вказують на можливе зниження показника. Числа, котрі більше найбільш очікуваного значення (розташовані справа на шкалі дійсних чисел) є результатом дії факторів анти-ризику, оскільки вони вказують на можливе збільшення показника. Таким чином, область визначення нечіткого числа можна розділити на дві області: область ризику і область анти-ризику (область стійкості). Якщо нечітке число описує показник, який бажано зменшити, то області ризику і стійкості змінюються місцями. Отже, запропонована ризик-функція нечіткого числа може використовуватись для опису не лише ризику втрат, але й можливості придбань.

Алгоритм розрахунку часових показників. Алгоритм базується на відомих алгоритмах сітьового планування [27], але розрахунки здійснюються з нечіткими числами. У сітьовому плануванні кожна дуга графу G навантажена часом виконання. Як головні показники використовуються:

загальний час виконання проєкту $\tilde{t}^{critical}(G)$;

ранній строк початку роботи $\tilde{t}^{early}(\overrightarrow{v_i, v_{i+1}})$;

пізній строк закінчення роботи $\tilde{t}^{late}(\overrightarrow{v_i, v_{i+1}})$;

резерви часу роботи $\tilde{t}_{\Delta}(\overrightarrow{v_i, v_{i+1}})$.

Ці показники розраховуються за допомогою алгоритму, де операції порівняння здійснюються за центром тяжіння нечітких чисел.

Крок 1. Розрахунок ранніх строків початку робіт $\tilde{t}^{early}(\overrightarrow{v_i, v_{i+1}})$.

Розрахунок здійснюється послідовно, починаючи з робіт, яким не передує жодна робота, і закінчується, коли розраховані ранні строки початку усіх робіт. Для робіт, які виходять з початкової вершини орієнтованого графу проєкту, ранній строк початку встановлюється рівним нулю: $\tilde{t}^{early}(\overrightarrow{v_i, v_{i+1}}) = 0$.

Для усіх інших робіт ранній строк початку розраховується як максимальна тривалість шляху серед усіх шляхів, які виходять з початкової вершини до цієї роботи:

$$\tilde{t}^{early}(\overrightarrow{v_\iota, v_{\iota+1}}) = \max_{k=\overline{1,K}} \tilde{t}(\overrightarrow{v_1, \dots, v_\iota})_k.$$

Крок 2. Розрахунок загального часу виконання проєкту.

Загальний час виконання проєкту розраховується як максимальна тривалість шляху серед усіх шляхів, які виходять з початкової до кінцевої вершини:

$$\tilde{t}^{critical}(G) = \max_{k=\overline{1,K}} \tilde{t}(\overrightarrow{v_1, \dots, v_I})_k.$$

Цей шлях є критичним шляхом проєкту.

Крок 3. Розрахунок пізніх строків закінчення робіт $\tilde{t}^{late}(\overrightarrow{v_\iota, v_{\iota+1}})$.

Розрахунок здійснюється послідовно, починаючи з робіт, за якими не слідує жодна робота, і закінчується, коли розраховані пізні строки закінчення усіх робіт.

Для робіт, які закінчуються кінцевою вершиною, пізній строк закінчення встановлюється рівним нулю: $\tilde{t}^{late}(\overrightarrow{v_\iota, v_I}) = 0$.

Для усіх інших робіт пізній строк закінчення розраховується як різність між загальним часом виконання проєкту і максимальною тривалістю шляху від закінчення цієї роботи до кінцевої вершини:

$$\tilde{t}^{late}(\overrightarrow{v_\iota, v_{\iota+1}}) = \max_{k=\overline{1,K}} \tilde{t}(\overrightarrow{v_\iota, \dots, v_I})_k.$$

Крок 4. Розрахунок резервів часу робіт.

Розрахунок здійснюється для усіх робіт. Резерв часу визначається як різниця між пізнім строком закінчення роботи і раннім часом її початку:

$$\tilde{t}_\Delta(\overrightarrow{v_\iota, v_{\iota+1}}) = \tilde{t}^{late}(\overrightarrow{v_\iota, v_{\iota+1}}) - \tilde{t}^{early}(\overrightarrow{v_\iota, v_{\iota+1}}).$$

Роботи з резервом часу $\tilde{t}_\Delta(\overrightarrow{v_\iota, v_{\iota+1}}) = 0$ належать критичному шляху проєкту.

Алгоритм розрахунку ресурсних показників. Головним ресурсним показником є обсяг певного ресурсу, який має бути витрачений в кожний момент часу. Цей показник може бути представлений у вигляді дискретизованої функції $Res^m(p)$, де m – індекс ресурсу, $p = \overline{1,P}$ – дискрета часу, P – максимальний час виконання проєкту. Графік витрачання ресурсу розраховується для кожного ресурсу як сума обсягів витрачання цього ресурсу під час виконання кожної роботи $(res_n^m)_p$:

$$Res^m(p) = \sum_{n=1}^{N} (res_n^m)_p.$$

Загальні обсяги потрібних ресурсів розраховуються як сума $Res^m(p)$ по усіх часових дискретах:

$$Res_\Sigma^m = \sum_{p=1}^{P} Res^m(p).$$

На основі цього графіку визначається графік потрібного забезпечення ресурсами проєкту, а також графік фінансування проєкту:

$$Fin(p) = \sum_{m=1}^{M} Cost^m(p) \cdot Res^m(p),$$

де $Cost^m(p)$ – вартість m-го ресурсу;

M – кількість ресурсів.

Вартість ресурсу визначена як показник, що може змінюватись у часі. Це дає змогу враховувати інфляцію цін у процесі виконання проєкту. Загальний обсяг фінансування проєкту розраховується як сума:

$$Fin_\Sigma = \sum_{p=1}^{P} Fin(p).$$

Алгоритм розрахунку обсягу створюваного результату проєкту. Як було зазначено, алгоритм використовується на етапі виконання проєкту. Вимірювання обсягу створюваного результату здійснюється в контрольних точках проєкту, де закінчується створення системного значимих часткових результатів. Ідея алгоритму полягає у порівнянні сукупності поточних вимірювань обсягів часткових результатів з неадитивною функцією, яка описує залежність повноти кінцевого результату проєкту від сукупності створених часткових результатів. Ця функція має бути побудована на етапі планування проєкту. Вона має враховувати синергію системи, створюваної в результаті виконання проєкту. Синергія кінцевого результату може бути описана у вигляді додаткового внеску, що виникає за рахунок взаємодії часткових результатів.

Тут ключовим моментом стає універсальна множина – та множина, на базі якої будуються методи обробки даних і вирішення задач. На рис. 4 показано два найбільш поширених типи дискретної універсальної множини, яка описують систему з трьох елементів $\{x_i, i = 1,2,3\}$.

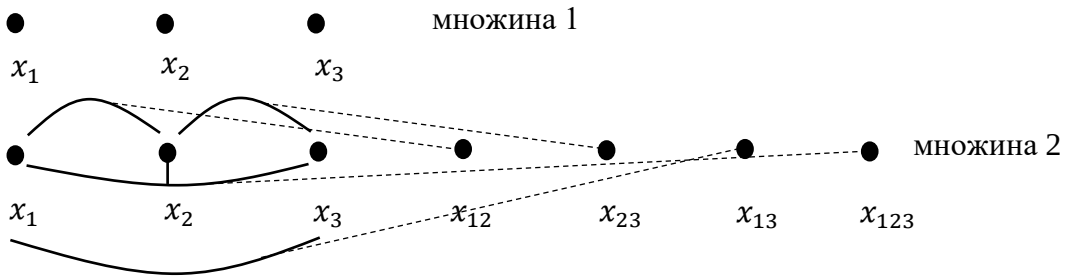


Рис. 4. Два варіанти дискретних універсальних множин

Перша множина складається виключно з цих трьох елементів. Цю множину використовують найбільш розповсюджені методи, такі як метод порівнянь або обробки нечітких множин. Для побудови на цій множині функцій експертним шляхом (що є досить поширеним для оборонних проєктів), експертам задають питання стосовно лише елементів системи. Вплив взаємодій елементів тут не може бути врахований у принципі. Щоб це зробити, потрібно використовувати другу універсальну множину, яка лежить в основі інших методів, зокрема теорії нечітких мір. Під час побудови нечітких мір експертам задаються додаткові питання стосовно підмножин системи, з взаємодій яких формується їх синергія.

Враховуючи це, алгоритм розрахунку обсягу створюваного результату проєкту полягає у визначенні обсягу виконання проєкту залежно від обсягу виконання робіт проєкту в контрольних точках, пов'язаних зі створенням функціонально закінчених частин результату. Позначимо множину контрольних точок як $V = \{v_j, j = \overline{1,J}\}$, де J – кількість контрольних точок. Нехай нечітка міра Сугено $g_V(\cdot): 2^V \to [0,1]$ описує залежність обсягу створюваного результату від кількості і складу реалізованих частин проєкту. Замітимо, що 2^V позначає множину усіх підмножин множини V. Звідси видно, що нечітка міра враховує не лише окремі елементи множини V, але й усі взаємодії між ними, тобто синергію системи V. Також нехай функція належності $\mu(v_i): V \to [0,1]$ описує реальні обсяги створених частин результату. Тоді нечіткий інтеграл Сугено

$$W = (s)\int_V \mu(v_i) \circ g_V(\cdot)$$

розраховуватиме обсяг реально створюваного результату проєкту, який враховує недоробки частин проєкту та їх вплив на повноту кінцевого результату відповідно до синергії взаємодії частин. Нечітку міру, як й функцію належності, можна завдати кількома відомими способами [28].

Алгоритм розрахунку якості створюваного результату проєкту. Алгоритм базується на міркуваннях, аналогічних тим, що покладені в основу попереднього алгоритму.

Оцінювання якості виконання частин проєкту також здійснюється на етапі виконання проєкту в контрольних точках. Нечітка міра $g_Q(\cdot)$ описує залежність якості створюваного результату від якості реалізованих частин проєкту. Результати оцінювання якості часткових результатів представляються у вигляді функції належності $\eta(v_i)$. Тоді нечіткий інтеграл Сугено

$$Q = (s)\int_V \eta(v_i) \circ g_Q(\cdot)$$

розраховує якість кінцевого результату проєкту залежно від якості його частин з урахуванням синергії їх поєднання.

Зазначимо, що оцінювання якості виконання частин результату проєкту є однією з найважливіших функцій проєктного менеджменту. Головним завданням оцінювання якості є вимірювання ступеня відповідності властивостей частини результату вимогам споживача. Оскільки вимоги споживача, частіше за усе, можуть бути описані якісними категоріями, оцінювання якості і ризиків якості концептуально відрізняється від підходів, застосованих до кількісних величин, і буде здійснено в інших публікаціях.

Основні часові і ресурсні ризики виконання проєктів. Застосовуючи характеристики нечітких чисел (див. рис. 2) до часових і ресурсних показників проєктів, що розраховуються за допомогою викладених алгоритмів, можна визначити основні часові і ресурсні ризики виконання проєктів. Зокрема, використовуються такі характеристики нечітких чисел: песимістична оцінка x^{amax}, оптимістична оцінка x^{amin}, найбільш очікувана оцінка x^{MEV}, рівноважна оцінка x^{CG}, відносний діапазон можливих змін $\left|x^{amax} - x^{amin}\right|/x^{CG}$, ризик песимістичної

оцінки $\rho(x^{\alpha max})$, ризик оптимістичної оцінки $\rho(x^{\alpha min})$. Ці характеристики застосовуються до визначених вище часових і ресурсних показників проєкту і окремих робіт.

Напрями подальшого розвитку аналітичної підтримки проєктного менеджменту. На основі сітьової моделі виконання проєкту і алгоритмів розрахунку кількісних показників можна побудувати кілька важливих для проєктного менеджменту задач. У загальному випадку, залежність певного показника від параметрів робіт проєкту може бути описана функціоналом $Y(p) = F(x_1, \dots, x_I)$.

Якщо в якості множини визначення функціоналу завдати строки початку робіт $\tilde{t}^{early}(\overrightarrow{v_i, v_{i+1}})$, що мають резерви часу $\widetilde{t_\Delta}(\overrightarrow{v_i, v_{i+1}}) > 0$, а в якості значення функціоналу визначити рівномірність фінансування проєкту $\left|\max\limits_{p=\overline{1,P}} Fin(p) - \min\limits_{p=\overline{1,P}} Fin(p)\right|$, то можна сформулювати задачу пошуку ранніх строків початку робіт, за якими забезпечується рівномірність графіку фінансування проєкту. Ця задача є класичною задачею проєктного менеджменту. Її рішення дозволяє зменшити навантаження на фінансове забезпечення проєкту і уникнути або мінімізувати обсяги зовнішніх дорогих кредитів.

Запропоновані показники дають змогу розширити коло аналітичних задач, які можуть вирішуватись в межах менеджменту оборонних проєктів.

Зокрема, якщо ввести функцію зміни вартості ресурсів в часі (фактор інфляції цін), завдати максимально можливий обсяг складів для накопичення ресурсів, вартість зберігання ресурсів на складах і вартість транспортування ресурсів до складів і зі складів до місця виконання проєкту, можна сформулювати задачу визначення оптимального графіку закупок ресурсів $Buy(p)$ за критерієм мінімальної вартості забезпечення проєкту ресурсами.

Інша задача. Якщо проєкт виконується в складних умовах (наприклад, фізичної протидії), стає актуальним питання визначення мінімально припустимих обсягів виконання робіт, за якими виконання проєкту ще може вважатись задовільним, тобто коли обсяг створеного результату проєкту буде перевищувати завданий поріг. Аналогічна задача може бути сформульована стосовно якості виконання робіт проєкту.

Зауважимо, що можливість вирішення оптимізаційних задач в умовах невизначеності сьогодні є доведеною в ланці робіт, наприклад [28], хоча й потребує додаткового дослідження.

Висновки. У статті запропоновано методичний підхід до визначення кількісних показників оборонних проєктів, який полягає у поєднанні відомих методів сітьового планування з методами теорії нечітких мір та інтегралів Сугено. Зокрема, запропоновано показники, які розраховуються на етапі планування проєктів, і показники, які розраховуються на етапі виконання проєктів у контрольних точках проєкту. До перших відносяться часові та ресурсні показники, до других – показники обсягу та якості створюваного результату, які враховують синергію поступового поєднання і перетворення окремих частин у загальний результат. Запропоновано підхід до оцінювання ризиків проєкту, який полягає у представленні часових і ресурсних показників у вигляді нечітких чисел і використанні їх характеристик як показників ризиків. Запропоновано алгоритми розрахунку показників. Пропоновані у статті рішення дають змогу забезпечити вимірність оборонних проєктів, тобто те, що вимагають нормативні документи Міністерства оборони України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Наказ Міністерства оборони України від 14.08.2020 р. № 283 URL: http://surl.li/eeizr.
2. Методичні рекомендації з управління проектами. Міністерство оборони України, 2019, 50 с. URL: https://www.mil.gov.ua/content/oboron_plans/Metod_recomendacii_z_ypravlinnia_proektamy.pdf.
3. Плетнева Л. А. Исследование операций по разделам: “Теория игр и сетевое планироваие” : методические указания. Москва : МАДИ, 2013. 48 с. URL: http://surl.li/eawbg.
4. Wilson J. M. Gantt charts: A centenary appreciation // European Journal of Operational Research. 2003. Vol. 149, No. 2. С. 430–437. URL: http://surl.li/eawbo.
5. Graph theory with applications / J. A. Bondy et al. London : Macmillan, 1976. Т. 290. URL: http://surl.li/eawbq.
6. Purdy G. ISO 31000: 2009 – setting a new standard for risk management // Risk Analysis: An International Journal. 2010. Vol. 30, No. 6. P. 881–886. URL: https://cutt.ly/B1dxjoR.
7. Кофман А., Дебазей Г. Сетевые методы планирования и их применение. Москва : Прогресс, 1968.

8. Ehsan A., Yang Q. State-of-the-art techniques for modelling of uncertainties in active distribution network planning: A review // Applied energy. 2019. T. 239. C. 1509–1523.
9. You S., Bindner H. W., Hu J., Douglass P. J. An overview of trends in distribution network planning: A movement towards smart planning. IEEE PES T&D Conference and Exposition. 2014. P. 1–5. DOI: 10.1109/TDC.2014.6863446.
10. Sadegheih A. Optimization of network planning by the novel hybrid algorithms of intelligent optimization techniques // Energy. 2009. T. 34, № 10. C. 1539–1551.
11. Risk assessment of urban network planning in china based on the matter-element model and extension analysis / Y. He et al. // International Journal of Electrical Power & Energy Systems. 2011. T. 33, №. 3. C. 775–782.
12. Опыт оценки рисков подземного строительства / Л. Л. Кауфман и др. // Наука и прогресс транспорта. Вестник Днепропетровского национального университета железнодорожного транспорта. 2010. № 32. С. 55–60.
13. Gazdik, "Fuzzy-Network Planning – FNET," in IEEE Transactions on Reliability. Aug. 1983. Vol. R-32, No. 3. P. 304–313. DOI: 10.1109/TR.1983.5221657.
14. Kanmohammadi S., Rahimi F., Sharifian M. B. B. Analysis of different fuzzy CPM network planning procedures. ICECS : 10th IEEE International Conference on Electronics, Circuits and Systems, 2003. Vol. 3. P. 1074–1077. DOI: 10.1109/ICECS.2003.1301696.
15. Mares M. Weak arithmetics of fuzzy numbers. Fuzzy Sets and Systems. Vol. 91. 1997. P. 143–153. DOI: 10.1016/S0165-0114(97)00136-X.
16. Iwona Pisz, Anna Chwastyk, Iwona Łapuńka. Assessing the profitability of investment projects using ordered fuzzy numbers // Scientific Journal of Logistics. Vol 15, No. 3. 2019. P. 377–389. http://doi.org/10.17270/J.LOG.2019.342.
17. Barnabás Bede. Product Type Operations between Fuzzy Numbers and their Applications in Geology. Acta Polytechnica Hungarica. Vol. 3. No. 1. 2006. P. 123–139.
18. Olga Kosheleva, Sergio D. Cabrera, Glenn A. Gibson, Misha Koshelev. Fast implementations of fuzzy arithmetic operations using fast Fourier transform (FFT). Fuzzy Sets and Systems. Vol. 91. Issue 2. 1997. P. 269–277. DOI: 10.1016/S0165-0114(97)00147-4.
19. Stefanini, Luciano & Sorini, Laerte & Professor, Maria. Fuzzy Numbers and Fuzzy Arithmetic. 2008. In book: Handbook of Granular Computing. P. 249 – 283. DOI: 10.1002/9780470724163.ch12.
20. Haitao Liu and Sizong GUO. Equality and Identity of Fuzzy Numbers and Fuzzy Arithmetic with Equality Constraints. International Conference on Intelligent Systems and Knowledge Engineering 2007. P. 334–339. DOI: 10.2991/iske.2007.56.
21. Методичні рекомендації з управління проектами. Міністерство оборони України, 2019, 50 с. URL: https://www.mil.gov.ua/content/oboron_plans/Metod_recomendacii_z_ypravlinnia_proektamy.pdf.
22. Lushi I. et al. A literature review on ISO 9001 standard //European Journal of Business, Economics and Accountancy. 2016. T. 4, №. 2. C. 81–85. URL: http://surl.li/edldp.
23. Zadeh L A (1975) The Concept of linguistic variable and its applications to approximate reasoning. Information Sciences. DOI: https://doi.org/10.1016/0020-0255(75)90046-8.
24. Sveshnikov S, Bocharnikov V. Computational Algorithm and Tools of Fuzzy Arithmetic Based on the Principle of Maximum Entropy. Research Article. URL: https://assets.researchsquare.com/files/rs-1254409/v1_covered.pdf?c=1642605797.
25. Slavka Bodjanova. Median value and median interval of a fuzzy number. Information Sciences. Vol. 172. Issue 1. 2005. pp. 73–89. DOI: 10.1016/j.ins.2004.07.018.
26. Коршунов Ю. М. Математические основы кибернетики. 3-е изд., перераб. и доп. Москва : Энергоатомиздат, 1987. 496 с.
27. Бочарніков В. П., Свєшніков С. В., Тимошенко Р. І., Павленко В. І. Технологія аналізу воєнно-політичної обстановки. Київ : НУОУ імені Івана Черняховського, 2017. 397 с.
28. Tang J. et al. Understanding of fuzzy optimization: theories and methods // Journal of Systems Science and Complexity. 2004. T. 17, №. 1. C. 117–136. URL: http://surl.li/egoqi/

Стаття надійшла до редакційної колегії 12.06.2023

Assessing the effectiveness and risks of implementing defense projects based on fuzzy integral calculus

Annotation

The Russian-Ukrainian war clearly showed the relevance of the development of the Armed Forces of Ukraine based on defense planning, which should ensure high-quality training of the Ukrainian Armed Forces for the defense of Ukraine and contribute to their effective use in the future. In crisis financial and economic conditions, the state is moving towards solving the problems of defense planning on the basis of project management, which ensures the orientation of defense policy towards the final, functionally completed result.

In project management, which is carried out under conditions of uncertainty, there is a problem of forming and measuring indicators that ensure the measurability of defense projects at the stages of both planning and implementation. They must take into account the uncertainty of a quantitative and

qualitative nature. In this article, consideration of the results of the study is carried out only in relation to quantitative indicators.

A methodical approach to determining the quantitative indicators of defense projects is proposed, which consists of combining the known methods of network planning with the methods of the theory of fuzzy measures and Sugeno integrals. In particular, indicators calculated at the project planning stage and indicators calculated at the stage of project implementation at project milestones are proposed. The former include time and resource indicators, and the latter - indicators of the volume and quality of the result being created, taking into account the synergy of the gradual combination and transformation of individual parts into a common result. An approach to project risk assessment is proposed, which consists of presenting time and resource indicators in the form of fuzzy numbers and using their characteristics as risk indicators. Algorithms for calculating indicators are proposed.

Keywords: defense planning; defense project; efficiency; risk; network planning; fuzzy-integral calculus.

УДК 354+359.07 DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/68-73

Полевий В. І., кандидат юридичних наук, старший науковий співробітник
0000-0001-9212-2475

Навчально-науковий центр стратегічних комунікацій у сфері забезпечення національної безпеки та оборони Національного університету оборони України, Київ

Оборонне планування у сфері стратегічних комунікацій сил оборони України на основі пріоритетних завдань та на основі спроможностей

Резюме. У статті проведено аналіз та порівняння історичного досвіду і перспектив розвитку оборонного планування на основі загроз і пріоритетних завдань та на основі спроможностей. Виокремлено проблемні питання переходу на новий процес планування, надані рекомендації щодо вдосконалення підходів до планування спроможностей сил оборони у сфері стратегічних комунікацій.

Ключові слова: стратегічні комунікації; оборонне планування; спроможності; ефекти; носій спроможностей.

Постановка проблеми. З 2017 року Україна перейшла до оборонного планування на основі спроможностей (далі – ОПОС). Слід зазначити, що нова практика планування не вкоренилася як звична та зрозуміла, органи військового управління не мають відповідних робочих методик, а отриманий досвід потребує узагальнення. Усе перелічене повною мірою стосується стратегічних комунікацій сил оборони, які, зі свого боку, також є новим об'єктом досліджень для безпекового сектору. Разом з тим, оборонне планування на основі спроможностей є, *по-перше*, необхідною умовою для досягнення достатньої сумісності Збройних Сил України та інших складових сектору безпеки і оборони з відповідними структурами держав – членів НАТО, а, *по-друге*, – знайшло відображення і передбачене чинним законодавством (ст. 27 Закону України "Про національну безпеку України" [1]). Аналіз оборонного планування у сфері стратегічних комунікацій сил оборони України на основі пріоритетних завдань та на основі спроможностей обумовлює актуальність дослідження.

Аналіз останніх досліджень і публікацій. Тема розвитку оборонного планування на основі спроможностей останніми роками набула широкого резонансу у військових наукових колах. Науковцями було проведено порівняння систем оборонного планування Збройних Сил України (далі – ЗС України) та структур країн – членів НАТО [2]. Проаналізовано поточний стан і перспективи оборонного планування на основі спроможностей в Україні [3] та підходи до розроблення алгоритму огляду спроможностей [4].

Дослідження стратегічних комунікацій у діяльності сил оборони є окремим науковим напрямом. Науковцями проаналізовано інституційний розвиток стратегічних комунікацій у центральних органах влади України [5], досліджено основи стратегічних комунікацій у сфері забезпечення національної безпеки і оборони [6]. Водночас, феномен централізації і структурування стратегічних комунікацій, який мав місце з початком повномасштабного вторгнення ще неосмислений на науковому рівні належним чином.

Отже на сьогодні ця тематика лише частково висвітлена в наукових дослідженнях щодо оборонного планування на основі спроможностей у сфері стратегічних комунікацій сил оборони. Порівняння оборонного планування у сфері стратегічних комунікацій сил оборони України на основі пріоритетних завдань й на основі спроможностей раніше не проводилось, що обумовлює актуальність поставленої мети.

Метою статті є дослідження переваг ОПОС над плануванням на основі задач та визначення напрямів розвитку планування у сфері стратегічних комунікацій сил оборони.

У процесі дослідження використовувались як загальнонаукові, так і конкретно-наукові **методи**: системно-структурного та історичного аналізу, порівняльний, моделювання та інші.

Виклад основного матеріалу. Варто зазначити, що у рекомендаціях Міністерства оборони України з ОПОС присутнє твердження, що: "На відміну від планування на основі загроз, ОПОС полягає в зосередженні зусиль не на створенні нових організаційних структур для забезпечення противаги відповідному бойовому потенціалу противника, а на розвитку спроможностей військ (сил) для ефективного виконання

визначених завдань”[7]. Погоджуючись з висновком [3], що планування на основі спроможностей не виключає появу нових структур, слід наголосити, що планування з урахуванням переліку бажаних ефектів з визначеним результатом, чітким описанням процесів для досягнення цих ефектів [8], є ключовою рисою ОПОС і дає змогу виявити та усунути випадки дублювання функцій підрозділів і неефективного використання ресурсів. Наразі, стратегічні комунікації у державних установах потребують описання у вигляді процесів, коли “кожен співробітник організації обслуговує якийсь процес і вносить свій внесок у нього, а кожен процес має конкретного власника, який відповідає за ефективність цього процесу” [9]. Для стратегічних комунікацій кожен процес також повинен мати визначений результат (продукт) та свою аудиторію (споживача). Результати у комунікаціях можуть бути сформовані у вигляді *ефектів*, тобто змін, яких планується досягнути у середовищі. У нашому випадку – це когнітивно-поведінкові зміни цільових аудиторій, а когнітивно-поведінковий підхід наразі є основоположним у доктрині НАТО [10].

Адміністрування процесів у теорії менеджменту є ознакою “зрілої” організації, на противагу “новонародженій” організації, яка розвивається завдяки правильним ідеям та енергії носіїв цих ідей. Справді, стратегічні комунікації, як окрема функція, є відносно новим явищем у силах оборони України, що дає надію на упорядкування комунікаційних процесів не за принципом пріоритетності створення нового підрозділу, а саме для розвитку нових спроможностей, що складаються з процесів, які мають своїх власників, результат, аудиторії і спрямовані на досягнення військових цілей у когнітивній площині.

Досить часто акцент на існуванні підрозділу як організаційного елементу створює передумови дублювання функцій, зокрема у сфері стратегічних комунікацій. У структурах ЗС України та Міністерства оборони України (далі – МО України), наприклад, є структурно та функціонально ідентичні підрозділи зі створення відео-контенту: телерадіостудія МО України “Бриз”, Центральна телерадіостудія МО України, медіацентр при Центрі досліджень воєнної історії ЗС України управління стратегічних комунікацій Апарату Головнокомандувача ЗС України. Разом з тим, з погляду процесів і кінцевого продукту цих підрозділів – відеоматеріалів різних форматів, маємо ідентичну за змістом і формою діяльність, яка дублюється в різних структурах для виконання відмінних (різних) завдань цих підрозділів.

Розглянемо інший приклад – актуальну загрозу щодо поширення ворожої пропаганди та інформаційно-психологічних операцій (ІПсО). Стандартний підхід оборонного менеджменту передбачав описання нової функції як “протидію ворожій пропаганді та ІПсО”. Реалізацію цієї функції покладали, як правило, на якусь нову структуру, наприклад, “Центр протидії дезінформації (ЦДП)” [11], до завдань якого і відносили зазначену протидію. ЦПД забезпечує здійснення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері. Новостворена з певною метою структура починала роботу з формування завдань (тобто визначення змісту протидії, процесів, які вона включає і результату) та організаційно-штатної структури (який персонал і ресурси будуть виконувати зазначені задачі). Схематично процес планування виглядав і, як правило, виглядає нині як показано на рис. 1.

На основі переліку завдань, визначених унаслідок аналізу загроз, формувалися функції, для реалізації яких часто створювалися нові підрозділи. Так, для нейтралізації ІПсО важливим також є високий рівень медіа грамотності, інформаційної гігієни та патріотичне виховання наших аудиторій (наприклад, військових чи майбутніх військовозобов’язаних - молоді).

ОПОС передбачає більш широку рамку планування і чіткіші та вимірювані результати, які досягаються за рахунок процесів, стандартизованих за рахунок описання ефектів, яких потрібно досягнути. Здатність досягати результатів ефектів є сутністю спроможностей, носіями яких є підрозділи, окремі засоби або системи. Для вирішення нових завдань підбираються існуючі підрозділи, які є носіями необхідних спроможностей як показано на рис. 2.

Рис. 1. Процес планування залучення підрозділів до ОПОС

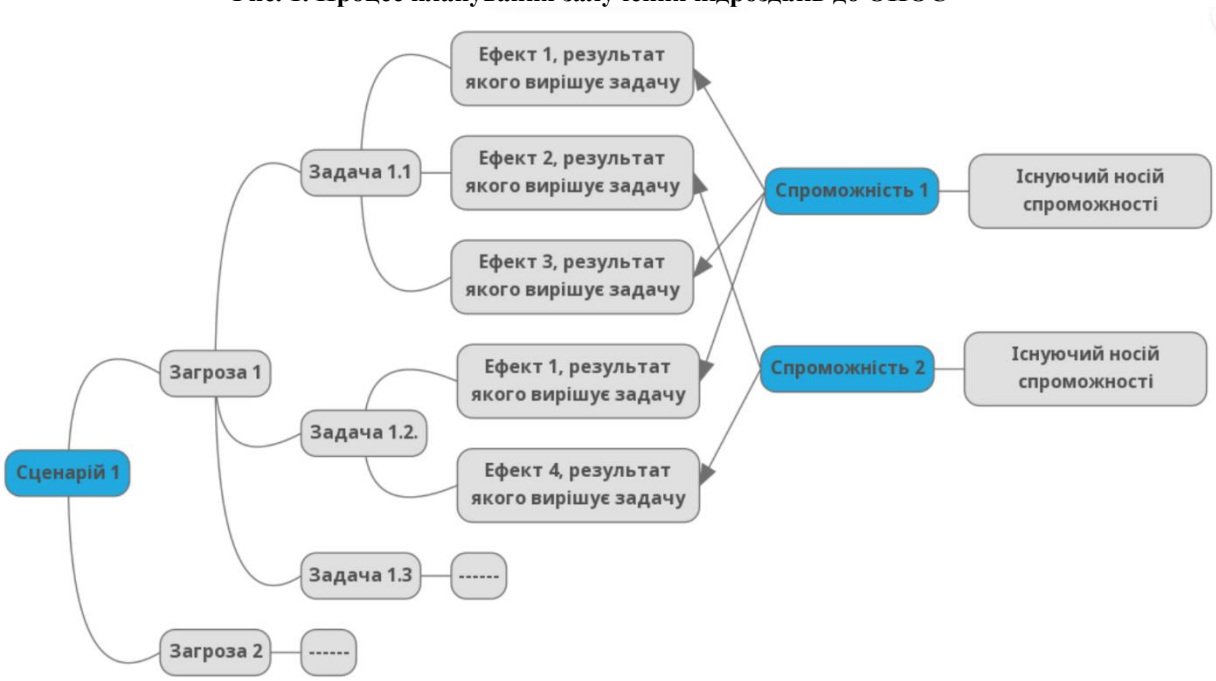


Рис. 2. Процес залучення підрозділів на основі ОПОС

По-перше, ОПОС, окрім аналізу загрози, передбачає визначення національних інтересів та цінностей у певній сфері, які отримуються шляхом аналізу доктринальних документів (Конституції України, Закону України "Про національну безпеку України" тощо) та стратегій. У частині стратегічних комунікацій це будуть, наприклад, дотримання свободи слова та права на доступ до інформації, повага до гідності та особистого життя, формування аудиторій до воєнної політики держави, підтримання позитивного іміджу сил оборони. Чим детальніше прописані цілі стратегій – тим краще для планування. Як взірець варто навести Стратегію комунікації з питань європейської інтеграції України на період до 2026 року [12] з її чітко виписаними цілями та критеріями досягнення цілей, наприклад: "Стратегічна ціль 1. Громадяни України свідомо підтримують реалізацію стратегічного курсу держави на набуття повноправного членства України в Європейському Союзі та розуміють процес реалізації державної політики у сфері європейської інтеграції, його вплив на життя кожного громадянина".

По-друге, оцінюється "майбутнє безпекове середовище" (термін запозичене з документів країн – членів НАТО), на основі чого робляться прогнози щодо "сценаріїв для оборонного планування". Узагальнивши, в тому числі й вимоги нормативних документів [13], цикл (повторюваний процес) ОПОС у сфері комунікацій можемо зобразити у вигляді послідовності етапів, які наведені у Табл. 1.

Таблиця 1

Цикл ОПОС у сфері стратегічних комунікацій

№	Назва етапу	Виходи	Результат
1.	**Оцінювання інформаційного середовища**	Оцінка середовища	Комунікаційна стратегія. Визначення аудиторій та наративів для них
		Сценарії	
2.	**Оцінювання характеру наших комунікацій. Які цілі ми досягаємо?**	Перелік завдань (типових завдань)	Ефекти-завдання та показники їх ефективності (KPI)
		Перелік ефектів на досягнення цілей комунікації	
3.	**Визначення конфігурації спроможностей і відповідної структури сил**	Уточнення каталогу спроможностей	Визначені спроможності, їх носії та пропозиції щодо необхідних сил і засобів
		Уточнення структури носіїв спроможностей	
4.	**Пропозиції щодо програм розвитку відповідно до стратегічних цілей**	Пропозиції до СОБ	Програми розвитку базуються на спроможностях
5.	**Пропозиції щодо проєктів та програм проєктів розвитку спроможностей**	Описання проєктів	Пропозиції до планів підготовки сил та до державних програм, які теж враховують спроможності
		Описання програм	
		Попередня оцінка вартості проєктів і програм	
6.	**Розроблення проєктних пропозицій (статутів проєктів та програм проєктів)**	Деталізовані документи	Визначення команд і відповідальних, які готують статути
7.	**Оцінювання необхідних ресурсів за планами утримання та розвитку**	Попередня загальна оцінка вартості	Визначення бюджетів
8.	**Коригування планів діяльності і бюджетів**	Відкориговані плани і бюджети	Початок реалізації
9.	**Фінансування заходів повсякденної діяльності та планів розвитку**	Реалізація повсякденних процесів	Реалізація заходів розвитку
		Управління спроможностями Управління ресурсами	
10.	**Узагальнення досвіду**	Звіти на основі донесень про комунікаційні кампанії	Матеріали узагальнення досвіду використовуються виконавцями
11.	**Коригування, реагування на зміну ризиків**	Корекція планів	Реагування на зміни

Задача протидії загрозі у вигляді “ворожої пропаганди та ІПсО” за планування на основі спроможностей залишається, але описується у вигляді ефектів, які необхідні для досягнення поставленої цілі (мети), що, зі свого боку, передбачає опис результатів, яких слід досягнути, наприклад, “рівень довіри до офіційних ресурсів України в три і більше разів переважає рівень довіри до ресурсів ворога”. Пропонується сформулювати перелік ефектів та процесів, необхідних для досягнення результату (у дужках подана назва ефекту, який використовується у менеджменті НАТО):

оцінити і визначити аудиторії для комунікацій;

створити інформаційний продукт, який відповідає критеріям оперативності, достовірності, якості та з урахуванням нашої аудиторії;

зробити його максимально доступним для наших аудиторій (Promote);

викрити методи та інструменти ворожої пропаганди (Amplify);

знецінити інформацію ворога (Corrupt) та обмежити її поширення (Contain);

переконати аудиторію у надійності наших джерел (Convince).

Наступний результат може бути сформульований як “рівень обізнаності аудиторії про стратегічні цілі та поточні дії на досягнення цієї цілі”. Під цей результат формується інший перелік ефектів, основний

акцент серед яких буде на комунікації з аудиторією (Communicate).

Далі передбачено урахування обмеженості ресурсів та формування кінцевої спроможності, як здатності її носія досягати ефектів у встановлених умовах із визначеними результатами. Носіями спроможностей, відповідно до чинних рекомендацій, виступають визначені:

з'єднання, військові частини, установи, організації та їх підрозділи;

органи військового управління;

окремі засоби (літаки, вертольоти, безпілотні авіаційні комплекси, кораблі, судна, ракетні комплекси та комплекси ППО);

програмні та програмно-технічні комплекси та системи (автоматизованого управління військами (силами), обміну даними розвідки та обстановки, оповіщення, управління оборонними ресурсами, захисту інформації тощо) [14].

У частині комунікацій носіями спроможностей виступатимуть окремі з'єднання, військові частини, установи, організації та їх підрозділи, а також органи військового управління.

Далі може виявитися, що оскільки в системі сил оборони уже існують носії, спроможні досягати визначених результатів шляхом реалізації ефектів, то створювати новий підрозділ під нейтралізацію загрози (наприклад, та сама пропаганда та ІПсО, але вже білоруська чи угорська) буде недоцільно.

Планування на основі спроможностей дає змогу встановити, що потрібні ефекти досягаються діями різних, уже наявних структур, а протидія (нейтралізація) новій загрозі (ворожа пропаганда та ІПсО) може бути організована у межах існуючої структури із визначенням одного відповідального координатора процесу.

Повертаючись до прикладу з телестудіями у структурі ЗС України та МО України такі ефекти, як інформування та висвітлення подій за допомогою відеоматеріалів, переконання аудиторій тощо можуть виконуватися однією телестудією, яка виконуватиме завдання різних Замовників на різних рівнях: підрозділів зв'язків з громадськістю, морально-психологічного забезпечення, цивільно-військового співробітництва. Тобто знімальна група телестудії може виготовити контент і для задоволення потреб певного оперативного угруповання військ. Зрештою, переважна більшість такої продукції може бути створена незалежними студіями на договірних засадах.

Таким чином, ОПОС дає змогу краще описати цілі, які потрібно досягнути, конкретні результати та ефекти, які повинні вміти реалізовувати носії спроможностей. ОПСО дає змогу провести якісний функціональний аудит і виявити напрями подальшого розвитку СО.

Висновок. ОПОС у сфері стратегічних комунікацій є новим для сил оборони України процесом, який потребує подальшого методологічного опрацювання, описання у вигляді процесів та їх оптимізації. Кілька ітерацій такого планування можуть вивільнити додаткові ресурси та зробити комунікації більш гнучкими та ефективними в частині впливу на цільові аудиторії.

Перспектива подальших досліджень полягає в описанні окремих комунікативних процесів, визначенні критеріїв ефективності процесів, їх носіїв; у продовженні формування напрямів розвитку окремих спроможностей у сфері стратегічних комунікацій з можливим логічним поєднанням їх у каталозі спроможностей за рахунок "перехресних посилань".

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII : станом на 31.03.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 01.06.2023)
2. Дєнєжкін М. М., Наливайко А. Д., Поляєв А. І. Особливості оборонного планування у державах-членах НАТО, на основі спроможностей // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2017. № 2. С. 34–38.
3. Малишев О. В., Малишева Н. Р., Калмиков В. Г., Левчук О. В. Оборонне планування на основі спроможностей в Україні: поточний стан і перспективи // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2020. № 3 (70). С. 54–61.
4. Корендович В. С., Ткач І. М., Потетюєва М. В. Щодо підходів до розробки алгоритму огляду спроможностей // Організація оборонного планування на основі спроможностей та управління ризиками в секторі безпеки та оборони : матеріали Міжвідом. наук.-практ. семінару (м. Київ, 26 жовт. 2022 р.) / Нац. ун-т оборони України ім. І. Черняховського. Київ, 2022. С. 55–59.
5. Соловйов С. Г. Інституційний розвиток стратегічних комунікацій в Україні (на прикладі міністерств) // Вісник Київського національного університету імені Тараса Шевченка. Державне управління. 2022. № 1(15). С. 37–41.

6. Основи стратегічних комунікацій у сфері забезпечення національної безпеки та оборони : навч. посіб. / О. Ф. Сальнікова, І. В. Іжутова, В. О. Кушнір та ін. Київ : НУОУ, 2020.
7. Рекомендації з оборонного планування на основі спроможностей в Міністерстві оборони України та Збройних Силах України : затв. Міністром оборони України 12.06.2017 р. 49 с. URL: https://www.mil.gov.ua/content/other/Recommendationson_CBP_120617.pdf (дата звернення: 10.06.2023).
8. BPM CBOK: Guide to the business process management common body of knowledge: version 3.0. 1st. edition. Springfield : Association of Business Process Management Professionals (ABPMP). 2013. 444 с. ISBN 978-1-4905-1659-2.
9. BS-6143-1. Guide to the economics of quality. Process cost model. British Standard Institute. 1992. ISBN 0-580-20440-5.
10. AJP-1 ALLIED JOINT DOCTRINE. URL: https://www.gov.uk/government/publications/ajp-01-d-allied-joint-doctrine (дата звернення: 10.06.2023).
11. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року "Про створення Центру протидії дезінформації" : Указ Президента України від 19.03.2021 р. № 106/2021. URL: https://zakon.rada.gov.ua/laws/show/1155-2022-%D1%80#Text (дата звернення: 01.06.2023).
12. Про схвалення Стратегії комунікації з питань європейської інтеграції України на період до 2026 року : Розпорядження Кабінету Міністрів України від 09.12.2022 р. № 1155-р. URL: https://zakon.rada.gov.ua/laws/show/1155-2022-%D1%80#Text (дата звернення: 01.06.2023).
13. Порядок організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони : наказ Міністерства оборони України від 22.12.2020 р. № 484. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 01.06.2023).
14. Основи оборонного менеджменту у діяльності Збройних Сил України : навч. посіб. / І. М. Ткач, С. А. Бондаренко, М. Я. Ткач та ін. Київ : НУОУ ім. І. Черняховського, 2021. 264 с.

Стаття надійшла до редакційної колегії 29.06.2023

Defense planning in the field of strategic communications of the Ukrainian defense forces based on priority tasks and based on capabilities

Annotation

Since 2017, Ukraine has switched to capability-based defense planning (hereinafter CBDP). It should be noted that the new planning practice has not taken root as a familiar and understandable one, military command and control bodies do not have appropriate working methods, and the experience gained needs to be generalized. All of the above relates to the strategic communications of the defense forces, which, in turn, is also a new object of study for the security sector. A comparison of defense planning in the field of strategic communications of the defense forces of Ukraine on the basis of priority tasks and on the basis of capabilities has not been previously carried out, which determines the relevance of the article.

As an example, an actual threat is considered - the spread of hostile propaganda and information and psychological operations (IPSO). The standard defense management approach was to describe the new function as "countering hostile propaganda and IPOCs". The implementation of this function was assigned, as a rule, to some new structure. The CBDP provides for a broader planning framework and clearer and more measurable results achieved through processes that are standardized and descriptions of the effects to be achieved. The ability to achieve the results of effects is the essence of abilities, the carriers of which are units, individual means, or systems. To solve new problems, existing units are selected, which are carriers of the necessary abilities.

The CBDP, in addition to threat analysis, provides for the determination of national interests and values in a certain area, obtained by analyzing doctrinal documents and strategies. In addition, the "future security environment" is assessed, on the basis of which forecasts are made regarding "defense planning scenarios". Having summarized, including the requirements of regulatory documents, the EPOS cycle in the field of communications can be implemented sequentially in accordance with the proposed stages.

Keywords: strategic communications; defense planning; capabilities; effects; ability carrier.

УДК 355.018 : [477: (470+571)] DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/74-79

Косарецький Є. І., доктор філософії (0000-0001-9601-8544)
Сотник В. В., кандидат економічних наук (0000-0003-0507-2348)
Слюсаренко А. В. (0009-0006-8740-3524)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Дослідження впливу воєнних дій на національну економіку України: фактичні збитки та втрати

Резюме. Розглянуто основні фактори та проблеми в системі оцінки збитків та втрат заподіяних унаслідок воєнних дій. Досліджені галузі економіки, які найбільше постраждали від впливу воєнних дій, та галузі, які почали найбільшими темпами розвиватися.

Ключові слова: бізнес-процес; відшкодування; воєнні дії; втрати; збитки; недоотриманий прибуток; суб'єкти підприємницької діяльності.

Постановка проблеми. Бойові дії та бомбардування території України впливають на всі сфери життя людей, зокрема і на економічну. Руйнування або ушкодження об'єктів, на яких проводиться господарська діяльність, призводить не лише до витрат, необхідних на відновлення об'єкта, а також і до втрат від простоїв та не відновлювальних ресурсів. Складовою проблеми, яку створює для економіки України воєнний стан, є також введення комендантської години, обмеження авіасполучення, порушення логістичних процесів всередині країни та поза неї. Проблемою оцінки збитків та втрат, завданих воєнними діями, є те, що підхід до такої оцінки може варіюватися залежно від різних установ і факторів, які беруться до уваги проведення досліджень. Отже висновки, які будуть зроблені у цій статті, можуть бути використані підприємцями для оптимізації їх підприємства, оскільки вони мають обмежену кількість ресурсів через збитки та втрати, заподіяних воєнними діями. Від ефективності діяльності суб'єктів господарювання залежить рівень податкових надходження до державного бюджету, які потім перерозподіляються на оборонну сферу.

Аналіз досліджень і публікацій. Проблеми оцінки збитків та втрат, заподіяних воєнними діями, вивчали такі дослідники, як І. Бойчук [1], Т. Захарова [2], Н. Колісніченко [3], І. Приступа [4], О. Буряченко [5] та інші науковці. І. Бойчук у своїй статті детально аналізує навколишнє середовище та його безпосередній вплив на можливості суб'єктів господарювання в умовах нестабільності та війни. Крім цього автор наводить нові методи просування бізнесу на ринку B2B (це маркетинговий підхід, за яким "бізнес направляється на бізнес") в умовах діючого маркетингового середовища [1]. Т. Захарова в своїх дослідженнях зосереджує увагу на оцінюванні наслідків війни у сфері туризму та виокремлює перспективи його післявоєнного відновлення. Автор акцентує увагу на тому, що розвиток туризму має бути ефективним засобом для диверсифікації економіки країни, джерелом формування додаткових робочих місць, повне задоволення ділових, соціально, культурних і рекреаційних споживчих потреб туристів [2]. Н. Колісніченко в своїй праці детально розглянув ризики, які пов'язані із кризою та війною зокрема виокремив такі проблеми: відсутність нормативно-законодавчої бази для регулювання промисловості під час війни; недосконаліть інвестиційної та інноваційної політики держави, значні корупційні збитки для країни внаслідок тіньових схем; низька купівельна спроможність населення; недостатність фінансової підтримки суб'єктів господарювання та висока ціна їх оновлення [3]. Група авторів, таких як: М. Приступа, Т. Неклюєнко, Н. Луцкевич у своїх дослідженнях показали вплив війни на демографію в країні, що впливає на суспільний розвиток країни [4]. Проте вплив ефективності діяльності суб'єктів господарювання на обороноздатність країни не достатньо досліджується зазначеними вченими.

Мета статті полягає в оцінюванні збитків, руйнувань і ушкоджень та аналізі впливу воєнних дій на економічну діяльність суб'єктів господарювання.

Виклад основного матеріалу. Унаслідок повномасштабної війни з боку Росії суб'єкти підприємницької діяльності вимушені працювати в умовах обмеженої інформації: плани щодо діяльності бізнесу не можуть мати тривалий термін, і у разі відсутності гнучкості плану підприємці не

можуть налагодити свою діяльність в умовах воєнного стану. Тобто, окрім вже отриманих збитків за рахунок простоїв через повітряну тривогу, збільшення витрат діяльності через інфляцію, та зменшення доходів населення (і, відповідно, попиту з боку населення), підприємці також не мають можливості задіяти наявні ресурси підприємства таким чином, щоб бути впевненими у їх поверненні та примноженні. Проте оцінити втрати від впливу війни непросто, оскільки різні підходи до досліджень враховують різні фактори впливу на показник втрат.

Насамперед, необхідно оцінити зміну такого ключового показника, як внутрішній валовий продукт (ВВП), оскільки будь-які зміни в економіці одразу відбиваються у ВВП країни.

Проаналізуємо зміну ВВП України згідно з даними Державної служби статистики України.

Таблиця 1

ВВП України за 2019–2022 рр.*

ПОКАЗНИК	2019	2020	Відхилення, 2020–2019	2021	Відхилення, 2021–2020	2022	Відхилення, 2022–2021
ВВП у фактичних цінах, млн грн	3977198	4222026	244828	5450849	1228823	5191028	-259821
ВВП у цінах попереднього року, млн грн	3674214	3827941	153727	4367501	539560	3865780	-501721
Зміна обсягу ВВП за рік, %	3.2	-3.8	-7	3.4	7.2	-29.1	-32.5

Джерело: складено на основі [8]

За даними Табл. 1 можна зазначити зменшення ефективності діяльності підприємств у 2022 році порівняно з 2021 роком. Навіть не зважаючи на кризу, спричинену у світовій економіці через коронавірус, економіка України постраждала менше, ніж через рік війни.

Також слід ураховувати рівень інфляції. За даними Мінфіну, у 2022 році індекс споживчих цін склав 126,6 %. Це свідчить про те, що реальний ВВП України у 2022 році є значно меншим за номінальний.

За результатами досліджень, проведених Європейською Бізнес Асоціацією, збитки суб'єктів господарської діяльності оцінюються близько 100 тис. дол. у розрахунку на кожного п'ятого підприємця [6].

Згідно з повідомленнями BBC News Україна, близько половини компаній зменшили обсяг своєї діяльності за географічною ознакою, тобто втратили частину ринку тих територій, які вони перестали обслуговувати з тих чи інших причин. П'ята частина українських компаній повністю або частково перевела своїх працівників на дистанційну роботу, і п'ята частина українських компаній припинила роботу певних відділень, які компанії не мали змоги фінансувати надалі [7].

Також зазначається, що лише половина суб'єктів підприємницької діяльності зберегли заробітну плату на довоєнному рівні, кожна чотирнадцята компанія змушена була відправити працівників у неоплачувану відпустку, кожна тридцять третя компанія звільнила частину працівників, а 1 % компаній не можуть виплачувати заробітної плати.

Слід зазначити, що збитки та недоотримані прибутки, пов'язані зі зміною структури трудових ресурсів країни, розрахувати найважче. Коли працівник не працює, він не приносить доходів підприємству, а також потребує допомоги з боку держави. Однак, на жаль, враховуючи важкі виклики війни, бойові дії та бомбардування, втрати у випадку смерті людини оцінити неможливо – ні з погляду моралі, ні з погляду економіки (коли гине людина, вона не завжди залишає нащадків, які формують майбутнє будь-якої країни).

Прем'єр-міністр України ще наприкінці травня 2022 року зазначив, що втрати України від інфраструктурних руйнувань та наслідки, які вони викликали, склали понад 1 трлн дол. США.

Така оцінка була побудована з урахуванням таких факторів: інфраструктурні руйнування, які включають дороги і мости, будівлі (в тому числі, військової інфраструктури); недоотриманий прибуток згідно очікувань підприємств та інвестиції, які не були вкладені в економіку України через воєнні дії, а також їх відтік; втрати, які очікуються через підірвану діяльність великих підприємств, які формували основу ВВП України. Київська школа економіки також провела дослідження щодо збитків, завданих війною з боку Росії, враховуючи при цьому

зниження ВВП, припинення інвестиційних проєктів, відтік за кордон робочої сили, та втрати, спричинені додатковими витратами на оборонний сектор України. Збитки всього за 4 місяці війни склали близько 600 млрд. дол. США.

Задокументовано, що збитки від руйнувань інфраструктури складають близько 100 млрд дол. США, збитки від руйнувань житла – близько 35 млрд дол. США, збитки від руйнувань та ушкоджень інших об'єктів промисловості склали близько 11 млрд. дол. США (особливо слід зазначити втрату таких промислових гігантів, як "Азовсталь" та "ММК Ілліча", які давали 30 % металургійної продукції у ВВП України) [7].

Рис. 1. Збитки, заподіяні повномасштабною війною, оцінка у млрд дол. США*
Джерело: складено на основі [7].

Окремої уваги також заслуговує туристична галузь України, оскільки вона зазнала впливу, перш за все, через закриття повітряного простору. За прогнозами, це спричинить втрати щонайменше у розмірі 14 млрд дол. США у рамках глобальної індустрії авіаперевезень. Також необхідно вносити корективи щодо авіаперевезень між Європою та Азією.

Іншим важливим фактором збільшення втрат туристичної галузі є руйнування або обмеженість доступу до нерухомої культурної спадщини природних туристичних локацій (як, наприклад, Олешківські піски, Асканія-Нова, Кінборська коса, Джарилгач, побережжя Азовського моря (Геніческ і Рожеві солені озера, Кирилівка, Скадовськ, Бердянськ, Очаків, частково Скіфський курган). Мінування моря призводить до неможливості використовувати значну кількість природних туристичних об'єктів, заснованих на водних ресурсах.

Якщо деякий бізнес можна перенести на іншу територію, навіть враховуючи витрати, які для цього потрібні, то аграрний сектор не може бути релоковано через об'єктивні причини, а саме прив'язку діяльності до землі. Тому у діяльності на замінованих територіях неможливо поновити діяльність до завершення самого процесу розмінування. На жаль, в Україні занадто велика кількість об'єктів, на яких потрібне розмінування, однак на ринку України лише декілька учасників, які можуть забезпечити виконання цієї задачі. Це призводить до збитків, пов'язаних із витратами на розмінування, а також із неможливістю своєчасно засіювати землю сільськогосподарськими культурами. Деякі аграрії не мають фінансової можливості розміновувати свої земельні угіддя [9].

Довідка. *Релокація*, або *релокейт* (від англ. слова relocate, relocation – переміщувати, переміщення), – це переміщення бізнесу з однієї країни в іншу. Іншим значенням цього слова може бути переїзд усіх або частини працівників компанії з однієї країни в іншу, або переїзд бізнесу / працівників з одного місця на інше в межах однієї країни.

Потрібно (пропонується) розробити систему надання фінансової допомоги для аграріїв на покриття або часткове покриття витрат процедури розмінування, оскільки збереження аграрного сектору є важливим через необхідність забезпечення продовольчої безпеки на території України, а також підтриманню торгівельних відносин на міжнародному рівні, які наразі є напруженими через заборону на реалізацію української сільськогосподарської продукції у низці країн Європи.

Актуальною для суб'єктів підприємницької діяльності є можливість фіксації збитків, завданих війною згідно з Пам'яткою щодо фіксації збитків [9]. У жовтні 2022 року ця сфера також була доповнена

таким наказом – Методикою визначення шкоди та завданих збитків унаслідок збройної агресії [10]. Окрім збитків, оцінюється також упущена вигода та потреба у відновленні майна задля подальшої діяльності суб'єкта підприємницької діяльності. Проте на ринку існує дуже обмежена пропозиція експертів, які оцінюють такі види втрат [11]. Також складність оцінки полягає в необхідності особисто відвідати об'єкт оцінки, а у випадку, якщо такий об'єкт розташований на території бойових дій або на тимчасово окупованій території, то провести процедуру визначення шкоди та заданих збитків може бути неможливою.

На рис. 2 відобразимо вплив воєнних дій на економічну діяльність суб'єктів господарювання за даними компанії Gradus (Gradus Research).

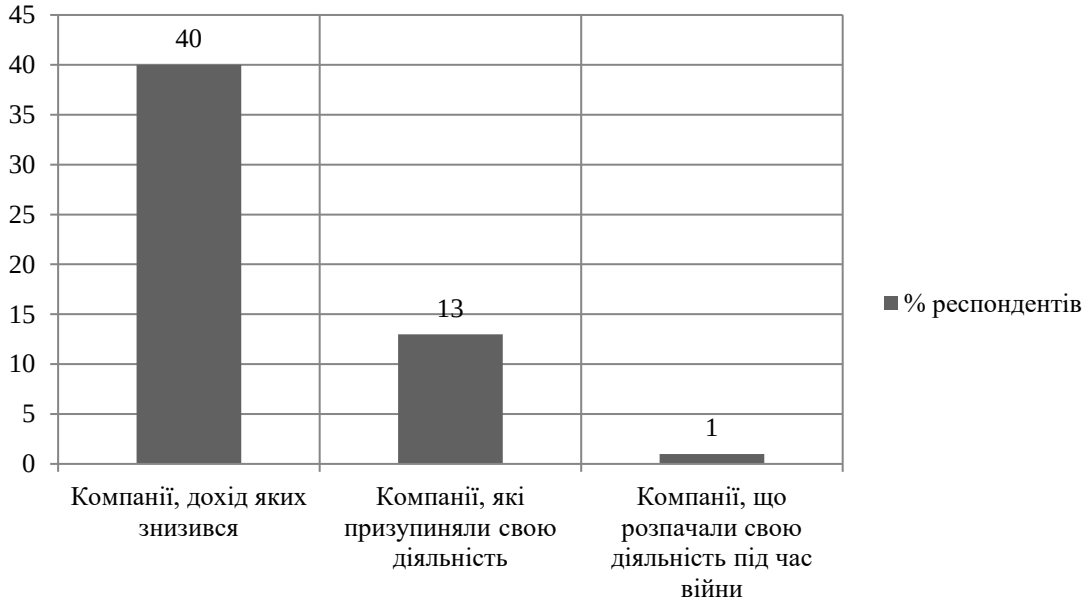


Рис. 2. Вплив на економічну діяльність воєнних дій згідно дослідження компанії Gradus*
Джерело: складено на основі [11]

Було встановлено, що дохід понад 40 % українських підприємств знизився на дві третини, кожна восьма компанія призупиняє свою діяльність (деякі з респондентів відновили свою діяльність), і близько 1 % респондентів дослідження зазначили, що розпочали свою діяльність після початку війни [12]. Найбільш інтенсивно під час війни почали розвиватись компанії галузі IT, будівництва, страхування, оптової та роздрібної торгівлі, комунікаційні послуги [12].

Причиною збільшення витрат діяльності підприємств, що також може стати причиною втрат, є порушення логістичного процесу. Через неможливість забезпечити найбільш оптимальне транспортування продукції, експорт та імпорт не можна здійснювати у великих обсягах. Наприклад, судно здатне перевезти більшу кількість вантажу за невеликих витрат, ніж вантажівка, до того ж, слід враховувати, що не всі дороги призначені для перевезення вантажів та деякі з них зруйновані. Крім того може з'явитись необхідність прокладати новий маршрут, з урахуванням очікування під час комендантської години. Відчутних проблем зазнав бізнес у аграрній, енергетичній, металургійній та логістичній сферах.

Підприємство не має змоги вплинути на шкоду, яку завдає війна, однак необхідною є адаптація бізнес-процесів. Ефективним бізнес-процесом можна назвати той, який передбачає наявність альтернатив, чіткі сценарії та умови вибору альтернативи, інструменти вибору альтернативи, визначення цілей, заради яких обирається певний сценарій, та їх постійний моніторинг із негайним повідомленням у разі виявлення значних змін. Бізнес-процес має бути розроблений під керівництвом експертів, які мають знання щодо конкретної сфери діяльності, щоб урахувати всі ризики та виключити випадки, коли усі альтернативи побудовані на тій самій основі.

Висновки. Можна дійти висновку, що неможливо встановити точну цифру збитків та втрат, заподіяних воєнними діями, оскільки прогнозування втрат може відрізнятися за методом, здійснюваним різними закладами, різними експертами. Наразі на зменшення показників діяльності підприємств впливають дуже багато факторів: руйнування в результаті

бойових дій, відтік кадрів за кордон, зменшення доходів населення, яке не є платоспроможним і не може придбати деякі товари, перебої у логістиці, які не дають змоги швидко доставляти вантажі до місць призначення, обмеженість виробничих ресурсів (дорого купити, тяжко завезти, тяжко організувати безперебійне виробництво під час повітряної тривоги), невизначеність у подальшій економічній (рівень росту інфляції, партнерські зв'язки із закордонними компаніями) та політичній ситуації (будь-яке загострення одразу впливає і на економіку).

Напрямки подальших досліджень. Для пристосування до сьогоденних умов необхідна взаємодія держави та бізнесу. Держава має створювати програми, які зменшать фінансові навантаження на бізнес. Це сприятиме його подальшій діяльності. Зі свого боку, окремі підприємства не мають змоги вплинути на воєнний стан, однак адаптація до сучасних умов дасть змогу наповнювати бюджет держави, з якого, в тому числі, фінансується оборонний сектор України. Стратегічного планування майже не стало, оскільки довгострокове планування не є можливим у мінливому середовищі. Однак створення під керівництвом експерта та забезпечення таких бізнес-процесів, які можуть бути змінені та адаптовані до нових економічних умов, дозволить легше пристосовуватись підприємствам до змін, які кидає їм війна, в тому числі, до збитків та втрат, які можуть бути завдані цим підприємствам. Актуальним напрямом подальших досліджень залишається удосконалення існуючих методик, які стосуються оцінки збитків та руйнувань внаслідок війни для того, щоб їх ефективно використовувати на практиці. Крім цього варто надати пропозиції щодо затвердження на законодавчому рівні відповідальних виконавців та фахівців, які будуть оцінювати збитки в різних напрямках господарювання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бойчук І. Зміни маркетингового функціонування підприємств на B2B ринку // Економічні науки. 2022. № 6, Т. 1. С. 83–87. URL: https://doi.org/10.31891/2307-5740-2022-312-6(1)-12.
2. Захарова Т. Напрямки розвитку туристичного бізнесу України // Економіка та суспільство. 2023. Випуск 49. URL: https://doi.org/10.32782/2524-0072/2023-49-6.
3. Колісніченко Н. Глобальна продовольча криза, спричинена війною в Україні : виклики для управління // Економіка і організація управління. № 2 (46). 2022. С. 8–14. URL: https://doi.org/10.31558/2307-2318.2022.2.1.
4. Приступа М., Неклюєнко Т., Луцкевич Н. Соціально-демографічна криза в Україні внаслідок війни: стан, наслідки та шляхи подолання // Вісник Луганського національного університету імені Тараса Шевченка : Педагогічні науки. 2022. № 6 (354). С. 147–152. URL: https://doi.org/10.12958/2227-2844-2022-6(354)-147-152.
5. Бур'яченко О. Відновлення України через діалог усіх українців світу. Об'єднавшись – зробити неможливе, всупереч усьому! // Укрінформ. 2022. 1 листоп. URL: https://www.ukrinform.ua/rubric-ato/3605567-vidnovlenna-ukraini-cerez-dia-log-usih-ukrainciv-svitu-obednavsis-zrobiti-nemozlive-vsuperec-usomu.html.
6. Оцінка від війни. BDO Україна. URL: https://www.bdo.ua/uk-ua/services-2/consulting/valuation-practice/war-damage-assessment.
7. Зануда А. Зростання цін та діра в бюджеті. Як виживає Україна під час війни. 2022. URL: https://www.bbc.com/ukrainian/features-61594911.
8. Офіційний сайт Державної служби статистики України. URL: https://www.ukrstat.gov.ua/.
9. Пам'ятки щодо фіксації збитків. URL: https://boi.org.ua/upload/ya/4o/pam'yatka%20cshodo%20fiksaciyi%20zbitkiv%20boc%20pravo%20justice.pdf.
10. Про затвердження Методики визначення шкоди та обсягу збитків, завданих підприємствам, установам та організаціям усіх форм власності внаслідок знищення та пошкодження їх майна у зв'язку із збройною агресією Російської Федерації, а також упущеної вигоди від неможливості чи перешкод у провадженні господарської діяльності : наказ Міністерства економіки України від 18.10.2022 № 3904/1223. URL: https://zakon.rada.gov.ua/laws/show/z1522-22#Text.
11. Бізнес на деокупованих територіях. Життя чи виживання? 2023. URL: https://www.epravda.com.ua/columns/2023/04/7/698878/.
12. Релокація бізнесу: скільки підприємств уже поновили роботу. URL: https://www.epravda.com.ua/news/2022/08/17/690505/.

Стаття надійшла до редакційної колегії 19.09.2023

Study of the impact of military actions on the national economy of Ukraine: actual damage and loss

Annotation

The hostilities and bombardment of the territory of Ukraine affect all spheres of people's lives, including the economic one. Destruction of or damage to business facilities leads not only to the costs required to restore the facility, but also to losses from downtime and non-renewable resources. The level of tax revenues to the state budget, which are then redistributed to the defense sector, depends on the efficiency of business entities.

The purpose of the article is to assess losses, destruction and damage and to analyze the impact of hostilities on the economic activity of economic entities.

It is documented that losses from infrastructure destruction amount to about USD 100 billion. The losses from the destruction of infrastructure amounted to about USD 100 billion, losses from the destruction of housing - about USD 35 billion. Losses from the destruction and damage to other industrial facilities amounted to about USD 11 billion. The loss of such industrial giants as Azovstal and Ilyich Iron and Steel Works, which accounted for 30% of Ukraine's GDP, is particularly noteworthy.

The article analyzes the change in Ukraine’s GDP according to the State Statistics Service of Ukraine. It should be noted that the efficiency of enterprises decreased in 2022 compared to 2021. Even despite the crisis caused by the coronavirus in the global economy, Ukraine’s economy suffered less than a year after the war. The inflation rate has been taken into account: according to the Ministry of Finance, the consumer price index was 126.6% in 2022. This indicates that Ukraine’s real GDP in 2022 will be significantly lower than the nominal GDP.

The company cannot influence the damage caused by the war, but it is necessary to adapt business processes. An effective business process is one that provides for alternatives, clear scenarios and conditions for choosing an alternative. A business process should be developed under the guidance of experts who have knowledge of a particular field of activity in order to take into account all risks and exclude cases where all alternatives are built on the same basis.

Keywords: business process; reimbursement; military actions; losses; damages; lost profits; business entities.

УДК 519.85 004.42 DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/80-86

Галаган В. І., кандидат військових наук, доцент (0000-0001-9578-0895)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Порядок та особливості оцінювання стану проєкту створення інформаційних систем військового призначення

Резюме. У статті розглядаються питання щодо визначення особливостей методики затратно-часових показників під час розроблення інформаційних систем військового призначення та надання пропозицій щодо її використання для підготовки та ведення проєктів інформатизації у Збройних Силах України.

Ключові слова: створення інформаційних систем; методика затратно-часових показників; ведення проєкту інформатизації.

Постановка проблеми. У сучасних умовах силового протистояння наявна ресурсна база Збройних Сил (ЗС) України не гарантує достатнього рівня готовності до виконання завдань за призначенням, якщо ресурсний потенціал не буде раціонально організований. Глобальні виклики та потреби спонукають ЗС України постійно створювати, адаптувати та впроваджувати нові або удосконалювати існуючі технології для утримання та розширення необхідних спроможностей.

Зазначене потребує від ЗС України використання інформаційних систем, як елементу передових технологій, і швидкого їх розроблення (завершення) без втрати належної якості. Тому, важливою складовою ведення проєктів інформатизації є система контролю за процесом ведення проєктів, яка базується на методиках оцінювання стану розроблення та ведення проєкту інформатизації.

З отриманого досвіду, під час практичної роботи з'ясовано, що методи оцінки стану проєктів у цивільному секторі не повною мірою підходять для оцінювання, оскільки, в основному, спрямовані на отримання прибутку або збільшення виробництва продукції (товарів).

Проблема визначення порядку та особливостей застосування методики затратно-часових показників під час розроблення інформаційних систем військового призначення полягає у відсутності єдиного розуміння та використанні різних підходів до її застосування. Це, як правило, призводить до великих часових затримок реалізації проєкту, або його повної зупинки.

Аналіз останніх досліджень та публікацій. На сьогодні в більшості фахових публікацій [1–4] з розроблення та впровадження інформаційних систем не має чіткого поняття щодо порядку вибору та застосування методик для оцінювання стану ведення проєктів інформатизації. Широкий набір методик, таких як: оцінювання за аналогіями раніше проведених проєктів, оцінювання за параметрами (параметричне оцінювання), оцінювання за 3-ма точками (аналітичний метод, який використовує три оцінки вартості або тривалості, що відображають оптимістичний, найбільш імовірний і песимістичний сценарії та застосовується для підвищення точності оцінок вартості або тривалості, коли вихідний елемент операції або вартості неясний), експертне оцінювання здебільшого мають низку недоліків – невисоку точність і значний час для виконання розрахунків.

У роботах [5–7] надаються тільки основні положення методики затратно-часових показників та можливі загальні напрями її використання, а проведений аналіз застосування є більш декларативним та повною мірою не деталізує її особливостей. Тим більше, що зовсім не розглядаються порядок та особливості застосування методики для проєктів інформаційних систем військового призначення.

Таке положення викликає необхідність визначення порядку та виявлення особливостей застосування методики затратно-часових показників під час розроблення інформаційних систем військового призначення та врахування їх в процесі підготовки та ведення проєктів інформатизації.

Метою статті є визначення порядку та виявлення особливостей застосування методики затратно-часових показників під час розроблення інформаційних систем військового призначення та надання пропозицій щодо її використання для підготовки та ведення проєкту інформатизації.

Виклад основного матеріалу. Одним з основних завдань керівного складу ЗС України та команди проєкту щодо управління проєктом інформатизації є контроль за загальним веденням проєкту на основі обґрунтованих показників та коригування (у разі необхідності) його ходу шляхом реалізації відповідних управлінських рішень. Водночас контроль за веденням проєкту має враховувати не тільки стан проєкту на контрольну дату, а і можливість прогнозування подальших відхилень реалізації проєкту інформатизації за визначеними показниками. Прогнозування стану проєкту в часі дасть змогу вирішувати проблемні питання не по мірі їх виникнення, а з передбаченням їх появи – для ліквідації та врахування у подальшій діяльності.

Ураховуючи, що основні критерії спроможності будь-якого проєкту (зокрема і проєкту інформатизації) залежать від трьох важливих чинників (змісту, обмежень і ризиків) найбільш простою та ефективною є відома світова методика оцінки затратно-часових показників ведення проєктів інформатизації (Cost/Schedule Control Systems Criteria (C/SCSC)) [7].

Довідка. За допомогою цієї методики є можливість контролювати виконання проєкту за двома найважливішими критеріями – термінами та ресурсами. Центр логістики ВПС США в Оклахомі (перша державна організація США, сертифікована в 1996 р. за четвертим рівнем моделі CMMI *(Capability Maturity Model Integration)* (включає атестат зрілості (із п'яти можливих), що свідчать про досягнуту якість процесу розроблення проєктів), що налічує 600 співробітників, використовує цю методику з 1985 р., і за 15 років у жодному зі своїх проєктів не перевищив терміни і ресурси. Серед його проєктів – створення системи управління зброєю для бомбардувальників B-1 і B-2.

Загалом, методика затратно-часових показників ведення проєктів ґрунтується на широковідомих мережевих моделях планування та управління проєктами (PERT/Cost-методі аналізу затрат, принципах декомпозиції робіт), а також розробленні різних сценаріїв ведення проєктів, що дає змогу оцінити стан ведення проєкту на рівні окремих операцій або груп операцій на початкових та наступних етапах реалізації проєкту. У межах концепції затратно-часових показників стан може бути оцінений як на рівні різних етапів, так і окремих операцій проєкту на основі: співвідношення обсягу запланованих і виконаних робіт щодо реалізації проєкту, а також запланованих та фактичних витрат на реалізацію проєкту.

Для дієвого контролю робіт, що виконуються за проєктом, спочатку необхідно визначити та знати можливості й завантаженість персоналу, що залучається до створення інформаційної системи військового призначення, розробити план робіт детально за кожним співробітником, визначити вартість кожного етапу робіт та методи обчислення затрат. Відповідно, тоді у загальному випадку обсяг проєкту інформаційної системи військового призначення буде характеризуватися його бюджетом.

До вхідних даних методики віднесено показники, які наведені у Табл. 1.

На основі вхідних даних проводиться розрахунок значень відхилень проєкту від планових. До ***показників відхилення*** віднесено:

Відхилення за обсягом робіт (ВП(t)). Дає змогу визначити на скільки проєкт відстає або випереджає графік планових робіт. Розраховується за формулою

$$ВП(t) = ОО(t) - ПО(t), \qquad (4)$$

де *ПО(t)* – запланований обсяг робіт за базовою вартістю, що відображені в календарному плані виконання проєкту на момент часу (t).

Знак "–" (від'ємне значення) *ВП(t)* означає, що проєктні роботи затримуються відповідно до планових термінів. У разі знаку "+" (позитивне значення) означає, що виконані проєктні роботи випереджують планові терміни.

Відхилення за вартістю ВВ(t). Показник відхилення фактичної вартості виконаних робіт від планової вартості на момент часу (t). Дає змогу визначити, на скільки бюджет проєкту перевищує або не досягає запланованої вартості, тобто чи вкладається проєкт в бюджет або виходить за нього. Розраховується за формулою

$$ВВ(t) = ОО(t) - ФВ(t). \qquad (5)$$

Знак "–" (від'ємне значення) означає, що проєкт перевищує запланований бюджет. У разі знаку "+" (позитивне значення) означає, що відбувається економія бюджету у процесі ведення проєкту.

За допомогою показників розраховуються індекси, які характеризують стан розроблення інформаційної системи. До *основних індексів* віднесено:

Індекс виконання плану розроблення проєкту ІВП(t). Показує хід виконання

проєкту та заходів за графіком, запланованим для цього проєкту.

Цей індекс показує відношення фактичного стану проєкту (тобто кількості виконаних робіт) до планового на конкретний момент часу t. Розраховується за формулою

$$ІВП(t) = ОО(t) / ПО(t). \quad (6)$$

Якщо індекс дорівнює 1, то це означає, що проєкт відповідає графіку, запланованому для нього. Якщо менше 1, то проєкт відстає від запланованого графіку, а якщо більше 1, то проєкт випереджає запланований графік.

Таблиця 1

Вхідні дані методики оцінки затратно-часових показників

	Показники	Тлумачення (фізичний зміст)	Джерело
1.	Бюджет проєкту $БП$	Показник запланованої вартості проєкту на його завершення. Використовується для визначення загальної вартості проєкту, яка була визначена на етапі планування проєкту, і відображає вартість усіх ресурсів, які будуть витрачені на проєкт	Календарний план проєкту інформатизації
2.	Планові обсяги проєкту $ПО(t)$	Показує запланований обсяг робіт на момент часу t. Визначається як $$ПО(t) = \sum_{i=1}^{N_1} БВ_{робіт}(t), \quad (1)$$ де $БВ_{робіт}$ – бюджетні вартості робіт, які мають бути виконані на момент часу *(t)* відповідно до календарного плану проєкту; N_1 – кількість робіт, які мають бути виконані на момент часу *(t)*	Календарний план проєкту інформатизації, проведений розрахунок
3.	Освоєні обсяги проєкту $ОО(t)$	Реально виконаний обсяг робіт від запланованого вказаний у плановому бюджеті проєкту на момент часу (t): $$ОО(t) = БП \times (P_{викр}(t) / 100), \quad (2)$$ де $БП$ – бюджет проєкту; $P_{викр}(t)$ – відсоток реально виконаних робіт за календарним планом проєкту на момент часу (t). Визначається керівником проєкту шляхом перевірки виконання календарного плану проєкту	Календарний план проєкту інформатизації, отримані контрольні дані на момент часу t, проведений розрахунок
4.	Фактична вартість виконаних робіт $ФВ(t)$	Реальна вартість виконаних робіт на момент часу (t). Визначається як $$ФВ(t) = \sum_{i=1}^{N_2} РВ_{робіт}(t), \quad (3)$$ де $РВ_{робіт}$ – реальна вартість робіт, які виконані на момент часу *(t)* відповідно до календарного плану проєкту; N_2 – кількість робіт, які виконані на момент часу *(t)*	Отримані контрольні дані на момент часу t, проведений розрахунок

Індекс виконання вартості проєкту $ІВВ(t)$. Показує продуктивність витрат на проєкт, та вимірює рівень використання коштів на проєкті.

Розраховується за формулою

$$ІВВ(t) = ОО(t) / ФВ(t). \quad (7)$$

Якщо $ІВВ(t)$ дорівнює 1, то це означає, що реальні витрати на проєкт дорівнюють запланованим витратам. Якщо менше 1, то реальні витрати на проєкт перевищують заплановані витрати, а якщо більше 1, то реальні витрати на проєкт менше запланованих.

До **прогнозних показників** віднесено:

Прогнозована тривалість проєкту (ПТП(t)). Цей показник дає змогу оцінити час, який залишився для завершення проєкту, враховуючи фактичні витрати на даний момент часу і прогнозовані витрати на майбутнє. Використовується для прогнозування терміну, коли проєкт буде завершено, а також для планування ресурсів і контролю за виконанням проєкту. Розраховується за формулою

$$ПТП(t) = \frac{ПлТр}{ІВП(t)}, \quad (8)$$

де $ПлТр$ – планова тривалість проєкту, яка була встановлена в затвердженому календарному плані на його початок.

Якщо значення *ПТП(t)* виявляється більшим за плановану тривалість проєкту (визначена в календарному плані) це означає, що проєкт затримується, і необхідно знайти методи і способи скоротити час виконання робіт. Якщо значення є меншим за плановану тривалість проєкту, то проєкт може бути завершений раніше запланованого терміну.

Прогнозована тривалість проєкту дає змогу керівнику та команді проєкту коригувати плани, щоб досягти заплановані цілі у встановлені терміни з використанням необхідних ресурсів.

Прогнозована вартість проєкту (ПВП(t)). Показує прогнозовану суму витрат, яку потрібно буде витратити для завершення проєкту, враховуючи фактичні витрати та прогнозовану вартість залишкової роботи за проєктом. Розраховується для розуміння того, чи буде проєкт завершений за запланованою вартістю.

Розраховується за формулою

$$ПВП(t) = БП / ІВВ(t). \qquad (9)$$

Для перевірки працездатності методики проведено тестовий розрахунок на даних максимально наближених до реального стану.

Умови. Припустимо, що проєкт полягає у розробленні окремого програмного продукту (інформаційної системи). Для простоти та точності розрахунків приймемо, що проєкт складається з одного завдання.

На виконання проєкту виділено 10 виконавців, визначено обсяг робіт та терміни розроблення: планові працевитрати склали 160 людино-годин.

Виконавці працюють над завданням 100 % свого робочого часу (враховуємо 8-годинний робочий день), а вартість людино-години – дорівнює 10$.

Отже, бюджет проєкту складатиме 1600$.

Визначений і погоджений з виконавцем термін розроблення проєкту дорівнює двом дням (16 годин робочого часу).

Припустимо, що завдання стартує в понеділок, і в середу замовник та керівник проєкту розраховують отримати очікуваний результат щодо розроблення програмного продукту.

Стан робіт на кінець понеділка.

Розрахунок робочого часу за понеділок склав 80 годин за завданням, за планом на вівторок складе 80 годин.

Припустимо, що, за фактом виконаних робіт на кінець понеділка (відповідно до календарного плану виконання робіт проєкту), виконавці не встигли виконати запланований обсяг робіт. Зрозуміло, що за вказаний термін завершити розроблення не вдасться, та за попередніми розрахунками керівника проєкту необхідно буде використати ще 20 людино-годин у середу. Загалом, прогнозовані працевитрати на проєкт наведені в Табл. 2.

Таблиця 2

Працевитрати, годин	Понеділок	Вівторок	Середа (прогноз)
План загальний	80	80	0
Фактичні витрати	80	80	20

Проведемо розрахунки для визначення показників характеристик проєкту інформатизації.

Бюджет проєкту *(БП)* – бюджет для завершення проєкту, який фіксується на старті проєкту, як сума затвердженого бюджету на весь проєкт. У тестовому прикладі він дорівнює 1600$.

Планові обсяги *ПО (t)* – запланований обсяг робіт на момент часу (t) – кінець вівторка. У тестовому прикладі *ПО (t)* дорівнює 1600$, оскільки базовий обсяг робіт, який має бути виконаний за дві доби, дорівнює 160 людино-годинам, а базова ціна складає 10$ за годину роботи розробника (формула 1, Табл. 1).

Освоєні обсяги *ОО (t)* – реально виконаний обсяг робіт від запланованого. У тестовому прикладі *ОО (t)* дорівнює 1420$, оскільки *%* виконання за проєкт визначений керівником дорівнює 88 %, а бюджет проєкту становить 1600$ (формула 2, Табл. 1).

Фактична вартість *ФВ (t)* – реальна вартість виконаних робіт за проєктом на кінець вівторка. У тестовому прикладі, *ФВ (t)* дорівнює 1600$, оскільки фактично виконавець витратив 160 годин, а погодинна оплата складає 10$ (формула 3, Табл. 1).

Проводимо розрахунок показників відхилень:

відхилення за обсягом робіт (*Schedule Variance) ВП(t)* (формула 4):

1420$ – 1600$ = –180$;

відхилення за вартістю *(Cost Variance) ВВ(t)* (формула 5):

1420$ – 1600$ = –180$;

індекс виконання плану розроблення *(Schedule Performance Index) ІВП(t)* (формула 6):

1420$ /1600$ = 0,88

100%-88%=12%.

У тестовому прикладі, відставання за термінами виконання проєкту складає 12%.

індекс виконання вартості проєкту (*Cost Performance Index*) *ІВВ(t)* (формула 7):

1420$ /1600$ = 0,88

100%-88%=12%.

У тестовому прикладі, перевищення бюджету складає 12%.

прогнозована тривалість проєкту (*Time Estimate at Completion*) *ПВП(t)* (формула 8).

2 робочі дні /0,88 = 2,27 робочих дня.

Тобто, термін реалізації всіх заходів проєкту, а значить і його тривалість складе 2,27 робочих дні.

прогнозована вартість проєкту (*Estimate at Completion*) *ПВП(t)* (формула 9):

1600$ /0,88 = 1800$.

Цей показник показує очікувану загальну вартість проєкту після завершення робіт, що залишилися невиконаними. На даний час, оціночна прогнозована вартість заходів проєкту складає 1800$.

У тестовому прикладі, індекси *ІВТ(t)* та *ІВВ(t)* збіглись, але потрібно розуміти, що так буде не завжди.

Виходячи з результатів тестового розрахунку, можна надати та обґрунтувати наступний прогноз: якщо, заходи календарного плану проєкту виконуватимуться відповідно до фактичних витрат, то бюджет проєкту складатиме 1800$, а термін реалізації всіх заходів проєкту складе 2,27 робочих дні.

Отже, за отриманими результатами тестового розрахунку можна здійснити детальний прогноз щодо збільшення термінів розроблення проєкту та підвищення його вартості.

Порядок застосування методики затратно-часових показників для посадових осіб, які задіяні в розробленні інформаційних систем військового призначення, буде полягати у такому:

1. За планувальними документами проєкту інформатизації визначаються дані щодо *бюджету проєкту* (*БП*) та розраховуються *планові обсяги проєкту* (*ПО(t)*).

2. Відповідно до плану та графіку виконання проєкту інформатизації зацікавленими посадовими особами (замовник, розробник, організація супроводження) проводиться моніторинг ведення проєкту та перевіряються:

дані щодо реально виконаного обсягу робіт від запланованого на певну календарну дату (час), яка визначена в календарному плані проєкту інформатизації та проводиться розрахунок *освоєних обсягів проєкту* (*ОО(t)*);

розраховується реальна вартість виконаних робіт на момент часу *фактична вартість* (*ФВ(t)*).

3. За результатами роботи з планувальними документами та результатами перевірки (планової чи позапланової) отримуються первинні (вхідні) дані з конкретними числовими значеннями (*ПО(t); ОО(t); ФВ(t); БП*).

Довідка. Крім запланованих перевірок ведення проєкту, можливі й позапланові перевірки за умови погодження із розробником.

4. Використовуючи отримані контрольні фактичні значення (первинні дані): проводиться розрахунок відхилень (*ВП(t)*), *ВВ(t)*, індексів (*ІВП(t)* і *ІВВ(t)*). За їх значеннями розраховуємо прогнозні показникі (*ПТП(t)* і *ПВП(t)*) щодо термінів завершення проєкту та витрати ресурсу.

5. На основі проведеного розрахунку за значеннями відхилень та індексів визначаємо:

на скільки проєкт відстає від графіку або випереджує його (за обсягом робіт та часом);

прогнозні показники тривалості проєкту та очікуваний обсяг витрачених ресурсів.

6. За допомогою розрахованих значень посадова особа (замовник, розробник, організація супроводження, керівник проєкту) проводить їх аналіз та робить висновок щодо прийняття обґрунтованого управлінського рішення щодо здійснення певних корегувальних дій і заходів.

Також, необхідно враховувати, що для реалізації великого проєкту інформатизації (до яких можна віднести будь-який проєкт інформатизації військового призначення) доцільно вводити декілька показників, що дає змогу детальніше спланувати графік управління проєктом, простіше та швидше здійснювати реалізацію та контроль проєкту.

Практичний досвід проведення розрахунків під час розроблення проєкту інформатизації військового призначення дав змогу виявити такі **особливості застосування** цієї методики:

1. Застосування методики передбачає, що проєкт виконуватиметься за правилами проєктного менеджменту, тобто як мінімум має бути розроблений календарний план проєкту з детальним графіком виконання робіт та здійснення витрат за проєктом інформатизації. Пропонується використовувати для розроблення базового плану виконання проєкту, наприклад,

шаблони наведені в PMB (*англ. Performance Measurement Baseline*) – Звід знань з управління проєктами);

2. Повноцінно та адекватно проводити розрахунки за цією методикою можливо тільки після того, як буде виконана деяка частина проєкту (за досвідом – близько 15 %–20 %), що дає змогу накопичити достатню статистику про вже виконані заходи. Тоді й показники, що входять у методику, будуть розраховані адекватно та викликатимуть довіру. До даного моменту (отримання повноцінного комплекту вихідних даних для використання цієї методики), пропонується оцінювати виконання початкових заходів ведення проєкту за окремим планом (наприклад, за допомогою спеціалізованого програмного забезпечення для ведення проєктів *Microsoft Project*, що використовує діаграму Ганта – планування та контроль задач. Кожна смуга на діаграмі представляє окрему задачу у складі проєкту (вид роботи), її кінці – моменти початку та завершення роботи, її довжина – тривалість роботи. Вертикальною віссю діаграми є список завдань. Крім того, на діаграмі можуть бути відзначені сукупні завдання, відсотки завершення, покажчики послідовності та залежності робіт, мітки ключових моментів (віхи);

3. Витрати за проєктом інформатизації, як правило, можуть бути розділені на прямі видатки (вартість заходів проєкту, заробітна плата), які оцінюються за допомогою призначення і вартісної оцінки ресурсів, необхідних для виконання заходів (робіт) і накладні видатки (господарчі, обслуговування, організація робіт), які не можуть бути співвіднесені з тими чи іншими заходами проєкту. У розрахунках методика передбачає тільки прямі видатки на проведення заходів (робіт) відповідно до базового плану проведення проєкту інформатизації.

Таким чином, за отриманими значеннями показників, індексів та прогнозних значень методики оцінки затратно-часових показників є можливість з'ясувати сутність проблеми, яка, як правило зводиться до перевищення бюджету або порушенню термінів завершення проєкту інформатизації. Використовуючи цю методику зацікавлені особи проєкту зможуть швидко визначити основні проблемні моменти під час ведення проєкту інформатизації, сформувати обґрунтовані управлінські рішення та здійснити корегування базового календарного плану проєкту.

Висновки. Отже, методика оцінювання затратно-часових показників ведення проєктів інформатизації з урахуванням наданого порядку її використання та виявленими особливостями застосування дає змогу адекватно і достовірно оцінювати стан ведення проєкту, прогнозувати подальший його розвиток. Методика може бути використана керівним складом ЗС України (проєктною групою) для прийняття управлінських рішень щодо обґрунтованого коригування календарного плану проєкту інформатизації.

Подальші дослідження за даною тематикою доцільно зосередити на питаннях удосконалення контролю за процесом виконання робіт під час управління проєктами інформатизації військового призначення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Маматова В. Управління проєктами : навч. посіб. Київ : ДРІДУ НАДУ, 2018. 215 с.
2. Гудкова К. Методи та підходи до оцінки ефективності ІТ-проєктів // Економічний вісник Донбасу. 2016. № 3 (45). С. 193–196.
3. Гриценко В. Методологія впровадження інформаційно-аналітичних систем. URL: https://lib.iitta.gov.ua/706322/1/202016.pdf (дата звернення: 02.01.2023).
4. Проектування інформаційних систем. URL: https://ela.kpi.ua/bitstream/123456789/33651/1/PIS_KL.pdf (дата звернення: 02.01.2023).
5. Колосова Е. Методика освоенного объёма в оперативном управлении проектами. URL: https://www.researchgate.net/publication/274390518_Metodika_osvoennogo_obema_v_operativnom_upravlenii_proektami (дата звернення: 02.01.2023).
6. Хігні Д. Основи управління проєктами. Київ : Фабула, 2020. 262 с.
7. Хелдман К. Профессиональное управление проєктом. Киев : Бином. Лаборатория знаний, 2005. 261с.

Стаття надійшла до редакційної колегії 17.01.2023

The procedure and features of assessing the status of projects for creating military information systems

Annotation

In the current conditions of military confrontation, the existing resource base of the Armed Forces of Ukraine (AFU) does not guarantee a sufficient level of readiness to perform assigned tasks if the resource potential is not rationally organized. Global challenges and needs prompt the Armed Forces of Ukraine to constantly create, adapt and implement new or improve existing technologies to maintain and expand the necessary capabilities. The above requires the Armed Forces of Ukraine to use information systems as an element of advanced technologies and requires their rapid development (completion) without losing proper quality. Therefore, an important component of informatization projects is a project management system based on methods for assessing the status of development and management of an informatization project.

The article discusses the issues of determining the features of the methodology of cost and time indicators in the development of military information systems. In general, the methodology of cost and time indicators of project management is based on well-known network models of project planning and management (PERT/Cost method of cost analysis, principles of work decomposition), as well as the development of various project management scenarios, which allows to assess the status of project management at the level of individual operations or groups of operations at the initial and subsequent stages of project implementation.

Based on the obtained values of the indicators, it is possible to find out the essence of the problem, which usually boils down to exceeding the budget or delaying the completion of the information project. Using these indicators, project officials will be able to quickly identify the main problematic issues during the course of an information project, formulate sound management decisions, and adjust the basic project plan.

Keywords: creation of information systems; methodology of cost and time indicators; management of an information project.

УДК 004.9.005.95 DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/87-97

Кірпічніков Ю. А., кандидат технічних наук (0000-0001-6893-3569)
Рибидайло А. А., кандидат технічних наук, старший науковий співробітник (0000-0002-6156-469X)
Литовченко Г. Д. (0000-0002-8625-1438)
Бутенко М. П. (0000-0001-7272-5826)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Обґрунтування підходу до удосконалення інформаційної інфраструктури Міністерства оборони України для функціонування в умовах збройної агресії

Резюме. Проведено аналіз підходів до побудови інформаційної інфраструктури Міністерства оборони України, яка має функціонувати в умовах збройної агресії. Обґрунтовано порядок модернізації існуючої інформаційної інфраструктури Міністерства оборони України з урахуванням використання сучасних ІТ-технологій.

Ключові слова: інформаційна інфраструктура; модель життєвого циклу; інформаційна система; каскадна, інкрементна, еволюційна стратегії; верифікація; валідація.

Постановка проблеми. В умовах воєнно-політичної кризи та збройної агресії проти України, її державним інститутам, зокрема Міністерству оборони (МО) України, належить виробити і застосувати нові сучасні підходи до розвитку власного інформаційного простору, забезпечення його стійкості та безпеки. Одним із пріоритетних напрямів є цифровізація діяльності та впровадження сучасних інформаційних технологій у сфері оборони для оперативного забезпечення посадових осіб різних рівнів управління Збройними Силами (ЗС) України певними комунікаційними, інформаційними та специфічними за напрямами їх діяльності функціональними сервісами [1]. Ці сервіси має реалізовувати інформаційна інфраструктура, головними вимогами до якої є надійність та безперервність надання якісних сервісів, кібернетична безпека тощо.

Довідка. *Інформаційна інфраструктура* (у загальному розумінні) – сукупність інформаційних (автоматизованих) систем, інформаційних ресурсів, електронних комунікаційних мереж, організаційно-технічних структур, механізмів, що забезпечують їх функціонування [2].

Інформаційна інфраструктура МО України – комплексна структура, яка об’єднує програмно-технічні засоби, організаційні заходи, нормативні документи, персонал та забезпечує функціонування, розвиток інформаційної взаємодії та інформаційного середовища МО та ЗС України [3].

Проблемним питанням є той факт, що інформаційна інфраструктура МО України перебуває на початку свого оновлення, а окремі теоретичні дослідження не охоплюють всього циклу її розвитку. Особливостями розвитку інформаційної інфраструктури на сучасному етапі є високий рівень уніфікації апаратних, зокрема обчислювальних засобів (інфраструктура як сервіс), системного програмного забезпечення (базових сервісів), впровадження різного за призначенням прикладного спеціального програмного забезпечення (функціональних сервісів). У зв’язку з цим необхідно визначити шляхи забезпечення якості як самих сервісів, так і своєчасність та безперервність їх надання. Забезпечення належної якості сервісів є динамічною задачею, складність якої пропорційна завданням та вимогам до інформаційної інфраструктури і, відповідно, до програмно-апаратного обладнання інформаційних систем і мереж, на базі якого побудовані ці системи.

Вирішення цієї задачі полягає в інтеграції програмного забезпечення та обладнання в інформаційні системи, які існують або створюються, та узгодження їх повноцінного використання для досягнення запланованих переваг від провадження цих змін. Нагальною вбачається задача аналізу сучасних підходів щодо удосконалення інформаційної інфраструктури МО України, визначення технологічних підходів та організаційно-технічних заходів із забезпечення її надійного функціонування для забезпечення гарантованого надання якісних сервісів у будь-яких несприятливих умовах. Особливої значимості означене завдання набуває в умовах збройної агресії.

Аналіз останніх досліджень і публікацій. Сучасні підходи щодо розбудови інформаційної інфраструктури розглядаються у багатьох джерелах, зокрема у [4–12], де висвітлюються:

сутність основних підходів до створення інформаційної інфраструктури, їх основні переваги і недоліки;

базові стратегії застосування відомих підходів до розроблення інформаційної інфраструктури;

основні переваги застосування хмарних технологій для надання сервісів;

основні переваги, недоліки і умови застосування блокчейну для забезпечення безпеки, прозорості та надійності даних і транзакцій.

Особливе значення для критично важливих інформаційних систем та сервісів має поняття живучості системи. У роботі [12] розглянуті питання аналізу живучості інформаційних систем і мереж в умовах деструктивних інформаційних впливів, наведена класифікація інформаційних атак в інформаційних мережах та методи їх виявлення.

Довідка. *Живучість* – здатність комп'ютерної (комп'ютеризованої) системи (КС) виконувати задані специфікацією функції при зміненні нормальних зовнішніх умов функціонування на більш жорсткі, навіть за наявності елементів і складових частин, що перебувають у стані відмови, не допускаючи їх переходу у критичні відмови, поки не досягнуто граничного стану [13].

У роботах [14–16] представлено методи забезпечення живучості інформаційно-комунікаційної мережі на основі перерозподілу ресурсів мережі, використання механізмів резервування, реорганізації та реконфігурації для обслуговування потоків вимог у разі виникнення несприятливих впливів. Розглянуті методи дають змогу оцінити інформаційно-комунікаційної мережі та підвищити час її життя. Проте факторів, які враховуються, недостатньо для повноцінного оцінювання якості сервісів і стану інформаційної інфраструктури.

Як показав аналіз, підходи щодо забезпечення функціонування інформаційної інфраструктури, та попередження усіх видів несприятливих впливів ще недостатньо розвинуті. В означених джерелах систематизований аналіз використання відомих підходів та сучасних інформаційних технологій до створення інформаційної інфраструктури в умовах збройної агресії не наведено Це являє собою важливу наукову проблему системного характеру, яка потребує комплексних наукових і прикладних досліджень. Тому актуальною є задача суттєвого підвищення рівня живучості інформаційної інфраструктури, її ефективності та працездатності за рахунок оптимізації її структури, введення надлишкових (апаратних, програмних, часових та ін.) засобів покращання показників відмовостійкості та зниження складності структури таких систем.

Мета статті – обґрунтування рекомендацій щодо шляхів удосконалення інформаційної інфраструктури Міністерства оборони України з урахуванням можливостей новітніх ІТ-технологій для забезпечення її функціонування та надійного застосування в умовах збройної агресії.

Виклад основного матеріалу. Аналіз досвіду забезпечення функціонування інформаційної інфраструктури МО України в контексті збройної агресії, окупації частини території країни та ведення бойових дій виявив низку основних вимог:

можливість швидкого розгортання та надання сервісів, розширення їх функціональності, масштабування, відповідно до значного зростання інформаційних потреб органів військового управління;

створення єдиного інформаційного простору для всіх його учасників, не зважаючи на розосереджене розгортання військ на територіях, розділених силами супротивника, мобільність підрозділів і частин та високу динаміку переміщень угруповань військ у цілому;

забезпечення швидкого надання сервісів безпосереднім учасникам бойових дій (рівнів батальйон – рота – взвод – окремий солдат), у тому числі за допомогою мобільних пристроїв по будь-яким каналам зв'язку;

забезпечення стійкості інформаційної інфраструктури для гарантованого надання сервісів, враховуючі можливість ураження окремих її елементів як кінетичною зброєю, так і шляхом проведення кібератак.

Умови збройної агресії можуть серйозно впливати на функціонування інформаційної інфраструктури МО України. Деякі з основних чинників, які можуть впливати на забезпечення функціонування інформаційної інфраструктури (ІнфІ) в умовах збройної агресії наведені у Табл. 1.

Таблиця 1

Чинники збройної агресії, які впливають на функціонування інформаційної інфраструктури

№	ЧИННИКИ	НАСЛІДКИ ВПЛИВУ
1	***Фізичне пошкодження ІнфІ***	Фізичне пошкодження інформаційних мереж, комп'ютерів, серверів та інших пристроїв, які є складовими частинами ІнфІ
2	***Відключення від мережі***	Відключення від мережі операторів електронних комунікацій, хостинг-провайдерів та інших постачальників послуг, що може призвести до відключення частини ІнфІ
3	***Вразливість мережевої безпеки***	Зростання рівня кіберзагроз: кібератаки, хакерські атаки та віруси, що можуть порушити функціонування ІнфІ та зашкодити їй
4	***Втручання в управління***	Може включати: блокування доступу до деяких вебсайтів та інших дій, що можуть обмежити доступ до інформації та вплинути на функціонування ІнфІ
5	***Недоступність ресурсів***	Відсутність електропостачання та доступу до Інтернету/Інтранету окремих складових ІнфІ може обмежити повноту її функціонування
6	***Нехватка кваліфікованих кадрів***	Відтік кваліфікованих ІТ-спеціалістів може призвести до нестачі кваліфікованих кадрів для підтримки ІнфІ

Одним із перспективних шляхів розвитку інформаційної інфраструктури є використання сучасних потужних програмно-апаратних платформ, сховищ даних з використанням блокчейн-технології, засобів віртуалізації обчислювальних та мережевих ресурсів, а також хмарних технологій.

Побудова інформаційної інфраструктури для оборонних потреб може бути реалізована за допомогою різних підходів, які наведені у Табл. 2.

Таблиця 2

Підходи до реалізації інформаційної інфраструктури

№	ПІДХОДИ	ТЛУМАЧЕННЯ	ВИКОРИСТАННЯ
1	***Централізований***	Уся інформація зберігається в єдиній централізованій базі даних (центр обробки даних), яка забезпечує доступ до інформації всім зацікавленим сторонам у реальному часі	Великі організації та органи управління
2	***Децентралізований***	Кожний підрозділ має власну базу даних (центр обробки даних), яка зберігає інформацію, необхідну для виконання своїх завдань	Організації, де різні підрозділи мають спеціалізовані функції
3	***Гібридний***	Використовуються елементи як централізованого, так і децентралізованого підходів	Територіальна розгалуженість споживачів
4	***Датацентричний***	Усі компоненти інфраструктури мають бути побудовані навколо датацентру та підкорятися його вимогам і потребам, що дає змогу досягти оптимальної ефективності, надійності та безпеки роботи інфраструктури	Дозволяє забезпечити оптимальний рівень обробки і зберігання даних та досягти високої надійності і безпеки роботи інфраструктури
5	***Хмарний***	Інформаційна інфраструктура реалізується на основі сервісів, які надаються приватною хмарою або хмарними провайдерами	Необхідність високої гнучкості та масштабованості
6	***З використанням блокчейну***	Інформація зберігається в розподіленій мережі вузлів, які забезпечують високий рівень безпеки та захисту даних	Необхідність високого рівня безпеки та конфіденційності даних

Аналіз сучасного стану інформаційної інфраструктури МО України показує, що здебільшого їй притаманно використання децентралізованого підходу. Завдання щодо інтеграції окремих інформаційних ресурсів, інформаційних, інформаційно-аналітичних систем та автоматизованих систем управління військами та зброєю не ставилось. *Децентралізований підхід під час побудови інформаційної інфраструктури* базується на використанні розподілених систем, які не залежать від єдиного центру управління та мають можливість забезпечувати працездатність та безпеку інформаційної інфраструктури в умовах обмеженого зв'язку та доступності до ресурсів. Децентралізовані системи можуть забезпечувати високу швидкість та надійність передачі даних й

доступу до цих даних, що є особливо важливим в умовах збройної агресії. Однак слід враховувати, що децентралізовані системи потребують великих витрат на їх розроблення, впровадження та підтримку. Такі системи можуть бути більш складними у використанні для звичайних користувачів, що може потребувати додаткового навчання та підтримки. Крім того, децентралізовані системи можуть бути більш уразливими до атак, оскільки вони не мають єдиного центру управління, який міг би забезпечити захист від зломів та атак хакерів. Для забезпечення безпеки необхідно використовувати спеціальні технології та протоколи. Варто зазначити, що в децентралізованих системах необхідно встановити чіткі правила та процедури для прийняття рішень та вирішення конфліктних ситуацій, оскільки відсутність централізованого управління може призвести до неузгоджених дій та неефективного використання ресурсів.

Отже, для створення сучасної інформаційної інфраструктури доцільно більш детально розглянути підходи, які передбачають *інтеграцію інформаційних ресурсів МО України*, а саме: централізований, гібридний та датацентричний підходи.

Централізований підхід до побудови інформаційної інфраструктури в умовах збройної агресії передбачає, що всі інформаційні (інформаційно-комунікаційні) системи, електронні комунікаційні мережі та інформаційні ресурси керуватимуться централізовано. Це означає, що всі рішення, налаштування та зміни, що приймаються, здійснюватимуться центральним органом управління, який контролює всі аспекти інфраструктури.

Такий підхід має нозку переваг в умовах збройної агресії, коли інформаційна інфраструктура може бути схильна до руйнування або злому. Централізований підхід дає змогу створити більш надійний захист інформації та швидше реагувати на будь-які інциденти, пов’язані з безпекою, краще контролювати доступ до інформації та її використання, а також реагувати на можливі загрози. Перевагою централізованого підходу є можливість оптимізації використання ресурсів та забезпечення рівномірного доступу до інформації. В умовах збройної агресії це особливо важливо, оскільки необхідно забезпечити швидке та ефективне прийняття рішень, що може бути досягнуто лише за наявності доступу до актуальної та достовірної інформації. Ще однією перевагою централізованого підходу є простіше адміністрування складових інформаційної інфраструктури, оскільки всі ресурси знаходяться під контролем центрального вузла. Це дає змогу забезпечити єдиний рівень сервісів та підтримки користувачів, а також швидкого реагування на проблеми та збої в роботі.

Однак такий підхід також має свої недоліки. При централізованому підході необхідно враховувати ризики, пов’язані з єдиною точкою відмови, тобто якщо центральний вузол вийде з ладу, вся інформаційна інфраструктура може стати недоступною. Це може призвести до затримки надання сервісів і, як наслідок, несвоєчасного прийняття управлінських рішень. Крім того, у разі відключення центрального вузла вся інформаційна інфраструктура може стати недоступною.

Під час використання централізованого підходу в умовах збройної агресії необхідно забезпечити ефективне управління та контроль за всіма системами та ресурсами. Це можна досягти через впровадження систем моніторингу та управління, які дають змогу швидко реагувати на можливі проблеми та усувати їх.

Важливим аспектом централізованого підходу є також навчання та підготовка персоналу, який керуватиме всіма системами та ресурсами. Необхідно забезпечити не лише технічну, а й організаційну підготовку персоналу, щоб він міг ефективно працювати в умовах стресу та позаштатних ситуацій.

Ще одним важливим аспектом централізованого підходу в умовах збройної агресії є необхідність постійного оновлення та модернізації систем і ресурсів. Це дасть змогу забезпечити належний рівень функціональності, безпеки та стійкості роботи всієї інфраструктури.

Отже у процесі використання централізованого підходу мають бути враховані його недоліки, такі як: більш висока залежність від центрального вузла; менша гнучкість та можливість повільнішої реакції на зміни зовнішнього середовища. Також використання централізованого підходу може бути більш витратним, оскільки потрібно забезпечити високу надійність та доступність центрального вузла та пов’язаних із ним ресурсів.

Гібридний підхід під час побудови інформаційної інфраструктури за умов збройної агресії передбачає комбінацію централізованого та децентралізованого

підходів. Такий підхід може бути корисним, коли необхідно поєднати переваги обох підходів та зменшити їх недоліки. Наприклад, централізована система може використовуватися для управління спільними ресурсами, тоді як децентралізована система може використовуватися для зберігання та обміну інформацією.

Гібридний підхід доцільно використовувати у ситуаціях, коли уповноважені особи мають різні рівні доступу та контролю. Наприклад, централізована система може використовуватися для управління високорівневими завданнями, такими як розподіл ресурсів, а децентралізована система – для управління процесами нижчестоящими, такими як обмін інформацією між групами і підрозділами. Гібридний підхід за умов збройної агресії може бути ефективним, якщо використовуються найбільш підходящі елементи кожного підходу. Однак перш ніж реалізовувати гібридний підхід, необхідно провести ретельний аналіз ситуації, щоб вибрати оптимальний підхід та оцінити потенційні ризики та переваги.

Недоліком гібридного підходу є складніша архітектура, яка потребує більш високого ступеня інтеграції між різними компонентами інформаційної інфраструктури. Це також може потребувати вищого рівня експертизи та технічних знань для проєктування та управління. Слід зазначити, що гібридний підхід може потребувати додаткових витрат на інфраструктуру та обладнання для інтеграції різних елементів. Це може бути особливо значущим в умовах збройної агресії, коли доступ до ресурсів може бути обмеженим або недоступним. Також гібридний підхід може бути більш складним у реалізації та управлінні, ніж один із підходів окремо. Тому для успішної реалізації гібридного підходу необхідно спланувати та реалізувати кожну його частину, враховуючи конкретні потреби та умови.

Гібридний підхід може включати використання різних технологій і програмних засобів, які дають змогу забезпечувати більш ефективну роботу в умовах збройної агресії:

засоби автоматизованого резервного копіювання даних дають змогу швидко відновлювати дані у разі їх втрати або пошкодження;

використання розподіленого зберігання та обробки даних, спільно з локальними серверами та засобами електронних комунікацій;

різні методи моніторингу та аналізу роботи інфраструктури дають змогу швидко виявляти і усувати можливі проблеми;

методи виявлення вторгнень і захисту від шкідливих програм дають змогу захиститись від зовнішніх загроз;

використання різних стратегій управління інформаційною інфраструктурою, які дають змогу ефективно розподіляти ресурси і вирішувати виникаючі завдання (наприклад, можна використовувати стратегії управління за принципом “розподіленого управління”, коли рішення приймаються лише на рівні локальних об’єктів, а не централізовано).

Для успішної реалізації гібридного підходу необхідно провести аналіз вимог щодо інформаційної інфраструктури в умовах збройної агресії, оцінити всі фактори та ресурси, визначити необхідні технології та програмні засоби для реалізації інфраструктури, а також розглянути потенційні ризики та переваги.

Датацентричний підхід – це архітектурний підхід, у якому інформаційна інфраструктура створюється навколо загальнодоступного сховища даних та полягає в тому, що центральним елементом стає дата центр (центр обробки даних). *Датацентр* – це фізичне місце, де розміщуються сервери, мережеве обладнання та інші компоненти інфраструктури для зберігання, обробки та надання доступу до даних. Сутність датацентричного підходу полягає в тому, що всі інші компоненти інфраструктури повинні бути побудовані навколо датацентру та підкорятися його вимогам і потребам. Це дає змогу досягти оптимальної ефективності, надійності та безпеки роботи інфраструктури.

Для забезпечення високої доступності та надійності інфраструктури, датацентри мають бути забезпечені системами резервного живлення, охолодження, пожежної безпеки та захисту від несанкціонованого доступу. Датацентричний підхід дає змогу забезпечити стійке функціонування інформаційної інфраструктури, що є особливо важливим в умовах зростаючого обсягу даних та недопущення їх втрати в умовах збройної агресії.

Датацентричний підхід має свої недоліки: високі витрати на створення та управління датацентром, складність підтримки та розвитку датацентру, а також ризик виникнення технічних проблем, таких

як відмова обладнання. Тому, прийняття рішення про використання датацентричного підходу має базуватися на аналізі потреб ЗС України та оцінці переваг та недоліків цього підходу в контексті виконання завдань, які покладені на воєнне відомство та стратегії його розвитку. У Табл. 3 наведені переваги і недоліки датацентричного підходу при застосуванні інформаційної інфраструктури в умовах збройної агресії.

Таблиця 3

Переваги і недоліки датацентричного підходу

№	ПЕРЕВАГИ	НЕДОЛІКИ
1	*Централізоване керування*. Дає змогу ефективно керувати і контролювати ІнфІ навіть в умовах збройної агресії, де можуть бути обмежені ресурси та доступ до них	*Залежність від централізованого вузла*. Передбачено наявність централізованого вузла, який забезпечує функціонування всієї ІнфІ. Це означає, що у разі пошкодження або знищення датацентру може виникнути повна втрата доступу до даних і відсутність роботи ІнфІ
2	*Захист інформації*. Дає змогу використовувати передові заходи безпеки, такі як багаторівнева автентифікація, шифрування даних та моніторинг активності, для запобігання несанкціонованому доступу до інформації	*Уразливість до кібератак*. Зосередження великої кількості даних і ресурсів у датацентрах робить їх привабливою мішенню для кібератак. Атака на централізований датацентр може призвести до значних наслідків, таких як втрата конфіденційності, пошкодження або видалення даних
3	*Масштабованість*. Забезпечується можливість легкого масштабування ІнфІ - за необхідності можна швидко додати нові сервери, збільшити ємність зберігання даних та розширити мережеві ресурси, що дає змогу забезпечити стійкість і надійність системи навіть у разі збройної агресії	*Залежність від мережевого зв'язку*. Для ефективного функціонування датацентричної інфраструктури необхідне стійке і надійне мережеве з'єднання. У випадку збройної агресії може бути порушено мережевий зв'язок, що призведе до відсутності доступу до даних і зниження продуктивності

Ураховуючи ці переваги і недоліки, під час застосування датацентричного підходу в умовах збройної агресії необхідно ретельно збалансувати заходи безпеки, резервування даних і стійкість мережевого зв'язку, щоб забезпечити стійку роботу інформаційної інфраструктури навіть у складних умовах.

Датацентричний і централізований підходи являють собою різні моделі організації обчислювальних ресурсів і зберігання даних. Основні відмінності між ними полягають у розташуванні, управлінні та доступі до ресурсів. У Табл. 4 наведені відмінності датацентричного і централізованого підходів під час побудови інформаційної інфраструктури.

Таблиця 4

Відмінності датацентричного і централізованого підходів

№	Відмінність	ПІДХОДИ	
		Централізований	**Датацентричний**
1	***Розташування***	Обчислювальні ресурси та зберігання даних знаходяться в одному фізичному місці або декількох центральних локаціях	Ресурси розподілені у вигляді датацентрів, розташованих в різних географічних областях
2	***Управління***	Управління обчислювальними ресурсами та зберіганням даних здійснюється централізовано. Відомство в цілому або військове формування приймає рішення щодо розподілу ресурсів і забезпечує їх функціонування	Кожний датацентр може мати власну команду управління, що робить його більш автономним
3	***Доступ до ресурсів***	Доступ до ресурсів здійснюється через мережу, зв'язок з центральними серверами або системами зберігання даних	Доступ до ресурсів може бути розподіленим між різними датацентрами, що забезпечує резервування та більшу надійність
4	***Відмовостійкість***	Відмова одного центрального сервера або системи може призвести до зупинки всієї інфраструктури	Ресурси розподілені по різних датацентрах, і в разі відмови одного датацентру інші можуть продовжувати роботу
5	***Масштабованість***	Масштабування може бути обмеженим обсягом ресурсів, що доступні у центральній локації	Дозволяє більш гнучко масштабувати ресурси шляхом додавання або видалення датацентрів у відповідності до потреб

Обидва підходи мають свої переваги та недоліки, і вибір між ними залежить від конкретних потреб і вимог воєнного відомства. Можна також використовувати гібридні підходи, комбінуючи централізовану та датацентричну моделі, щоб поєднати переваги обох підходів.

Сутність *хмарного підходу* полягає в тому, що комп'ютерні ресурси та послуги надаються через глобальну мережу Інтернет з використанням технологій віртуалізації та розподілу ресурсів. Замість того, щоб використовувати окремі фізичні сервери та обладнання, можна розмістити їх у приватній хмарі воєнного відомства або орендувати потрібні ресурси від хмарних провайдерів.

Хмарний підхід в умовах збройної агресії може мати низку переваг, які можуть забезпечити ЗС України ефективне подолання викликів та ризиків (Табл. 5).

Таблиця 5

Переваги хмарного підходу

№	ПЕРЕВАГИ	ТЛУМАЧЕННЯ
1	***Гнучкість***	Дає змогу швидко масштабувати та налаштовувати ресурси відповідно до поточних потреб, що особливо важливо в умовах збройної агресії, коли організація може зіткнутися з несподіваними та екстреними ситуаціями, які потребують швидкого реагування
2	***Розподілене зберігання та обчислення***	Дані можуть зберігатися в різних регіонах і центрах обробки даних, що забезпечує доступність та надійність. Користувачі можуть отримувати доступ до ресурсів та даних з будь-якого місця, де є Інтернет. Високий рівень доступності та надійності дає змогу організації підтримувати працездатність своєї інформаційної інфраструктури навіть в умовах збройної агресії
3	***Захист даних***	Високий рівень захисту даних, використовуючи різні сучасні технології та механізми шифрування, що може допомагає зберегти секретність даних, навіть якщо вона піддається кібератакам чи іншим формам збройної агресії
4	**Самообслуговування**	Користувачі можуть самостійно замовляти та налаштовувати ресурси через панель управління хмарним провайдером без необхідності втручання інженерів
	Автоматизація	Багато операцій, таких як резервне копіювання, моніторинг та автоматичне масштабування, можуть бути автоматизовані, що спрощує управління інфраструктурою
4	***Спільна робота***	Хмарні послуги зазвичай надають можливість спільної роботи над документами та проєктами, що може бути корисним для командної роботи в умовах збройної агресії
5	***Економічна ефективність***	Хмарні послуги можуть бути економічно ефективнішими, ніж локальні системи, оскільки вони дають змогу уникнути витрат на придбання (постійну модернізацію) та обслуговування устаткування

Загалом, хмарний підхід дає змогу зосередитися на основних завданнях, зменшуючи необхідність у великих капіталовкладеннях у фізичне обладнання та забезпечуючи гнучкість та швидкість в розвитку інформаційних рішень.

Використання блокчейну в умовах збройної агресії може бути корисним підходом для забезпечення безпеки, надійності зберігання даних.

Довідка. *Блокчейн* – це децентралізована та неруйнівна база даних, яка зберігає інформацію в ланцюжку блоків, кожен з яких містить інформацію про транзакцію та хеш попереднього блоку. Це дає змогу створювати ланцюжок блоків, який не може бути змінений або підроблений, і забезпечує надійність зберігання даних [8].

Використання блокчейн-технології в умовах збройної агресії може бути використаний для більш надійної реалізації функціональних сервісів воєнного відомства:

зберігання та управління даними у децентралізованій мережі, забезпечуючи високий рівень безпеки та захисту від несанкціонованого доступу;

підвищення ефективності процесів постачання та логістики шляхом використання блокчейн-рішень для управління ланцюгами постачання та відстеження руху вантажів;

використання смарт-контрактів для автоматизації та управління різними видами операцій: закупівля, контроль і облік запасів, управління бюджетами та інші;

створення децентралізованих систем обміну інформацією та координації між різними відділами та підрозділами військових формувань, забезпечуючи швидкий обмін інформацією та прийняття оперативних рішень;

управління інтелектуальною власністю та захисту авторських прав, що може бути корисним у галузі оборони та безпеки, де інтелектуальна власність є ключовим ресурсом;

управління даними та аналітики, що може допомогти швидше та точніше аналізувати дані та приймати рішення на їх основі.

Наприклад, блокчейн може використовуватися для зберігання та обміну медичною інформацією військовослужбовців, для забезпечення прозорості бюджетування та фінансового управління, а також для зберігання та обміну інформацією про

логістичні та інші операції. Блокчейн може забезпечити захист від хакерських атак та інших видів кібератак шляхом створення неруйнівних ланцюжків даних та зменшення ризиків несанкціонованого доступу до ресурсів.

Для реалізації підходу з використанням блокчейну необхідно провести такі етапи (рис. 1):

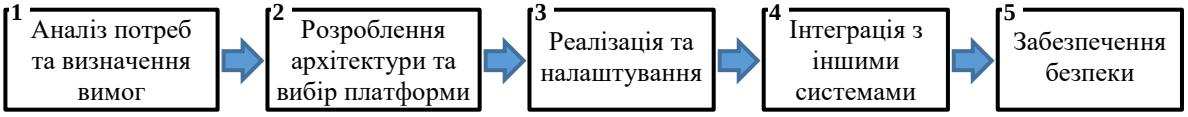


Рис. 1. Порядок реалізації блокчейну

Етап 1. *Аналіз потреб та визначення вимог* – визначаються дані та операції, які зберігатимуться та оброблятимуться в блокчейні, потрібні рівні доступу та контролю інформації, алгоритми та протоколи шифрування.

Етап 2. *Розроблення архітектури та вибір платформи* – на основі аналізу вимог розроблення архітектури блокчейн-рішення, вибір платформи та інструментів для реалізації, визначення параметрів мережі та її конфігурації.

Етап 3. *Реалізація та налаштування* – створення вузлів мережі, налаштування алгоритмів та протоколів, проведення тестування та оптимізації продуктивності.

Етап 4. *Інтеграція з іншими системами* для обміну інформацією та управління даними.

Етап 5. *Забезпечення безпеки* – проведення заходів забезпечення безпеки блокчейн-рішення, які включають захист від хакерських атак, контроль доступу та автентифікацію, моніторинг та аналіз дій користувачів.

Під час використання блокчейну слід враховувати деякі фактори – обмежена масштабованість та висока вартість створення та підтримки блокчейн-систем. Крім того, необхідно забезпечити безпеку доступу до блокчейн-системи та інформації, що зберігається в ній. Важливим аспектом також є вибір відповідної платформи блокчейну для конкретних потреб та завдань, а також забезпечення відповідної підтримки та навчання персоналу.

Проведений аналіз дає змогу дійти висновку – кожному з підходів притаманні власні переваги і недоліки та їх використання доцільне за певних умов і цілей створення інформаційної інфраструктури. Отже, у якості ***рекомендацій*** стосовно шляхів удосконалення інформаційної інфраструктури МО України для забезпечення її функціонування та надійного застосування в умовах збройної агресії. нагальним вважається поєднання розглянутих підходів для послаблення недоліків кожного з підходів та посилення їх переваг при комплексному використанні.

Для реалізації об’єднаного підходу у процесі створення інформаційної інфраструктури в умовах збройної агресії необхідно провести аналіз потреб та можливостей у рамках конкретного контексту конфлікту (або збройної агресії). Такий аналіз має враховувати не лише технічні аспекти, а й культурні, соціальні та політичні аспекти. Крім того, потрібно врахувати потреби посадових (службових) осіб МО і ЗС України. Тобто, необхідно розробити стратегію доступу до інформації та зв’язку у межах повноважень посадових осіб.

Розглянемо більш детально ***аспекти***, які потрібно враховувати під час реалізації об’єднаного підходу у процесі створення інформаційної інфраструктури, яка має зберігати функціональність в умовах збройної агресії.

Управління даними. В умовах збройної агресії управління даними може стати критично важливим для забезпечення їх безпеки та своєчасності прийняття управлінських рішень. Важливо розробити стратегію управління даними. У межах цієї стратегії можна використовувати технології блокчейну для забезпечення цілісності та безпеки даних, а також для створення системи керування доступом до даних. Це дасть змогу запобігти несанкціонованому доступу до даних та забезпечити контроль над їх використанням.

Безпека даних. Можна використовувати різні методи та технології:

шифрування даних;

застосування багатофакторної автентифікації – використання пароля, біометричних даних (наприклад, відбитків пальців або сканування особи), а також апаратних (наприклад, токенів) та програмних (наприклад, програмне забезпечення аутентифікації, що встановлюється на смартфони посадових осіб) засобів аутентифікації.

Довідка. *Токен* (захищений носій) – компактний пристрій у вигляді USB-флешки, призначений для забезпечення інформаційної безпеки користувача, віддаленого доступу до інформації та використовується для ідентифікації його власника. На токені зберігається кваліфікований електронний підпис, який генерується у акредитованих центрах сертифікації ключів за безпосередньої участі власника ключа.

Важливим фактором є навчання користувачів та посилення культури безпеки. Користувачі повинні знати, як правильно використовувати інформаційну інфраструктуру та як захищати свої дані, а також розуміти наслідки порушення правил безпеки. Потрібно мати плани та процедури реагування на можливі порушення безпеки, включаючи резервне копіювання даних, детектування та запобігання атак, та відновлення після порушень.

Надійність та доступність. Гібридна інфраструктура може використовувати як локальні, так і хмарні ресурси, що дає змогу підвищити доступність систем та забезпечити їхню працездатність у разі відключення будь-якої з частин інфраструктури. Технологія блокчейну може також підвищити надійність системи, оскільки вона дає змогу створення надійних та стійких до змін систем зберігання даних. Крім того, блокчейн-технологія дає змогу захистити дані від несанкціонованого доступу та внесення змін до них.

Масштабованість системи. Хмарні рішення можуть бути використані підрозділами ЗС України за потреби швидкої масштабованості інформаційної інфраструктури в умовах збройної агресії. Залежно від ситуації, обсяг даних і кількість користувачів може значно змінюватися, і застосування хмарних сервісів дає змогу швидко масштабувати інфраструктуру для задоволення нових потреб.

Таким чином, удосконалення інформаційної інфраструктури на основі об’єднаного підходу в умовах збройної агресії є складним проєктом. Виходячи з проведеного у роботі аналізу, у Табл. 6 сформульовані вимоги до удосконаленої інформаційної інфраструктури, які потрібно задовольнити під час реалізації проєкту.

Таблиця 6

Вимоги до нової інформаційної інфраструктури МО України

№	ВИМОГИ
1	Необхідність дотримання міжнародних стандартів безпеки інформації ISO/IEC 27001 і національних стандартів України, якими імплементовані міжнародні стандарти безпеки інформації ISO/IEC 270XX, що забезпечить довіру до інформаційної інфраструктури міжнародних партнерів
2	Урахування можливих ризиків та уразливостей системи – DDOS-атаки, кібершпигунство, виток даних та інші види кіберзагроз. Для чого необхідно включити в проєкт заходи захисту інформації та введення механізмів швидкого реагування на інциденти безпеки
3	Визначення стратегії резервного копіювання та відновлення даних в умовах збройної агресії може відповідно до плану резервного копіювання даних та процедури відновлення
4	Визначення процедур керування доступом до інформації. Для запобігання несанкціонованому доступу до даних відповідно до стратегії управління доступом на основі рольової моделі доступу, двофакторної автентифікації та інших сучасних методів
5	Визначення місця розміщення ІнфІ для забезпечення можливості захисту від можливих ударів та терористичних актів супротивника, а також забезпечити її захист від природних катастроф, таких як землетруси, повені та інші
6	Врахування вимог до енергозабезпечення. В умовах збройної агресії можливі перебої в енергопостачанні, тому необхідно врахувати цей фактор під час вибору місця розміщення компонентів ІнфІ та визначення резервних джерел живлення
7	Розроблення стратегії моніторингу та аналізу інформації про стан ІнфІ у режимі реального часу для оперативного реагування на можливі загрози та вразливості
8	Кадрове забезпечення. Для забезпечення ефективної роботи ІнфІ необхідно готувати професійних фахівців, які мають відповідні знання та досвід роботи з сучасними ІТ-технологіями
9	Визначення плану дій при евакуації у разі виникнення загрози життю та здоров’ю персоналу

Для успішної реалізації такого проєкту потрібне проведення організаційних заходів, які наведені на рис. 2.

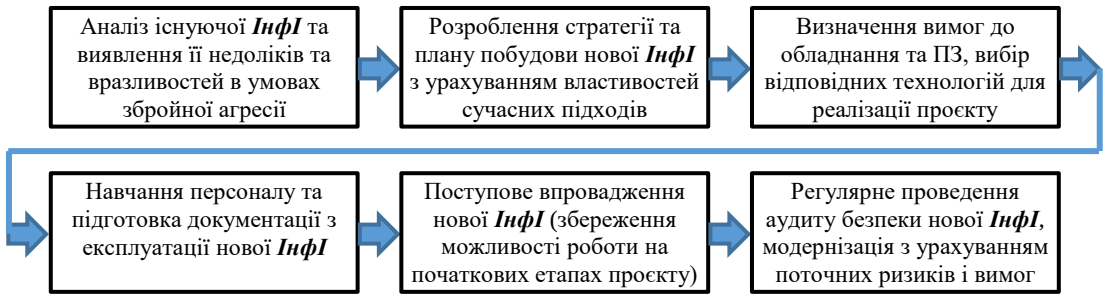


Рис. 2. Порядок удосконалення інформаційної інфраструктури МО України

Необхідно враховувати, що процес реалізації такого проєкту може зайняти тривалий час і вимагати значних інвестицій. У будь-якому випадку проведення ретельного аналізу та розроблення детального плану проєкту допоможе мінімізувати ризики та підвищити шанси на успіх.

Висновок. Розвиток інформаційної інфраструктури МО України має збільшити швидкість, точність і якість процесу прийняття рішень, які є критичними для прийняття стратегічних рішень та успіху операцій і бойових дій. Це дасть змогу повною мірою використовувати переваги обміну потрібною інформацією через всі домени інформаційного простору – від стратегічної до тактичної ланки, усунути принцип "ізольованості" існуючих інформаційних систем та забезпечити задоволення потреб в інформації, яка необхідна для швидкого прийняття рішень.

Подальші дослідження доцільно зосередити на аналізі можливих ризиків під час функціонування інформаційної інфраструктури та обґрунтуванні заходів щодо їх уникнення або нівелювання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року "Про Стратегічний оборонний бюлетень України" : Указ Президента України від 17.09.2021 р. № 473/2021. URL: https://zakon.rada.gov.ua/laws/show/473/ 2021#Text (дата звернення: 10.07.2023).
2. Інформаційна інфраструктура // Матеріал з Вікіпедії – вільної енциклопедії. URL: https://uk.wikipedia.org/wiki/Інформаційна_інфраструктура (дата звернення: 10.07.2023).
3. Концепція розвитку ІТ-інфраструктури Міністерства оборони України та Збройних Сил України.
4. Інформаційне забезпечення інноваційного розвитку: світовий та вітчизняний досвід: монографія / Т. В. Писаренко, Т. К. Кваша, Н. В. Березняк, О. В. Прудка. Київ : УкрІНТЕІ, 2015. 239 с.
5. Інформаційні системи і технології на підприємствах : конспект лекцій / В. М. Охріменко, Т. Б. Воронкова. Харків : ХНАМГ, 2006. 185 с. URL: http://eprints.kname.edu.ua/17149/1/In.form_systens_et_technologies_Ochrimenko.pdf (дата звернення: 11.07.2023).
6. Попова І. А., Сєрєбряк К. І. Модернізація інформаційної інфраструктури задля активізації міжрегіонального співробітництва // Інвестиції: практика та досвід. 2015. № 24. С. 49–52. URL: http://nbuv.gov.ua/UJRN/ipd_2015_24_12 (дата звернення: 11.07.2023).
7. Лазебник Л. Л., Войтенко В. О. Інформаційна інфраструктура в цифровізації бізнес-процесів підприємства // Науковий вісник Міжнародного гуманітарного університету. 2020. DOI: https://doi.org/10.32841/2413-2675/2020-42-3.
8. Демчишак Н. Б., Радик В. В. Розвиток цифрової інфраструктури та блокчейн-технологій в Україні // Інноваційна економіка. 2020. № 3–4. DOI: https://doi.org/10.37332/2309-1533.2020.3-4.27.
9. Мануйлов Я. С. Використання технології "блокчейн" у телекомунікаціях // Вчені записки ТНУ імені В.І. Вернадського. Серія: Технічні науки. 2021. Том 32 (71). № 3. DOI: https://doi.org/10.32838/2663-5941/2021.3/20.
10. Визначення технологічних рішень щодо створення Єдиної інформаційної системи управління оборонними ресурсами / Ю. А. Кірпічніков та ін. // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2019. № 1 (65). С. 86–91. DOI: https://doi.org/10.33099/2304-2745/2019-1-65/86-91.
11. Застосування дата-центричного підходу під час побудови інформаційної інфраструктури з використанням хмарних технологій для оборонних потреб / Ю. А. Кірпічніков та ін. // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2022. № 3 (76). С. 68–75. DOI: https://doi.org/10.33099/2304-2745/2022-3-76/68-75.
12. Додонов А. Г., Ландэ Д. В. Живучесть информационных систем. Київ : Наук. думка, 2011. 256 с.
13. ДСТУ ISO/IEC 2382:2017.

14. Грищенко И. В. Метод повышения живучести инфокоммуникационной сети // Холодильна техніка і технологія. 2013. № 6. (146). С. 66–70.
15. Князева Н. О., Грищенко И. В., Шестопалов С. В. Метод обеспечения живучести телекоммуникационной сети на основе перераспределения ресурсов сети // Холодильная техника и технология. 2014. № 4 (150). С. 65–71.
16. Зінченко А. А., Масесов М. О., Пантась І. О. Аналіз методів підвищення живучості телекомунікаційних мереж // Сучасні інформаційні технології у сфері безпеки та оборони. 2021. № 2 (41). DOI: https://doi.org/10.33099/2311-7249/2021-41-2-5-10.

Стаття надійшла до редакційної колегії 11.08.2023

Justification of the approach to improving the information infrastructure of the Ministry of Defense of Ukraine for functioning in conditions of armed aggression

Annotation

In the context of the military-political crisis and armed aggression against Ukraine, its state institutions, in particular the Ministry of Defense (MoD) of Ukraine, have to develop and apply new modern approaches to the development of its own information space, ensuring its stability and security. The peculiarities of information infrastructure development at the current stage are a high level of unification of hardware, including computing (infrastructure as a service), system software (basic services), and the introduction of special purpose application software (functional services). Ensuring the proper quality of services is a dynamic task, the complexity of which is proportional to the tasks and requirements for the information infrastructure.

The purpose of the article is to substantiate recommendations on ways to improve the information infrastructure of the Ministry of Defense of Ukraine, taking into account the capabilities of the latest IT technologies to ensure its functioning and reliable use in the context of armed aggression.

Building an information infrastructure for defense needs can be realized using different approaches. Each of the approaches has its own advantages and disadvantages, and their use is advisable under certain conditions and goals of information infrastructure creation. Implementation of a unified approach to the creation of information infrastructure for its sustainable functioning in the context of armed aggression requires an analysis of needs and capabilities within the specific context of the conflict (or armed aggression). Improving the information infrastructure based on a unified approach is a complex project. The author proposes a procedure for improving the information infrastructure of the Ministry of Defense of Ukraine.

Keywords: information infrastructure; life cycle model; information system; cascade, incremental, evolutionary strategies; verification; validation.

УДК 355.41 DOI: https://doi.o rg/10.33099/2304-2745/2023-2-78/98-107

Телегін В. В., (0000-0001-6896-3848)
Ганненко С. О., кандидат технічних наук (0000-0002-8285-1145)
Кивлюк В. С., кандидат економічних наук (0000-0002-5269-576X)
Половенко В. М., кандидат військових наук (0000-0002-1753-395X)

Національний університет оборони України, Київ

Впровадження автоматизованої системи управління матеріальними ресурсами Збройних Сил України

Резюме. У статті представлений аналіз автоматизованої системи управління забезпеченням матеріальними ресурсами збройних сил провідних країн світу на прикладі інформаційно-комунікаційної системи (далі – ІКС) LOGFAS та обґрунтовано рекомендації щодо подальшого удосконалення та впровадження ІКС на оперативному рівні управління системою забезпечення матеріальними ресурсами.

Ключові слова: система забезпечення матеріальними ресурсами; автоматизована система управління; інформаційні технології; спеціалізоване програмне забезпечення LOGFAS; широкомасштабна збройна агресія.

Постановка проблеми. Широкомасштабне вторгнення збройних сил Російської Федерації 24 лютого 2022 року на територію України та подальші бойові дії проти агресора свідчать, що сучасна війна це не тільки протистояння між людськими, матеріальними, інформаційними ресурсами, а й між системами забезпечення військ (сил). Повне й своєчасне забезпечення матеріальними ресурсами в ході ведення операції (бойових дій) відіграє основну роль в досягненні успіху. Якісне матеріальне забезпечення неможливе без ефективного управління системою забезпечення матеріальними ресурсами.

Аналіз поточного стану системи забезпечення матеріальними ресурсами (далі – СЗМР) Збройних Сил України (далі – ЗС України), досвіду ведення бойових дій по відбиттю нападу агресора, оцінка стану сектору безпеки і оборони, виявили низку проблем, Які суттєво ускладнюють процес забезпечення та управління системою забезпечення матеріальними ресурсами ЗС України, а саме [1]:

недосконаліть управління системою забезпеченням матеріальними ресурсами ЗС України впливає на виконання завдань забезпечення матеріальними ресурсами ЗС України;

недостатній рівень обсягів постачання ресурсів для забезпечення заходів розвитку, підготовки та застосування військ (сил) призводять до зниження боєздатності та ефективності застосування військ (сил);

відсутність інтегрованої автоматизованої системи управління СЗМР ЗС України не дає змоги повною мірою використовувати інтелектуальний потенціал органів військового управління, можливості сил та засобів, раціонально управляти матеріальними та іншими необхідними ресурсами і, як наслідок, не дає змоги повною мірою використовувати бойові спроможності військ (сил);

відсутність дієвого інструменту для обліку міжнародної військово-технічної допомоги;

низький рівень застосування сучасних інформаційних технологій у ЗС України.

Для ефективного управління процесами із забезпечення матеріальними ресурсами ЗС України необхідне використання системного рішення стосовно формування автоматизованої системи управління забезпеченням матеріальними ресурсами (далі – АСУЗМР), вибору інформаційно-програмної платформи відповідної функціональності та масштабу для автоматизації процесів управління забезпеченням, побудови інформаційної інфраструктури системи забезпечення матеріальними ресурсами.

Ефективність зусиль “об’єднаної логістики” визначається оптимальним розподілом функцій між командуваннями ЗС, видами ЗС, органів військового управління, детально сплановаим функціонуванням виконавців заходів забезпечення, які у цілому утворюють єдину СЗМР. Інформаційно-аналітичне забезпечення процесів управління СЗМР – це основа своєчасного, якісного та ґрунтовного рішення, ефективних процесів управління та контролю. Зрозуміло, що

управління всіма підсистемами забезпечення, виконавцями, ресурсами та забезпечення ЗС усім необхідним для їх надійного функціонування в умовах ведення бойових дій потребують використання найсучасніших методів і засобів, інформаційних технологій, постійного пошуку нестандартних (нешаблонних) рішень під час бою, коли ситуація змінюється безперервно і непередбачуване.

Створення нових і модернізація існуючих автоматизованих систем управління матеріальними ресурсами на основі передових інформаційних технологій, дозволить підвищити ефективність управління матеріальними потоками ЗС України, скоротити час на одержання і всебічну оцінку відомостей про наявні матеріальні ресурси на всіх етапах їх руху, підвищити ефективність системи забезпечення, а також покращити взаємодію з аналогічними системами країн – партнерів НАТО. Автоматизація процесів має бути одним з пріоритетних напрямків роботи з підвищення ефективності управління системи забезпечення ЗС України.

Аналіз останніх досліджень і публікацій. Аналіз останніх наукових досліджень і публікацій [2–14] свідчить про те, що підвищенню ефективності системи забезпечення матеріальними ресурсами присвячена низка робіт попередників, які в свій час зробили вагомий внесок у розвиток теорії військової науки. Однак аналіз запропонованих ними підходів свідчить про те, що вони розглядали окремо матеріальне забезпечення та не враховували вплив ефективності управління на СЗМР, а також не були враховані чинники, які суттєво впливають на своєчасність та ефективність системи забезпечення, а саме використання автоматизованої системи управління забезпеченням матеріальними ресурсами. Саме тому, дані методики у наявному вигляді не можуть бути використані у повному обсязі для дослідження автоматизованої системи управління забезпеченням матеріальними ресурсами, але можуть бути обрані за основу для подальшого удосконалення.

Мета статті – аналіз ІКС LOGFAS для формування обґрунтованих рекомендацій щодо його удосконалення та впровадження на оперативному рівні ІКС управління системою забезпечення матеріальними ресурсами.

Виклад основного матеріалу. Побудова та функціонування ефективної системи забезпечення матеріальними ресурсами неможлива без чітко налагодженої системи управління в реальному масштабі часу з інформаційними потоками, які циркулюють в середині системи на усіх рівнях ієрархії.

Керуючись вимогами [15], основні функції системи забезпечення ЗС України полягають у постачанні матеріальних ресурсів для забезпечення потреб ЗС, управлінні інформацією логістичного забезпечення. Разом з тим, кожна із функцій системи забезпечення спрямована на виконання відповідних заходів. Враховуючи ті зміни, які відбулись в системі забезпечення ЗС України [15, 16], завдання з планування забезпечення під час застосування ЗС України та інших складових Сил оборони, узагальнення потреби у матеріальних ресурсах, планування забезпечення матеріально-технічними засобами, покладені на Головне управління логістики ЗС України з підпорядкованими органами управління на оперативному і тактичному рівні у об’ємі відповідного рівня ієрархії [17]. Тобто, Головне управління логістики ЗС України під час планування логістичного забезпечення, у відповідності до визначених форм і способів застосування ЗС України, визначає загальну потребу військ (сил) у матеріальних ресурсах тощо для виконання поставленого завдання.

Забезпечення військових частин (підрозділів) відповідними матеріальними ресурсами повинно здійснюватись з урахуванням вимог системного підходу, тобто подачу окремої номенклатури матеріальних ресурсів, у якій існує потреба необхідно розглядати, як складову частину усієї сукупності підсистем – органів управління та військових частин (підрозділів) забезпечення на різних рівнях ієрархії, інформаційних та матеріальних потоків, які через них проходять.

Виконання завдань по забезпеченню матеріальними ресурсами буде в повній мірі залежати від своєчасного, безперебійного і повного забезпечення відповідними матеріальними ресурсами потреб військових частин (підрозділів).

На сьогодні потреба в матеріальних ресурсах визначається на основі поданих донесень (зведень) та заявок на поповнення матеріальних ресурсів. Заявка від військової частини перш ніж попасти до відповідного органу забезпечення проходить довгий шлях. Узагальнення органами управління тактичного, оперативного та стратегічного рівня поданих заявок та донесень потребує часу на оброблення великого обсягу

інформаційних потоків щодо визначення потреби військ у матеріальних ресурсах. Усі ці ступені оброблення інформації збільшують час подачі матеріальних ресурсів до споживача [14].

Для своєчасно та повного забезпечення матеріальними ресурсами оперативно-стратегічного угруповання військ необхідно, щоб система забезпечення матеріальними ресурсами відповідала функціональному призначенню, для ефективного функціонування якої потрібно створити автоматизовану систему, яка б об'єднала у єдине ціле органи управління та військові частини (підрозділи) на усіх рівнях ієрархії, та включала управління матеріальними потоками та контроль наявних матеріальних ресурсів (облік).

Отже, для своєчасного забезпечення військ (сил) в ході ведення бойових дій матеріальними ресурсами та ефективного управління матеріальними потоками необхідно у будь-який момент часу мати інформацію про номенклатуру матеріальних ресурсів, які є в наявності, або потребують поставки. Вирішити дану проблему можна шляхом впровадження підсистеми автоматизованого управління матеріальними потоками, здатної ідентифікувати (розпізнавати) окремі номенклатури матеріальних ресурсів. Ця підсистема забезпечить можливість оброблення інформації в режимі реального масштабу часу, що дозволить системі матеріального забезпечення своєчасно реагувати на потреби військ (сил) в оптимальні терміни. Також підсистема дасть змогу скоротити час на обробку інформаційних потоків (обробку заявок тощо), а також допоможе визначити: місця знаходження матеріальних ресурсів, оптимальний маршрут підвезення, обсяг матеріальних ресурсів, автоматизувати їх облік.

З урахуванням структури системи забезпечення матеріальними ресурсами та підсистем автоматизованого управління матеріальними потоками і обліку матеріальних ресурсів, які входять у автоматизовану систему забезпечення, необхідно визначити інформаційні потоки щодо потреби та наявності матеріальних ресурсів, які циркулюватимуть у середині системи матеріального забезпечення.

При цьому, на усіх рівнях ієрархії необхідно сформулювати вихідні дані для структуризації інформаційних потоків, які протікатимуть у автоматизованій системі матеріального забезпечення. Тобто, на тактичному рівні до цієї системи необхідно внести інформацію про наявність матеріальних ресурсів у підрозділах і на складах військових частин, про номерний облік озброєння та військової техніки (далі – ОВТ), стан укомплектованості; на оперативному – внести інформацію про наявність матеріальних ресурсів на розподільчих центрах оперативного рівня; на стратегічному – внести інформацію про наявності матеріальних ресурсів в логістичних центрах стратегічного рівня.

На основі вихідних даних, що містяться в автоматизованій системі матеріального забезпечення, які система автоматично отримує в режимі реального масштабу часу, проводиться порівняльна оцінка фактичної витрати матеріальних ресурсів із наявними. На основі порівняльної оцінки система матеріального забезпечення на усіх рівнях ієрархії від тактичного до стратегічного дає сигнал про потребу у забезпеченні відповідними матеріальними ресурсами, при цьому система автоматично визначає місце знаходження матеріальних ресурсів, які необхідні для забезпечення потреб, визначає оптимальний маршрут їх підвезення.

За оцінкою фахівців, широке застосування передових інформаційних технологій в процесі створення нових і модернізації існуючих систем зможе забезпечити більш ефективне управління системою забезпечення ЗС, скоротить час на отримання інформації та всебічну оцінку відомостей щодо матеріальних ресурсів на всіх етапах руху, зменшить ризики несвоєчасного або недостатнього за силами і засобами реагування на загрози, підвищить ефективність та взаємодію логістичних підрозділів військових формувань ЗС України.

Для впровадження підсистеми автоматизованого управління матеріальними ресурсами необхідні такі вихідні дані:

фактичні витрати матеріальних ресурсів у підрозділах за рівнями ієрархії;

наявність потрібних матеріальних ресурсів на складах, базах і арсеналах (облік і аудит складських ресурсів);

наявність і технічний стан транспортних ресурсів;

укомплектованість і підготовка підрозділів забезпечення

Отже, впровадження автоматичної системи управління забезпеченням матеріальними ресурсами призначено для

автоматизованої підтримки на всіх рівнях військового управління процесами планування та управління забезпеченням військ (сил), що зі свого боку забезпечить:

підтримку процесів діяльності планування забезпечення військ (сил) матеріальними ресурсами з метою підвищення ефективності планування логістичного забезпечення, підвищення рівня сумісності з НАТО (постачання матеріальних ресурсів за п'ятьма класами постачання);

автоматизацію збору, зберігання та надання повної, актуальної, достовірної інформації щодо фактичного стану забезпечення військ (сил) матеріальними ресурсами та їх кількість;

надання органам військового управління стратегічного, оперативного рівня та підрозділам тактичного рівня достовірної інформації, необхідної для прийняття рішень щодо питань забезпечення матеріальними ресурсами;

обробка гігантських потоків інформації на всіх рівнях військової ієрархії системи управління;

активне використання у підрозділах матеріального забезпечення інформаційні системи контролю за матеріальними потоками;

оснастити усі військові вантажі, контейнери та пакувальні матеріали пасивними радіочастотними мікрочіпами-ідентифікаторами RFID для безконтактної радіочастотної ідентифікації;

використання стандартів та концепції планування НАТО потреб в матеріальних ресурсах дасть змогу взаємної сумісності.

Світова тенденція по створенню великомасштабних автоматизованих систем для збройних сил з управління ресурсами у більшості провідних країн світу (членів НАТО) бере свій початок з другої половини 90-х років і полягає у поетапній модульній автоматизації управлінських процесів та інтеграції модулів в загальну функціональну інформаційну систему на одній програмній платформі ERP-класу. Така система об'єднує в єдиному програмному середовищі та інформаційному просторі найбільш важливі процеси забезпечення життєдіяльності, розвитку та застосування збройних сил (матеріальне забезпечення, фінансова діяльність, менеджмент особового складу, ведення організаційної структури, оборонне планування, управління інфраструктурою [18].

До числа основних завдань АСУЗМР, на погляд американських військових експертів, входять [19]:

взаємодія і інтеграція інформації об'єднаних і видових систем забезпечення збройних сил, включаючи систему постачання зброї і матеріальних засобів, фінансового, медичного, технічного забезпечення і перевезення;

взаємодія інформаційних систем логістики країн – членів НАТО, а також союзників США, під час спільного врегулювання конфліктів і криз;

взаємодія процесів забезпечення угруповань сил і оперативного управління ними, а також надання можливості командуючим оперативними формуваннями вибору з більшого числа тактичних варіантів дій;

планування логістики;

забезпечення доступу до постійно обновлюваної інформації від різних джерел централізованої бази даних логістики (відстеження запасів, стану і місця розташування боєприпасів, паливо-мастильних матеріалів та іншого майна);

централізація інформації про потреби бойових підрозділів у матеріальних засобах (далі – МтЗ);

взаємодія з постачальниками МтЗ і підрядниками з доступом посадових осіб до постійно підтримуваної загальної бази забезпечення і системам електронної комерції.

Військові експерти провідних країн світу вважають основними критеріями оцінки ефективності функціонування системи забезпечення такі [19]:

час очікування поставки (виконання заявки) – з моменту реєстрації замовлення в системі постачання до підтвердження про одержання замовлених ресурсів;

точність за часом поставки (виконання заявки) – у межах установленого інтервалу.

Крім того, важливими критеріями є такі:

здатність забезпечити розгортання угруповань сил (в еквівалентних формуваннях, тис. чоловік);

швидкість розгортання (забезпечення мобільності) угруповань військ (сил);

здатність забезпечити автономність дій сил (тривалість бойових дій);

інтенсивність бойового забезпечення (доставки МтЗ) у ході бойових дій та ін.

Характерними рисами діючих і перспективних АСУЗМР стануть: найвищий

рівень автоматизації всіх основних функцій; здатність виконувати безперебійне постачання і будь-які вимоги угруповань сил у надзвичайних умовах; гнучкість і адаптивність системи забезпечення.

Система забезпечення ЗС США спрямована на повне задоволення потреб угруповань сил у всіх фазах:

розгортання в районах бойового призначення;

підготовки до перших операцій, початку бойових дій;

забезпечення сил під час бойових дій (постачання, перегрупування і евакуація, відновлення боєздатності);

згортання бойових дій і передислокація до місць постійного базування.

Інформатизація і роботизація збройної боротьби висувають на перший план низку питань щодо: перевезення; технічного обслуговування і ремонту; відновлення боєздатності ОВТ поряд зі збереженням актуальності медичного і іншого видів забезпечення.

Отже, стратегія і тактика є основою планування бойових дій, а система забезпечення забезпечує засоби для їх ведення [19]. Результат бойових дій (оборонної операції) залежить від стійкого і безперебійного функціонування системи забезпечення. На сьогодні система забезпечення зазнає змін і розвивається під безпосереднім впливом військової стратегії, досягнення цілей якої вона покликана забезпечити.

Таким чином, як вважають військові фахівці ЗС США, революція в системі забезпечення опирається, головним чином, на вдосконалювання інформаційних систем і створення більш швидких транспортних систем меншої вартості, оскільки однією з ключових складових в автоматизації поля бою і сил XXI століття є концепція досягнення панування в ситуаційній поінформованості, тобто знання всього того, що відбувається на полі бою, місця розташування, статусу, стану ресурсів своїх сил і сил противника, пересування і прогнозу поповнення запасів кожного елемента сил. Крім того, для повноти картини логістики має забезпечуватися загальна видимість ресурсів об'єднаних сил (JTAV), тобто їхнє місце розташування, стан, кількість, склад та інше. ЗС США зможуть надійно випереджати противника в циклі бойового управління і прийняття рішень і, таким чином, різко підвищити ефективність дій своїх сил.

З моменту повномасштабного вторгнення ЗС РФ на територію України, та виділенням країнами-партнерами міжнародної військово-технічної допомоги, постало питання обліку зарубіжних матеріальних ресурсів. Впровадження автоматизованих систем управління з використанням ІКС LOGFAS дає змогу вирішити питання обліку, введення, редагування та видалення даних в підрозділах що обліковують міжнародну технічну допомогу

Метою створення та використання інформаційно-комунікаційної системи планування та управління матеріальним забезпеченням відповідно [20, 21] є облік, узагальнення, обробки даних та надання звітних матеріалів щодо матеріального забезпечення в рамках отриманої міжнародної технічної допомоги України (далі – МТД).

Система функціональних областей LOGFAS – це програмне забезпечення НАТО для сфери автоматизованої системи управління логістики, що дає змогу здійснювати обмін даними між штаб-квартирою НАТО, підрозділами та державами, що їх виділяють, на всіх етапах планування та проведення забезпечення військ за рахунок використання серії інтегрованого програмного забезпечення [22-25].

ІКС LOGFAS призначена для планування забезпечення матеріальними ресурсами, підтримки процесів переміщення та транспортування військ (сил), матеріальних ресурсів, планування стратегічного розгортання військ (сил) у визначених операційних зонах (районах).

Основними завданнями ІКС в ЗС України є автоматизація таких процесів:

збір, зберігання, узагальнення та надання інформації щодо фактичного стану забезпечення військ (сил) за п'ятьма класами постачання [26] з метою визначення потреби ЗС України (сил оборони) під час спільного виконання завдань, у мирний час та під час особливого періоду (введення правового режиму воєнного стану в державі), а саме:

клас I – продовольство (харчові продукти та корм), що споживається особовим складом та тваринами, для якого встановлено єдині норми;

клас II – матеріально-технічні засоби, що видаються за встановленими нормами забезпечення, штатами та табелями до них (озброєння та зброя, військова (спеціальна) техніка та технічні засоби, обмундирування та

спорядження, запасні частини, інструменти та приладдя тощо);

клас III – усі види нафтопродуктів та пально-мастильних матеріалів, паливо;

клас IV – предмети постачання, норму забезпечення якими не визначено встановленими штатами та табелями (фортифікаційні та будівельні матеріали);

клас V – усі види ракет, боєприпасів та інших вибухових речовин;

планування забезпечення матеріальними ресурсами військ (сил) на всіх рівнях ієрархії (оперативно-стратегічний, оперативно-тактичний, тактичний);

планування (визначення) потреби в матеріальних ресурсах ЗС України (сил оборони);

планування розподілу матеріальних ресурсів відповідно до п’яти класів постачання за територіальним принципом, відповідно до стандартів НАТО;

планування (визначення) обсягів (потреби) транспортного забезпечення (засобів для логістичного забезпечення стратегічного розгортання та виконання завдань ЗС України (силами оборони));

планування здійснення транспортування для забезпечення військ (сил);

планування здійснення розгортання (переміщення) військ (сил) у частині логістичного забезпечення;

планування надання підтримки приймаючою країною (host nation support, HNS);

моніторинг виконання планів забезпечення військ (сил);

підтримка розроблення документів планування забезпечення, формування визначених форм звітності, обмін визначеними даними щодо планування логістичного забезпечення військ (сил);

визначення потреб в озброєнні, військовій техніці (далі – ОВТ) та матеріально-технічних засобах за класами постачання, які необхідні для забезпечення стратегічного розгортання ЗС України та їх застосування;

ведення обліку матеріальних ресурсів та планування забезпечення ними ЗС України (здійснення розподілу матеріальних ресурсів між угрупованнями військ (сил), військовими частинами, організація їх підвезення (транспортування) до споживачів; створення угруповань сил і засобів логістичного забезпечення;

формування необхідної інформації щодо стану забезпеченості військ (сил) матеріальними ресурсами, забезпечення обміну логістичною інформацією між органами військового управління, військовими частинами ЗС України та іншими складовими Сил оборони.

Також ІКС LOGFAS призначена для забезпечення надійного зберігання інформації, розмежування і оперативності доступу до неї для всіх користувачів системи, у тому числі територіально-розподілених.

ІКС має забезпечити виконання таких вимог:

конфіденційність (confidentiality): тільки авторизовані користувачі та процеси повинні мати доступ до даних або змінювати їх;

цілісність (integrity): дані мають підтримуватися в правильному стані, і ніхто не повинен мати можливості неправильно змінити їх випадково або зловмисно;

доступність (availability): авторизовані користувачі повинні мати доступ до даних, коли їм це потрібно.

спостережність (observability) – усі дії користувача і процесів використання об’єктів мають бути зафіксовані та ідентифіковані.

Відповідно до наведеної схеми (рис. 1) до складу ІКС входить інформаційна система та користувацький сегмент, який складається з пристроїв кінцевих користувачів з встановленим програмних забезпеченням і здійснюється обмін інформацією із використанням електронної комунікаційної системи.

Електронна комунікаційна система зі свого боку складається з електронних комунікаційних мереж і засобів криптографічного захисту інформації (далі – засоби КЗІ), що забезпечують захищене з’єднання між інформаційною системою та пристроями кінцевих користувачів.

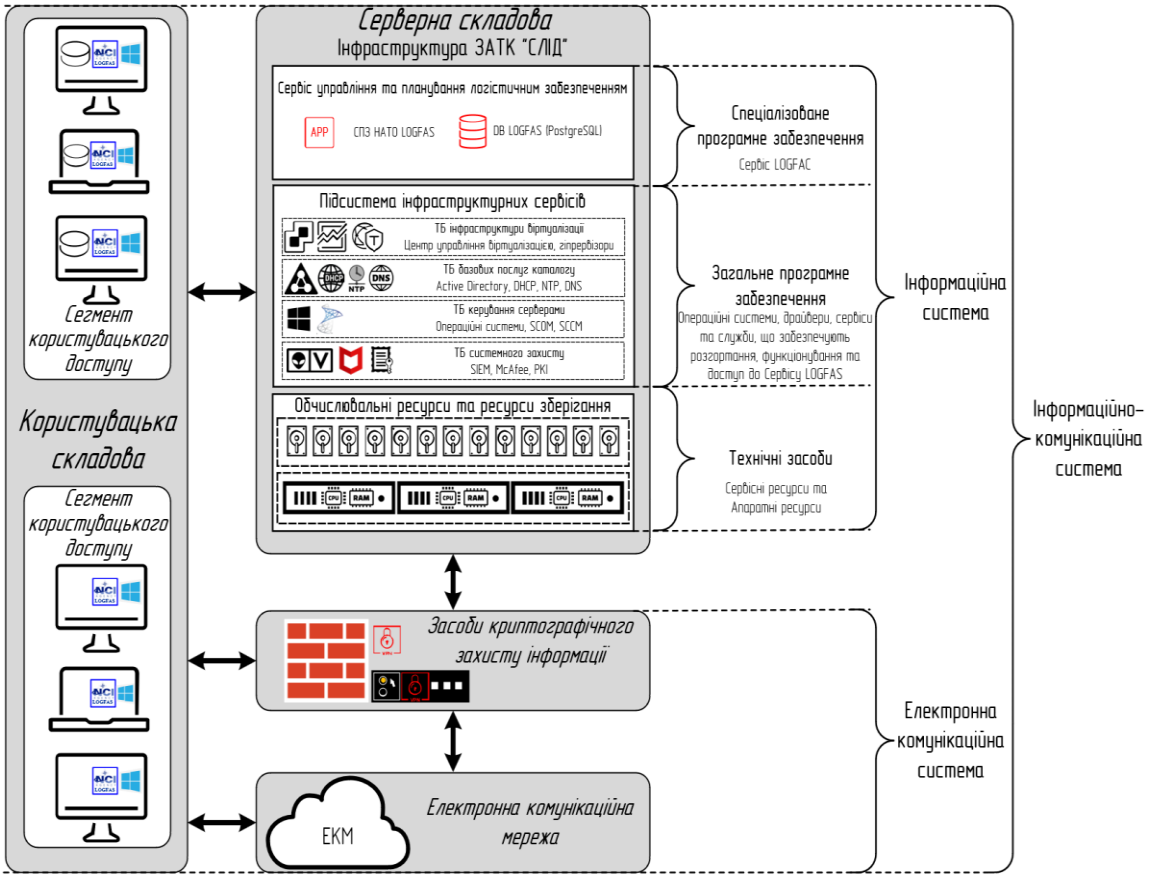


Рис. 1. Схема ІКС LOGFAS

ІКС LOGFAS складається з таких основних елементів:

інформаційна система (далі – ІС):

сервіс планування та управління логістичним забезпеченням (далі – Сервіс LOGFAS) (сервери з інстальованим спеціалізованим програмним забезпеченням НАТО LOGFAS, що розгортаються з використанням потужностей ЗАТК “СЛІД”);

базові сервіси, служби, виділені обчислювальні ресурси та ресурси зберігання інфраструктури ЗАТК “СЛІД”, що забезпечують розгортання, функціонування та доступ до Сервісу LOGFAS.

електронна комунікаційна система:

електронні-комунікаційні мережі (електронна-комунікаційна мережа ЗС України, мережа Інтернет тощо);

апаратні, програмно-апаратні засоби криптографічного захисту інформації, через які ПКК здійснюють підключення до Сервісу;

користувацький сегмент (далі – КС):

пристрої кінцевих користувачів тактичного рівня з інстальованими ІКС LOGFAS;

пристрої кінцевих користувачів оперативного рівня з інстальованими ІКС LOGFAS;

пристрої кінцевих користувачів стратегічного рівня з інстальованими ІКС LOGFAS;

пристрої кінцевих користувачів – стаціонарні ПЕОМ, ноутбуки, інші пристрої під керуванням операційної системи Windows з інстальованим спеціалізованим програмним забезпеченням;

засоби криптографічного захисту інформації – апаратно-програмні та апаратні засоби, що призначені для криптографічного захисту інформації.

На етапі організації заходів щодо створення комплексної системи захисту інформації ІКС визначається:

класифікація інформації, що оброблюється в ІКС;

політика безпеки, яка має визначати:

ресурси ІКС, що потребують захисту;

категорії інформації, яка обробляється в ІКС;

загрози до недопущення витоку інформації;

вимоги щодо ознайомлення користувачів ІКС з положеннями політики безпеки і вимоги до персональної відповідальності за їх дотримання;

відповідальність за відмову від авторства та за відмову від отримання інформації у процесі роботи в ІКС;

рівні користувачів та регламенти надання доступу за рівнями, матриця доступу до об'єктів ІКС;

вимоги до користувачів за їх рівнями доступу до ІКС, що включають опис необхідних пройдених курсів, екзаменів, сертифікатів щодо СПЗ, тощо;

вимоги до підрядної організації, яка буде виконувати супровід компонентів СПЗ та вносити зміни до них;

контроль версій змін до програмного коду компонентів СПЗ, порядок постановки задач на зміни та прийняття виконаних робіт розробника.

Спеціалізоване програмне забезпечення (далі – СПЗ) [27], що розгортається на серверній складовій ІКС та в свою чергу надає користувачам ІКС – Сервіс планування та управління логістичним забезпеченням "Сервіс LOGFAS".

СПЗ LOGFAS інсталюється як на сервер (серверна складова ІКС), так і на пристроях кінцевих користувачів (Користувацька складова ІКС). Цей розділ присвячений серверній складовій ІКС. Розгортання СПЗ в користувацьких сегментах ІКС на пристроях кінцевих користувачів.

СПЗ LOGFAS – інструмент, який використовується для надання командуванням, штабам на всіх рівнях детальної, точної і своєчасної інформації.

Також СПЗ LOGFAS – це програмне забезпечення НАТО, яке можна використовувати для участі в програмі "Партнерство заради миру" та інших уповноважених країнах і організаціях. Програмне забезпечення є продуктом НАТО "off the shelf" (з полиці), без ліцензійне і може бути встановлене на будь-якій робочій станції (мережевих і автономних комп'ютерах, включаючи ноутбуки).

Як зазначалось вище сервіс LOGFAS, окрім виконання своїх спеціалізованих функції, щодо планування та управління системою забезпечення матеріальними ресурсами також забезпечує управління базами даних користувачів та їх реплікацією.

Особливістю цієї СПЗ є те, що бази даних користувачів зберігаються на пристроях кінцевих користувачів та за допомогою додаткового спеціалізованого компонента здійснюється реплікація в централізовану базу даних сервера ІКС.

Використання СПЗ НАТО LOGFAS дає змогу працювати з окремими масивами даних, зокрема з даними окремих країн. Для використання LOGFAS для потреб України необхідно підготувати у форматі вхідних даних системи та завантажити значний обсяг даних. Крім того, низка алгоритмів, використаних у процесі створенні ІКС не надаються і не розкриваються, оскільки є інформацією з обмеженим доступом.

Враховуючи зазначене, потенційне впровадження системи LOGFAS в Україні потребує:

радикальних змін у доктринальній та нормативній базі для приведення їх у відповідність з нормативною базою НАТО, що лежить в основі ІКС LOGFAS;

значних зусиль для підготовки або завантаження та підтримки в актуальному стані вхідних даних логістичного планування;

створення вітчизняного математичного забезпечення (моделей, методів, алгоритмів) підтримки прийняття управлінських рішень у системі забезпечення матеріальними ресурсами.

Система LOGFAS може забезпечити частину необхідних функцій планування логістичної підтримки системи забезпечення в Україні щодо логістичних аспектів оборонного та оперативного планування.

За допомогою впровадженої системи LOGFAS можливе ведення обліку наявності та переміщення матеріальних засобів, оформлення заявок на переміщення та інших документів, що є важливою складовою системи забезпечення матеріальними ресурсами.

Основними перевагами використання ІКС LOGFAS в Україні є можливість швидкого запуску в експлуатацію і отримання практичних результатів (програмне забезпечення LOGFAS вже готове і не потребує часу і зусиль на розроблення).

Отже, за допомогою удосконалення та впровадження ІКС LOGFAS на оперативному рівні можливо підвищити ефективність управління системою забезпечення матеріальними ресурсами.

Висновки. Автоматизація управління системою забезпечення матеріальними ресурсами має бути одним з пріоритетних напрямів роботи з підвищення ефективності управління системою забезпечення матеріальними ресурсами ЗС України. Створення нових і модернізація існуючих автоматизованих систем управління на основі передових інформаційних технологій, дозволить підвищити ефективність управління системою забезпечення матеріальними ресурсами ЗС України, скоротити час на одержання і всебічну оцінку відомостей про

матеріальні ресурси на всіх етапах їх руху, підвищити ефективність системи забезпечення, а також поліпшити взаємодію з аналогічними системами країн – членів НАТО.

Узагальнюючи викладене, слід зазначити, що система СЗМР має бути адаптивна та своєчасно реагувати на виклики, які виникають.

Формування ефективної системи забезпечення матеріальними ресурсами в ЗС є вимогою часу і сприяє вирішенню важливого питання, яке полягає у скороченні часу та витрат на своєчасному забезпечення в повному обсязі матеріальними ресурсами військ (сил).

СЗМР може ефективно функціонувати за умови отримання необхідного обсягу інформації і ефективним управлінням потоками інформації та прийнятті раціональних управлінських рішень. Для розвитку СЗМР потребує постійного вдосконалення система інформаційних потоків за допомогою таких інструментів, як спеціалізоване програмне забезпечення LOGFAS.

Подальші дослідження доцільно зосередити на аналізі Дорожньої карти впровадження у СЗМР МО України СПЗ LOGFAS та оцінці ймовірності її успішної реалізації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Звіт російсько-української війни. Збірник № 4-8.
2. Задорожнюк Н. О. Сучасне програмне забезпечення для здійснення бізнес-аналізу // Економічний вісник НТУУ “Київський політехнічний інститут”. 2021. URL: http://ev.fmm.kpi.ua/article/view/230070.
3. Стрюк А. М. Інженерія програмного забезпечення: перші 50 років становлення та розвитку // Інформаційне право. 2018. URL: http://www.economy.nayka.com.ua/?op=1&z=4780.
4. Дядюн О. О. Програмне забезпечення як нематеріальний актив підприємства: обліковий аспект // Бухгалтерський облік. 2018. № 3. URL: https://journals.indexcopernicus.com/api/file/viewByFileId/399575.pdf.
5. Роїк М. В. Огляд програмних засобів статистичного аналізу даних // Ефективна економіка. 2017. № 7. URL: http://www.economy.nayka.com.ua/?op=1&z=5676.
8. Ролін І. Ф., Морозов І. Є. , Минько О. В. Зміст основних термінів у сфері логістичного забезпечення військових формувань // Системи озброєння і військова техніка. 2017. № 1 (49). С. 61–64.
9. Основні положення щодо логістичного забезпечення національної гвардії України / О. Г. Бондаренко та ін. // Вісник економіки транспорту і промисловості. 2018. № 61. С. 230–240.
10. Вироблення єдиних поглядів щодо створення сучасної державної системи логістики Збройних Сил України / В. С. Кивлюк та ін. // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2016. Вип. 51. С. 100–109.
11. Основи логістики : навч. посіб. / В. О. Дачковський та ін. Київ : НУОУ ім. Івана Черняховського, 2018. 204 с.
12. Закалад М. А., Педан Ф. П., Романченко О. А. Підходи до формування основних характеристик АСУ логістичного забезпечення ЗС України // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2018. № 1. С. 97–101.
13. Науменко М. О., Морозова Л. В. Удосконалення організаційної та функціональної структури логістичного забезпечення Збройних сил України // Бізнес Інформ. 2016. № 3. С. 279–284. URL: http://nbuv.gov.ua/UJRN/binf_2016_3_43.
14. Дачковський В. О., Сампір О. Алгоритм функціонування системи логістичного забезпечення // Сучасні інформаційні технології у сфері безпеки та оборони. 2019. № 35 (2). С. 87–92. URL: https://www.researchgate.net/publication/337461598_ALGORITM_FUNKCIONUVANNA_SISTEMI_LOGISTICNOGO_ZABEZPECENNA.
15. Основні положення логістичного забезпечення Збройних сил України : наказ МОУ від 11.10.2016 р. № 522. URL: http://www.mil.gov.a/ministry /normativnopravova-baza/nakazi-ministra oboroniukraini/nakazi-ministerstva-oboroni-ukrainiza-2016-rik. html.
16. Положення про управління правового забезпечення Генерального штабу ЗС України : затв. наказом Генерального штабу Збройних Сил України від 16.05.2011 р. № 90 : із змінами.
17. Положення про Головне управління логістики Збройних Сил України : затв. наказом Генерального штабу Збройних Сил України від 16.06.2017 р. № 209.
18. Ганненко Ю., Закалад М. Аналіз ефективності функціонування системи логістики у провідних країн світу з використанням автоматизованої системи управління // Сучасні інформаційні технології у сфері безпеки та оборони. 2023. № 1. URL: http://tta.org.ua/index.php/2311-7249/article/view/190490.
19. Battle Command and Sustainment Support System (BCS3). URL: https://www.globalsecurity.org/military/systems/ground/bcs3.htm.
20. Про впровадження у дослідну експлуатацію інформаційно-комунікаційної системи планування та управління логістичним забезпеченням з використанням спеціалізованого програмного забезпечення НАТО LOGFAS :

наказ Міністерства оборони України від 18.08.2022 р. № 242.
21. Дорожня карта впровадження у Міністерстві оборони України та Збройних Силах України інформаційно-комунікаційної системи планування та управління логістичним забезпеченням з використанням спеціалізованого програмного забезпечення НАТО LOGFAS (від 20.07.2022 № 16481/з/2)
22. AJP-4(A). ALLIED JOINT DOCTRINE FOR LOGISTICS. NATO. 2018. 84 с.
23. AJP-4.4(A). ALLIED JOINT MOVEMENT AND TRANSPORTATION DOCTRINE: NSA. 2013. 90 с.
24. AJP-01(D) : Доктрина об'єднаних сил НАТО : довідкові матеріали. Київ : НУОУ ім. Івана Черняховського, 2016. 130 с.
25. NATO Logistics Handbook. Brussels : NATO HQ, 2012. 207 с.
26. Про затвердження Основних положень логістичного забезпечення ЗС України : наказ Міністерства оборони України від 11.10.2016 р. № 522.
27. Спеціалізоване програмне забезпечення LOGFAS. URL: https://lognet.nato.int/.

Стаття надійшла до редакційної колегії 04.08.2023

Implementation of an automated system for managing material resources of the Armed Forces of Ukraine (defense forces)

Annotation

An analysis of the current state of the system for providing material resources (SPMR) of the Armed Forces of Ukraine, the experience of conducting combat operations to repel an attack by an aggressor, revealed a number of problems, as a result of which it is impossible to properly provide material resources to the Armed Forces of Ukraine. For effective management of the processes for providing material resources to the Armed Forces of Ukraine, it is necessary to use a system solution for the formation of an automated system for managing the provision of material resources (ASMPMR).

The information and communication system LOGFAS (provided by the partner countries as international military-technical assistance) is designed to plan the provision of material resources, support the processes of movement and transportation of troops (forces), material resources, plan the strategic deployment of troops (forces) in certain operational zones (areas).

The purpose of the article is to analyze the LOGFAS software to form reasonable recommendations for its implementation when creating an automated control system for a system providing material resources.

The main advantages of using IS LOGFAS in Ukraine are the ability to quickly put it into operation and obtain practical results (the LOGFAS software is ready and does not require time and effort to develop) and full compliance with NATO standards.

The LOGFAS system can be one of the components of the information system, with the help of which it is possible to increase the efficiency of managing the system for providing material resources to operational-tactical groupings of troops in the course of combat operations.

Keywords: system of providing material resources; automated management system; Information Technology; specialized LOGFAS software; large-scale armed aggression.

УДК 004.7 DOI: https://doi.org/10.33099/2304-2745/2023-2-78/108-120

Ліпко І. О. (0009-0001-6663-5899)
Звір В. Б. (0000-0002-6823-7552)
Миколенко Ю. М., кандидат військових наук (0000-0001-9740-2521)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Модель досягнення взаємосумісності комунікаційних та інформаційних систем: запровадження досвіду НАТО в інтересах сил оборони держави

Резюме. У статті проведено дослідження доктринального та нормативного забезпечення взаємосумісності комунікаційних та інформаційних систем в НАТО, діючого нормативного забезпечення впровадження інформаційних технологій у Міністерстві оборони України. За результатами проведених досліджень запропонована модель доктринального та нормативного забезпечення заходів із досягнення взаємосумісності комунікаційних та інформаційних систем сил оборони.

Ключові слова: доктринальне та нормативне забезпечення; FMN; взаємосумісність комунікаційних та інформаційних систем.

Постановка проблеми. Стратегічними документами держави визначені напрями зосередження основних зусиль складових сектору безпеки і оборони щодо європейського та євроатлантичного прагнення України.

Основою Стратегії воєнної безпеки України є всеохоплююча оборона України, одним із основних напрямів її досягнення є упровадження в силах оборони передового досвіду, принципів і стандартів держав – членів НАТО, участь у спільних операціях та навчаннях для досягнення критеріїв членства в НАТО з подальшою інтеграцією в євроатлантичні безпекові структури [1].

Розвиток оперативних, бойових і спеціальних спроможностей сил оборони має бути зосереджено на запровадженні, у тому числі інформаційних технологій та електронних комунікацій. Їх запровадження має здійснюватися у рамках Стратегічної цілі 1. Завдання 1.5: Цифровізація діяльності та впровадження сучасних інформаційних технологій, зокрема електронних комунікацій, у сфері оборони.

Також слід зауважити, що практично у всіх стратегічних цілях відслідковуються вимоги щодо розвитку складових сил безпеки та оборони відповідно до підходів та стандартів НАТО.

Для виконання стратегічних цілей та завдань у листопаді 2022 року Міністром оборони України було затверджено Статут програми проєктів "Впровадження ефективного оборонного менеджменту і системи об'єднаного керівництва силами оборони та військового управління у Збройних Силах України", яким визначено Завдання 1.5. У рамках визначеного завдання мають бути організовані заходи щодо стандартизації, оптимізації та забезпечення взаємосумісності комунікаційних та інформаційних систем сил оборони держави. Очікуваним результатом вказаного мають бути розроблені відомчі документи щодо створення, функціонування та забезпечення Об'єднаної мережі оборони та мереж операцій з урахуванням стандартів та підходів НАТО.

Таким чином, вбачається актуальним розроблення структури відомчих документів для досягнення визначеного запланованого результату.

Аналіз останніх досліджень і публікацій. Розвиток сучасної ІТ-інфраструктури в силах оборони розглядається як розвиток спеціальних спроможностей цих сил. Такий розвиток здійснюється у рамках оборонного планування розвитку військ (сил) на основі спроможностей за базовими складовими спроможності DOTMLPFI (*en: Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability; укр: Доктринальна база, Організація, Підготовка, Ресурсне забезпечення, Управління та освіта, Персонал, Військова інфраструктура, Взаємосумісність*), порядок щодо організації та його здійснення визначені у наказі [2] та доктринальному документі [3].

Протягом останніх років вітчизняними науковцями була проведена значна кількість досліджень як з питання оборонного планування, так і з питання імплементації документів і стандартів НАТО [4–9] (вказаний перелік наукових досліджень не є вичерпним). Внаслідок вказаного у Міністерстві оборони України (далі – МО України) та Збройних Силах України (далі – ЗС України)

побудовано цілісну систему оборонного планування, яка відповідає підходам та стандартам НАТО.

Таким чином, з урахуванням вказаних джерел одним із важливих аспектів розвитку спроможностей є розвиток доктринальної та нормативної бази D *(Doctrine)*. Під розвитком доктринальної та нормативної бази розуміється процес створення необхідних концепцій, настанов, стандартів, процедур, інструкцій тощо, що визначають методи та способи виконання завдань з розвитку конкретної спроможності, у тому числі, створення нових спроможностей, у нашому випадку – з розвитку комунікаційних та інформаційних систем та ІТ-сервісів (далі для позначення ІТ-сервісів використовується термін "сервіс").

Водночас, у [2–9] не враховані особливості доктринального та нормативного забезпечення розвитку такої специфічної сфери, як ІТ-сфера, яка є високотехнологічною, характеризується швидкою та постійною зміною технологій обробки даних й інформації, у тому числі обладнання, на якому здійснюється така обробка (у середньому життєвий цикл інформаційної технології становить близько 3-5 років). Наглядним прикладом вказаного є порівняння можливостей сучасного смартфона та смартфона, який використовувався у 2018 році. При цьому, спроможності сучасного смартфона перевищують спроможності ПЕОМ 2013 року. Хмарні обчислення, які є тенденцією сьогодення, на початку 2010-х років були на початковому рівні розвитку. І таких прикладів в ІТ-сфері можливо навести безліч.

Відповідно до положень [1] у силах оборони України має бути розгорнута об'єднана мережа оборони та мережі операцій, обмін інформацією в яких здійснюється відповідно до технічних та процедурних принципів та рівнів взаємосумісності НАТО.

Під *об'єднаною мережею оборони* розуміється єдина мережа, яка поєднує в собі окремі мережі та/або інформаційні, електронні комунікаційні, інформаційно-комунікаційні системи складових сил оборони, обмін інформацією між якими здійснюється відповідно до технічних, процедурних принципів, принципів захисту інформації та рівнів взаємосумісності.

У свою чергу, *мережа операції* являє собою єдиний комплекс спроможностей, який включає в себе сукупність незалежних електронних комунікаційних та інформаційних систем, управління, процеси і процедури, створені для проведення операції, навчання, тренування або перевірки на взаємосумісність.

На сьогодні, в НАТО досягнення взаємосумісності здійснюється у рамках ініціативи FMN *(en: Federated Mission Networking, укр: Об'єднана мережа для проведення операцій)* [10], яку було започатковано в НАТО з 2015 року.

У МО України в продовж останніх років було напрацьовано ряд відомчих документів, які є підґрунтям запровадження вказаної ініціативи НАТО FMN. Основними такими документами є:

Концепція розвитку ІТ-інфраструктури МО України та ЗС України (затверджена у листопаді 2021 року Міністром оборони України);

ключова доктрина "Зв'язок та інформаційні системи" (затверджена у липні 2020 року Головнокомандувачем ЗС України);

Об'єднана оперативна концепція сил оборони 2030 (затверджена у листопаді 2021 року начальником Генерального штабу ЗС України).

При цьому, положення вказаних доктринальних документів також розповсюджуються на складові сектору безпеки та оборони України.

Слід зазначити, що систематизованих досліджень з питання розвитку доктринальної та нормативної бази в інтересах сил оборони для досягнення технічних та процедурних принципів та рівнів взаємосумісності з НАТО в доступному для аналізу україномовному домені не знайдено. У науковій літературі висвітлена, в основному, тематика, що стосується технічної сторони взаємосумісності комунікаційних та інформаційних систем. Так, публікації [11–13] направлені на досягнення цієї взаємосумісності у тактичному просторі – на рівні, так званих, "солдатських" мереж передачі даних. У дослідженнях [14–15] розглянуто дата-центричний підхід, який, згідно положень ініціативи FMN, є основою побудови інформаційної інфраструктури із використанням хмарних технологій.

Мета статті – на основі аналізу підходів НАТО щодо доктринального забезпечення ініціативи FMN та набутого вітчизняного досвіду розробити модель структури доктринальних та нормативних документів з питання досягнення взаємосумісності комунікаційних та інформаційних систем.

Виклад основного матеріалу. На засіданні Комісії Україна-НАТО на рівні глав держав та урядів (у рамках Саміту НАТО в Уельсі) було проголошено про створення С4-Трастового фонду Україна – НАТО *(en: NATO Ukraine C4 Trust Fund)* (далі – С4-фонд). Виконавчим органом фонду було визначено Агенцію НАТО зі зв'язку та інформації *(en: NATO Communications and Information Agency, NCIA Agency)*. Керівництво фондом було покладено на такі держави – члени НАТО: Німеччина, Канада, Велика Британія. Також до спонсорства у фонді було залучено Данію, Ісландію, Латвію, Польщу, Туреччину та Сполучені Штати Америки. Починаючи з грудня 2021 року всі трастові фонди та програми, які були направлені на допомогу Україні, у тому числі, й С4-фонд, були об'єднані в єдиний Трастовий фонд НАТО з Комплексного пакету допомоги Україні *(en: NATO-Ukraine Comprehensive Assistance Package (CAP) Trust Fund)*.

Довідка. В НАТО [16] запроваджено концептуальну семантичну модель, яка складається з:

- домену С3-системи *(en: Consultation, Command and Control (C3) systems)*, який у свою чергу включає у себе:

консультації *(en: Consultation)* – політичні консультації, кризисне управління, консультації з питань застосування ядерної зброї, співробітництво у сфері партнерства заради миру, захисту цивільного населення тощо, що є відповідальністю цивільної структури НАТО;

систему управління (командування та управління) *(en: Command and Control, C2)*, яка є відповідальністю військової структури НАТО;

сенсорні системи та командні пункти;

- комунікаційних та інформаційних систем *(en: Communication and information systems, CIS)*, які забезпечують підтримку С3-системи. Наприклад, С2-системи *(en: Command and Control (C2) systems)* забезпечують управління підпорядкованими органами управління та частинами (підрозділами).

Також у збройних силах США широко використовуються такі поняття для С-систем:

С3-системи *(en: Command, Control and Communication (C3) systems)* – є узагальнюючим терміном для позначення сукупності стратегічних та тактичних комунікаційних та інформаційних систем, за допомогою яких здійснюється передача інформації та даних;

С4ISR-системи *(en: Command, Control, Communication and Computers (C4) Intelligence, Surveillance and Reconnaissance (ISR) systems)* – є концепцією побудови сучасних комунікаційних та інформаційних систем разом із системами спостереження та розвідки для забезпечення переваги у ситуаційній обізнаності, у т.ч. про противника і навколишнє середовище, та скорочення часу на визначення та ураження цілей;

С5ISR-системи *(en: Command, Control, Communication, Computers and Cyber (C5) Intelligence, Surveillance and Reconnaissance (ISR) systems)* – є концепцією побудови майбутніх комунікаційних та інформаційних систем разом із системами спостереження та розвідки для забезпечення переваги над противником у кіберпросторі;

С6ISR-системи *(en: Command, Control, Communication, Computers, Cyber and Combat (C6) Intelligence, Surveillance and Reconnaissance (ISR) systems)* – є також концепцією побудови майбутніх комунікаційних та інформаційних систем із застосуванням бойових тактичних систем.

Слід зауважити, що [16] запроваджено військовим стандартом ВСТ 01.112.004 – 2017 (01) "Військовий зв'язок та інформаційні системи. Словник НАТО з систем зв'язку та інформаційних систем (AAP-31 (Edition 3), IDT)".

Основним завданням С4-фонду є трансформація ЗС України завдяки модернізації їх С4-спроможностей, а також підвищення взаємосумісності із С4-системами НАТО. Вказаний фонд виявився ефективним механізмом досягнення вказаного завдання, у рамках якого здійснюється обмін знаннями, постачання обладнання, побудова спільних мереж тощо.

Завдяки вказаному фонду представникам складових сектору безпеки та оборони було надано доступ до інформаційного ресурсу НАТО *Tidepedia* (https://tide.act.nato.int), який є надсучасною базою С4-знань НАТО, та є платформою обміну знаннями з експертами НАТО у відповідних сферах діяльності. Слід зауважити, що Tidepedia це те джерело інформації, завдяки якому представники сил оборони мають можливість доступу до інформації про ініціативу FMN.

Довідка. Вікі Tidepedia є частиною ініціативи НАТО TIDE, яка спирається на Технології *(en: Technologies)* з метою досягнення переваги в Інформації *(en: Information)*, Прийняті рішень *(en: Decision)* та Застосуванні військ *(en: Execution)*. Метою вікі є забезпечити в мережі Інтернет всеохоплююче і стійке середовище співпраці та сховище інформації для спільноти оперативних експертів, менеджерів програм та проєктів, розробників спроможностей та менеджерів вимог, дослідників, експериментаторів та організацій підтримки, які зацікавлені в консультаціях, командуванні та управлінні *(en: consultation, command and control, C3)* НАТО, держав – членів та партнерів НАТО, а також асоційованих наукових та промислових підприємств. Цей веб-сайт розміщений на ресурсах Союзного командування НАТО з трансформації *(en: Allied Command Transformation, ACT)*.

У загальному вигляді концептуальна модель доктринального забезпечення взаємосумісності комунікаційних та інформаційних систем в НАТО наведена на рис. 1.

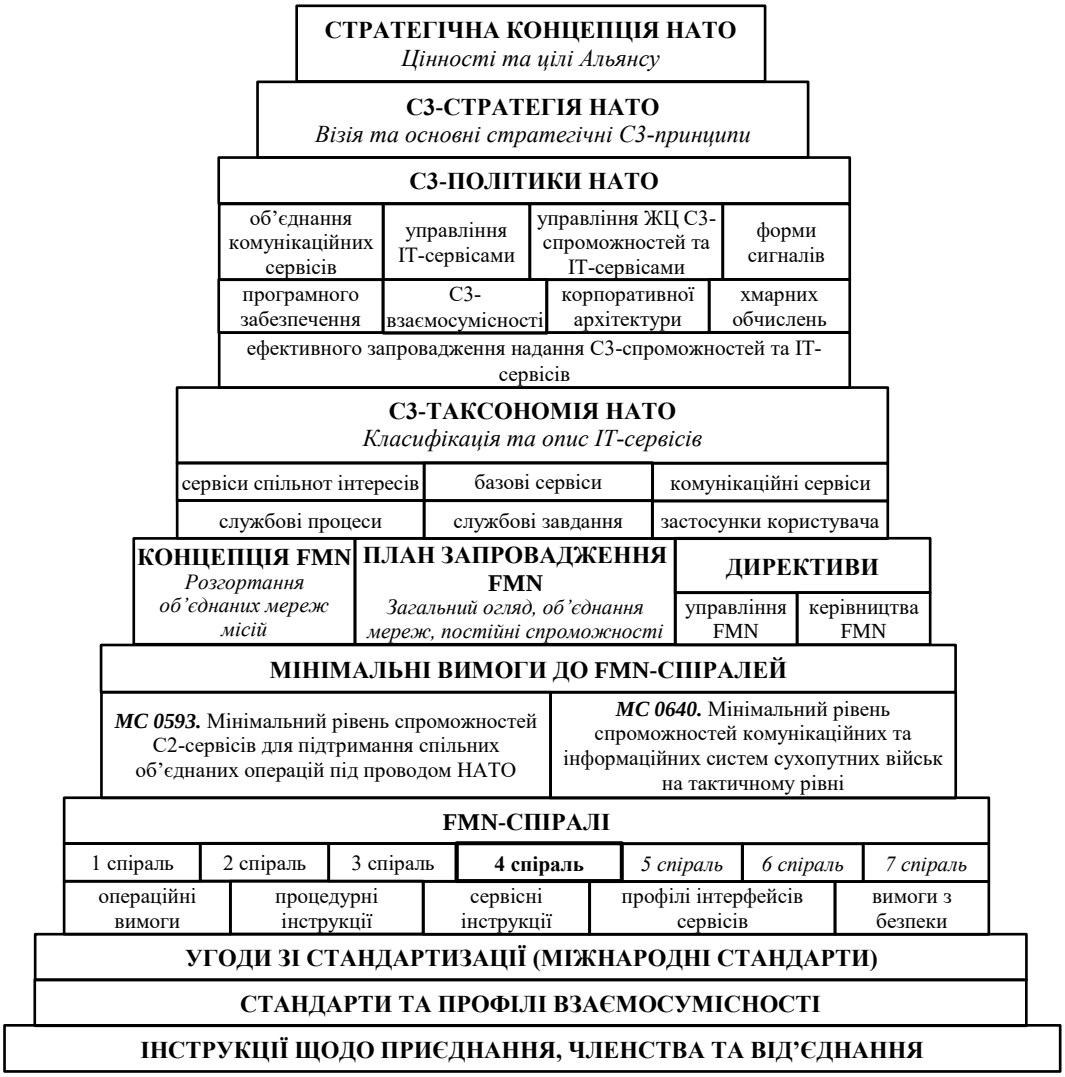


Рис. 1. Концептуальна модель доктринального забезпечення взаємосумісності комунікаційних та інформаційних систем в НАТО

Стратегічна концепція НАТО *(en: NATO Strategic Concept)* є ключовим документом, що визначає цінності та цілі Альянсу. У ній міститься колективна оцінка викликів безпеці, що існують для держав – членів НАТО, визначаються політичні і воєнні завдання щодо протидії цим викликам. У останній концепції, яку було прийнято у минулому році на Саміті НАТО у Мадриді, зазначено що одним із основоположних завдань НАТО є цифрова трансформація НАТО, запровадження новітніх технологій, вдосконалення комп'ютерних мереж та інфраструктури тощо [17].

С3-стратегією Альянсу *(en: Alliance C3 Strategy)* визначено візію та основні стратегічні принципи, якими повинні керуватися зацікавлені сторони НАТО під час своєї діяльності. Вказаною візією визначено, що інформаційна перевага та перевага у швидкості прийняття рішень досягається за рахунок ефективного використання ІТ-технологій шляхом надання зацікавленим сторонам розширених С3-спроможностей. Прикладами вказаних принципів є: забезпечення розвитку С3-спроможностей та сервісів відповідно до DOTMLPFI, С3-спроможності визначаються та надаються в якості сервісів тощо. При цьому, стратегічною ціллю для держав – членів НАТО та держав – партнерів НАТО, у разі їх залучення в операціях під проводом НАТО, повинно бути дотримання принципів FMN.

С3-політики Альянсу *(en: Alliance C3 Policy)* є фундаментальним механізмом забезпечення виконання Альянсом своїх основних завдань шляхом узгодженого запровадження та надання взаємосумісних та сучасних С3-спроможностей та сервісів. С3-політики складаються з таких окремих політик, які наведено у Табл. 1.

Таблиця 1

Перелік С3-політик НАТО

№	ПОЛІТИКА	ТЛУМАЧЕННЯ
1	**Управління ІТ-сервісами** *NATO Information and Communications Technology Service Management Policy*	Обов'язкові принципи щодо надання, використання та управління сервісами в НАТО відповідно до положень ITIL *(Information Technology Infrastructure Library)*
2	**Управління життєвим циклом С3-спроможностей та ІТ-сервісів** *C3 Capabilities and ICT Services Lifecycle Management Policy*	визначає основні напрями розвитку, запровадження, використання та еволюції С3-спроможностей та сервісів НАТО, функції та завдання різного роду зацікавлених сторін в цих процесах
3	**З питання форми сигналів** *Waveform Policy*	визначає принципи направлені на досягнення взаємосумісності безпровідних мереж із використанням технологій програмованого радіозв'язку та сучасних сумісних форм сигналів коливань
4	**С3-взаємосумісності** *Alliance Consultation, Command and Control (C3) Interoperability Policy*	визначає принципи та основні завдання з розвитку та ефективного використання С3-спроможностей та сервісів з метою досягнення взаємосумісності та підтримки обміну інформацією через основні виміри: технічні, процедурні та людські
5	**Об'єднання комунікаційних сервісів** *Federation of Communications Services Policy*	визначає принципи об'єднання мереж через сервіс-провайдерів НАТО та національних сервіс-провайдерів з мето підтримки процесів, завдань та місій НАТО
6	**Програмного забезпечення** *NATO Software Policy*	визначає заходи з підвищення якості, економічної ефективності, взаємосумісності як у межах НАТО, так і поза ним, національного використання та безпеки НАТО програмного забезпечення, яке придбане або знаходиться під управлінням структур НАТО
7	**Ефективного запровадження надання С3-спроможностей та ІТ-сервісів** *Policy on the Efficient Implementation of C3 Capabilities and ICT Services Delivery*	визначає принципи зі сприяння, розвитку, оцінки, вибору та запровадження пропозицій щодо визначення вимог до С3-спроможностей та сервісів для їх вчасного придбання у найбільш ефективний спосіб
8	**Корпоративної архітектури** *NATO Enterprise Architecture Policy*	описує вимоги для стандартизації С3-спроможностей та взаємосумісних сервісів з метою досягнення цілей НАТО та супроводження щоденних службових процесів, заходів, тренувань та навчань
9	**Хмарних обчислень** *NATO Cloud Computing Policy*	визначає принципи забезпечення, підтримки та використання спільної сервіс-орієнтованої обчислювальної інфраструктури (хмари) для досягнення більшої доступності, гнучкості, безпеки та мобільності з метою зменшення витрати

Як було раніше зазначено у С3-стратегії Альянсу, С3-спроможності визначаються та надаються в якості сервісів. Ураховуючи вказане, класифікацію та опис сервісів в НАТО визначено у документі С3-таксономія *(en: C3 Taxonomy)*. На це час, С3-таксономія складається з таких окремих таксономій:

сервіси спільнот інтересів *(en: C3 Community of Interest Services Taxonomy)*;

базові сервіси *(en: C3 Core Services Taxonomy)*;

комунікаційні сервіси *(en: C3 Communications Services Taxonomy)*;

службові процеси *(en: C3 Business Processes Taxonomy)*;

службові завдання *(en: C3 Business Roles Taxonomy)*;

застосунки користувача *(en: C3 User Applications Taxonomy)*.

Слід зауважити, що протягом наступних років до вказаної таксономії заплановано включити додаткові таксономії, у яких класифікують та нададуть опис С3-спроможностей, обладнання та інформаційних продуктів.

Запровадження ініціативи FMN здійснюється відповідно до:

Концепції FMN *(en: FMN Concept)*: описує підходи із забезпечення комплексного керівництва з розгортання об'єднаних мереж місій, які будуть спроможними до ефективного обміну інформацією між НАТО, державами – членами НАТО, державами – партнерами НАТО та не-НАТО організаціями, які приймають участь в операціях;

Плану запровадження (реалізації) ініціативи FMN в НАТО *(en: NATO FMN Implementation Plan),* який є комплексним документом, що складається з трьох основних розділів та більше 20 додатків до них, у яких викладено:

загальний опис запровадження ініціативи FMN;

принципи об'єднання мереж;

постійні спроможності НАТО.

У цих документах закладено основна парадигма FMN: об'єднані мережі місій повинні будуватись на довірі й узгодженості та бути спроможними забезпечити командування та управління в операціях під проводом НАТО.

На підставі вказаних документів розроблено відповідні директиви НАТО, якими визначені:

завдання та повноваження, відповідальність та обов'язки, функції та процеси структур, які задіяні в керівництві FMN – у Директиві з керівництва FMN *(en: FMN Governance Directive)*;

завдання, структуру та основні обов'язки структур з управління FMN, зокрема визначені процеси, ключові продукти та взаємозв'язок між цими продуктами та структурами – у Директиві з управління FMN *(en: FMN Management Directive)*.

Основою для розроблення вимог до сервісів, що визначаються у "спіралях FMN", є Мінімальні вимоги до FMN-спіралей. Вказані вимоги розробляються відповідно до таких документів Військового комітету НАТО:

мінімальний рівень спроможностей С2-сервісів для підтримання спільних об'єднаних операцій під проводом НАТО *(en: MC 0593. Minimum Level of C2 Service Capabilities in Support of Combined Joint NATO Led Operations)*;

мінімальний рівень спроможностей комунікаційних та інформаційних систем сухопутних військ на тактичному рівні *(en: MC 0640. Minimum Level of CIS Capabilities at Land Tactical Level)*.

Розвиток FMN спирається на так звані "спіралі FMN", якими визначаються переліки сервісів, які повинні функціонувати протягом проведення операцій під проводом НАТО, та вимог щодо їх побудови для забезпечення їх взаємосумісності. Реалізація спіралей здійснюється в рамках 4-х річного циклу від затвердження вимог до їх реалізації у діючих комунікаційних та інформаційних системах. На сьогодні вже розроблено 4 спіралі та здійснюється робота над 5 спіраллю.

Зазвичай спіралі складаються з операційних вимог *(en: Operational Requirements)*, процедурних *(en: Procedural Instructions)* та сервісних *(en: Service Instructions)* інструкцій, профілів інтерфейсів сервісів *(en: Service Interface Profile)* та вимог з безпеки *(en: Security Requirements)*.

Операційними вимогами визначені загальні вимоги до системи в цілому, які реалізовані у цій спіралі та можуть у подальшому удосконалюватися.

У процедурних інструкціях описуються процеси, інформаційні продукти та завдання.

Вимоги з технічної побудови сервісів та завдання з їх запровадження визначені у сервісних інструкціях.

А у профілях інтерфейсів сервісів визначені інтерфейси для сервісів, які використовують різні протоколи, для їх взаємодії в рамках однієї коаліційної мережі операцій.

Діюча 4 спіраль FMN складається з:

специфікації спіралі, у якій описані загальні положення про взаємосумісність, архітектуру взаємосумісності, коротка характеристика процедурних та сервісних інструкцій разом із описом внесених до них змін, терміни та їх визначення, надано перелік стандартів та їх короткий опис, наведено посилання на використані джерела інформації тощо;

загального опису операційних вимог, які були використані для розроблення цієї спіралі та попередніх спіралей;

загального опису вимог до безпеки, які були використані для розроблення цієї спіралі та попередніх спіралей;

процедурних інструкцій, якими описано 13 процесів (наприклад, Процедурною інструкцією з комунікації визначені правила розподілу фізичних IP-адрес та номерів автономних систем для різних типів мереж й інтерфейсів; залежності цієї інструкції від інших та з іншими процедурними та сервісними інструкціями тощо);

сервісних інструкцій, якими визначені технічні вимоги до 22 сервісів (наприклад, Сервісною інструкцією з комунікації визначені профілі стандартів (тобто, наборів стандартів) доступу до комунікацій та транспорту комунікацій; опис концепції системи; залежності цієї інструкції від інших та з іншими процедурними та сервісними інструкціями тощо);

11 профілів інтерфейсів сервісів (наприклад, Профілем інтерфейсу сервісу для зв'язування метаданих із загальними форматами даних визначено використання відкритого XML-формату, який описано у міжнародному стандарті ISO/IEC 29500, та офісних застосунків корпорації Microsoft (Word, Excel, PowerPoint) тощо).

Довідка. Розроблення процедурних інструкцій здійснюється з урахуванням положень директив, політик, союзних публікацій НАТО у відповідній сфері. Наприклад, Процедурну інструкцію для командування та управління сухопутними операціями розроблено на виконання таких документів: директиви Військового комітету НАТО МС 0640, об'єднаної публікації США JP 3.2 "Сухопутні операції", союзних об'єднаних

публікацій AJP-3.2 “Союзна об’єднана доктрина для сухопутних операцій”, AJP-3 “Союзна об’єднана доктрина для ведення операцій”, AJP-5 “Союзна об’єднана доктрина планування операцій” тощо.

Технічні вимоги до сервісів визначаються відповідно до положень угод зі стандартизації НАТО (STANAGs), міжнародних стандартів, розроблених різного роду міжнародними організаціями, як от, Міжнародною організацією зі стандартизації (стандарти ISO), Міжнародною електротехнічною комісією (стандарти IEC), Міжнародною спілкою електрозв’язку (стандарти ITU), W3-консорціумом (стандарти HTML, XML, CSS тощо) тощо, та достатньо широко використовуються стандарти мережі Інтернет – запити коментарів RFC.

Відповідно до принципів С3-взаємосумісності НАТО, викладених у Політиці НАТО із С3-взаємосумісності:

стандарти та профілі повинні бути включені до Стандартів та профілів взаємосумісності НАТО *(en: NATO Interoperability Standards and Profiles, NISP)*;

структури НАТО повинні розробляти та публікувати в *NISP* профілі інтерфейсів сервісів, що стосуються С3-спроможностей та сервісів, та ці профілі повинні бути доступними для верифікації та валідації протягом тестування структурами НАТО та державами – членами НАТО.

На цей час, діючий *NISP* викладено у союзній публікації з даних *ADatP-34(N)* 14 версії від 26.05.2021 [18] та затверджено угодою зі стандартизації *STANAG 5524*. Оновлення вказаної публікації здійснюється фактично один раз на 1-2 роки.

Особливістю *NISP* є те що, у ньому наведено перелік стандартів та профілів та посилання на них в мережі Інтернет які є:

обов’язковими до запровадження;

інформативними, необов’язковими до запровадження, але вони можуть через деякий час набути статус – обов’язкові до запровадження.

Приклад побудови одного із сервісів наведено у Табл. 2.

Таблиця 2

Приклад вимог до сервісу згідно *NISP*

СЕРВІС	**ВИМОГИ ДО СЕРВІСУ**
Сервіс відео-конференційного зв’язку	*STANAG 4705* (Міжнародна мережева нумерація для систем зв’язку, що використовуються в НАТО); *STANAG 5046* (Система каталогів військових комунікацій НАТО). *Вказані угоди запроваджені в Україні у якості військових стандартів ВСТ 01.112.008 – 2020 (01) та ВСТ 01.112.012 – 2020 (01) відповідно*
	використовувати протоколи *SIP (Session Initiation Protocol), SDP (Session Description Protocol)* та *BFCP (Binary Floor Control Protocol)*, які визначені стандартами мережі Інтернет – запитами коментарів *RFC 3621, 3622, 3264, 4566, 4582* тощо
	використовувати кодеки G.722.1, G.711 та H.264, вимоги до яких визначено Міжнародною спілкою електрозв’язку, а саме: ITU-T G.722.1:2005, ITU-T G.711:1988, ITU-T H.264:2017 тощо

Для кожної мережі операції розробляються Інструкції щодо приєднання, членства та від’єднання *(en: FMN Joining, Membership and Exit Instructions, FMN JMEI),* які складаються з розділів, у яких визначається:

процес приєднання до мережі;

членство (функціонування) у складі мережі;

процес від’єднання від мережі;

технічні інструкції розгортання сервісів.

Питання взаємосумісності досліджуються та вивчаються у двох площинах: теоретичній та практичній:

TIDE-спринти (en: TIDE Sprints) являють собою, так звані, “мозкові центри” сприяння розвитку та запровадження інновацій, обміну концептуальними та практичними ідеями що стосується взаємосумісності С2-систем та сервісів між НАТО та її партнерами;

TIDE-хакатони (en: TIDE Hackathons) є середовищем обміну знаннями між експертами та новачками, яке спрямоване на вирішення ряду проблем, що складно вирішуються традиційними методами;

навчання із взаємосумісності CWIX *(en: Coalition Warrior Interoperability eXploration, eXperimentation, eXamination eXercise)* протягом яких здійснюється тестування спроможностей та сервісів на взаємосумісність згідно розроблених протоколів та профілів із залученням оперативного складу, технічного персоналу та представників розробника.

Таким чином, в НАТО реалізовано комплексний підхід (так званий *comprehensive approach*) із запровадження бачення НАТО щодо побудови сучасних збройних сил, які будуть спроможні протистояти викликам з безпеки, що існують для держав – членів НАТО, та відповідатимуть стратегічній концепції НАТО:

на стратегічному рівні розроблені відповідні стратегії та політики, якими визначено основні напрями розвитку комунікаційних та інформаційних систем;

здійснено класифікацію сервісів та відповідних процесів для запровадження сервіс-орієнтованої архітектури;

розроблено концепцію та директивні документи з питань досягнення взаємосумісності, якими визначені підходи, процеси запровадження та організаційна структура, завдання та функції особового складу;

на підставі оперативних вимог визначені мінімальні вимоги до комунікаційних та інформаційних систем та сервісів, які повинні надаватися оперативному складу через ці системи;

визначено перелік сервісів та процедурні, технічні й безпекові вимоги до них на підставі угод зі стандартизації НАТО та міжнародних стандартів;

розроблені (стандартизовані) перелік та шаблони (приклади) документів, на підставі яких розробляється визначений пакет документів для кожної операції під проводом НАТО (мережі операцій) та у яких зазначаються конкретні вимоги до сервісів, які повинні функціонувати протягом цієї операції (місії);

практичне опробування теоретичних вимог впродовж ряду спеціалізованих навчань НАТО та навчань направлених на підготовку сил і засобів НАТО для реагування на кризові ситуації.

У МО України, крім зазначених вище доктринальних документів, відпрацьовано такі відомчі документи:

доктринальні документи зі зв'язку та інформаційних систем видів та родів військ (сил) ЗС України;

накази МО України та Генерального штабу ЗС України, якими визначені вимоги до функціонування декількох комунікаційних та інформаційних систем та модернізації озброєння та військової техніки;

наказ Головнокомандувача ЗС України, яким визначено перелік сервісів, які мають бути розгорнуті на пунктах управління органів військового управління;

Модель життєвого циклу інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем в системі МО України (затверджено Міністром оборони України 10.04.2023);

Перелік процесів моделі життєвого циклу інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем в системі МО України (затверджено заступником Міністра оборони України з питань цифрового розвитку, цифрових трансформацій і цифровізації 07.06.2023);

військові стандарти, якими запроваджено декілька угод зі стандартизації НАТО, які включені до Переліку стандартів та профілів взаємосумісності НАТО та застосовуються у 4 спіралі.

Порівняння доктринального та нормативного забезпечення взаємосумісності комунікаційних та інформаційних систем НАТО та МО України наведено у Табл. 3.

Таблиця 3

ПОРІВНЯННЯ ДОКТРИНАЛЬНОГО ТА НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ	
Стратегічні підходи щодо досягнення взаємосумісності	
НАТО	**МО України**
Стратегічна концепція НАТО;	Стратегія національної безпеки України; Стратегія воєнної безпеки України; Стратегічний оборонний бюлетень України.
СЗ-стратегія Альянсу;	В МО України розроблено: Концепція розвитку ІТ-інфраструктури МО України та ЗС України; ключова доктрина "Зв'язок та інформаційні системи"; Об'єднана оперативна концепція сил оборони 2030.
СЗ-політики Альянсу	***Не розроблено єдиного бачення щодо порядку запровадження політик НАТО***
Класифікація сервісів	
СЗ-таксономія, уточнення якої здійснюється раз на 1-2 роки	Положеннями Додатку 1 Доктрини "Зв'язок та інформаційні системи" визначена необхідність розроблення Класифікатора та опису сервісів
Концепція та директивні документи з питань досягнення взаємосумісності	
Концепція FMN; План запровадження (реалізації) ініціативи FMN в НАТО; Директива з керівництва FMN; Директива з управління FMN	Концепція розвитку ІТ-інфраструктури МО України та ЗС України (зміст Концепції потребує доопрацювання)

ПОРІВНЯННЯ ДОКТРИНАЛЬНОГО ТА НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ	
Мінімальні вимоги до комунікаційних та інформаційних систем та сервісів	
Директиви Військового комітету НАТО МС 0593 та МС 0640	Наказ Головнокомандувача ЗС України від 14.12.2020 № 221 “Про затвердження Матриці надання мінімально необхідних сервісів (базових та функціональних) оперативному складу органів військового управління на пунктах управління ЗС України” (визначено лише перелік сервісів, які повинні бути розгорнуті на пунктах управління органів військового управління)
FMN-спіралі: перелік сервісів та процедурні, технічні й безпекові вимоги до них	
4 спіраль FMN: специфікації спіралі; загальний опис операційних вимог; загальний опис вимог до безпеки; 13 процедурних інструкцій з описами процесів; 22 сервісні інструкції з технічними описами сервісів; 11 профілів інтерфейсів сервісів	Накази МО України та Генерального штабу ЗС України з питань функціонування комунікаційних та інформаційних систем (спеціального програмного забезпечення): електронного документообігу; використання мережі Інтернет (вперше були описані сервіси, як складові системи); використання безпровідних мереж; електронної комунікаційної мережі ЗС України; функціонування автоматизованої системи управління ЗС України “Дніпро” (описані деякі сервіси разом з процедурними та технічними вимогами); інтеграційної платформи “Дельта”; комплексів “Ореанда”, “Дзвін-АС” тощо; спеціального програмного забезпечення “Віраж-Планшет”, “Коровай” тощо
Стандарти та профілі взаємосумісності	
STANAG 5524 / Союзна публікація з даних ADatP-34(N) Стандарти та профілі взаємосумісності НАТО	Положеннями Додатку 1 Доктрини “Зв’язок та інформаційні системи” визначена необхідність розроблення Переліку стандартів та профілів взаємосумісності
Стандартизовані перелік та шаблони (приклади) документів мережі операцій	
Інструкції щодо приєднання, членства та від’єднання (FMN JMEI)	Окремі підходи (форми документів) використовуються в розпорядчих та планувальних документах
Практичне опробування під час навчань	
Спеціалізовані навчання НАТО CWIX; TIDE-хакатони; TIDE-спринти	Участь представників МО України у навчаннях CWIX; Проведення національних хакатонів із залученням представників сил оборони та участь переможців цих хакатонів у TIDE-хакатонах; Участь представників сил оборони у TIDE-спринтах

Ураховуючи викладене, можна дійти висновку, що у МО України відсутній комплексний підхід запровадження доктринального та нормативного забезпечення взаємосумісності комунікаційних та інформаційних систем за таких причин:

потребують доопрацювання стратегічні концептуальні документи з питань взаємосумісності згідно стратегій та політик НАТО;

відсутні класифікація сервісів та не визначено мінімальний рівень вимог до них;

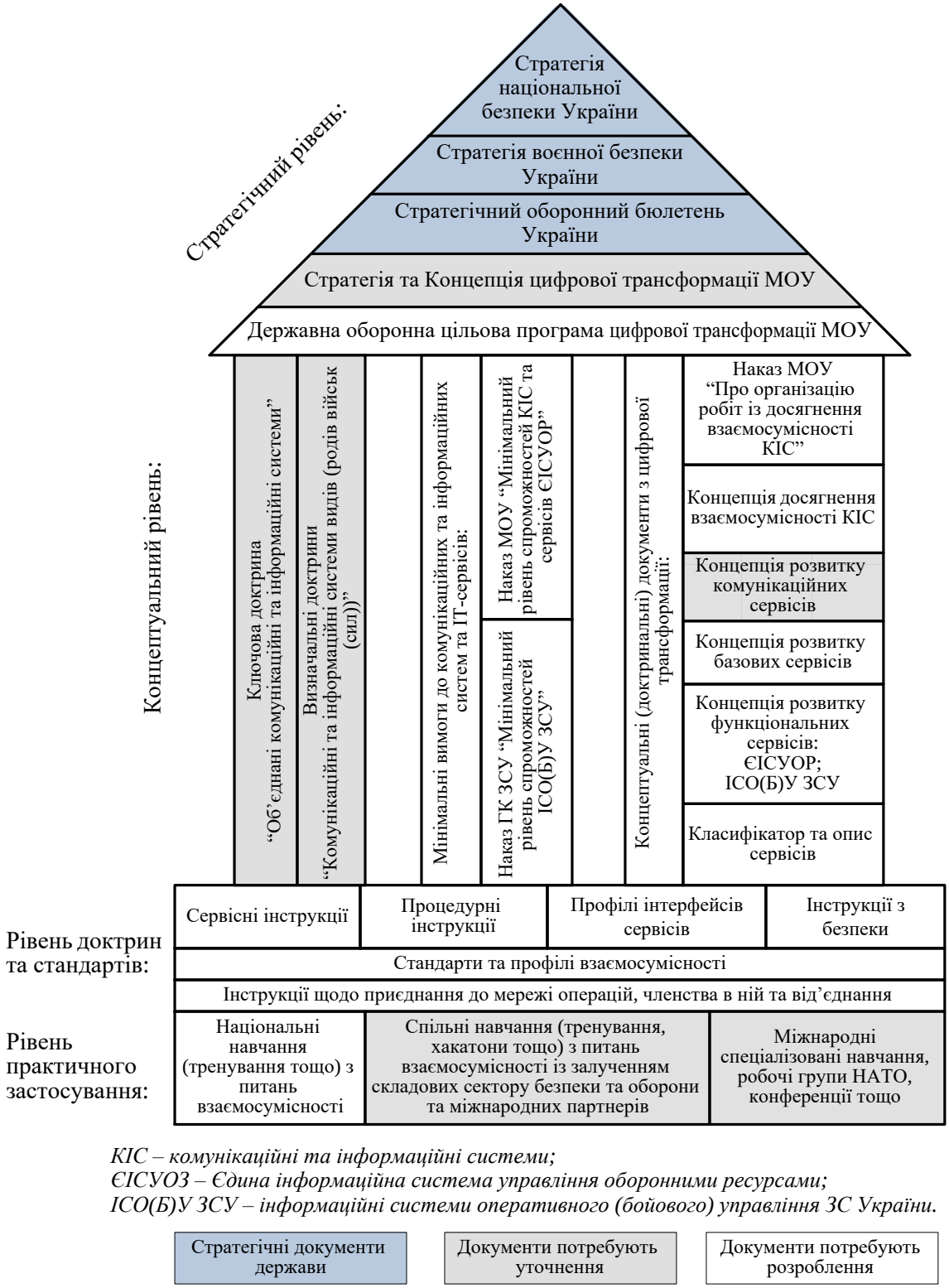
не організовано роботу відповідних робочих груп, їх завдання та обов’язки;

робота щодо запровадження процедурних та технічних інструкцій здійснюється окремими підрозділами, при цьому обмін відповідною інформацією між ними не здійснюється.

Для вирішення вказаного проблемного питання та з урахуванням досвіду НАТО розроблена модель доктринального та нормативного забезпечення взаємосумісності комунікаційних та інформаційних систем, яку наведено на рис. 2.

Вказана модель являє собою складну систему – “будівлю” – так званий “Будинок КІС – взаємосумісності”, що має чотири рівня.

Стратегічний рівень або “дах будівлі” представлений стратегіями національної і воєнної безпеки та стратегічним оборонним бюлетенем. Цифрову трансформацію МО України пропонується здійснювати за окремою Державною цільовою оборонною програмою цифрової трансформації МО України. Для цього необхідно розробити на довгострокову перспективу відповідні Стратегію та Концепцію цифрової трансформації МО України. Їх розроблення пропонується здійснити з урахуванням С3-стратегії й С3-політик НАТО та розробленої Концепції розвитку ІТ-інфраструктури МО України та ЗС України.



КІС – комунікаційні та інформаційні системи;
ЄІСУОЗ – Єдина інформаційна система управління оборонними ресурсами;
ІСО(Б)У ЗСУ – інформаційні системи оперативного (бойового) управління ЗС України.

Рис. 2. Модель доктринального та нормативного забезпечення взаємосумісності комунікаційних та інформаційних систем ("Будинок КІС – взаємосумісності")

У рамках вказаної програми доцільно здійснювати удосконалення доктринального та нормативного забезпечення, розроблення, зокрема модернізацію, нових спроможностей комунікаційних та інформаційних систем й сервісів, як інноваційних проєктів. Керівником програми призначити одного із заступників Міністра оборони України. При цьому, в рамках програм розвитку видів і родів військ (сил) планувати заходи із утримання діючих спроможностей комунікаційних та інформаційних систем,

постачання військ (сил) озброєнням та військовою технікою, зокрема спеціальною технікою, прийнятою на озброєння (постачання), або із визначеними технічними характеристиками. Застосування вказаного підходу потребує удосконалення нормативних документів з оборонного планування у МО України, а саме: положень [2–3]. На сьогодні, розвиток спроможностей комунікаційних та інформаційних систем здійснюється в рамках окремих програм розвитку видів і родів військ (сил), які не завжди є взаємоузгодженими.

Концептуальний рівень або "стіни будівлі" містить три складових:

1. Доктринальні документи представлені ключовою доктриною (об'єднані комунікаційні та інформаційні системи) та визначальними доктринами (з управління радіочастотним ресурсом в операціях, операцій в кіберпросторі та радіоелектронної боротьби в операціях), доктриною Військ зв'язку та кібербезпеки ЗС України, бойовими статутами видів та родів військ (сил) щодо організації комунікаційних та інформаційних систем в операціях.

2. Мінімальні вимоги до комунікаційних та інформаційних систем та сервісів відповідно до висунутих до них оперативних вимог. Вказані вимоги доцільно викласти у двох наказах:

Міністерства оборони України, яким визначити мінімальний рівень спроможностей комунікаційних та інформаційних систем та сервісів Єдиної інформаційної системи управління оборонними ресурсами;

Головнокомандувача ЗС України, яким визначити мінімальний рівень спроможностей інформаційних систем оперативного (бойового) управління ЗС України.

3. Концептуальні (доктринальні) документи з цифрової трансформації якими визначити:

структуру, завдання та функції робочих груп, відповідальних за відпрацювання (оновлення) документів з питання взаємосумісності;

концепцію взаємосумісності та концептуальні напрями розвитку функціональних, базових та комунікаційних сервісів тощо.

Рівень доктрин та стандартів або "фундамент будівлі" визначає процедурні та технічні вимоги до сервісів, вимоги до безпеки сервісів, шаблони (приклади) документів для розгортання мереж операцій тощо. Цей рівень є найбільш трудомістким, в частині що стосується документального забезпечення, та наявності підготовленого особового складу. Вирішення вказаного проблемного питання потребуватиме залучення як фахівців з інших складових сил оборони держави, так і цивільних фахівців з державних та комерційних структур.

Рівень практичного застосування або "середовище для побудови будівлі" є практичним випробуванням теоретичних рішень з побудови комунікаційних та інформаційних систем: навчання, тренування, хакатони тощо.

Висновки. Ураховуючи прагнення України до вступу в НАТО запровадження положень концепції НАТО FMN в силах оборони є важливим фактором інтеграції України у євроатлантичні безпекові структури та досягнення спроможностей забезпечення оборони території України й протиборства у кіберпросторі як складовій інформаційного простору держави.

У статті проведено детальний аналіз доктринального та нормативного забезпечення взаємосумісності комунікаційних та інформаційних систем в НАТО та МО України, на підставі якого розроблена відповідна модель доктринального та нормативного забезпечення, яку доцільно запровадити у МО України, а в подальшому, після її апробації, і в силах оборони держави. Як показує досвід запровадження доктринальних документів у МО України, складові сектору безпеки і оборони використовують доктринальні документи МО України або на їх основі розробляють власні, із незначними уточненнями, що стосуються завдань та функцій цих складових.

Подальші дослідження доцільно зосередити на детальному аналізі змісту розглянутих документів НАТО, їх адаптації в МО України в рамках оборонного планування. При цьому першочерговим заходом має бути розроблення власного Класифікатора сервісів та визначення мінімальних вимог до сервісів, які повинні надаватися оперативному складу пунктів управління ЗС України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стратегічний оборонний бюлетень України : Указ Президента України від 17.09.2021 р. № 473. URL: https://www.president.gov.ua/documents/4732021-40121 (дата звернення: 10.07.2023).
2. Про затвердження Порядку організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони : наказ Міністерства оборони України від 22.12.2020 р.

№ 484. URL: https://zakon.rada.gov.ua/laws/show/z0196-21#Text (дата звернення: 10.08.2023).
3. Доктрина з оборонного планування у Збройних Силах України (ВКП 5-00(67)01.01) : затверджена Головнокомандувачем Збройних Сил України 13.11.2020.
4. Руснак І. С., Петренко А. Г., Яковенко А. В., Романюк І. М., Кохно В. Д. Оборонне планування на основі спроможностей: особливості та перспективи впровадження // Наука і оборона. 2017. № 2. С. 3–10.
5. Оборонна реформа: системний підхід до оборонного менеджменту : монографія / А. Павліковський та ін. ; за заг. ред. д-ра військ. наук А. Сиротенка. Київ : НУОУ, 2020. 276 с.
6. Щипанський П. В., Саганюк Ф. В., Мудрак Ю. М. Оборонний менеджмент: підходи до управління процесами оборонного планування // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2021. № 1 (71). С. 52–58.
7. Малишев О. В., Малишева Н. Р., Калмиков В. Г., Левчук О. В. Оборонне планування на основі спроможностей в Україні: поточний стан і перспективи // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2020. № 3 (70). С. 54–61.
8. Поляєв А. І. Підходи щодо розроблення методики імплементації концептуальних документів стратегічного та оборонного планування // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2021. № 2 (72). С. 78–83.
9. Мудрак Ю. М. Підходи до імплементації стандартів НАТО у Збройних Силах України // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2020. № 2 (69). С. 6–10.
10. Ліпко І. О., Капілевич В. О. Актуальні підходи щодо забезпечення взаємосумісності інформаційних систем складових сил оборони України // Комп'ютерні системи та мережні технологій (CSNT-2023) : зб. тез доп. XIV Міжнар. наук.-практ. конф. (м. Київ, 13-14 квіт. 2023 р.) / Нац. авіац. ун-т. Київ, 2023. С. 109–112.
11. Слюсар В. І. Тактичні перспективи FMN // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я : тези доп. XXVIII Міжнар. наук.-практ. конф. MicroCAD-2020 (м. Харків 21-23 жовт. 2020 р.) у 5 ч., Ч. V / Національний технічний університет "Харківський політехнічний інститут. Харків, 2020. С. 229.
12. Слюсар В. І. Федеративна мережа місій як середовище поширення даних доповненої реальності // Перспективи розвитку озброєння та військової техніки Сухопутних військ : зб. тез доп. Міжнар. наук.-техн. конф. (м. Львів, 16-17 трав. 2019 р.) / Національна академія Сухопутних військ ім. Гетьмана Петра Сагайдачного. Львів, 2019. С. 263–264.
13. Корольов В. М., Заєць Я. Г. Щодо вимог до інформаційних (автоматизованих) систем тактичного рівня з урахуванням стандартів НАТО // Перспективи розвитку озброєння та військової техніки Сухопутних військ : зб. тез доп. Міжнар. наук.-техн. конф. (м. Львів, 17-18 трав. 2023 р.) / Національна академія Сухопутних військ ім. Гетьмана Петра Сагайдачного. Львів, 2023. С. 200–201.
14. Кірпічніков Ю. А., Капілевич В. О., Андрощук О. В., Петрушен М. В. Застосування дата-центричного підходу під час побудови інформаційної інфраструктури з використанням хмарних технологій для оборонних потреб // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2022. № 3 (76). С. 68–75.
15. Кірпічніков Ю. А., Головченко О. В., Андрощук О. В., Петрушен М. В., Розумний О. Д. Модель оцінювання альтернативних варіантів впровадження інформаційно-комунікаційних сервісів з використанням хмарних технологій для оборонних потреб // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2023. № 1 (77). С. 79–88.
16. STANAG 5064 (Ed: 1) / AAP-31 (Ed: 3) (2005) (Ver. 1). NATO glossary of communication and information systems terms and definitions. URL: https://nso.nato.int/nso/nsdd/main/list-promulg (дата звернення: 10.07.2023).
17. Стратегічна концепція НАТО – 2022 : ухвал. главами держав і урядів на Мадридському саміті НАТО 29.06.2022 р. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept-ukr.pdf (дата звернення: 10.07.2023).
18. NATO Interoperability Standards and Profiles. URL: https://nhqc3s.hq.nato.int/Apps/Architecture/NISP/index.html (дата звернення: 10.07.2023).

Стаття надійшла до редакційної колегії 11.08.2023

Model for achieving interoperability of communication and information systems: implementation of NATO experience in the interests of the national defense forces

Annotation

The basis of Ukraine's Military Security Strategy is the comprehensive defense of Ukraine. One of the main directions to achieve this is the integration of advanced practices, principles, and standards of NATO into the national defense forces, participation in joint operations and exercises to meet NATO membership criteria, and subsequent integration into Euro-Atlantic security structures. The defense forces of Ukraine should establish a joint defense network and mission networks, with information exchange aligned with NATO's technical and procedural principles and interoperability levels. Currently, NATO interoperability is pursued through the Federated Mission Networking (FMN) initiative, initiated within NATO since 2015.

The goal of the article is to develop a model for the doctrinal and normative documents' structure based on the analysis of NATO's approaches to doctrinal support for the FMN initiative and the experience gained domestically. This model aims to achieve interoperability of communication and information systems.

The article provides a detailed analysis of doctrinal and normative support for interoperability of communication and information systems within NATO and the Ukrainian Ministry of Defense. Based on this analysis, an appropriate model for doctrinal and normative support has been developed, intended for implementation within the Ukrainian Ministry of Defense, and subsequently, after its approval, within the national defense forces. The experience of implementing doctrinal documents within the Ukrainian Ministry of Defense shows that the security and defense sectors use these documents, sometimes with slight modifications, for their roles and responsibilities.

Keywords: doctrinal and normative support; FMN; interoperability of communication and information systems.

УДК 354.404.4+355.40:629.783 DOI: https://doi.org/10.33099/2304-2745/2023-2-78/121-126

Мосов С. П., доктор військових наук, професор

Інститут державного управління та наукових досліджень з цивільного захисту, Київ

Особливості розвитку безпілотної авіації військового призначення в країнах Центральної Азії

Резюме. У статті наведено результати дослідження особливостей розвитку безпілотної авіації військового призначення в країнах Центральної Азії. Рекомендовано напрямами подальших досліджень щодо країн Центральної Азії вважати: аналіз на системних засадах тактико-технічних і оперативно-тактичних характеристик безпілотних авіаційних комплексів, що виробляються на теренах цих країн; підходи до підготовки фахівців з експлуатації та застосування БпЛА тощо.

Ключові слова: безпілотна авіація; Центральна Азія; безпілотний літальний апарат.

Безпілотні літальні апарати (БпЛА) вже давно перестали бути прерогативою тільки наддержав. На теперішній час ця індустрія переживає лавиноподібний рух у всьому світі. Особливий інтерес до безпілотних авіаційних комплексів (БпАК) проявився після недавніх воєнних конфліктів у світі. Поява БпЛА зробила справжню “революцію” в оперативному мистецтві й тактиці застосуванні військ і озброєння.

Згідно з даними, опублікованими у цьому році, понад ста держав світу використовують БпЛА у воєнних цілях, водночас уже близько сорока країн мають безпілотники, оснащені зброєю. Очікується, що ринок БпАК воєнного призначення перевищить $21 млрд у 2027 році за середньорічного темпу зростання майже 7%. До регіонів, що охоплені глобальним ринком воєнних безпілотників, відносяться: Азіатсько-Тихоокеанський регіон, Західна Європа, Східна Європа, Північна Америка, Південна Америка, Близький Схід і Африка. Найбільшим регіоном на ринку таких безпілотників у 2022 році був Азіатсько-Тихоокеанський регіон [1], до складу якого входять також країни Центральної Азії (ЦА): Киргизька Республіка (Киргизстан), Республіка Таджикистан (Таджикистан), Республіка Казахстан (Казахстан), Республіка Узбекистан (Узбекистан) і Туркменістан [2].

Постановка проблеми. Тривалий час, під час дослідження питань щодо розвитку безпілотної авіації воєнного призначення в різних країнах світу, практично не зверталась увага на країни ЦА, які стали приділяти значну увагу розвитку безпілотної авіації, що обумовлено, як світовими тенденціями, так і внутрішніми протиріччями між низкою центральноазіатських країн щодо прикордонних земель [3] і користування прісною водою з транснаціональних річок [4].

Актуалізація питання щодо визначення особливостей розвитку безпілотної авіації воєнного призначення в центральноазіатському регіоні в інтересах національної безпеки та оборони обумовлена її перевагами, що вже проявилися в ході сучасних прикордонних конфліктів, особливо між Вірменією й Азербайджаном у 2020 році [5], а також Таджикистаном і Киргизстаном у 2021 і 2022 роках [6].

Визначення особливостей розвитку безпілотної авіації в країнах ЦА має відповісти на питання щодо реакції цих країни на безпілотну авіацію, як на дієвий засіб в інтересах забезпечення їх національної безпеки та оборони, а також отримання переваг у ході можливих (імовірних) бойових дій.

Аналіз останніх досліджень і публікацій. Питаннями, пов’язаними із дослідженнями щодо підходів до оснащення БпАК країн ЦА в інтересах їх національної безпеки й оборони та виявлення особливостей розвитку безпілотної авіації військового призначення у цих країнах займалася незначна кількість фахівців і вчених.

Так, у [7] проведено аналіз підходів центральноазіатських країн до оснащення БпАК.

БпЛА воєнного призначення пострадянських країн, до складу яких входять і країни ЦА, проаналізовано в [8].

Інформація щодо оснащення БпАК окремих країн ЦА наведена в [9–13] і в інших джерелах.

Результати аналізу джерел свідчить про відсутність досліджень щодо визначення особливостей розвитку безпілотної авіації воєнного призначення в центральноазіатському регіоні в інтересах національної безпеки й оборони країн на системних засадах.

Метою статті є визначення особливостей розвитку безпілотної авіації воєнного призначення в країнах ЦА в інтересах національної безпеки й оборони.

Виклад основного матеріалу. Під час загострення прикордонного збройного конфлікту між Вірменію й Азербайджаном навколо Нагорного Карабаха у вересні-листопаді 2020 року обома сторонами широко застосовувалися БпЛА різного призначення. Безпілотники використовувалися Азербайджаном і Вірменією і раніше, проте саме під час вказаних дій висока інтенсивність застосування систем БпЛА ознаменувала початок масованого застосування безпілотної авіації в конфліктах середньої інтенсивності. Ця важлива подія стала знаковою в світовому масштабі, у тому числі для центральноазіатських країн [14].

Країни ЦА активно нарощують свої безпілотні сили. Усі країни прагнуть розширити можливості своїх БпЛА подібним чином. Їхня конкретна оборонна стратегія, бюджетне становище і вибір іноземних партнерів є факторами, що визначають, який тип БпАК вони купують і в яких постачальників. Спочатку країни ЦА зробили ставку на відомі безпілотники іноземного виробництва. Після повільного старту нині вони розглядають безпілотники як доповнення, якщо не ключовий компонент своїх збройних сил. У БпЛА в регіоні є сильні аргументи як у якості спеціалізованих ресурсів, так і в якості недорогих альтернатив для посилення можливостей атаки “повітря-земля”.

Кожна з країн ЦА добре усвідомлює зростаючу роль безпілотників різного призначення у війнах та оперативно адаптується до цієї нової реальності. При цьому БпЛА можуть стати дешевою альтернативою для країн з обмеженим оборонним бюджетом і скромними силами ВПС (наприклад, Киргизстан і Таджикистан).

Киргизька Республіка. У Киргизстані активно розвивається напрямок, пов’язаний з оснащенням БпАК воєнного призначення, насамперед в інтересах забезпечення національної безпеки та оборони держави. Донедавна на оснащенні збройних сил перебували розвідувальні БпЛА WJ-100 китайського виробництва [7]. З огляду на результати активного застосування з боку Азербайджану БпЛА турецького виробництва в прикордонному конфлікті з Вірменією, Киргизстан у 2021 році закупив у Туреччини ударні БпАК Bayraktar TB2 для Прикордонної служби ДКНБ [15]. Також з РФ було укладено угоду про придбання розвідувальних БпАК Орлан-10Е [16]. Важливим моментом такого придбання стало те, що Киргизстан вперше придбав їх за бюджетні гроші.

Лінійка безпілотників турецького виробництва в Киргизстані поповнилася також ударним БпАК Akinci, розвідувальними БпАК Aksungur і БпАК Anka [9].

Після чергового зіткнення з Таджикистаном у 2021 році особлива увага в країні приділяється зміцненню збройних сил і національної безпеки. Останнім часом загострення прикордонного конфлікту між Киргизстаном і Таджикистаном зумовлено незавершеністю поділу кордону між державами, а також поглибленням проблеми прісного водокористування. Обидві держави мають спільний кордон протяжністю понад 970 км, з яких понад 519 км залишаються невизначеними [17].

У 2021 році воєнні безпілотники в центральноазіатському регіоні вперше були активно задіяні в прикордонному конфлікті, що в черговий раз загострився між Киргизстаном і Таджикистаном [18]. Успішне використання киргизьких БпЛА турецького виробництва у збройному зіткненні між Киргизстаном і Таджикистаном показало, яку важливу роль вони можуть відігравати як атакуюча сила. Ураховуючи цей факт, Киргизстан активно нарощує запас БпЛА шляхом нових закупівель турецьких безпілотників воєнного призначення [9].

Щодо ударного БпЛА Bayraktar TB2, то слідує звернути увагу, що його ефективність достатньо висока за умов слабкої протиповітряної оборони (ППО). В умовах високої щільності сучасних засобів ППО виникають проблеми щодо застосування БпЛА Bayraktar TB2, що з часом змінило з 2022 року способи застосування такого БпЛА в Україні в ході війни проти РФ [19].

Паралельно в країні у 2022 році вперше було розроблено та зібрано воєнний багатоцільовий БпАК SAARA-02 власного виробництва. Безпілотник призначений не тільки для виконання розвідувальних, а й інших бойових завдань у тактичній глибині [20, 21]. Киргизстан став третьою країною в ЦА після Казахстану та Узбекистану, яка розробила власний БпАК.

Республіка Узбекистан. Узбекистан, як й інші країни ЦА, активізував зусилля для нарощування свого безпілотного потенціалу. Джерелом перших БпЛА для Узбекистану став Китай, який поставив розвідувально-

ударний БпЛА Wing Loong I у межах угоди з оплати узбецького газу. З 2019 року в країні почалося переозброєння [22]. У галузі розвідувальних безпілотників в Узбекистані є БпЛА ZALA 421-16E російського виробництва і БпЛА RQ-11 Raven американського виробництва [18]. У 2021 році з боку РФ були поставлені багатофункціональні комплекси з БпЛА Орлан-10E [23]. Більше Узбекистан не закуповував БпЛА іноземного виробництва, що, можливо, означає, що Ташкент певною мірою відстає в цьому напрямку від деяких своїх центральноазіатських сусідів.

Узбекистан став першою країною в ЦА, яка запустила власне виробництво БпАК різного призначення. Науково-виробничим центром безпілотних авіаційних комплексів з лютого 2022 року розпочалося виробництво БпАК Lochin (Сокіл), що повністю відповідають міжнародним технічним вимогам і стандартам. Безпілотники призначені для використання в декількох цілях: виконання завдань розвідки; нанесення ударів з повітря; спостереження в масштабі реального часу; оперативне отримання інформації; управління процесом артилерійського вогню, а також для картографування, топогеодезії, моніторингу заповідників, доріг, соціальної інфраструктури та інших важливих об'єктів у сільському, нафтогазовому, лісовому, залізничному та геологічному секторах [10].

Республіка Таджикистан. Таджикистан тривалий час перебуває у стані затяжного прикордонного конфлікту з Киргизстаном, під час якого неодноразово застосовувалась зброя і військова техніка. Причиною розбрату є 31,6% лінії спільного кордону і прісне водокористування. Ні з боку Бішкека, ні з боку Душанбе не виявляється жодного бажання йти один одному на поступки і шукати компромісні рішення. Прикордонне питання було точкою конфлікту між Таджикистаном і Киргизстаном навіть за часів СРСР, а розпад Союзу дуже серйозно загострив проблему і максимально ускладнив процес врегулювання.

У 2021 році військові безпілотники були задіяні під час збройних зіткнень між Киргизстаном і Таджикистаном з обох сторін. За оцінкою військових експертів, "Байрактари" змогли компенсувати військову перевагу Таджикистану, що мала місце тривалий час. Результати зіткнення безпосередньо вплинули на формування поглядів щодо безпілотної авіації в Таджикистані. На момент збройного зіткнення на кордоні Таджикистан мав тільки розвідувальні БпЛА Орлан-10E російського виробництва [7].

Для нарощування потенціалу безпілотників Таджикистан звернувся до Ірану, який у 2022 р. запустив у м. Душанбе підприємство з виробництва іранських безпілотників Ababil-2, що стало першою виробничою лінією країни за кордоном. БпЛА призначені, в основному, для ведення повітряної розвідки і спостереження. Разом з тим, вони можуть бути також оснащені вибуховими речовинами і використовуватися як бойові БпЛА-камікадзе, перетворюючись на керовану ракету [24]. Для Таджикистану відкриття виробництва іранських БпАК можна розглядати як важливий крок до диверсифікації своїх військових партнерів, а також посилення можливості стримування сусідніх держав, які здебільшого вже придбали ударні БпЛА або експлуатують їх [11]. Відкриття заводу з виробництва безпілотників у м. Душанбе відбулося менш як за рік після того, як сусідній із Таджикистаном Киргизстан, якому також бракує ефективних ВПС, придбав турецькі БпЛА Bayraktar TB2. Слід також підкреслити, що співпраці Ірану і Таджикистану сприяє також те, що Іран і Таджикистан володіють спільною іранською ідентичністю і розмовляють варіантами перської мови.

У рамках допомоги від США Таджикистан отримає розвідувальні безпілотники Puma. Вони використовуватимуться для спостереження за повітряним простором країни на кордоні [25].

Республіка Казахстан. На розробку безпілотної авіації Казахстан націлився вже давно – у межах Цільової програми з розвитку в Казахстані науково-технічного і промислового потенціалу авіабудівної галузі в напрямку створення БпАК на 2009-2020 рр. Метою було позначено розвиток науково-технічного та промислового потенціалу авіабудівної галузі у напрямку створення БпАК, які планувалося використовувати не тільки для внутрішніх потреб країни, а й поставляти за кордон [12].

З вересня 2021 року міністерство оборони Казахстану активізувало реалізацію національного проєкту "Безпечна країна", одним із напрямів якого визначена модернізація збройних сил на основі диверсифікації поставок, багатовекторної підготовки командних кадрів, нових договорів із країнами СНД і далекого зарубіжжя у сфері

воєнного та воєнно-технічного співробітництва [26,27].

У Казахстані триває активна робота з впровадження та розвитку БпАК. Сухопутні війська оснащені тактичними БпЛА SkyLark-1LEX ізраїльського виробництва. На озброєнні ВПС перебуває розвідувально-ударний БпЛА WingLoong китайського виробництва, здатний виконувати не тільки завдання ведення повітряної розвідки, а й наносити високоточні удари керованими ракетами і бомбами [28]. Вони застосовуються під час бойової підготовки військ, зокрема на великомасштабних навчаннях.

У 2022 році Казахстан підписав із Туреччиною угоду про військове співробітництво, у рамках якої Анкара зобов'язалася поставити кілька розвідувально-ударних БпАК Anka і передати технології, а також навчити персонал для технічного обслуговування і ремонту БпАК Anka для казахстанської армії. Казахстан став першою зарубіжною країною, де за ліцензією буде налагоджено виробництво турецьких БпАК Anka за межами Туреччини [12, 29, 30].

Казахстан також перебуває на шляху створення безпілотника національної розробки і виробництва. У країні розроблено розвідувальний БпЛА "Шагала" (Чайка), який здійснив свій перший випробувальний політ на початку 2021 року і через кілька місяців вийшов на завершальний етап випробувань [30].

Туркменістан. Туркменістан можна вважати країною ЦА, яка постійно розширювала свій безпілотний арсенал, щоб не відставати від новітніх тенденцій. У 2011 році Італія поставила Туркменістану розвідувальний комплекс із БпЛА Falco XN [31].

Перший формальний крок у напрямку виробництва БпАК був зроблений в 2015 році президентом Туркменістану щодо першого зразка туркменського БпАК "Асуда асман" ("Спокійне небо") [8]. У 2016 році Білорусь поставила Туркменістану розвідувальні БпАК Бусел-М.

Водночас було розпочато виробництво БпАК Бусел-М на території Туркменістану [32]. Запуск виробничої лінії безпілотників у Туркменістані став помітним досягненням, оскільки до створення Центру БпЛА в країні не було оборонної промисловості.

За останнє десятиліття Туркменістан наростив свій потенціал БпЛА завдяки придбанню декількох типів БпАК у Китаї (CASIC WJ-600, CH-3A), Туреччині (Bayraktar TB2), Ізраїлі (Orbiter-2B, Orbiter-3B), Італії (Selex ES Falco) [33, 34].

Розвідувально-ударні БпЛА китайського виробництва CASIC WJ-600, CH-3A посилили безпілотний потенціал Туркменістану в середині 2010 року. Принцип багатовекторності по відношенню до формування парка воєнної безпілотної авіації став підставою для закупівлі розвідувально-ударних БпЛА Bayractar TB2 турецького виробництва і розвідувальних БпЛА Selex ES Falco італійського виробництва [34, 35].

Після збройного прикордонного конфлікту між Вірменією і Азербайджаном в Нагорному Карабаху в 2020 році Туркменістан зробив наступний крок щодо впровадження абсолютно нових можливостей у свій парк безпілотної авіації. Це проявилося через придбання в Ізраїлю боєприпасів SkyStriker, що баражують і які були успішно використані Азербайджаном проти вірменських військ під час війни 2020 року. Схоже, що шляхом придбання Bayraktar TB2 і SkyStrikers Туркменістан прагне відтворити безпілотні наступальні можливості Азербайджану, які виявилися вирішальними під час 44-денного збройного протистояння. Ще одне розширення його зростаючого арсеналу відбулося за рахунок придбання БпАК ScanEagle 2 для використання на корветі ВМС Туркменістану Deniz Han [34].

Придбання китайських і турецьких БпЛА та ізраїльських боєприпасів, що баражують, перетворило Туркменістан на регіональну державу безпілотників. З огляду на часті інвестиції країни в нове озброєння та обладнання, Туркменістан, ймовірно, буде й надалі розвивати свої безпілотні можливості, щоб забезпечити перевагу своїх збройних сил над будь-яким можливим противником.

Аналіз підходів до розвитку безпілотної авіації в країнах ЦА свідчить також про чітке розуміння з їхнього боку тих обставин, що треба не лише зміцнювати свій безпілотний потенціал, а також треба володіти засобами і способами протидії ворожим безпілотникам. На важливість вирішення зазначеного питання зверталась увага ще у 2016 році у [36], де йшла мова про актуальність розроблення Концепції "ЗЗЗ": Знищення, Захоплення, Захист в інтересах України щодо протидії ворожій безпілотній авіації.

Висновки. Проведений аналіз особливостей розвитку безпілотної авіації в країнах ЦА для вирішення завдань забезпечення національної безпеки та оборони дає змогу дійти таких висновків:

джерелом стимуляції розвитку безпілотної авіації є збройні конфлікти, що відбулися, тривають, виникли або можливі (ймовірні) збройні конфлікти, в яких бере участь або буде (може) брати участь країна;

підставою для нарощування потенціалу безпілотної авіації воєнного призначення є необхідність забезпечення високого рівня національної безпеки та обороноздатності країни на сучасній науково-технічній платформі;

придбання сучасних зарубіжних БпАК воєнного або подвійного призначення, здатних ефективно виконувати спеціальні функціональні завдання;

придбання сучасних зарубіжних розвідувально-ударних і ударних БпЛА, здатних успішно впливати на ведення бойових дій;

організація виробництва зарубіжних БпАК воєнного призначення за ліцензією на території країни;

організація виробництва різнотипних БпАК воєнного призначення власної розробки на території країни;

диверсифікація воєнних партнерів країни з позиції придбання БпАК, що зумовлено різними причинами (політичними, економічними, територіальними, ресурсними тощо).

Досвід країн ЦА може стати корисним для України щодо розвитку безпілотної авіації на її теренах після закінчення війни.

Напрямами подальших досліджень щодо країн ЦА слід вважати:

аналіз на системних засадах тактико-технічних і оперативно-тактичних характеристик БпАК, що виробляються на теренах цих країн;

способи їхньої кооперації з передовими країнами світу з позиції розроблення та виробництва сучасних зразків БпАК;

підходи до підготовки фахівців з експлуатації та застосування БпЛА тощо.

***Подяка**. Статтю підготовлено в межах дослідження, що фінансується Комітетом науки Міністерства науки і вищої освіти Республіки Казахстан (Грант № AP14869765).*

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Military Drones Global Market Report 2023. URL: https://www.reportlinker.com/ p06240599/Military-Drones-Global-Market-Report.html?utm_source=GNW.
2. Центральна Азія. URL: https://uk.wikipedia.org/ wiki/Центральна Азія.
3. Мосов С. П., Салий С. М., Нероба В. Р. Особенности применения минного оружия в войнах и приграничных конфликтах // Багдар : военно-теоретический журнал. 2020. № 2 (86). С. 10–15.
4. Горбулін В. П., Мосов С. П. Водні конфлікти як індикатор загострення світової кризи прісної води // Вісник НАН України. 2023. № 2. С. 3–11. DOI: https://doi.org/10.15407/visn2023.02.003.
5. Dixon R. Azerbaijan's drones owned the battlefield in Nagorno-Karabakh – and showed future of warfare. URL: https://www.bing.com/search?q=Drones+in+the+Karabakh +conflict+2020&qs=n&form=QBRE&sp=-1&lq=0&pq=drones+in+the+karabakh+conflict+ 2020&sc=12-36&sk=&cvid=86706D8D93545DA9170ECF28930341A &ghsh=0&ghacc= 0&ghpl.
6. Конфлікт між Киргизстаном та Таджикистаном (2022). URL: https://uk.wikipedia.org/wiki/ Конфлікт_між_Киргизстаном_та_Таджикистаном_(2022).
7. Olmos By F. Dawn of the Drone Age in Central Asia Central Asian countries have been stepping up their drone capabilities. URL: https://thediplomat.com/2022/11/dawn-of-the-drone-age-in-central-asia/.
8. Спаткай Л. Боевые БПЛА постсоветских стран (1/21). URL: https://bsblog.info/ boevye-bpla-postsovetskix-stran-1-21/.
9. Bisht I. Kyrgyzstan Reveals Fresh Turkish Military Drone Purchase. URL: https://www.thedefensepost.com/ 2023/01/20/kyrgyzstan-turkish-drone-purchase.
10. Sealander D. Domestic Production of Drones: The Latest in Uzbekistan's Military Modernization Drive. URL: https://www.caspianpolicy.org/research/technology-policy/ domestic-production-of-drones-the-latest-in-uzbekistans-military-modernization-drive.
11. Gosselin-Malo E. Drone race in Central Asia in the wake of the Taliban takeover. URL: https://trendsresearch.org/ insight/drone-race-in-central-asia-in-the-wake-of-the-taliban-takeover/.
12. В Казахстане будет развиваться беспилотная авиация. URL: https://online.zakon.kz/Document/?doc_id=30393275.
13. В Туркменістані вперше показали придбані в Туреччині ударні БПЛА Bayraktar TB2. URL: https://defence-ua.com/weapon_and_tech/ v_turkmenistani_vpershe_pokazali_pridbani_v_turechchini_udarni_bla_bayraktar_tb2-4875.html.
14. Sternen B. Drones playing big role in Nagorno-Karabakh fight. URL: https://asiatimes.com/2020/10/ drones-playing-big-role-in-nagorno-karabakh-fight/#:~:text=Drones%20are%20playing%20a%20big%20role%20in%20the,vehicles%2C%20multiple%20rocket%20launchers%20and%20air%20defense%20platforms.
15. Калыков М. На вооружение Кыргызстана поступили беспилотники "Байрактар". URL: https://kloop.kg/blog/ 2021/12/18/na-vooruzhenie-kyrgyzstana-postupili-bespilotniki-bajraktar/?tztc=1.
16. Куденко А. Кыргызстан покупает у России и Турции беспилотники "Орлан" и "Байрактар" – Ташиев. URL: https://ru.sputnik.kg/20211021/kyrgyzstan-bespilotniki-priobretenie-1054304646.html.
17. Щур М. Що сталося на киргизько-таджицькому кордоні і чому це важливо. URL: https://www.radiosvoboda.org/a/prykordonnyj-konflikt-kyrgyzstan-tajykistan/31239801.html.
18. Кыргызстан станет третьей страной в Центральной Азии, разработавшей собственный беспилотник, – The Diplomat. URL: https://tiraj.kg/kyrgyzstan-stanet-tretej-stranoj-v-czentralnoj-azii-razrabotavshej-sobstvennyj-bespilotnik-the-diplomat/.
19. Українське командування повністю засекретило застосування Bayraktar TB2 у рамках нової стратегії.

URL: https://bastion.tv/ukrayinske-komanduvannya-povnistyu-zasekretilo-zastosuvannya-bayraktar-tb2-u-ramkah-novoyi-strategiyi_n46935.
20. Уралиев М. Кыргызстане собрали первый отечественный военный беспилотник. Видео. URL: https://kaktus.media/doc/469101_v_kyrgyzstane_sobrali_pervyy_otechestvennyy_ voennyy_bespilotnik._video.html.
21. Коргоо министри SAARA-02 учкучсуз аппараты тууралуу суроого жооп берди. URL: https://sputnik.kg/20221019/saara-02-uchkuchsuz-dron-ministr-1069128097.html.
22. Ермаков А. Истребители, беспилотники, броневики: Узбекистан начал перевооружение. URL: https:// eurasia.expert/uzbekistan-nachal-perevooruzhenie/.
23. Russia delivers military equipment to Uzbekistan. URL: https://tashkenttimes.uz/national/7791-russia-delivers-military-equipment-to-uzbekistan.
24. В Таджикистане будут производить иранские беспилотники Ababil-2. URL: https://fergana.agency/ news/126161/.
25. Таджикистан теперь получит беспилотники и от США. URL: https://vesti.kg/politika/item/99676-tadzhikistan-teper-poluchit-bespilotniki-i-ot-ssha.html.
26. Министр обороны Казахстана рассказал о развитии армии в рамках нацпроекта “Безопасная страна”. URL: https://www.zakon.kz/5087232-ministr-oborony-kazahstana-rasskazal-o.html.
27. Для чего Казахстану турецкие беспилотники Anka. URL: https://www.zakon.kz/5087232-ministr-oborony-kazahstana-rasskazal-o.html.
28. Guardians Of The Steppe – Kazakhstan’s UAVs. URL: https://www.oryxspioenkop.com/2022/01/guardians-of-steppe-kazakhstans-uavs.html.
29. Алтаев Д. Кто станет основным поставщиком ударных БПЛА для казахстанской армии? URL: https://mk-kz.kz/politics/2021/12/08/kto-stanet-osnovnym-postavshhikom-udarnykh-bpla-dlya-kazakhstanskoi-armii.html.
30. Испытан казахстанский БПЛА “Шагала”. URL: https://bsblog.info/ispytan-kazaxstanskij-bpla-shagala.
31. Хищные птицы Бердымухамедова: итальянский БПЛА Falco XN в Туркменистане. URL: https://www.oryxspioenkop.com/2021/12/Berdimuhamedow-birds-of-prey-italian.html.
32. В Туркменистане наладили сборку белорусских дронов “Бусел–М”. URL: https://www.belvpo.com/%D0%B2-%D1%82%D1%83%D1%80%D0%BA%D0%BC%D0%B5%D0%BD%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D0%.
33. Военно-воздушные силы и войска ПВО Туркменистана. URL: https://ru.wikipedia.org/wiki/%D0%92%D0%BE%D0%B5%D0%BD%D0%BD%D0%BE-%D0%B2%.
34. Mitzer S., Oliemans J. Turkmenistan’s Path To Drone Power. URL: https://www.oryxspioenkop.com/2022/02/turkmenistans-path-to-drone-power.html.
35. Туркменистан закупил турецкие БПЛА Bayractar TB2. URL: https://bsblog.info/turkmenistan-zakupil-tureckie-bpla-bayractar-tb2/.
36. Мосов С.П., Гурак С. П. Перемогти у боротьбі з БПЛА // Оборонний вісник. 2016. № 9. С. 20–25.

Стаття надійшла до редакційної колегії 03.06.2023

Features of the development of unmanned aircraft for military purposes in the countries of Central Asia

Annotation

The actualization of the issue of determining the features of the development of unmanned military aircraft in the Central Asian region in the interests of national security and defense is due to its advantages, which have already manifested themselves during modern border conflicts, especially between Armenia and Azerbaijan in 2020, as well as Tajikistan and Kyrgyzstan in 2021 and 2022 Determining the features of the development of unmanned aircraft in the Central Asian countries should answer the questions of the reaction of these countries to unmanned aircraft, as an effective means in the interests of ensuring their national security and defense, as well as obtaining advantages during possible (probable) military operations.

The analysis of the features of the development of unmanned aircraft in Central Asian countries to solve problems of ensuring national security and defense allows us to draw the following conclusions:

the source of stimulation for the development of unmanned aircraft are armed conflicts that have occurred, ongoing or likely in the future;

The basis for increasing the potential of unmanned military aircraft is the need to ensure a high level of national security and defense capability of the country on a modern scientific and technical platform.

The activities of the Central Asian countries are carried out in the following areas:

acquisition of modern foreign military or dual-use UAVs capable of effectively performing special functional tasks;

acquisition of modern foreign reconnaissance and attack UAVs capable of successfully influencing the conduct of combat operations;

organizing the production of foreign military-grade armored vehicles under license on the territory of the country and various types of military-purpose armored vehicles of our own design in the country;

diversification of the country’s military partners from the perspective of acquiring ВрК, which is due to various reasons (political, economic, territorial, resource, etc.).

The experience of Central Asian countries may be useful for Ukraine in developing unmanned aircraft on its territory after the end of the war.

Keywords: unmanned aircraft; Central Asia; unmanned aerial vehicle.

УДК 349.3 DOI: https://doi.org/10.33099/2304-2745/2023-2-78/127-132

Бейкун А. Л., кандидат юридичних наук, доцент[1] (0000-0003-2016-2077)
Топольніцький В. В., кандидат юридичних наук [2] (0000-0001-5573-4149)
Каптан М. В.[2] (0009-0008-3610-4633)
Матвієць С. Я.[1] (0009-0004-6562-564X)

[1] – Київський інститут Національної гвардії України, Київ;
[2] – Національний університет оборони України, Київ

Проблемні та дискусійні питання сфери нормативного забезпечення соціальної адаптації військовослужбовців з огляду на їх системність та ефективність

Резюме. У статті окреслюється проблематика узагальнення етимологічного та правового змісту соціальної адаптації військовослужбовців як правової категорії, проаналізовано військово-соціальну нормативно-правову базу та програмні документи з огляду на їх ефективність та практичне значення.

Ключові слова: військовослужбовці; соціальний захист; соціальне забезпечення; соціальна адаптація; військово-соціальне законодавство.

Постановка проблеми. Можливість реалізації військовослужбовцями своїх прав на різні види і форми соціального забезпечення особливо важлива в умовах критичного загострення зовнішніх загроз і небезпек для національної безпеки, головним чином в умовах дії особливих правових режимів. Отже, сучасна динаміка суспільних відносин потребує комплексного розв'язання проблем соціального забезпечення, соціального захисту та соціальної адаптації військовослужбовців, зокрема учасників бойових дій, включно з демобілізованими військовослужбовцями. І цілком очевидно, що "військово-соціальна" правова база перебуває в стані постійного вдосконалення. Додатковий імпульс до суттєвої зміни нормативно-правової бази в галузі соціального захисту військовослужбовців, і, зокрема, соціальної адаптації військовослужбовців до цивільного життя, дали події першої половини 2014 року. Природно, актуальність адекватнішого правового регулювання соціального захисту (зокрема соціальної адаптації) військовослужбовців зросла і у зв'язку з тим, що зовнішні загрози та небезпеки для суверенітету і територіальної цілісності держави постійно зростають до критичного рівня. Очевидно, що в умовах таких викликів національній безпеці, держава не може дозволити собі "розкіш" приділяти менше уваги адекватному соціальному захисту військовослужбовців та осіб, до них прирівняних.

Крім того, якісні зміни базових галузевих норм у сфері національної безпеки та оборони (пов'язані із запровадженням правового режиму воєнного стану та тривалим перебуванням держави у відповідному правовому режимі), ухвалення Президентом та Урядом нових програмних документів за основними напрямами внутрішньої та зовнішньої політики держави призвели до того, що військово-соціальне регулювання (насамперед, приведення військово-соціальної нормативно-правової бази до стандартів провідних країн світу, зокрема, країн Північноатлантичного альянсу) об'єктивно стало надважливим завданням.

Водночас, і майже через десять років після початку неоголошеної війни на Сході України, що переросла в повномасштабну збройну агресію, військово-соціальне законодавство все ще не повною мірою відповідає об'єктивній динаміці суспільних відносин, має певні недоліки й недоречності, страждає від суперечностей і колізій у юридичній термінології, "розпливчастістю" термінології, у тому числі й базових понятійних категорій.

Тому, одним із найактуальніших завдань є і залишається адекватне, ефективне та системне правове забезпечення соціальної адаптації військовослужбовців, що залишили ряди Збройних Сил України, інших військових формувань, правоохоронних та розвідувальних органів, зокрема, під час дії особливих правових режимів з підстав, передбачених чинним законодавством, до умов цивільного життя як одного із пріоритетних напрямів соціальної сфери військового будівництва.

Аналіз останніх досліджень і публікацій. Проблемні питання соціальної

адаптації військовослужбовців у своїх працях науковці піднімали у різний час [1–14].

Проаналізувавши праці цих та інших дослідників, можна дійти висновку про загальне розуміння наявних проблем недосконалого, неповного та, певною мірою, несистематизованого законодавства та інших нормативних актів щодо соціального забезпечення військовослужбовців, про що йшлося вище. Проте більшість науковців акцентують увагу, переважно, на розмежуванні етимологічного та правового змісту понятійних категорій: військово-соціального законодавства: "соціального забезпечення" та "соціального захисту", визначаючи їх співвідношення, допустимі рівні сумісності, розмежування та взаємозалежності.

Водночас, особливості саме соціальної адаптації як етимологічної та правової категорії рідко знаходять відображення в дослідженнях військових юристів. Дослідники також не зверталися до проблеми неузгодженості категоріального апарату, який міститься в численних законах, програмних документах і концепціях щодо соціального забезпечення військовослужбовців та членів їхніх сімей.

Метою дослідження є узагальнення етимологічного та правового змісту поняття "соціальна адаптація" військовослужбовців як правової категорії, а також аналіз нормативно-правової бази та програмних документів з питань соціальної адаптації військовослужбовців та осіб, до них прирівняних, з погляду їхньої ефективності та практичної значущості.

Виклад основного матеріалу. З моменту здобуття Україною незалежності, в постійних складних умовах державного розвитку, поступово формувалася і розвивалася соціально-правова система (і відповідний правовий інститут) адаптації військовослужбовців до умов цивільного життя, так звана "соціальна адаптація". Більш ніж за 30 років за ініціативою законодавчої влади, Президента, органів виконавчої влади, а також об'єднань громадян, міжнародних організацій та, навіть, окремих громадян було ухвалено низку актів законодавства, підзаконних нормативно-правових актів, прийняті програмні документи та розпорядчі рішення із запровадження нових форм і методів адаптації військовослужбовців до умов цивільного життя. Діяльність, що здійснюється у сфері соціальної адаптації військовослужбовців, тобто, певний алгоритм систематизованих практичних дій щодо впровадження нових форм і технологій соціальної роботи з громадянами України, які звільнились з військової служби, декларується як така, що ґрунтується на принципах нормативної універсальності та "програмної" спрямованості соціальної допомоги. Однак водночас виникає низка питань, а саме:

ефективність і повнота нормативного масиву з питань соціальної адаптації;

ефективність відповідних практичних методів, механізмів та інструментів реалізації;

адекватність фінансування;

рівень практичної ефективності державних і міжнародних програм тощо.

Таким чином, постає питання щодо необхідності системного аналізу чинної "військово-соціальної" нормативно-правової бази. Відповідно до Концепції Державної цільової програми соціальної і професійної адаптації військовослужбовців, які підлягають звільненню, та осіб, звільнених з військової служби, на період до 2017 року, схваленої розпорядженням Кабінету Міністрів України від 18 грудня 2013 р. № 1068-р, соціальна адаптація осіб, звільнених із військової служби визначалась як складний і тривалий суспільний процес [15]. У загальному концепті та розумінні вона передбачає освоєння норм і правил нового соціального середовища, пристосування до нових соціальних умов і завершується реалізацією права на працю, вільним вибором роботи, отриманням за неї справедливої та задовільної винагороди і, відповідно, гідних умов життя. Незважаючи на численні нормативно-правові акти та програмні документи, що проголошують соціальну адаптацію військовослужбовців та членів їхніх сімей одним із пріоритетів соціальної сфери військового будівництва та окремим напрямом державної соціальної політики, досі існує невизначеність, навіть на концептуальному рівні, у правовому регулюванні сфери відповідних суспільних відносин.

Відповідно, у вітчизняній правовій базі та в науковій літературі певний комплекс відносин, пов'язаних із підтримкою державними та недержавними структурами колишніх військовослужбовців у реалізації їхнього права на професійну перепідготовку та працевлаштування, позначається терміном "соціальна адаптація", що має умовний та узагальнений характер.

Вважається, що правова база соціальної адаптації почала формуватися з прийняттям

1992 року недержавної “Програми соціальної адаптації військовослужбовців”. Однак на рівні законодавчих актів нормативна база з питань соціальної адаптації фактично почала створюватися лише у 2004 році у зв’язку з ухваленням Закону України від 15 червня 2004 року № 1763-IV “Про державні гарантії соціального захисту військовослужбовців, які звільняються із служби у зв’язку з реформуванням Збройних Сил України, та членів їхніх сімей” [16]. Чинний Закон, вочевидь, замислювався як основний закон про соціальну адаптацію військовослужбовців, однак за своїм змістом він є лише органічним доповненням до Закону України від 20 грудня 1991 року № 2011-XII “Про соціальний і правовий захист військовослужбовців та членів їх сімей” [17], і спрямований, здебільшого, на регламентацію процедурних питань надання деяких виплат і компенсацій особам, що звільняються з лав Збройних Сил та інших військових формувань у зв’язку зі скороченням або іншими організаційними заходами.

Отже, як вбачається, побудова будь-якої галузевої правової бази не має сенсу без концептуального визначення базових правових категорій, що відображають конкретні соціальні процеси, явища та події. Водночас, концептуального визначення соціальної адаптації, хоча б як одного з елементів військової кар’єри, у законодавстві, на жаль, не закріплено. Разом з тим, Концепція Державної цільової програми соціальної і професійної адаптації військовослужбовців, які підлягають звільненню, та осіб, звільнених з військової служби, на період до 2017 року, схвалена розпорядженням Кабінету Міністрів України від 18 грудня 2013 р. № 1068-р, дає дещо неконкретизоване та “розмите” з правового погляду визначення адаптації: “Адаптацією військовослужбовців та членів їх сімей є соціальний процес їх активного пристосування до нових соціальних умов проживання в цивільному середовищі з ринковою системою відносин, який передбачає освоєння норм і правил такого середовища, оволодіння професією, спеціальністю, реалізацію прав, у тому числі на працю, формування нових правил поведінки і самоусвідомлення, що забезпечує комфортний перехід до нових умов життя” [15].

Крім того, у сучасних дослідженнях з цієї проблематики не існує єдиної етимологічної концепції соціальної адаптації осіб, звільнених з військової служби. До того ж, немає єдиної думки (ні юридично, ні концептуально) і щодо універсального складу суб’єктів, які потребують соціальної адаптації: Закон України від 15 червня 2004 року №1763-IV чітко та вичерпно визначає коло суб’єктів, які умовно підпадають під понятійну категорію “соціальна адаптація” (військовослужбовці, які вимушені достроково звільнитися з військової служби і члени їхніх родин), а також деякі соціальні преференції, що передбачені разом з підставами для їхнього надання (скорочення штатів та інші організаційні заходи). Крім того, як уже зазначалося, у даному випадку згаданий вище Закон передбачає лише окремі несистемні соціальні преференції, які більш змістовно “прилаштовані” до Закону України № 2011-XII “Про соціальний і правовий захист військовослужбовців та членів їх сімей” [17].

Таким чином, навіть на рівні єдиного законодавчого акта про соціальну адаптацію військовослужбовців [16], суб’єктний склад штучно звужений колом осіб, до яких застосовуються “організаційно-штатні заходи”. Водночас, загальний військово-соціальний Закон [17], що гарантує соціальну та професійну адаптацію військовослужбовців, розширює як суб’єктний склад, так і підстави для адаптації: “…яких звільнено у зв’язку із скороченням штатів або проведенням організаційних заходів, за станом здоров’я, а також військовослужбовцям строкової служби, які до призову на строкову військову службу не були працевлаштовані, а також членам сімей військовослужбовців за їх зверненням”.

Таким чином, наявні нормативні та теоретичні підходи до цієї проблеми можна умовно узагальнити та позиціонувати як:

“широке” розуміння соціальної адаптації як складової військової кар’єри [18–20];

“вузьке” розуміння соціальної адаптації, яке штучно обмежує предмет дослідження особами, звільненими з військової служби за організаційно-штатними заходами, яких за замовчуванням заведено вважати зовсім іншою категорією осіб, що потребує “окремого” правового регулювання [21–23].

Іншою, невизначеною категорією є “межі” державного втручання в розвиток кар’єри колишніх військовослужбовців після служби. Згадана вище Концепція [15] містить ретроспективний аналіз правової бази соціальної адаптації військовослужбовців та

посилається на існуючу на той момент правову базу: Програму соціальної і професійної адаптації військовослужбовців, звільнених у запас або відставку, на період до 2005 року, затверджену Указом Президента України від 21 вересня 2002 р. № 849 та Державну програму соціальної і професійної адаптації військовослужбовців, що підлягають звільненню, та осіб, звільнених з військової служби, на період до 2011 року, затверджену постановою Кабінету Міністрів України від 12 травня 2007 р. № 720.

У Концепції [15] визнається загальна низька ефективність реалізації цих програм, але наголошується на необхідності подальшого розв'язання цієї складної соціальної проблеми на основі "програмного підходу". Поряд із національними програмами в Україні реалізуються міжнародні проєкти та програми, що фінансуються Організацією Північноатлантичного договору (НАТО), Організацією з безпеки та співробітництва в Європі (ОБСЄ) та Міністерством закордонних справ Королівства Норвегія. Крім того, окремі державні структури, неурядові організації, громадські організації, вищі навчальні заклади та науково-дослідні інститути розв'язують питання соціальної адаптації військовослужбовців і цивільного персоналу без належної участі та уваги держави [24].

Однак, рівень "ефективності" таких і подібних програм з погляду їхніх масштабів і тематики, наочно показав заявлений у свій час проєкт Постанови Кабінету Міністрів (КМ) України "Про затвердження Державної цільової програми фізичної, медичної, психологічної реабілітації та соціальної і професійної реадаптації учасників антитерористичної операції та осіб, які залучалися та брали безпосередню участь у забезпеченні здійснення заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації у Донецькій та Луганській областях на період до 2022 року" [25], що був заявлений та виставлений на офіційний сайт Кабінету Міністрів України ще на початку 2018 року, але так і залишався на стадії обговорення до 05 грудня того ж року.

У цей період, судячи з усього, на нього просто не звертали уваги, причому, як вбачається, головним чином, завдяки розумінню очевидної практичної недоцільності такого документа. З іншого боку, припускаючи гіпотетичне існування ефективного, універсального та нормативно визначеного механізму контролю за реалізацією таких національних програм і, відповідно, механізму відповідальності компетентних посадовців за їх виконання (за умови ефективної реалізації в нормативній базі), згаданий проєкт, що став Постановою Кабінету Міністрів України [25], можна позиціонувати як важливий прорив у нормативно-правовому та програмному забезпеченні соціальної адаптації військовослужбовців.

По-перше, це пов'язано з уточненням визначення кола осіб, які потребують відповідної державної підтримки. По-друге, розширено обсяг державних заходів і послуг, що надаються відповідним цільовим групам, порівняно з аналогічними програмами, що діяли раніше. І по-третє, впровадження єдиної системи адміністрування потреб учасників бойових дій, Антитерористичної операції, операції Об'єднаних сил та інших осіб, які брали участь у реалізації заходів із забезпечення безпеки та оборони держави, відбиття та стримування збройної агресії Російської Федерації, було успішно сплановано, як на наш погляд. Єдиним недоліком цієї Державної цільової програми ми вважаємо те, що вона штучно обмежена колом суб'єктів, зазначеними в назві Постанови КМУ.

Висновки. Зважаючи на викладене необхідно, насамперед, визначити змістовні ознаки понятійної категорії "соціальна адаптація військовослужбовців". До речі, правові акти, державні програмні документи та управлінські рішення оперують одними й тими самими змістовними основними (щонайменше, п'ятьма) понятійними категоріями: "адаптація", "соціальна адаптація", "професійна адаптація", "соціально-професійна адаптація" та "соціальна та професійна адаптація до умов життя в цивільному середовищі".

Іншою проблемою є концептуальні, змістовні та процедурні суперечності військово-соціального, зокрема "військово-адаптаційного", законодавства. Нині існує ціла низка національних законів, міжнародних договорів, програмних документів, декларацій про наміри та протоколів, підзаконних актів, державних і недержавних програм щодо соціальної інтеграції військовослужбовців. Тому, ще одним важливим елементом належного регулювання соціальної адаптації людей означеної соціальної категорії слід вважати кодифікацію законодавства про соціальний і правовий захист

військовослужбовців шляхом ухвалення Військово-соціального кодексу.

Таким чином, проблему соціальної адаптації військовослужбовців не можна адекватно розв'язати без узагальнення правових норм, що містяться в правових актах різної юридичної значущості, та їхньої інтеграції в єдиний логічно структурований правовий акт, який системно і комплексно регулюватиме відповідну сферу суспільних відносин.

Слід також враховувати, що заходи, спрямовані на приведення соціального та адаптаційного законодавства Збройних Сил до єдиної стрункої та логічно впорядкованої системи, об'єктивно призведуть до необхідності внесення суттєвих змін до трудового законодавства та законодавства про соціальне забезпечення.

Подальші дослідження доцільно зосередити як на уніфікації правової термінології з питань соціально-правового забезпечення військовослужбовців, зокрема, їх соціальної адаптації, так і на розробленні універсального та дієвого нормативно-правового акту з питань соціальної адаптації військовослужбовців, що прийшов би на зміну численним програмним документам з означеного кола питань.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Актуальні проблеми соціально-правового статусу осіб, постраждалих під час проведення АТО : зб. матеріалів Всеукр. наук.-практ. конф. (м. Київ, 19 квіт. 2017 р.) / упор. Я. В. Журавель, О. С. Хопун ; заг. ред. Т. В. Семигіної ; Академія праці, соціальних відносин і туризму. Київ, 2017. 96 с.
2. Андрюшин О. Сто тисяч доларів військовому пенсіонеру, або про систему соціального захисту у Армії США // Народна армія. 2005. № 1. С. 43–45.
3. Афонін Е. А. Становлення Збройних Сил України: соціальні та соціально-психологічні проблеми : монографія. Київ : Інтерграфік, 1994. 315 с.
4. Болотіна Є. В., Кваша О. П., Степанова А. Е. Дослідження соціальних проблем військовослужбовців та їх сімей в умовах проведення антитерористичної операції // Вісник економічної науки України. 2020. № 2 (39). С. 117–122.
5. Гітіс Т. П., Чемерис Є. Т., Антонова В. І., Носаньова А. С. Дослідження сучасного рівня соціального захисту населення в Україні // Економічний вісник Донбасу. 2020. № 1 (59). С. 116–122.
6. Корольов С. С. Практичні аспекти створення, утвердження та нормативно-правового забезпечення гарантій соціального захисту військовослужбовців країн – членів НАТО // Збірник наукових праць Харківського університету Повітряних Сил. 2011. Вип. 3 (29). С. 280-283.
7. Марко І. Ю., Марко Є. І., Чернишова І. М. Зарубіжний досвід забезпечення соціальних гарантій військовослужбовців // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2019. № 2. С. 135–142.
8. Мозальов В. Є., Салій І. Ю. Соціальне забезпечення військовослужбовців Збройних Сил України в умовах збройної агресії Російської Федерації // Вісник Національного університету оборони України. 2022. № 5 (69). С. 110–115.
9. Мазуренко Л. І. Основні засади державної політики у сфері соціального захисту військовослужбовців: нормативно-правове забезпечення // Актуальні проблеми політики. 2023. Вип. 71. С. 223-231.
10. Новак-Каляєва Л. М. Нормативно-правові основи захисту прав військовослужбовців в Україні: соціальний аспект // Вісник національного університету „Львівська політехніка". 2007. № 584. с. 159.
11. Новікова О. Ф., Сидорчук О. Г., Панькова О. В. та ін. Стан та перспективи соціальної безпеки в Україні: експертні оцінки : монографія. Львівський регіональний інститут державного управління НАДУ; НАН України, Інститут економіки промисловості. Львів : ЛРІДУ НАДУ, 2018. 184 с.
12. Павленко В. С. Захист прав військовослужбовців та їх сімей: міжнародно-правовий аспект // Юридичний науковий електронний журнал. 2020. № 7. С. 131–133.
13. Пінчук Р. С., Письменна О. П. Покращення соціального і правового захисту військовослужбовців Збройних Сил України як запорука формування професійного війська // Науковий вісник Ужгородського національного університету. 2020. Серія: Право. Вип. 60. С. 83–89.
14. Цюкало Л. В. Соціальне забезпечення військовослужбовців Збройних Сил України та його суть // Ефективна економіка. № 7. 2017.
15. Про схвалення Концепції Державної цільової програми соціальної і професійної адаптації військовослужбовців, які підлягають звільненню, та осіб, звільнених з військової служби, на період до 2017 року : Розпорядження Кабінету Міністрів України від 18.12.2013 р. № 1068-р.
16. Про державні гарантії соціального захисту військовослужбовців, які звільняються із служби у зв'язку з реформуванням Збройних Сил України, та членів їхніх сімей : Закон України від 15.06.2004 р. № 1763-IV // Відомості Верховної Ради України (ВВР). 2004. N 36. Ст. 444.
17. Про соціальний і правовий захист військовослужбовців та членів їх сімей : Закон України від 20.12.1991 р. № 2011-XII //

Відомості Верховної Ради України (ВВР). 1992. № 15. Ст. 190.
18. Кондрюкова В. В., Слюсар І. М. Соціально-психологічна адаптація військовослужбовців силових структур, звільнених у запас : навч.-метод. посіб. Київ : Гнозіс, 2013. 116 с. URL: http://ifsa.kiev.ua/files/_book _2015_ I.pdf. (дата звернення: 11.08.2023).
19. Кондратенко О. Загальні засади нормативно-правового забезпечення державного управління у сфері соціального захисту учасників Антитерористичної операції та членів їх сімей // Вісник Національної академії державного управління при Президентові України. Серія Державне управління. 2015. № 4. С. 113–120.
20. Алещенко В. І. Соціальна адаптація звільнених військовослужбовців: стан, проблеми та напрями її удосконалення // Наука і оборона. 2006. № 3. С. 10–15.
21. Московчук Ю. А. Соціально-психологічний аспект адаптації звільнених військовослужбовців Збройних Сил України в умовах ринкової економіки // Нові технології навчання. Шляхи розвитку духовності та професіоналізму за умов глобалізації ринку освітніх услуг : зб. наук. праць / Спец. випуск № 48. Частина 1. 2007. С. 263–266.
22. Бідюк Н. М. Соціально-адаптаційне професійне навчання безробітних військовослужбовців, звільнених у запас // Вісник Черкас. ун-ту. Серія: Педагогічні науки. 2009. Вип. 147. С. 28–32.
23. Лазарєв В. В. Проблеми соціальної адаптації звільнених військовослужбовців (їхніх родин) // Стратегічна панорама. 2005. № 1. С. 130–138.
24. Норчук Ю., Доронін О. Актуальні питання розвитку соціального захисту військовослужбовців: з досвіду країн НАТО. Розвиток законодавства України у сфері оборони: проблеми адаптації до стандартів НАТО та шляхи їх вирішення: матеріали наук.-практ. конф., м. Київ, 23 квіт. 2021 р. Київ, 2021. С. 225–229.
25. Про затвердження Державної цільової програми з медичної, фізичної реабілітації та психосоціальної реадаптації постраждалих учасників Революції Гідності, учасників антитерористичної операції та осіб, які брали участь у здійсненні заходів із забезпечення національної безпеки і оборони, відсічі і стримування збройної агресії Російської Федерації в Донецькій та Луганській областях, забезпеченні їх здійснення, на період до 2023 року : Постанова Кабінету Міністрів України від 05.12.2018 р. № 1021. URL: ttps://zakon.rada.gov.ua/laws/show/1021-2018-%D0%BF#Text (дата звернення: 11.08.2023).

Стаття надійшла до редакційної колегії 19.09.2023

Problematic and debatable issues in the sphere of regulatory support for social adaptation of military personnel, taking into account their consistency and effectiveness

Annotation

The ability of servicemen to exercise their rights to various types and forms of social security is especially important in the context of critical aggravation of external threats and dangers to national security, mainly in the context of special legal regimes. One of the most urgent tasks is and remains adequate, effective and systematic legal support for social adaptation of servicemen who have left the Armed Forces of Ukraine, other military formations, law enforcement and intelligence agencies, in particular, during the period of special rights.

The article outlines the issues of generalization of the etymological and legal content of social adaptation of servicemen as a legal category, and analyzes the military-social regulatory framework and program documents with regard to their effectiveness and practical significance.

The problem of social adaptation of servicemen cannot be adequately addressed without generalizing the legal provisions contained in legal acts of different legal significance and integrating them into a single logically structured legal act which will systematically and comprehensively regulate the relevant area of social relations.

It should also be taken into account that measures aimed at bringing the social and adaptation legislation of the Armed Forces into a single coherent and logically ordered system will objectively lead to the need to make significant changes to labor and social security legislation.

Keywords: servicemen; social protection; social security; social adaptation; military and social legislation.

УДК 355. 42 DOI: https://doi.org/10.33099/2304-2745/2023-2-78/133-139

Криворучко І. Г.

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Методика оцінювання варіантів маневру (перегрупування) підрозділів для забезпечення перерозподілу сил і засобів у ході ведення оборонної операції за утримання рубежу оборони

Резюме. У статті обґрунтовано порядок вибору доцільних маршрутів для підрозділів, які здійснюють маневр на загрозливий напрямок смуги оборони угруповання військ (сил) з метою недопущення прориву рубежу оборони. Запропонований порядок базується на оцінці часу та ймовірності своєчасного проведення маневру (перегрупування) з урахуванням темпу просування противника.

Ключові слова: маневр (перегрупування); угруповання військ (сил); оборонна операція.

Постановка проблеми. Досвід ведення сучасних війн і збройних конфліктів, зокрема оборонних операцій під час відбиття широкомасштабної збройної агресії Російської Федерації (РФ), свідчить [1, 2], що сучасні бойові дії характеризуються високою динамічністю, маневреністю та різкими змінами обстановки. В умовах, коли противник має значну перевагу у військовому потенціалі, а оборона угруповання військ (сил) будується, як правило, в один ешелон, під час ведення оборонної операції набуває важливого значення маневр військ (сил).

Проведення своєчасного маневру має суттєвий вплив на успіх та ефективність ведення оборонної операції. Здійснення маневру в ході ведення оборонної операції угруповання військ (сил) обумовлюється змінами оперативної обстановки і насамперед направлено на:

заняття вигідного щодо противника положення створених угруповань військ (сил);

нарощування зусиль військ під час операції;

виведення військ з під ударів противника та більш ефективного їх використання для виконання поставлених, або знов виникаючих завдань [2, 3].

В оборонній операції проведення своєчасного маневру забезпечує: перенесення зусиль на інший напрямок та відбиття наступу противника на напрямках, раніше не передбачених або створення угруповань військ (сил) для нанесення контрудару. Іншими словами, маневр забезпечує перерозподіл сил і засобів у смузі оборони угруповання військ (сил) відповідно до змін обстановки, яка склалась в районі ведення операції.

Одним із прикладів можна розглянути обстановку, коли під час ведення наступальної операції противник, не досягнувши успіху на напрямку свого головного удару, а маючи успіх на іншому напрямку, змінить напрямок свого головного удару на зазначений напрямок, щоб забезпечити успіх свого наступу. Отже, це потребуватиме перерозподілу сил і засобів у смузі оборони угруповання військ (сил), що обороняється. Раціональний перерозподіл сил і засобів дасть змогу запобігти прориву оборонного рубежу, забезпечить стійкість оборони і недопущення просування противника в глибину.

За таких умов, важливо оцінити спроможність проведення своєчасного маневру, щоб гарантувати необхідний перерозподіл сил та засобів в ході ведення оборонної операції, та яким чином це вплине на стійкість оборони угруповання військ (сил) і ефективність оборонної операції зокрема. Тому, питання методики оцінювання своєчасності маневру в ході ведення оборонної операції – є актуальним науковим завданням.

Аналіз останніх досліджень і публікацій. Аналіз наукових робіт [4-6], свідчить про те, що питанням розроблення методики оцінювання здійснення маневру, як складової оборонної операції, приділяється значна увага.

Застосування методик, висвітлених у [4-6], дає можливість провести розрахунок показника часу здійснення маневру, який характеризує маневрені можливості військового формування в бою. Однак ці методики не враховують особливості ведення оборонної операції, зокрема темп просування противника. Розглянуті методики можуть бути використані лише для визначення часткових показників оцінювання ймовірності маневру в ході ведення оборонної операції.

У Каталозі спроможностей [7] визначено, що однією із основних вимог до спроможностей з ведення наземних бойових

дій є здатність військових формувань вести інтенсивні бойові дії та здійснювати маневрування з метою виконання оперативних і тактичних завдань, але кількісні та якісні показники, що характеризують цю здатність, не наводяться. Тобто, ці показники є лише вимогами.

Отже, на практиці виникає потреба обґрунтувати пропозиції, реалізація яких дозволила б максимально наблизитись до задоволення цих вимог.

Для цього необхідно мати відповідний науково-методичний апарат, використання якого дасть змогу оцінювати проведення маневру в ході ведення оборонної операції, зокрема оцінити ймовірність його своєчасного проведення для забезпечення перерозподілу сил і засобів в ході ведення оборонної операції за утримання рубежу оборони.

Метою статті є розкрити основні положення удосконаленої методики оцінювання варіантів маневру (перегрупування) підрозділів для забезпечення перерозподілу сил і засобів в ході ведення оборонної операції за утримання рубежу оборони.

Виклад основного матеріалу. Аналіз [8] свідчить, що на здійснення своєчасного маневру (перегрупування) військ (сил) в ході ведення оборонної операції впливають такі фактори:

по-перше, це кількість маршрутів, по яких здійснюється маневр, а також їх характеристики, такі як довжина, якість дорожнього покриття, ширина проїзджої частини, тип місцевості, погодні умови, а також можливі перешкоди (інженерні загородження, завали, руйнування тощо);

по-друге, це кількість і склад підрозділів, які беруть участь у маневрі.

Залежно від обстановки, яка склалася в районі ведення операції, та факторів, зазначених вище, різні за складом військові формування можуть здійснювати маневр у ході операції як вздовж лінії фронту, так і з висуванням з тилу до лінії фронту.

Виходячи з того, що своєчасність маневру (перегрупування) залежить від кількості та складу підрозділів, які беруть участь у маневрі (переміщенні), а також кількості маршрутів, по яких здійснюється маневр для кожного підрозділу, необхідно розрахувати ймовірність своєчасного маневру по декількох (різних) маршрутах. Це дасть змогу визначити доцільні маршрути, де ймовірності своєчасного маневру матимуть найвищі значення, а час здійснення маневру буде найкоротшим.

Для визначення часу та ймовірності своєчасного маневру (перегрупування) підрозділу можна застосувати підхід, запропонований у працях [5, 6]. До того ж, необхідно враховувати, що швидкість руху підрозділу під час зміни позицій (V) залежатиме від глибини колони та стану маршруту:

$$t_M = \frac{D}{V} + t_{зг} + t_{розг} + t_{затр}, \qquad (1)$$

де t_M – тривалість (час) зміни позицій, хв;

D – відстань до нових позицій, км;

V – швидкість руху під час зміни позицій, км/год;

$t_{зг}$ – час згортання підрозділу, хв;

$t_{розг}$ – час розгортання підрозділу, хв;

$t_{затр}$ – час затримки підрозділу на інженерних загородженнях, руйнуваннях та перешкодах під час переміщення.

У процесі розрахунку ймовірності своєчасного маневру важливо врахувати не лише напрямок, на який необхідно здійснити маневр (перегрупування), але й такий фактор, як швидкість переміщення лінії бойового зіткнення (ЛБЗ), яка залежатиме від темпу наступу противника. Ймовірність своєчасного маневру [6] визначається за формулою

$$P_{\text{СМ}_j} = 1 - e^{-\frac{\Delta D}{T_{\text{м}} V_{\text{лбз}}}}, \qquad (2)$$

де ΔD – відстань, на яку необхідно переміститися від фронту з урахуванням переміщення лінії бойового зіткнення, км;

T_M – тривалість (час) маневру, хв;

$V_{\text{лбз}}$ – швидкість переміщення лінія бойового зіткнення, км/год.

Методика оцінювання варіантів маневру (перегрупування) підрозділів для забезпечення перерозподілу сил і засобів угруповання військ (сил) в ході ведення бойових дій за утримання рубежу оборони з урахуванням темпу наступу противника полягає у визначенні маршрутів і підрозділів, які здійснюють переміщення по них з найвищою ймовірністю своєчасного маневру $(P_{CM_{\max}})$ та найменшим часом руху $(T_{M_{\min}})$, тобто зможуть здійснити перегрупування до визначеного рубежу в найкоротший термін. Водночас найнижчі показники ймовірності своєчасного маневру $(P_{CM_{\min}})$ та найбільший час $(T_{M_{\max}})$,

затрачений на його здійснення дадуть змогу зробити висновки про маршрути, які недоцільно використовувати для здійснення маневру.

Вхідні дані для проведення розрахунків:

кількість підрозділів, що здійснюють маневр $(N_{П})$;

нормативна швидкість руху підрозділів (V_i), км/год, $i=\overline{1,N_{П}}$;

час згортання підрозділу, що здійснює маневр $(t_i^{зг})$, хв;

час розгортання підрозділу, що здійснює маневр $(t_i^{розг})$, хв;

коефіцієнт зміни швидкості руху військ залежно від глибини колони підрозділу, що здійснює маневр (батальйон, рота, взвод) $(k_i^{ск})$;

кількість можливих маршрутів руху підрозділів, які залучаються до маневру (N_M);

відстань, на якій пролягає маршрут від лінії бойового зіткнення (ЛБЗ) (H_j), км, $j=\overline{1,N_M}$;

дальність маршруту, по якому здійснюється маневр (відстань від позиції на одному напрямку до нової позиції на іншому напрямку смуги оборони), км (D_j);

час затримки підрозділу на інженерних загородженнях, руйнуваннях і перешкодах, хв $(t_j^{затр})$;

коефіцієнт, що враховує пересіченість рельєфу місцевості $(k_j^{п})$;

коефіцієнт якості дорожнього покриття $(k_j^{дп})$;

ширина проїжджої частини, м $(k_j^{пр})$;

коефіцієнт, що враховує типи місцевості та погодні умови $(k_j^{м})$;

співвідношення сил сторін (C);

коефіцієнт фортифікаційного обладнання смуги оборони $(k_{фо})$;

коефіцієнт природної прохідності місцевості для наступу противника $(k_{м})$;

максимальний темп наступу (просування) противника $(V_{H\max})$.

Початковими даними також буде бінарна матриця $W(\omega_{ij})=N_{П}\times N_M$, яка визначає можливості здійснення маневру $N_{П}$ підрозділами за N_M маршрутами залежно від умови: чи пролягає *j*-й маршрут в районі розташування *i*-го підрозділу. Це дасть змогу виключити з розрахунків заздалегідь неприйнятні маршрути. Елементами матриці є $\omega_{ij}=0$, якщо *i*-му підрозділу не доступний *j*-й маршрут, і $\omega_{ij}=1$, якщо визначений маршрут доступний.

Таким чином, матриця (W) матиме вигляд

$$W(\omega_{ij})=\begin{bmatrix} \omega_{11} & \omega_{12} & \dots & \omega_{N_{П1}} \\ \omega_{21} & \omega_{22} & \dots & \omega_{N_{П2}} \\ \dots & \dots & & .... \\ \omega_{N_{M1}} & \omega_{N_{M2}} & \dots & \omega_{N_{П}N_M} \end{bmatrix},$$

та представлена у вигляді двовимірної таблиці (Табл.1), яка містить відповідність маршрутів підрозділам, які здійснюють маневр (перегрупування).

Таблиця 1

Варіант представлення бінарної матриці маршрутів підрозділам, які здійснюють маневр

Елементи	M_1	M_2	M_3	M_4	⋯	M_j
П1	1	0	1	0	⋯	0
П2	0	1	0	1	⋯	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮
Пі	0	0	0	0	⋯	1

З Табл. 1 видно, який підрозділ за якими маршрутами може здійснювати маневр (перегрупування). Кожен рядок цієї матриці представляє один підрозділ, а кожний стовпець представляє один маршрут, в той час як значення на їх перетині вказують на те, якими маршрутами може скористатися кожний підрозділ.

Обмеження, які прийняті у методиці:

маневр військ здійснюється своїм ходом на штатних засобах;

маршрути руху підрозділів під час здійснення маневру не пересікаються.

Структурно-логічна схема алгоритму удосконаленої часткової методики оцінювання варіантів маневру підрозділів для забезпечення перерозподілу сил і засобів в ході ведення бойових дій за утримання рубежу оборони наведена на (рис.1).

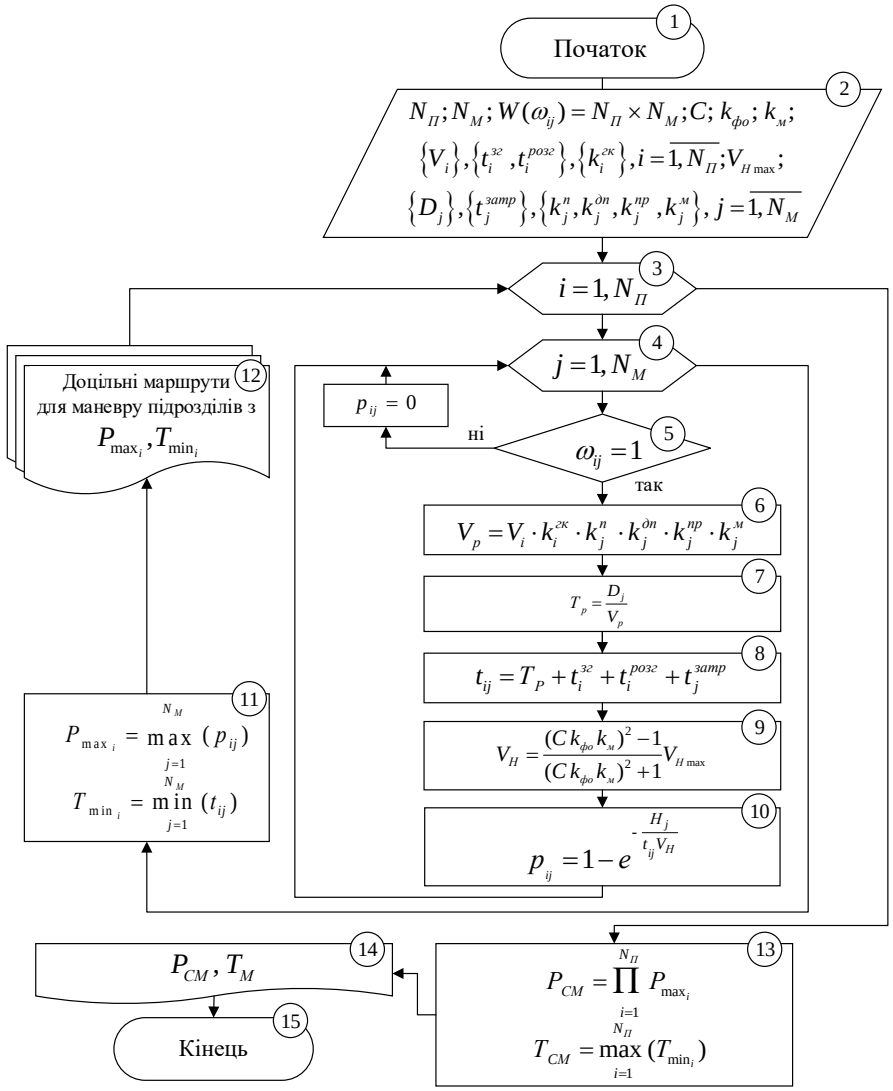


Рис. 1. Структурно-логічна схема методики оцінювання варіантів маневру підрозділів для забезпечення перерозподілу сил і засобів в ході ведення бойових дій за утримання рубежу оборони

Використовуючи вхідні дані *блоку 2*, у *блоках 3,4* проводимо циклічний послідовний перебір N_M маршрутів здійснення маневру для кожного з $N_П$ підрозділу. Це дасть змогу оцінити всі можливі варіанти маневрів для кожного підрозділу шляхом здійснення послідовного розгляду кожного маршруту.

Такий підхід дасть змогу визначити, який маршрут є найбільш доцільним для кожного підрозділу, що здійснює маневр, враховуючи при цьому вхідні дані. Кількість циклів перебору залежатиме від кількості підрозділів та маршрутів, по яких вони можуть здійснити маневр.

Слід зазначити, що цикл по кожному маршруту буде вкладений у цикл по кожному підрозділу. Цикл повторюватиметься доки не буде здійснено перебір усіх маршрутів для кожного підрозділу. Якщо підрозділ не може застосувати (використати) визначений маршрут $\omega_{ij} = 0$ (наприклад, маршрут проходить на великій відстані від розташування підрозділу тощо), тоді ймовірність своєчасного маневру *i*-го підрозділу по *j*-му маршруту приймаємо $p_{ij} = 0$. Якщо маршрут відповідає умові $\omega_{ij} = 1$ (*блок 5*), проводяться розрахунки в *блоках 6-9.*

У *блоці 6* розраховуємо орієнтовну швидкість руху окремо для кожного підрозділу, який здійснює маневр, по обраному (одному) маршруту залежно від нормативної швидкості руху, глибини його колон, коригувальних коефіцієнтів характеристик шляхів (табл. 2), а також типу місцевості і погодних умов (табл. 3) за формулою

$$V_p = V_i \cdot k_i^{ск} \cdot k_j^n \cdot k_j^{дп} \cdot k_j^{пр} \cdot k_j^м, \quad (3)$$

де V_i – нормативна швидкість руху, км/год (для колон з колісної техніки дорівнює 20-25 км/год; для змішаних колон або

колон з гусеничної техніки – 10-15 км/год);

k_j^n – коефіцієнт, що враховує пересіченість рельєфу місцевості;

$k_j^{оп}$ – коефіцієнт якості дорожнього покриття;

$k_j^{пр}$ – ширина проїжджої частини;

$k_i^{зк}$ – коефіцієнт зміни швидкості руху військ від глибини колони;

$k_j^м$ – коефіцієнт, що враховує типи місцевості та погодні умови.

Отримані результати розрахунку дають змогу визначити орієнтовну швидкість руху окремо кожного підрозділу, що здійснює маневр в умовах конкретної місцевості по одному маршруту.

Таблиця 2

Значення коригувальних коефіцієнтів врахування характеристик шляхів [8]

Коефіцієнт, що враховує пересіченість рельєфу місцевості, k_j^n								
Відносний ухил місцевості (i_γ)	0	0,2	0,3	0,4	0,5	0,6	0,7	0,8
Значення k_j^n	1	0,92	0,84	0,76	0,65	0,56	0,45	0,34
Коефіцієнт якості дорожнього покриття, $k_j^{оп}$								
Частка шляхів із ґрунтовим покриттям $(m_{гр})$	0	0,2	0,3	0,4	0,5	0,6	0,8	1,0
Значення $k_j^{оп}$	1	0,99	0,96	0,93	0,9	0,89	0,86	0,83
$k_j^{пр}$								
Ширина проїжджої частини ($_{в\ пр}$,м)	4,5		6,0		7,5		9,0	10,5
Значення $k_j^{пр}$	0,6		0,7		1,0		1,05	1,2
Коефіцієнт зміни швидкості руху військ від глибини колони, $k_i^{зк}$								
Склад колони	взвод		рота		батальйон		бригада	
Значення $k_i^{зк}$	1,2		1		0,95		0,88	

Таблиця 3

Значення коефіцієнта, що враховує типи місцевості та погодні умови при переміщенні ПУ [8]

Тип місцевості	**Коефіцієнт, що враховує типи місцевості та погодні умови, $k_j^м$**	
	нормальні погодні умови	дощ, сніг, бездоріжжя
Рівна	1,0	0,7
Слабо пересічена	0,9	0,63
Пересічена	0,8	0,56
Сильно пересічена	0,7	0,49
Болотиста	0,5	0,41

Після отримання результатів орієнтовної швидкості руху підрозділу по вибраному (одному) маршруту, залежно від дальності та швидкості руху, у *блоці 7* проводимо розрахунок очікуваного часу руху підрозділу по цьому маршруту за допомогою формули

$$T_p = \frac{D_j}{V_p}, \qquad (4)$$

де D_j – дальність маршруту, по якому здійснюється маневр одним підрозділом;

V_p – швидкість руху підрозділу, що здійснює маневр з урахуванням впливу характеристик місцевості.

Результати розрахунку дадуть змогу визначити (прогнозувати) очікуваний час, необхідний підрозділу для пересування по обраному (одному) маршруту.

Для визначення часу здійснення маневру *i*-го підрозділу по *j*-му маршруту у *блоці 8* додаємо до часу руху (T_p), визначеного у *блоці 7*, час згортання $(t_i^{зг})$ та розгортання $(t_i^{розг})$ цього підрозділу, а також час його затримки $(t_j^{затр})$ на інженерних загородженнях, руйнуваннях та перешкодах під час переміщення, використовуючи при цьому формульний вираз

$$t_{ij} = T_P + t_i^{зг} + t_i^{розг} + t_j^{затр}, \qquad (5)$$

де T_P – очікуваний часу руху підрозділу, який здійснює маневр.

З метою врахування чинника, а саме темпу просування наступальних угруповань противника в смузі оборони угруповання військ (сил), у *блоці 9* проводиться його визначення за допомогою формули

$$V_H = \frac{(C k_{фо} k_м)^2 - 1}{(C k_{фо} k_м)^2 + 1} V_{H\max}, \quad (6)$$

де $V_{H\max}$ – максимальний темп просування механізованих з'єднань та частин, прийнято рівним 5 км/год.

Таблиця 4

Значення коефіцієнта фортифікаційного обладнання смуги оборони

Показники	**Значення показників**											
Орієнтовний час підготовки оборони	3 год	12 год	1 доба	1,5 доби	2 доби	3 доби	4 доби	5 діб	6 діб	7 діб	8 діб	9 діб
Відсоток виконання інженерних робіт	До 5% I черги	17% I черги	33% I черги	50% I черги	67% I черги	100% I черги	17% IIчерги	33% II черги	50% II черги	67% II черги	83% II черги	100% II черги
Коефіцієнт фортифікайного обладнання СО, $k_{фо}$	1	0,82	0,74	0,69	0,66	0,62	0,60	0,58	0,56	0,55	0,54	0,53

Отримані результати, а саме: дальність *j*-го маршруту, по якому здійснюється маневр *i*-м підрозділом, час його маневру, а також темп наступу противника дають змогу у *блоці 10* визначити ймовірність своєчасного маневру (переміщення на нову позицію) одного підрозділу по одному маршруту за формулою

$$p_{ij} = 1 - e^{-\frac{H_j}{t_{ij} V_H}}, \quad (7)$$

де p_{ij} – ймовірність своєчасного маневру *i*-го підрозділу по *j*-му маршруту.

Після перебору усіх можливих маршрутів для *i*-го підрозділу в *блоці 11* здійснюється пошук максимального значення ймовірності своєчасного маневру $(P_{\max_i})$ та мінімального часу $(T_{\min_i})$ переміщення для цього підрозділу. У результаті визначається доцільний маршрут для цього підрозділу, де ймовірність своєчасного маневру є найвищою, а час переміщення мінімальний (*блок 12*).

Після визначення доцільних маршрутів для всіх підрозділів, які здійснюють маневр переходимо до визначення у *блоці 13* ймовірності своєчасного маневру та часу на його проведення усіма підрозділами.

Виходячи з того, що маневри *i*-х підрозділів по *j*-х маршрутах є незалежними один від одного подіями, тому ймовірність своєчасного маневру всіма $N_П$ підрозділами може бути визначена як добуток максимальних значень імовірностей маневрів *i*-х підрозділів $(P_{\max_i})$ за формулою [10]:

$$P_{CM} = \prod_{i=1}^{N_П} P_{\max_i}, \quad (8)$$

де i – індекс підрозділів, що здійснюють маневр, $i = \overline{1, N_П}$;

$P_{\max_i}$ – максимальні значення ймовірності своєчасного маневру *i*-х підрозділів.

Час на проведення маневру (T_{CM}) визначається як максимальний час серед максимальних значень:

$$T_{CM} = \max_{i=1}^{N_П} (T_{\min_i}), \quad (9)$$

де $T_{\min_i}$ – мінімальний час маневру *i*-х підрозділів.

Це означає, що час проведення маневру відповідатиме показнику підрозділів з найдовшим часом маневру.

Отримані результати оцінки зазначених показників своєчасності маневру (перегрупування) дають змогу обрати найбільш доцільні маршрути руху підрозділів під час здійснення маневру з урахуванням темпу наступу противника.

Висновки. Отже, запропонована методика дає змогу оцінити ймовірність своєчасного маневру (перегрупування) військ в ході ведення оборонної операції ОТУВ, та на відміну від існуючих, дає змогу врахувати темп наступу противника під час визначення (вибору) доцільних маршрутів руху для підрозділів, які здійснюють маневр. Маршрути руху для підрозділів, які здійснюють маневр до визначеної позиції (рубежу) смуги оборони угруповання (військ), вибираються таким чином, щоб забезпечити найкоротший час руху і найвищу ймовірність здійснення маневру та його своєчасність виходячи з темпу наступу противника.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стрижевський В. В. Розвиток загальної тактики в локальних вйнах і збройних конфліктах другої половини XX та на початку XXI століть: монографія. Київ : НАОУ, 2006. 272 с.
2. Телилим В. М., Загорка О. М., Стрижевський В. В. Досвід створення та застосування угруповань військ (сил) у

локальних війнах і збройних конфліктах другої половини XX та на початку XXI століть : монографія. Київ : НУОУ, 2012. 336 с.
3. Бойовий статут Сухопутних військ. Частина 2. Батальйон, рота / А. В. Поливода. Київ : КСВ, 2016. 368 с.
4. Збірник тактичних розрахунків з прикладами : навч. посіб. / колектив авторів. Київ : НУОУ ім. Івана Черняховського, 2018. 96 с.
5. Вайнер А. Я. Тактические расчеты. 2-е изд., перераб. и доп. Москва : Воениздат, 1982. 176 с.
6. Черевко Р. М. Удосконалена математична модель маневреності пунктів управління // Social Development and Security. 2019. № 9 (3). С. 56–62.
7. Єдиний перелік (каталог) спроможностей Міністерства оборони України, Збройних Сил України та інших складових сил оборони : затв. Міністром оборони України 31.12.2021 р. 825 с.
8. Черних І. В., Коцюруба В. І., Філь В. М. Оперативні розрахунки завдань інженерного забезпечення : методики та приклади. Київ : НУОУ, 2016. 152 с.
9. Павловский Р. И., Чубаренко А. И., Сафонов Д. С. Основы теории боевой эффективности танков. Москва : ЦНИИИ, 1981. 264 с.
10. Абезгауз Г. Г. Справочник по вероятностным расчетам. Москва : Воениздат, 1970. 536 с.

Стаття надійшла до редакційної колегії 09.10.2023

Methodology for evaluating variants of maneuver (regrouping) of units to ensure the redistribution of forces and means during the conduct of a defensive operation to maintain the defense line

Annotation

The experience of conducting modern wars and armed conflicts, including defense operations when repelling large-scale armed aggression of the Russian Federation (RF), shows that modern military operations are characterized by high dynamism, maneuverability and sudden changes in the situation. In a defense operation, carrying out a timely maneuver ensures the transfer of efforts to the problematic direction and repulse the enemy's offensive or the creation of groupings of troops (forces) to launch a counterattack.

The implementation of maneuver during the conduct of a defense operation by a group of troops (forces) is determined by changes in the operational situation and is primarily aimed at:

occupying a position advantageous in relation to the enemy by the created groupings of troops (forces);

increasing troop efforts during the operation;

withdrawal of troops from enemy attacks and their more effective use to carry out assigned or newly emerging tasks.

The article substantiates the procedure for choosing appropriate routes for units maneuvering towards a threatening direction of the defense line of a group of troops (forces) in order to prevent a breakthrough of the defense line. The proposed procedure is based on an assessment of the time and probability of a timely maneuver (regrouping), taking into account the pace of enemy advance.

The improved methodology makes it possible to assess the likelihood of timely maneuver (regrouping) of troops during the conduct of a defensive operation of the operational-tactical grouping of troops (OTGT) and, unlike existing ones, allows one to take into account the pace of the enemy's offensive when determining (selecting) appropriate movement routes for units carrying out the maneuver. Movement routes for units maneuvering to a certain position (line) of the group's (troops') defense line are selected in such a way as to ensure the shortest movement time and the highest probability of completing the maneuver, and its timeliness based on the pace of the enemy's advance.

Keywords: maneuver (regrouping); grouping of troops (forces); defense operation.

ВІДОМОСТІ ПРО АВТОРІВ

БЕЙКУН А. Л. – доцент кафедри правового забезпечення діяльності Національної гвардії України Київського інституту Національної гвардії України, кандидат юридичних наук, доцент;

БОЧАРНІКОВ В. П. – головний науковий співробітник НДУ ЦВСД НУО України, доктор технічних наук, професор;

БУТЕНКО М. П. – науковий співробітник НДВ ЦВСД НУО України;

ВАВІЛОВА Н. В. – провідний науковий співробітник НДВ ЦВСД НУО України, кандидат історичних наук;

ГАЛАГАН В. І. – провідний науковий співробітник НДВ ЦВСД НУО України, кандидат військових наук, доцент;

ГАННЕНКО С. О. – старший викладач Інституту інформаційно-комунікаційних технологій та кібероборони НУО України, кандидат технічних наук;

ДЕЙНЕГА О. В. – головний науковий співробітник ЦНДІ Збройних Сил України, доктор військових наук, професор;

ЗАГОРКА О. М. – головний науковий співробітник ЦВСД, доктор військових наук, професор;

ЗВІР В. Б. – заступник начальника управління – начальник НДВ ЦВСД НУО України;

ЗУБКОВ В. П. – старший науковий співробітник НДВ ЦВСД НУО України;

КАПТАН М. В. – старший науковий співробітник НДВ ЦВСД НУО України;

КІРПІЧНІКОВ Ю. А. – начальник НДВ ЦВСД НУО України, кандидат технічних наук;

КИВЛЮК В. С. – доцент кафедри тилового забезпечення інституту логістики та підтримки військ (сил) НУО України, кандидат економічних наук;

КИРИЛЕНКО В. І. – начальник кафедри Київського національного економічного університету імені Вадима Гетьмана, доктор економічних наук, професор;

КОВАЛЬЧУК П. А. – старший науковий співробітник НДВ ЦВСД НУО України;

КОСАРЕЦЬКИЙ Є. І. – провідний науковий співробітник НДВ ЦВСД НУ України, доктор філософії;

КРИВОРУЧКО І. Г. – ад'юнкт НДВ ЦВСД НУО України;

КУЛЬЧИЦЬКИЙ О. С. – начальник НДЛ НДВ інституту стратегічних комунікацій НУО України;

ЛЕПІХОВ А. В. – головний консультант Центру безпекових досліджень Національного інституту стратегічних досліджень;

ЛІПКО І. О. – провідний науковий співробітник НДВ ЦВСД НУО України;

ЛИТОВЧЕНКО Г. Д. – старший науковий співробітник НДЛ НДВ ЦВСД НУО України;

МАЗУРЕНКО І. М. – начальник НДВ ЦВСД НУО України, доктор філософії;

МАТВІЄЦЬ С. Я. – курсант Київського інституту Національної гвардії України;

МИКОЛЕНКО Ю. М. – начальник командно-штабного інституту застосування військ (сил) НУО України, кандидат військових наук;

МОСОВ С. П. – професор кафедри авіації та авіаційного пошуку і рятування Інституту державного управління та наукових досліджень з цивільного захисту, доктор військових наук, професор;

ОСТАПЧУК О. П. – старший науковий співробітник НДЦ гуманітарних проблем ЗС України, кандидат історичних наук;

ПОЛЕВИЙ В. І. – старший науковий співробітник навчально-наукового центру стратегічних комунікацій у сфері забезпечення національної безпеки та оборони НУО України, кандидат юридичних наук, старший науковий співробітник;

ПОЛОВЕНКО В. М. – провідний науковий співробітник НДВ інституту логістики та підтримки військ (сил) НУО України, кандидат військових наук;

ПРОКОПЕНКО О. С. – начальник НДЛ НДВ інституту стратегічних комунікацій НУО України, доктор філософії;

РИБИДАЙЛО А. А. – провідний науковий співробітник НДВ ЦВСД НУО України, кандидат технічних наук, старший науковий співробітник;

СВЄШНІКОВ С. В. – провідний науковий співробітник НДВ ЦВСД НУО України, кандидат технічних наук, старший науковий співробітник;

СЛЮСАРЕНКО А. В. – старший науковий співробітник НДВ ЦВСД НУО України;
СОТНИК В. В. – старший науковий співробітник НДВ ЦВСД НУО України, кандидат економічних наук;
ТЕЛЕГІН В. В. – ад'юнкт кафедри економіки та фінансового забезпечення інституту логістики та підтримки військ (сил) НУО України;
ТОПОЛЬНИЦЬКИЙ В. В. – начальник НДВ ЦВСД НУО України, кандидат юридичних наук;
ФЕДОРІЄНКО В. А. – начальник НДВ інституту стратегічних комунікацій НУО України, кандидат технічних наук;
ФРОЛОВ В. С. – провідний науковий співробітник НДВ ЦВСД НУО України, кандидат військових наук, старший науковий співробітник;
ХРАПАЧ Г. С. – науковий співробітник НОВ ЦВСД НУО України;
ШЕВЧЕНКО М. М. – старший офіцер Управління забезпечення реагування на кризові ситуації МО України, кандидат філософських наук, доцент

ВИМОГИ ДО СТАТЕЙ

Відповідно до Постанови ВАК України № 7-05/1 від 15 січня 2003 року наукові статті мають містити такі елементи:

постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

аналіз останніх досліджень і публікацій, у яких започатковано розв'язання даної проблеми і на які спирається автор, виділення нерозв'язаних раніше частин загальної проблеми, яким присвячується стаття;

формулювання **мети статті** (постановка завдання);

виклад **основного матеріалу** дослідження з повним обґрунтуванням отриманих наукових результатів;

висновки і перспективи подальших досліджень розвитку в цьому напрямі;

анотація до статті та ключові слова – розміщуються після назви статті.

У статті слід дотримуватись загальноприйнятої термінології. Усі скорочення та нові терміни мають бути розкриті автором.

Назва, список авторів, назва установи, анотація (не більше 40 слів), ключові слова (7 слів) готуються на трьох мовах: українській, російській та англійській.

Обсяг статті разом із таблицями, рисунками та списком літератури не більше 10 сторінок А4.

Текст статті набирається в редакторі **Microsoft Word** шрифтом **Times New Roman 14. Вирівнювання по ширині. Інтервал між рядками тексту – 1,0.**

Формат сторінки – А4. Поля: ліве – 27 мм; верхнє і нижнє – 20 мм; праве – 20 мм.

Не використовуйте для форматування тексту пропуски, табуляцію тощо. Не встановлюйте ручне перенесення слів, не використовуйте колонтитули.

Між значенням величини та одиницею її вимірювання ставте нерозривний пропуск (Ctrl + Shift + пропуск).

Таблиці та рисунки виконуються в одному стилі, нумеруються та подаються після посилань на них у тексті.

Текст усередині таблиці набирається в редакторі **Microsoft Word** шрифтом **Times New Roman – кегль 10.**

Таблиці нумеруються, вирівнювання по центру, без відступів. Слово "Таблиця 1" – ***кегль 11***, вирівняний по правій стороні. Формат назви таблиці: вирівнювання по центру, напівжирний, положення – над таблицею. Після таблиці необхідно залишити один порожній рядок.

Рисунки нумеруються, вирівнювання по центру. Формат назви рисунку – вирівнювання по центру, положення – під рисунком, позначається скороченим словом "Рис.". Перед рисунком і після його підпису необхідно залишити один порожній рядок.

Текст у середині рисунка набирається в редакторі **Microsoft Word** шрифтом **Times New Roman – *кегль 9–10*.**

Формули виносяться на середину рядків. Набір здійснюється у редакторі формул *MathType* курсивом (крім особливих випадків) без обрамлення і заливки. Забороняється використовувати для набору формул графічні об'єкти, кадри і таблиці.

Вирівнювання по центру, нумерація – у дужках, праворуч. Нумерувати потрібно тільки ті формули, на які є посилання у тексті.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ складається у порядку посилання в тексті та подається наприкінці статті згідно з ДСТУ ГОСТ 7.1:2015. – ***кегль 12***

У редакцію надається друкований примірних рукопису.

На останній сторінці робиться припис – "**Стаття не містить відомостей, що розкривають державну таємницю та службову інформацію. Автори надають дозвіл на перевірку праці відповідальними особами, призначеними для перевірки праць на оригінальність і відсутність неправомірних запозичень. Автори гарантують, що ними одержано всі необхідні дозволи на використання у цій статті матеріалів, що охороняються авторським правом. Автори гарантують, що ця стаття раніше не публікувалась і не подавалась до інших видань**". *Підписи авторів*.

До редакційної колегії подаються такі документи:

1. Файли, які містять ***текст статті українською*** та ***анотації*** (не менше 1800 знаків) **українською, російською та англійською мовами** у форматі електронного документа **MS Word версія 2010**.

2. Довідка про авторів українською, російською та англійською мовами (П.І.Б. – повністю, установа, посада, вчений ступінь, вчене звання, контактна інформація).

3. Акт експертизи щодо відкритого публікування (для зовнішніх авторів).

УВАГА! Статті, які не задовольняють будь-якій з перелічених вимог, до видання не приймаються.

ШАБЛОН СТАТТІ

УДК 628. 8 – ***Times New Roman кегль – кегль 12 пт***

Бунін В. В., доктор технічних наук, професор[1]; – ***Times New Roman кегль – кегль 14 пт***
Іванов В. А.[2]
Бунин В. В., доктор технических наук, профессор[1];
Иванов В. О.[2]
V. Bunin, DsT[1], professor;
V. Ivanov[2]

[1] – Департамент воєнної політики та стратегічного планування Міністерства оборони України, Київ;
[2] – Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ
[1] – Департамент военной политики и стратегического планирования Министерства обороны Украины, Киев;
[2] – Центр военно-стратегических исследований Национального университета обороны Украины, Киев
[1] – Defence Policy and Strategic planning Department, Ministry of defence of Ukraine, Kyiv;
[2] – Center for Military and Strategic Studies of the National Defence University of Ukraine

Матрична модель OLAP-систем (*кегль 14 пт напівжирний*)
Матричная модель OLAP-систем
Matrix model of OLAP-systems

Резюме (2-3 речення). Розглянуто особливості матричних моделей … ***(кегль 12 пт)***
Анотація (1800 знаків).
Ключові слова: модель, OLAP-система, інформаційні технології.

Аннотация (1800 знаков).
Ключевые слова:

Annotation (1800 characters)
Keywords:

Постановка проблеми. Численні дослідницькі роботи направлені на розв'язання задач зниження енергоємності систем пневмотранспорту. **…**

Аналіз останніх досліджень і публікацій. У роботах [1, 2] розглянуто прикладні методики щодо … Проте не визначено…

Мета статті. Підвищення ефективності технологічних операцій щодо …

Виклад основного матеріалу. Автором пропонується використання аналітичних методів пошуку оптимального режиму …

1 інтервал

$$\sum_{p=1}^{N^2} X_{n_k}^{pk}$$

1 інтервал

де $\sum$ *– Times New Roman 18 шрифт;*
X *- Times New Roman 14 шрифт;*
N ; pk; p=1 ; n *– Times New Roman 10 шрифт;*
k ; ⤵ *– Times New Roman 8 шрифт.*

Висновки. … Найбільш ефективним за критерієм мінімуму витрат ресурсів виявився…
Напрями подальших досліджень. Уточнення показників щодо …

УВАГА! Під час виконання рисунків та набору формул забороняється використовувати графічні об'єкти, кадри і таблиці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ (згідно з ДСТУ ГОСТ 7.1:2015)

Відомості про авторів – прізвище, ім'я, по батькові (повністю); посада; установа; вчений ступінь; вчене звання.

УВАГА! Документи для включення статті в План до друку потрібно подавати на електронну адресу Редакційної колегії znp.cvsd@nuou.org.ua

Наукове видання

Збірник наукових праць
Центру воєнно-стратегічних досліджень
Національного університету оборони України

№ 2(78), 2023

Відповідальний за випуск А. А. Рибидайло
Технічний секретар Г. В. Руденська
Комп'ютерне верстання А. А. Рибидайло
Коректори Н. М. Андріянова, Т. В. Уварова, С. А. Терещенко
Підтримка вебсайту збірника Ю. А. Кірпічніков, М. В. Петрушен

Підписано до друку 20.06.2023. Формат 60x84 1/8.
Папір офсетний. Обл.- вид. арк. 8,208. Друк. арк. 18,0
Зам. 412. Наклад 100 прим.

Видання Національного університету оборони України
03049, м. Київ, Повітрофлотський пр-т, 28
http://znp-cvsd.nuou.org.ua

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої продукції, серія ДК № 2205 від 02.06.2005.

Надруковано у друкарні Національного університету оборони України
03049, м. Київ, Повітрофлотський пр-т, 28