ISSN 2304-2699

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

№ 2(72), 2021

УДК 355:623 (08)

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

Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ, 2021. № 2 (72).

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

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

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

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

Рекомендовано до друку рішенням Вченої ради НУО України імені Івана Черняховського (протокол № 10 від 30.08.2021)

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

CONTENT

ЗМІСТ

УДК 355.42 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/6-15

Загорка О. М., д-р військ. наук, професор (0000-0003-1131-0904)
Загорка І. О. (0000-0002-0693-1434)
Фучко А. Й. (0000-0002-8941-2217)

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

Методичний підхід до оцінювання спроможностей міжвидового угруповання військ під час планування реформування (розвитку) Збройних Сил України

Резюме. У статті наведений методичний підхід до оцінювання спроможностей угруповання військ, які пропонується характеризувати показниками ефективності бойових дій.

Ключові слова: оборонне планування; системний підхід; угруповання військ; спроможності; показники ефективності бойових дій.

Постановка проблеми. Реформування Збройних Сил (ЗС) України, яке відбувається на сучасному етапі їх розвитку, здійснюється з метою забезпечення можливості створення в особливий період угруповання військ, здатного виконувати завдання щодо відбиття агресії противника. Для визначення напрямів розвитку ЗС, термінів виконання завдань реформування і потрібних ресурсів у Міністерстві оборони України та ЗС впроваджується оборонне планування на основі спроможностей (ОПОС).

Відповідно до мети реформування (розвитку) ЗС спроможності, які необхідно враховувати під час оборонного планування, мають характеризувати здатність угруповання військ виконувати завдання за призначенням, тобто під час оборонного планування необхідно враховувати спроможності угруповання військ. Необхідність їх оцінювання під час оборонного планування потребує розроблення відповідного методичного підходу.

Аналіз останніх досліджень і публікацій. Поняття "спроможність (оперативна, бойова, спеціальна)", під якою розуміють здатність органів військового управління, з'єднань, військових частин, військових навчальних закладів, установ та організацій ЗС або сукупності сил і засобів сил оборони виконувати певні завдання (забезпечити реалізацію визначених військових цілей) за певних умов, ресурсного забезпечення та відповідно до встановлених стандартів, наведено у Єдиному переліку (каталозі) спроможностей Міністерства оборони України, Збройних Сил України та інших складових сил оборони [1]. У Каталозі наведені загальні вимоги до спроможностей. Каталог містить 8 функціональних груп, зокрема функціональну групу № 5 "Застосування", яка охоплює перелік спроможностей військових частин і підрозділів з виконання основних завдань за призначенням як самостійно, так і у складі міжвидових угруповань.

На сьогодні у фахових наукових виданнях за воєнною тематикою опубліковано багато праць, у яких розглядаються питання ОПОС.

Оборонне планування у ЗС України здійснюється з урахуванням досвіду оборонного планування в арміях держав – членів НАТО. Для організації ОПОС у державах – членах Альянсу прийнята модель, яка ґрунтується на таких ключових поняттях, як стратегія, кінцеві цілі, сили та засоби, ризики, середовище безпеки та обмеженість ресурсів [2]. Модель ОПОС розглядається як сукупність взаємозалежних процесів і процедур з оцінювання воєнно-політичної обстановки, планування сил, планування ресурсів та оцінювання ризиків. У праці [2] наведені етапи процесу ОПОС, одним з яких є визначення необхідних спроможностей для досягнення цілей застосування ЗС. Однак підходи до оцінювання спроможностей не розглянуті. Зміст етапів процесу ОПОС також розглянуто у праці [3]. Під час визначення спроможностей (другий етап) передбачається їх оцінювання, що тільки констатується. Це можна пояснити тим, що задача оцінювання спроможностей військ (сил) не ставилась.

У праці [4] відзначається, що зміст процесу оборонного планування НАТО полягає у визначенні кількісних і якісних параметрів військових спроможностей, необхідних для проведення усіх можливих

операцій кризового реагування, а також забезпечення своєчасного і повного виділення державами – членами НАТО ресурсів для формування відповідних військових можливостей Альянсу. Для визначення потреб у процесі планування використовуються інформаційно-аналітичні методики, сутність яких у статті не розкривається, та експертні методи оцінювання.

У праці [5] розглянута організаційна структура системи оцінювання та розвитку спроможностей сил оборони, у складі якої пропонується мати робочі групи з оцінювання спроможностей. Однак підрозділів для створення методичного апарату з оцінювання спроможностей у структурі не передбачено.

Відповідно до рекомендацій [6] критерієм вибору оптимального варіанта перспективного складу ЗС під час оборонного планування є співвідношення ефективності виконання завдань до вартості досягнення необхідних спроможностей. Водночас підходи до оцінювання ефективності виконання завдань з урахуванням спроможностей складових ЗС не розглянуті. У рекомендаціях основна увага приділена визначенню експертним шляхом рейтингу спроможностей, що доцільно використати під час розроблення методичного підходу до оцінювання спроможностей угруповання військ для обґрунтування потрібного бойового складу угруповання військ.

Методика визначення, так званих, групових носіїв спроможностей, зокрема угруповань військ, за функціональною групою спроможностей “Застосування” запропонована у статті [7]. Оцінювати інтегральну спроможність групового носія пропонується шляхом добутку декількох коефіцієнтів (семи), які визначаються відповідно до функціональних груп спроможностей, що приведені у Каталозі [1]. Основною складовою інтегральної спроможності групового носія спроможностей є коефіцієнт, який характеризує його застосування за призначенням (функціональна група “Застосування”), тому у методиці для протидіючих сторін оцінюються потенційні спроможності щодо нанесення ураження противнику. В іншому разі під час визначення основної складової інтегральних спроможностей пропонується використовувати вогневі спроможності угруповання військ, що обумовлює неоднозначність підходу до оцінювання його спроможностей. Крім того, використання вогневих спроможностей не дає змоги визначити спроможності міжвидового угруповання військ. Методичні підходи до визначення решти складових інтегральної спроможності групового носія спроможностей у статті не розглянуті.

З аналізу наведених праць випливає необхідність розроблення для використання під час проведення ОПОС методичного підходу до оцінювання спроможностей міжвидового угруповання військ, що і є **метою** статті.

Виклад основного матеріалу. Відповідно до рекомендацій з оборонного планування [6] визначення раціонального складу міжвидового угруповання військ має здійснюватися за допомогою порівняльного оцінювання спроможностей варіантів його кількісно-якісного складу на підставі використання єдиних для родів військ видів ЗС показників ефективності. Оцінювання спроможностей варіантів угруповання військ доцільно здійснювати на підставі застосування системного підходу, який передбачає розгляд угруповання військ у цілому, як складної військової системи організаційно-технічного типу, та його окремих складових частин [8], які також уважаються складними системами. До того ж потрібно враховувати принцип дуалізму [9], тобто угруповання розглядаються як війська (матеріальний об’єкт) і розглядаються форми та способи їх дій (процес). Принцип дуалізму застосований у працях [10, 11] для визначення способу бойових дій і складу угруповання військ (сил).

Відповідно до системного підходу необхідність урахування під час оцінювання спроможностей угруповання військ багаточисельних спроможностей функціональних груп, наведених у Каталозі [1], передбачає декомпозицію (членування) угруповання військ на окремі системи відповідно до цих спроможностей (рис. 1). Наведена структура є морфологічним зрізом складної системи (угруповання військ) за функціональною ознакою, тобто відповідно до завдань, які мають вирішуватися окремими системами [12]. Основною за призначенням є система ураження військ і об’єктів противника, вона характеризується всіма функціональними групами спроможностей. Систему ураження військ і об’єктів утворюють з’єднання, частини і підрозділи родів військ видів ЗС, які безпосередньо виконують завдання щодо знищення угруповання військ противника. Особливість оцінювання спроможностей угруповання

військ полягає в необхідності врахування впливу спроможностей решти систем на виконання завдань основною системою.

Є очевидним, що досягнення кінцевої мети операції (бойових дій) угрупованням військ переважно здійснюється завдяки завданню противнику комплексного ураження (вогневого, радіоелектронного, спеціальними засобами тощо) [9]. Отже, основною характеристикою, яка визначає здатність угруповання військ виконувати бойові завдання в операції (під час ведення бойових дій), є спроможність ураження противника, тобто завдання збитку (втрат) його військам і об'єктам. Це аксіоматичне положення за сутністю приводить до висновку, що, не зважаючи на різнорідність складу сил ураження, завдань, які виконуються ними, форм і способів дій військ, єдиним показником ефективності, який найбільш повно і об'єктивно характеризує їх кількісно-якісний стан, є їх бойові можливості, які оцінюються математичним сподіванням збитку (втрат), що завдається противнику під час виконання бойового завдання (завдань) [9]. Звідси випливає, що спроможність угруповання військ потрібно оцінювати з використанням єдиного для всіх сил ураження основного показника ефективності, який характеризує його здатність щодо завдання збитку (втрат) противнику, а не відверненого збитку, методичні положення визначення якого наведені у монографії [13]. Це відповідає рекомендаціям з оборонного планування [6], у яких приводиться критерій вибору варіанта перспективного складу ЗС на підставі врахування ефективності виконання завдань.

Показник відверненого збитку (втрат своїх військ) доцільно ураховувати під час визначення бойового складу угруповання військ як обмеження або число показників під час використання для розв'язання цієї задачі методів багатокритеріального аналізу, як це наведено у праці [10].

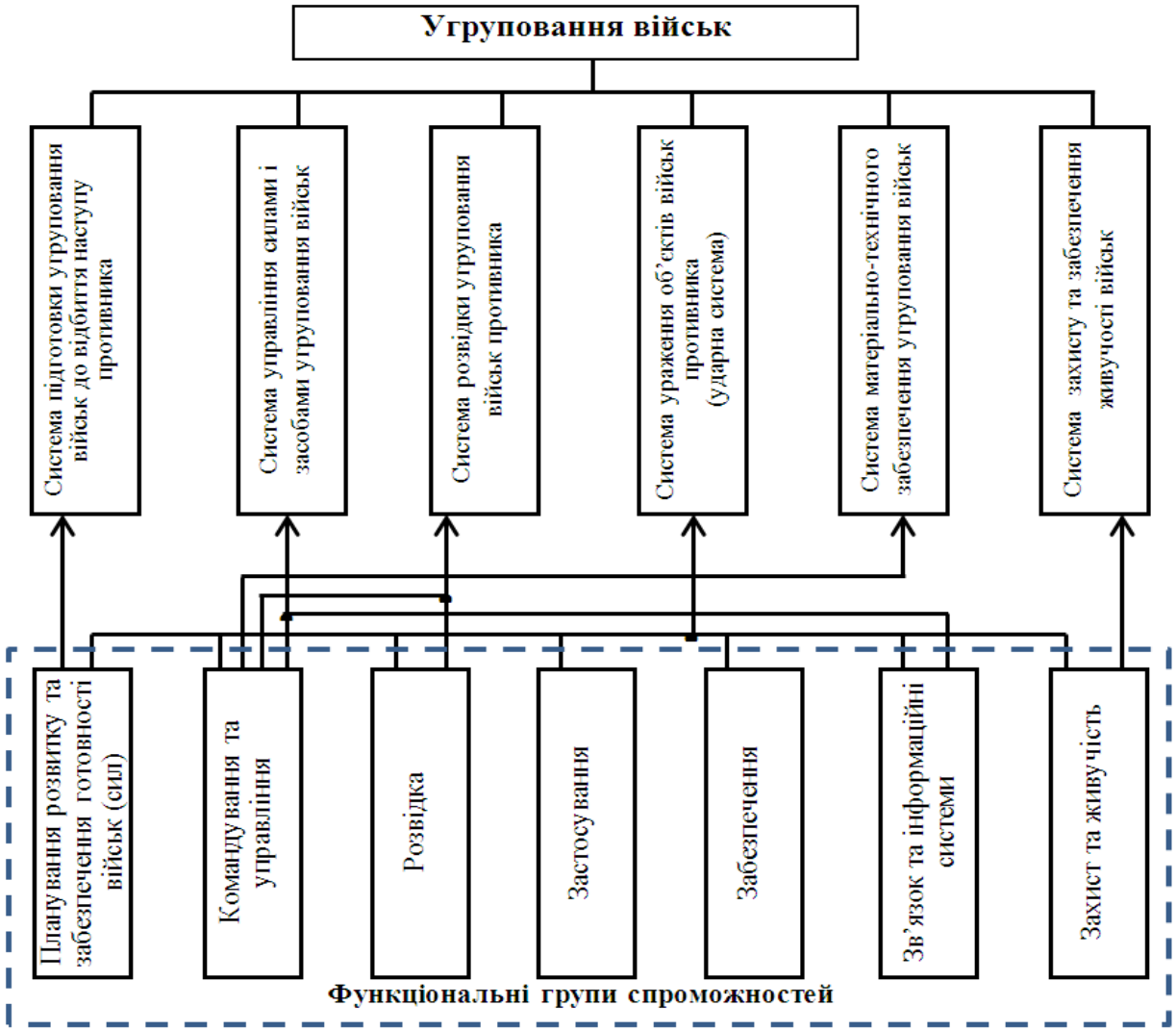


Рис. 1. Декомпозиція угруповання військ на окремі системи відповідно до функціональних груп спроможностей (варіант)

Під час оцінювання спроможностей угруповання військ визначається здатність ним виконання завдань шляхом порівняння ефективності, яка може бути реалізована в операції (під час ведення бойових дій), із заданою (потрібною), тобто практично отримується відповідь на питання: здатне або ні угруповання військ виконати поставлене завдання. Під час визначення заданої (потрібної) ефективності угруповання військ можуть розглядатися так звані критичні втрати. Так, у праці [14] відзначається, що сторона, яка наступає, відмовлялась від активних дій при втратах 30-50 %. Сторона, що обороняється, втрачала стійкість оборони при втратах 50-70 %.

Під час оборонного планування реформування (розвитку) ЗС розглядається декілька сценаріїв бойових дій [6]. Для кожного сценарію визначається і розглядається декілька варіантів складу угруповання військ. Оцінювання спроможностей угруповання військ, які можуть бути реалізовані в операції (під час ведення бойових дій), здійснюється для кожного варіанта складу угруповання військ у кожному сценарії бойових дій (рис. 2).

На підставі порівняння спроможностей, які можуть бути реалізовані в сценарії бойових дій, і спроможностей, що задані (потрібні), визначається варіант складу угруповання військ, який може розглядатися під час вибору раціонального варіанта складу, зокрема з використанням методів багатокритеріального аналізу.

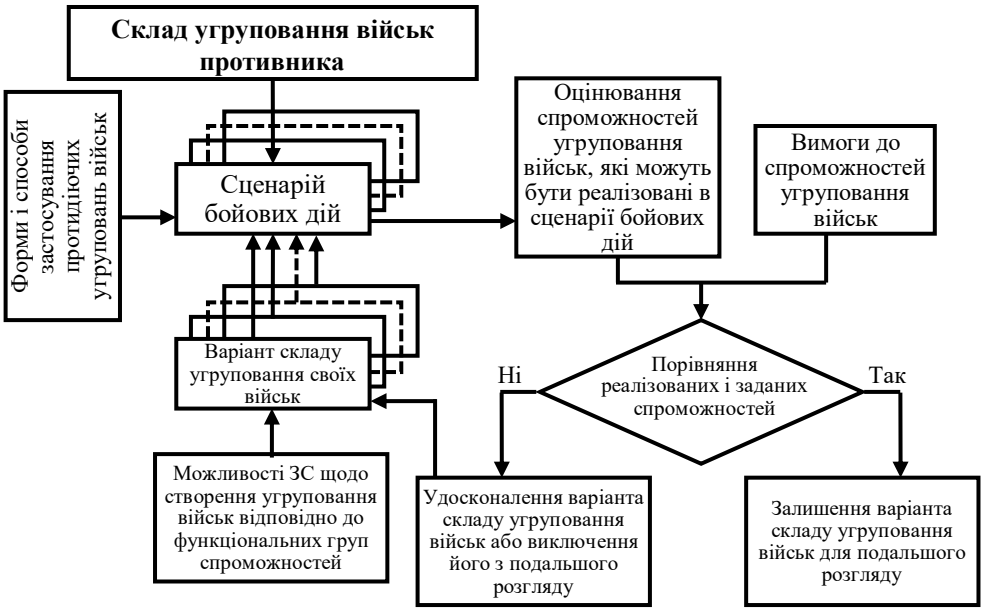


Рис. 2. Загальна схема визначення варіанта складу угруповання військ під час оборонного планування

Розроблення методичного підходу до оцінювання спроможностей міжвидового угруповання військ під час оборонного планування включає:

визначення показників для оцінювання спроможностей угруповання військ;

створення моделі бойових дій угруповань своїх військ і противника;

обґрунтування способів урахування функціональних груп спроможностей під час оцінювання спроможностей угруповання військ;

обґрунтування підходів до оцінювання показників, що характеризують спроможності угруповання військ.

Під час оцінювання спроможностей угруповання військ, крім основного показника, який характеризує здатність завдавати противнику збитку, доцільно використовувати показники, які характеризують здатність зберігати власні спроможності.

Отже, для оцінювання спроможностей угруповання військ, як варіант, можна пропонувати використовувати такі показники:

математичне сподівання величини відносних втрат, які можуть завдаватися військам противника нашим угрупованням військ;

математичне сподівання величини відносних втрат, що можуть завдаватися противником нашому угрупованню військ;

внески родів військ видів ЗС угруповання наших військ до загальних втрат, які можуть завдаватися противнику;

частки втрат, які можуть завдаватися противником родам військ видів ЗС угруповання наших військ.

Для визначення наведених показників відповідно до варіантів складу угруповання військ можуть використовуватися методи моделювання двосторонніх бойових дій і аналітичні методики.

Під час оборонного планування також оцінюється вартість угруповання військ у цілому і його складових (звичайно розраховується за вартістю озброєння і військової техніки).

Результати оцінювання спроможностей, які характеризуються сукупністю показників ефективності, та показників вартості дають змогу застосувати методи багатокритеріального аналізу, зокрема таксономії [11, 15] для вибору із безлічі варіантів (див. рис. 2) збалансованого варіанта складу угруповання військ.

Модель бойових дій містить сценарії, у яких відображається характер застосування угруповань військ протидіючих сторін у майбутній війні (збройному конфлікті). Сценарії мають ураховувати всі об'єкти ураження угруповань своїх військ і противника, всі засоби ураження родів військ видів ЗС, прогнозовані форми застосування військ і способи ведення ними бойових дій. У кожному сценарії (див. рис. 2) розглядається застосування угруповань наших військ, які мають різні варіанти бойового складу сил і засобів. Це дає змогу обрати раціональний варіант складу угруповання військ під час оборонного планування.

Сценарії мають містити характерні етапи застосування родів військ видів ЗС в операції (під час ведення бойових дій), що дає змогу обґрунтовано оцінювати спроможності угруповання військ.

Модель бойових дій містить оперативно-тактичні вихідні дані для визначення раціонального складу угруповання військ під час оборонного планування, зокрема для оцінювання його спроможностей за варіантами складу у кожному сценарії.

Способи врахування вимог функціональних груп спроможностей під час оцінювання спроможностей угруповання військ визначаються на підставі таких положень:

ефективність функціонування системи ураження військ і об'єктів противника залежить від функціонування решти систем угруповання військ (див. рис. 1);

кожна система угруповання військ функціонує (виконує завдання) відповідно до функціональних груп спроможностей, як наведено на рис. 1;

вплив вимог функціональних груп спроможностей на функціонування системи ураження військ і об'єктів противника виявляється через функціонування решти систем угруповання військ.

Відповідно до наведених положень спосіб урахування спроможностей функціональних груп під час оцінювання спроможностей угруповання військ полягає у визначенні часткових показників ефективності функціонування систем, крім основної, з урахуванням вимог до спроможностей і використанні їх чисельних значень під час оцінювання ефективності ураження військ і об'єктів противника. Для оцінювання часткових показників використовуються окремі методики. Такі методики потрібно створювати для видів ЗС і родів військ. Прикладом є методика оцінювання ефективності функціонування системи радіолокаційної розвідки повітряного противника [16], яка дає змогу врахувати вимоги функціональної групи спроможностей "Розвідка" під час застосування Повітряних Сил.

Іншим способом є врахування вимог до спроможностей функціональних груп у сценаріях бойових дій. Наприклад, вимоги до спроможностей до функціональної групи спроможностей "Командування та управління" можуть ураховуватися під час визначення етапів бойових дій, способів застосування військ, порядку ураження військ і об'єктів противника силами і засобами родів військ видів ЗС тощо.

Вимоги до спроможностей функціональних груп також можуть безпосередньо враховуватися у методиці оцінювання ефективності функціонування основної системи угруповання військ (системи ураження військ і об'єктів противника), тобто під час оцінювання показників, які характеризують спроможності угруповання військ.

Під час оцінювання показників, які характеризують спроможності угруповання військ, доцільно використовувати послідовне моделювання бойових дій [17]. Сутність послідовного моделювання бойових дій полягає в організації такої взаємодії (послідовності застосування) часткових моделей, методик, коли вихідні дані одних моделей або методик використовуються як

вхідні дані інших моделей, методик. Отже оцінювання показників здійснюється за етапами, які визначаються сценаріями бойових дій. Етапи доцільно визначати для повітряної і наземної фази ведення бойових дій.

Повітряна фаза має включати етапи завдання протидіючими сторонами ракетно-авіаційних ударів (РАУ) та їх відбиття силами ППО. У наземній фазі ведення бойових дій доцільно передбачити етапи застосування ракетних військ і артилерії, завдання авіацією зосереджених ударів по військах і об'єктах, відбиття ударів авіації силами ППО, бойових дій за оволодіння заданих рубежів і бойових дій за їх утримання тощо.

Застосування послідовного моделювання дає змогу використати відомі вже випробувані моделі та методики оцінювання ефективності бойових дій з'єднань, частин і підрозділів родів військ видів ЗС.

Порядок оцінювання показників ефективності застосування міжвидового угруповання військ в операції (під час ведення бойових дій) наведено на рис. 3.

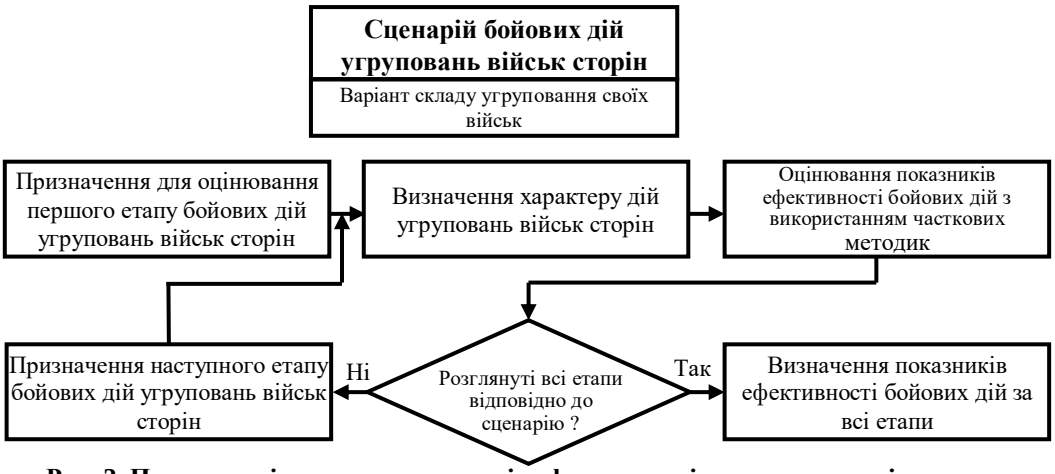


Рис. 3. Порядок оцінювання показників ефективності застосування міжвидового угруповання військ в операції (під час ведення бойових дій)

У часткових методиках вихідними даними для оцінювання ефективності бойових дій є об'єкти ураження, їх характеристика, можливості щодо ураження об'єктів різними засобами родів військ видів ЗС.

Можливі об'єкти ураження евентуального противника в операції (під час ведення бойових дій) вивчаються ще у мирний час, створюються їх каталоги з описанням характеристик. Необхідно також прогнозувати ураження об'єктів угруповання наших військ.

Під час повітряної фази бойових дій здійснюється обмін РАУ між сторонами. Для оцінювання показників, що характеризують втрати (збиток) угруповання військ від РАУ, може бути застосована аналітична методика [18], яка ґрунтується на використанні полігонних нарядів ракет і літаків для ураження об'єктів. У методиці, враховуючи наявність балістичних ракет і літаків в угрупованні військ, з використанням методу ітерації визначається кількість об'єктів за типами, по яких можуть завдаватися удари балістичними ракетами і літаками $m_{iБР}, m_{iлім}, i=\overline{1,N}$ (N – кількість типів об'єктів).

Математичні сподівання кількості об'єктів i-го типу, які можуть уражатися балістичними ракетами і літаками у разі завдання РАУ

$$M_{iБР}=m_{iБР}P_{БР},\ M_{iлім}=m_{iлім}P_{лім}, \qquad (1)$$

де $P_{БР}$, $P_{лім}$ – імовірність ураження об'єкта, що задається під час визначення полігонного наряду балістичних ракет і літаків відповідно.

Математичне сподівання величини відносних втрат угруповання військ, по якому завдається РАУ $Z_{вт}$ і внески балістичних ракет $\delta_{БР}$ та літаків авіації $\delta_{лім}$ у завдання втрат визначаються за формулами:

$$Z_{вт}=\frac{\sum\limits_i B_i\, Б_i\, M_{i\,БР}+\sum\limits_i B_i\, Б_i\, M_{i\,літ}}{\sum\limits_i B_i\, Б_i\, n_i};$$

$$\delta_{БР}=\frac{\sum\limits_i B_i\, Б_i\, M_{i\,БР}}{\sum\limits_i B_i\, Б_i\, M_{i\,БР}+\sum\limits_i B_i\, Б_i\, M_{i\,літ}};\ \delta_{літ}=\frac{\sum\limits_i B_i\, Б_i\, M_{i\,літ}}{\sum\limits_i B_i\, Б_i\, M_{i\,БР}+\sum\limits_i B_i\, Б_i\, M_{i\,БР}}, \quad (2)$$

де B_i – важливість об'єктів *i*-го типу;

n_i – кількість об'єктів ураження *i*-го типу в угрупованні військ;

$Б_i$ – бойовий потенціал об'єктів *i*-го типу.

Частка втрат, яка може завдаватися *к*-му роду військ виду ЗС в РАУ, визначається таким чином:

$$\omega_к=\frac{\sum\limits_i B_i\, Б_i\, m_{iк\,БР}\cdot P_{БР}+\sum\limits_i B_i\, Б_i\, m_{iк\,літ}\cdot P_{літ}}{\sum\limits_i B_i\, Б_i\, n_{iк}};\ к=\overline{1,K}, \quad (3)$$

де $m_{iк\,БР}$, $m_{iк\,літ}$ – кількість об'єктів *i*-го типу *к*-го рода військ видів ЗС, по яких можуть завдаватися удари балістичними ракетами, літаками відповідно;

$n_{iк}$ – кількість об'єктів *i*-го типу *к*-го рода військ видів ЗС в угрупованні військ;

K – кількість родів військ видів ЗС в угрупованні військ.

Коефіцієнти важливості об'єктів ураження *i*-х типів $B_i\left(i=\overline{1,N}\right)$ визначаються з використанням експертних методів, зокрема методу ранжирування [19]. Важливість типу об'єктів ураження експертами визначається з урахуванням їх можливостей завдання втрат (збитку) протидіючому угрупованню військ.

Експерт має розташувати типи об'єктів у порядку їх важливості (значущості) і приписати кожному типу об'єктів числа натурального ряду (ранг): $1,2,...N$. Після надання *j*-м експертом рангів типам об'єктів $r_{ij}\left(i=\overline{1,N},\ j=\overline{1,R}\right)$ розраховуються коефіцієнти, які характеризують вплив об'єктів *i*-го типу на завдання втрат (збитку) протидіючому угрупованню військ за формулою [20]

$$c_{ij}=1-\frac{r_{ij}-1}{N};\ i=\overline{1,N};\ j=\overline{1,R}, \quad (4)$$

де *R* – кількість експертів.

Далі значення коефіцієнтів C_{ij} нормуються

$$в_{ij}=\frac{C_{ij}}{\sum\limits_i C_{ij}};\ \sum_i в_{ij}=1. \quad (5)$$

Коли компетентність експертів однакова, коефіцієнт важливості

$$B_i=\frac{1}{R}\sum_j b_{ij},\ j=\overline{1,R}. \quad (6)$$

Коли компетентність *j*-го експерта оцінюється певним коефіцієнтом q_j, $\sum\limits_j q_j=1,\ j=\overline{1,R}$, то $B_i=\sum\limits_j q_j\cdot в_{ij}$. (7)

Для оцінювання показників, які характеризують ефективність бойових дій зенітних ракетних військ і винищувальної авіації щодо відбиття РАУ, можна використати методики, які наведені у працях [16, 21, 22]. Методики дають змогу визначати математичні сподівання кількості знищених засобів повітряного нападу (літаків ударної авіації) зі складу удару зенітними ракетними комплексами $m_{ЗРК}$ та винищувальною авіацією $m_{ВА}$, математичні сподівання кількості уражених зенітних ракетних комплексів $n_{ЗРК}$ та винищувачів $n_{ВА}$. Літаки ударної авіації, зенітні ракетні комплекси вважаються об'єктами ураження. Важливість (значущість) літака визначається коефіцієнтом $B_{літ}$. Математичне сподівання величини відносних втрат угруповання військ, яке завдає РАУ, від дій сил ППО з урахуванням (2) визначається за формулою

$$Z^*_{вт}=\frac{\left(m_{ЗРК}+m_{ВА}\right)Б_{літ}B_{літ}}{\sum\limits_i B_i\, Б_i\, n^*_i},i=\overline{1,N}, \quad (8)$$

де $Б_{літ}$ – бойовий потенціал літака;

n^*_i – кількість об'єктів *i*-го типу у складі угруповання військ, що завдає РАУ.

Внески зенітних ракетних військ і винищувальної авіації у завдання втрат складають

$$\delta_{ЗРВ} = \frac{m_{ЗРК}}{(m_{ЗРК} + m_{ВА})}\,;\ \delta_{ВА} = \frac{m_{ВА}}{(m_{ЗРК} + m_{ВА})}. \quad (9)$$

Частки втрат, які можуть завдаватися зенітним ракетним військам і винищувальної авіації угрупування військ, по якому завдається РАУ, визначаються за формулами:

$$\omega_{ЗРВ} = \frac{n_{ЗРК}}{N_{ЗРК}}\,;\ \omega_{ВА} = \frac{n_{ВА}}{N_{ВА}}, \quad (10)$$

де $N_{ЗРК}$, $N_{ВА}$ – кількість зенітних ракетних комплексів, винищувачів у складі угруповання військ, по якому завдається РАУ.

Для оцінювання втрат загальновійськових формувань в операції (бою) може використовуватися методика, яка наведена у працях [14, 23]. Методика дає змогу визначати прогнозовані втрати сил однієї зі сторін в операції (бою) при заданих втратах сил іншої сторони з урахуванням початкового співвідношення сил сторін, яке визначається з використанням бойових потенціалів озброєння. Методика базується на використані квадратичного закону Ланчестера.

Значення відносних втрат сторони, що наступає α_1, і сторони, що обороняється α_2, визначається за формулами:

$$\alpha_1 = 1 - \sqrt{1 - \frac{\alpha_2(2-\alpha_2)}{C_1^2}}\,;$$
$$\alpha_2 = 1 - \sqrt{1 - C_1^2\,\alpha_1(2-\alpha_1)}, \quad (11)$$

де C_1 – початкове співвідношення сил протидіючих сторін.

Кількість уражених об'єктів i-го типу угруповання військ, що наступає $m_i^{н}$, і угруповання військ, що обороняється $m_i^{об}$, в операції (бою)

$$m_i^{н} = n_i^{н}\,\alpha_1\,;$$
$$m_i^{об} = n_i^{об}\,\alpha_2\,, \quad (12)$$

де $n_i^{н}$, $n_i^{об}$ - кількість об'єктів i-го типу в угрупованні військ, що наступає і обороняється, які беруть участь в операції (бою).

Відносні втрати угруповання військ, що наступає, визначаються за формулою

$$Z_{вт}^{н} = \frac{\sum_i B_i\,Б_i\,m_i^{H}}{\sum_i B_i\,Б_i\,n_i^{H*}}, \quad (13)$$

де $n_i^{н*}$ – кількість об'єктів i-го типу всіх родів військ видів ЗС у складі угруповання військ, що наступає.

Відносні втрати угруповання військ, що обороняється

$$Z_{вт}^{об} = \frac{\sum_i B_i\,Б_i\,m_i^{об}}{\sum_i B_i\,Б_i\,n_i^{об*}}, \quad (14)$$

де $n_i^{об*}$ – кількість об'єктів i-го типу всіх родів військ видів ЗС у складі угруповання військ, що обороняється.

Внески родів військ видів ЗС угруповання військ, що наступає, і угруповання військ, що обороняється, визначаються за формулами:

$$\delta_к^{H} = \frac{\sum_i B_i\,Б_i\,m_{iк}^{об}}{\sum_i B_i\,Б_i\,m_i^{об}}\,;\ \delta_к^{об} = \frac{\sum_i B_i\,Б_i\,m_{iк}^{H}}{\sum_i B_i\,Б_i\,m_i^{H}}, \quad (15)$$

де $m_{iк}^{н}$, $m_{iк}^{об}$ – кількість уражених об'єктів i-го типу $к$-го роду військ.

Частки втрат, які можуть завдаватися родам військ протидіючих угруповань військ:

$$\omega_к^{H} = \frac{\sum_i B_i\,Б_i\,m_{iк}^{H}}{\sum_i B_i\,Б_i\,n_{iк}^{H}}\,;\ \omega_к^{об} = \frac{\sum_i B_i\,Б_i\,m_{iк}^{об}}{\sum_i B_i\,Б_i\,n_{iк}^{об}}, \quad (16)$$

де $n_{iк}^{н}$, $n_{iк}^{об}$ – кількість об'єктів i-го типу $к$-го роду військ у складі угруповань військ.

Показники ефективності бойових дій угруповання військ в операції визначаються за допомогою підсумовування (узагальнення) втрат, які оцінюються з використанням наведених методик за етапами бойових дій відповідно до сценарію, що розглядається.

Відповідно до загального визначення [1] під спроможностями угруповання військ пропонується розуміти його здатність виконувати завдання щодо відбиття нападу евентуального противника у воєнному конфлікті. Іншими словами – це здатність забезпечити в операції (під час ведення бойових дій) завдання військам евентуального противника неприйнятного збитку при допустимих втратах своїх військ. На підставі спроможностей під час оборонного планування реформування (розвитку) ЗС має здійснюватися обґрунтування потрібного складу угруповання військ для відбиття нападу евентуального противника.

Висновки

1. Відповідно до системного підходу під час оцінювання спроможностей угруповання

військ здійснюється його декомпозиція на окремі системи, функціонування яких визначається функціональними групами спроможностей. Основною вважається система ураження військ і об'єктів противника, ефективність функціонування якої визначає спроможність угруповання військ у досягненні мети операції (бойових дій). Функціонування решти систем здійснюється в інтересах застосування системи ураження військ і об'єктів противника.

2. За основний показник, який характеризує спроможності можливого угруповання військ, прийнятий єдиний для видів ЗС і родів військ показник ефективності бойових дій – математичне сподівання величини відносних втрат, що можуть завдаватися в операції (під час ведення бойових дій) військам противника нашим угрупованням військ. До інших показників, що характеризують спроможності угруповання військ, належать: математичне сподівання величини відносних втрат, що можуть завдаватися противником нашому угрупованню військ; внески родів військ видів ЗС угруповання наших військ до загальних втрат, які можуть завдаватися противнику; частки втрат, які можуть завдаватися противником родам військ видів ЗС угруповання наших військ.

3. Показники ефективності бойових дій, які характеризують спроможності угрупування військ, оцінюються за сценаріями для різних варіантів його складу, що дає змогу використати під час оборонного планування методи багатокритеріального аналізу, зокрема таксономії, для обґрунтування раціонального (збалансованого) складу угруповання військ. Для оцінювання показників ефективності бойових дій рекомендовано використовувати відомі методики, які дають змогу визначати втрати угруповань військ сторін в операції (під час ведення бойових дій) за етапами сценарію. Ефективність функціонування систем угруповання військ, крім основної, оцінюється частковими показниками, які є вихідними даними для оцінювання ефективності бойових дій угруповання військ.

4. Результати оцінювання спроможностей угруповання військ мають використовуватися під час оборонного планування для обґрунтування потрібного складу угруповання військ, яке передбачається створювати для відбиття нападу можливого противника. Надалі доцільно, використовуючи наведений підхід, розробити методику оцінювання спроможностей угруповання військ для застосування її під час планування реформування (розвитку) ЗС.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Єдиний перелік (каталог) спроможностей Міністерства оборони України, Збройних Сил України. Київ : Міністерство оборони України, 2019. 618 с.
2. Фролов В. С., Саганюк Ф. В., Мудрак Ю. М., Пушняков А. С. Досвід оборонного планування в НАТО, заснованого на спроможності військ (сил). *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2020. № 1 (68). С. 40–43.
3. 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.
4. Слюсар В. І., Кулагін К. К. Особливості процесу оборонного планування НАТО. *Наука і техніка Повітряних Сил Збройних Сил України*. Харків, 2019. № 3 (36). С. 47–59.
5. Павліковський А. К., Наливайко А. Д., Поляєв А. І. Обґрунтування пропозицій щодо впровадження системи оцінювання та розвитку спроможностей складових сил оборони: організаційний аспект. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2020. № 1 (68). С. 35–39.
6. Рекомендації з оборонного планування на основі спроможностей в Міністерстві оборони України та Збройних Силах України : затв. Міністром оборони України 12.06.2017 р.
7. Биченков В. В., Корецький А. А., Оксіюк О. Г., Вялкова В. І. Оцінювання спроможностей угруповань військ (сил) за функціональною групою застосування. *Східно-Європейський журнал передових технологій*. Харків, 2018. Т. 5, № 3 (95). С. 1–28.
8. Основы теории и методологии планирования строительства Вооруженных Сил Российской Федерации: военно-теоретический труд / под общ. ред. А. В. Квашнина. Москва : Воентехиздат, 2002. 232 с.
9. Бобриков А. А. Методика оценки боевых возможностей группировок войск в целях обоснования решений по строительству и применению ВС. *Военная мысль*. 2009. № 12. С.14–22.
10. Можаровський В. М., Загорка О. М. Основні положення методики визначення варіанта (способу) бойових дій та складу угруповання військ (сил) для відбиття агресії. *Наука і оборона*. 2011. № 1. С. 3–6.
11. Теоретичні основи управління угрупованням військ (сил) у сучасних умовах збройної боротьби : монографія / О. М. Загорка,

А. К. Півліковський, А. А. Корецький, С. О. Кириченко, І. О. Загорка ; за заг. ред. Руснака І. С. Київ : НУОУ ім. Івана Черняховського, 2020. 248 с.
12. Загорка О. М., Мосов С. П., Сбитнєв С. П., Стужук П. І. Елементи дослідження складних систем військового призначення. Київ : НАОУ, 2005. 100 с.
13. Теорія відверненого збитку : монографія / І. С. Романченко, В. О. Шуєнкін, В. М. Можаровський. Львів : НАСВ ЗС України, 2017. 244 с.
14. Элементы военной системологии применительно к решению проблем оперативного искусства и тактики общевойсковых объединений, соединений и частей : военно-теоретический труд / под ред. академика В. Д. Рябчука. Москва : Военная академия им. М. В. Фрунзе, 1995. 228 с.
15. Плюта В. Сравнительный многомерный анализ в экономических исследованиях: методы таксономии и факторного анализа / пер. с польск. В. В. Иванова ; науч. ред. В. М. Жуковский. Москва : Статистика, 1980. 151 с.
16. Теорія і практика боротьби з малорозмірними низьколітними цілями (оцінка можливостей, тенденції розвитку засобів протиповітряної оборони) : монографія / І. С. Романченко та ін. Житомир : Полісся, 2011. 344 с.
17. Основи моделювання бойових дій військ : підручник / за заг. ред. О. Ю. Пермякова. Київ : НАОУ, 2005. 483 с.
18. Онищенко С. І., Загорка О. М., Коваль В. В., Тюрін В. В. Прогнозування втрат військ і об'єктів від авіаційних ударів противника. *Системи озброєння і військова техніка*. Харків, 2011. № 2 (26). С. 2–8.
19. Бешелев С. Д., Гурвич Ф. Г. Математико-статистические методы экспертных оценок. Москва : Статистика, 1974. 160 с.
20. Денисов А. А., Колесников Д. Н. Теория больших систем управления : учебн. пособие для вузов. Ленинград : Энергоиздат, 1982. 288 с.
21. Городнов В. П. Методики прогноза эффективности группировок родов войск ПВО. Харьков : ХВУ, 1999. 32 с.
22. Городнов В. П., Дробаха Г. А., Єрмошин М. О., Смірнов Є. Б., Ткаченко В. Т. Моделювання бойових дій військ (сил) протиповітряної оборони та інформаційне забезпечення процесів управління ними (теорія, практика, історія розвитку : монографія. Харків : ХВУ, 2004. 410 с.
23. Загорка О. М., Поліщук С. В., Загорка І. О. Методичні положення прогнозування втрат сил протидіючих сторін у загальновійськовій операції (бою). *Наука і оборона*. 2020. № 1. С. 52–57.

Стаття надійшла до редакційної колегії 17.05.2021

Methodical approach to assessing the capabilities of an interspecific group of forces during the planning of reform (development) of the Armed Forces of Ukraine

Annotation

The main purpose of reforming (developing) the Armed Forces is to ensure the creation of a group of forces capable of carrying out tasks to repel an enemy attack. Given the experience of defense planning in NATO member countries, the ability of a group of forces is to perform tasks based on their capabilities, which in defense planning must be assessed according to combat scenarios for different options for the composition of the group of forces. The experience of such countries was borrowed for building defense planning based on capabilities of the Ukrainian Armed Forces.

In assessing the capabilities of a group of forces, a systematic approach is used, which provides for the decomposition of a group of forces into separate systems in accordance with the functional groups of capabilities adopted in the Armed Forces. The main system is considered to be the defeat of enemy forces and objects, other systems (training of forces, intelligence, management, etc.) perform tasks to ensure the functioning of the main system.

The capabilities of the interspecific grouping of forces are proposed to be characterized by the only indicators of the effectiveness of hostilities for the types of Armed Forces and military units, namely indicators characterizing the losses of groups of forces, types of Armed Forces and military units in operations (during hostilities). Estimation of losses of groups of forces is carried out on stages of scenarios of hostilities. For this purpose, methods of assessing the effectiveness of combat operations of units and subdivisions of the Armed Forces are used.

During the determining of the losses of opposing groups of forces, the combat potential of the targets and their importance are taken into account. Indicators of the effectiveness of combat operations of groups of forces per operation (combat operations) are determined by summing up the losses, which are estimated by the stages of the scenarios.

The methodical approach expediently to use in developing a methodology for assessing the capabilities of groups of forces in defense planning.

Keywords: defense planning; system approach; grouping of forces; opportunities; indicators of combat effectiveness.

УДК 327.5: 519.7 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/16-24

Биченков В. В., д-р техн. наук, ст. наук. співроб. (0000-0002-6080-6976)
Павліковський А. К., канд. військ. наук, доцент (0000-0002-0637-368X)
Левчук О. В., канд. екон. наук, доцент (0000-0002-2827-2134)
Бутенко М. П. (0000-0001-7272-5826)

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

Методика визначення сценаріїв розвитку держави на довгострокову перспективу

Резюме. Удосконалено метод сценарного прогнозування розвитку держави на довгострокову перспективу, що дало змогу визначати ступінь впливу держав, коаліцій держав на розвиток подій у регіоні. При цьому сформований опорний сценарій дає змогу: отримувати інформацію про деформацію в часі можливостей держав щодо впливу на події в регіоні; враховувати вплив важливих сфер функціонування держави на оцінку слабопрогнозованих важливих чинників; визначати конфігурації області припустимих сценаріїв задля врахування певної сукупності незапропонованих експертами у явному вигляді комбінованих сценаріїв.

Ключові слова: оборонне планування на основі спроможностей; безпекове середовище; метод сценарного прогнозу; довгострокове прогнозування; підвищення об'єктивності прогнозу.

Постановка проблеми. Метою будь-якої держави є сталий розвиток у сферах своєї діяльності: економічній, політичній, демографічній, технологічній тощо. Успішність вирішення завдання свого розвитку надає певних переваг у конкуренції з іншими державами в світі, регіоні. Успішність вирішення завдання сталого розвитку держави залежить від вірності обрання вектора свого розвитку, вміння передбачити вплив позитивних і негативних факторів, під впливом яких перебуватиме країна, здатність заздалегідь підготувати адекватні сили і засоби для вирішення завдань під час розвитку ймовірних сценаріїв на свою користь [1].

Для вирішення завдання об'єктивного оцінювання можливостей держави застосовуються різні прогнозні методи. Одним з них є метод сценарного прогнозування. Цей метод використовується під час вироблення стратегій керівництвами багатьох держав світу [2–4]. Останнім часом цей метод набув популярності у вітчизняному просторі. За його допомогою експерти намагаються визначити перспективи розв'язання конфлікту довкола Криму та на сході України [5–7]. Відомо, що ефективність передбачення змін у майбутньому залежить від якості інструментарію, який застосовується під час прогнозування. Отже актуальним питанням є розвиток відомих методів прогнозування. Метод сценарного прогнозування на сьогодні вже пережив декілька модифікацій. Однак можливості щодо його адаптації для вирішення завдання об'єктивної оцінки конкурентних можливостей держави не вичерпані.

Аналіз останніх досліджень і публікацій. Метод сценарного прогнозування пережив декілька модифікацій. Так, німецькі дослідники Мартін Вебер, доцент Школи менеджменту Аахенського університету (Німеччина) і Джутта Брауерс, науковий співробітник Школи менеджменту, у своїй роботі [8] зазначали, що аналіз сценаріїв – це якісна техніка прогнозування, корисна для стратегічного планування. Авторами було проведено огляд двох класів методів аналізу сценаріїв, описаних у сучасній науковій літературі. На основі обох класів розроблено метод, який на їх думку відповідає потребам стратегічного планування. У роботі метод складається з трьох етапів: визначення сумісних сценаріїв; визначення ймовірностей сценарію; визначення основних сценаріїв. Але удосконалення в цьому напрямі не вичерпане – у методі спостерігається недостатній горизонт прогнозування, відсутність визначення опорного сценарію, недостатній рівень кількісної оцінки сценаріїв.

Науковці з Об'єднаного Королівства Дж. Райт (Університет м. Дурхам, Велика Британія) та Пол Гудвін (Університет м. Бас, Велика Британія) у дослідженні [9] трактують аналіз сценаріїв як допомогу у визначенні майбутнього в умовах низької передбачуваності. Автори зазначають, що метод сценарного прогнозування містить слабкі місця. Це спонукало авторів до

вирішення питання розвитку цього методу. Вони визначили чотири загальні принципи, які мають сприяти посиленню ролі планування сценаріїв у разі низької прогнозованості: складні розумові рамки, розуміння людських мотивацій, розширення планування сценаріїв шляхом прийняття підходу до управління кризовими ситуаціями та оцінювання гнучкості, різноманітності та невиправданості стратегічних варіантів у структурованій оцінці варіанта сценарію. Тобто, автори визначили зону застосовності методу сценарного прогнозування, але питання підвищення якості прогнозування у визначених рамках ними не було вирішене.

Метод сценарного прогнозування, як і більшість відомих методів довгострокового прогнозування державного рівня, є експертним методом прогнозування. Здійснення процедури оброблення експертної бази базується на відомих класичних методах. Як проблемне питання відомий дослідник методу Делфі, професор Сиракузького університету (Італія) Тімоті Вівер [10] зазначав, що, призначенням експертних методів є встановлення хронології подій та визначення ймовірності настання тих чи інших сценаріїв розвитку певної ситуації за допомогою оброблення думок кількох експертів. Основним призначенням методу Делфі є переконання у тому, що зміни в оцінках розвитку сценарію відображають раціональне судження, а не вплив певних лідерів-науковців. У статті для вирішення питання підвищення об'єктивності прогнозу – авторами пропонується формалізація певних етапів роботи методу сценарного прогнозування.

Німецькі науковці Ханна Косов та Роберт Гаснер у дослідженні "Методи аналізу майбутнього та сценарного прогнозу" [11] оцінили методи дослідження ф'ючерсних прогнозів та методи аналізу сценаріїв для визначення їх меж застосовності. У своїй роботі автори визначили три основні категорії методик сценаріїв (сценарії, засновані на екстраполяції тренду, методики систематизованого формалізованого сценарію, методи творчо-розповідного сценарію) та обговорили загальні принципи їх застосування, сильні та слабкі сторони цих підходів. Ними було відмічено, що в науковій літературі є лише обмежені вказівки стосовно вибору методик сценарію та його оцінювання. Ця стаття спрямована на розширення відомостей з означеного питання.

На думку Пітера Бішопа, Енді Хайнса і Террі Коллінза [12], метод прогнозування сценаріїв є архетипним продуктом ф'ючерсних досліджень, оскільки він втілює центральні принципи: глибокий і творчий підхід до визначення прогнозів розвитку майбутнього; майбутнє непевне, тому слід бути готовими до кількох правдоподібних сценаріїв розвитку ситуації в країні та світі загалом, а не лише до того, якого ми очікуємо. Однак авторами не надано пропозицій щодо оцінок сценаріїв, стратегії поведінки в означеному полі ймовірних сценаріїв.

У результаті аналізу методу сценарного прогнозування, можливо відзначити, що метод не досконалий та потребує подальшого розвитку.

Мета статті полягає в удосконаленні науково-методичного апарату методу сценарного прогнозування для ефективного оцінювання ймовірних сценаріїв розвитку подій довкола країни.

Виклад основного матеріалу. Для об'єктивного оцінювання можливостей держави та обґрунтованого визначення пріоритетної низки заходів для ефективного розвитку можливостей держави необхідно провести таку роботу: визначити становище держави у її сферах діяльності (політичній, економічній і т. ін.) на теперішній час; здійснити ретроспективний аналіз цих питань в історичному аспекті; зважаючи на проведений аналіз зробити прогноз розвитку ситуації на визначену перспективу. Далі потрібно визначити інтереси країни та загрози можливих небажених змін у майбутньому безпековому середовищі. Вивчення означених питань дасть змогу побудувати бажаний вектор розвитку країни, визначити пріоритетну низку заходів для сприяння ефективному розвитку країни. Для вирішення означених питань пропонується використовувати удосконалений метод сценарного прогнозування, який містить такі етапи:

визначення горизонту прогнозування;

визначення основних суб'єктів (акторів) сценарію;

визначення ключових тенденцій і чинників;

ідентифікація екстремумів можливих результатів впливу відібраних чинників;

побудова поля сценаріїв;

визначення пріоритетних завдань за сценаріями;

визначення пріоритетних заходів за завданнями.

1. Визначення горизонту прогнозування. Як правило, ця інформація для дослідника є

початковими даними і визначається нормативними документами держави, які визначають періодичність і горизонт планування. Необхідно лише зауважити, що з одного боку, більш близький горизонт прогнозування дасть змогу зробити прогнози більш конкретними, але з іншого – набуття певних якісних змін у країні потребують певного часу. У межах статті обраний горизонт прогнозування 15 років.

2. Визначення основних суб'єктів (акторів) сценарію. Для вирішення питання пропонується ввести певний алгоритм оцінювання основних акторів сценарію. Основних "гравців" регіону пропонується визначати через їх відносні оцінки за такими показниками: *впливовість* (вага, авторитет) суб'єкта в політиці цього регіону (В(і) ~ [0..1] – зазначений фактор вимірюється у відносних величинах і змінюється в межах від 0 до 1); *важливість* для суб'єкта регіональної політики змін в регіоні (зацікавленість у лобіюванні власних інтересів) (З(і) ~ [0..1]); *рішучість* суб'єкта політики щодо здійснення змін в регіоні (готовність суб'єкта регіональної політики впливати на ситуацію в регіоні) (Р(і) ~ [0..1]); *незалежність* в прийнятті рішень від інших суб'єктів регіональної політики (Н ~ [0..1]); *прогнозованість* вектора впливу суб'єкта регіональної політики на ситуацію в регіоні впродовж прогнозного періоду (П(і) ~ [0..1]).

Вимірювання на цьому етапі пропонується здійснити експертним методом з отриманням числової оцінки ваг суб'єктів регіональної політики. Вага кожного з факторів може прийматись як різною, так і рівною до інших факторів. Це залежить від доцільності та можливості проведення відповідної градації. Оцінювати вагу впливу *і*-го суб'єкта регіональної політики на кризову політичну ситуацію в регіоні (*С(і)*) пропонується шляхом додавання оцінок показників, за якими оцінені суб'єкти регіональної політики: $C(i) = K_pP(i) + K_вB(i) + K_нH(i) + K_зЗ(i) + K_пП(i)$, де K_p, $K_в$, $K_н$, $K_з$, $K_п$ – ваги факторів оцінки впливовості акторів сценарію (пропонується здійснювати за методом регресійного аналізу [15]).

Отже, вирішення цього завдання дає змогу побудувати пріоритетний ряд суб'єктів впливу на розвиток подій довкола країни (приклад наведений у табл. 1).

Таблиця 1

Вплив суб'єктів політики на ситуацію в регіоні

Суб'єкт впливу	*Р(і)*	*В(і)*	*Н(і)*	*З(і)*	*П(і)*	*С(і)*
РФ	1	0,9	0,8	1	1	4,7
США	0,7	1	0,9	0,7	0,9	4,2
Україна	1	0,3	0,7	1	0,8	3,8
ЄС	0,5	0,8	0,6	0,8	0,7	3,4
НАТО	0,3	1	0,5	0,7	0,9	3,4
ОДКБ	0,3	0,9	0,3	0,9	0,9	3,3
Польща	0,6	0,5	0,2	1	0,9	3,2
Китай	0,3	0,7	0,7	0,6	0,6	2,9
ЄврАзЕС	0,2	0,7	0,4	0,8	0,7	2,8
Туреччина	0,4	0,6	0,6	0,7	0,5	2,8
Німеччина	0,3	0,5	0,4	0,8	0,7	2,7
Країни Балтії	0,8	0,2	0,1	0,7	0,9	2,7
Угорщина	0,4	0,3	0,1	0,8	0,7	2,3
Білорусь	0,1	0,4	0	0,8	0,9	2,2
Румунія	0,3	0,3	0,1	0,8	0,7	2,2
Словаччина	0,1	0,2	0,1	0,6	0,7	1,7
Молдова	0,1	0,1	0,1	0,6	0,3	1,2
Грузія	0	0	0,1	0	1	1,1
Болгарія	0	0	0	0	1	1

Таким чином, за результатами розрахунків найбільшим впливом на ситуацію довкола країни мають Російська Федерація, Сполучені Штати Америки, сама Україна, ЄС та блок НАТО.

3. Визначення ключових тенденцій і чинників. Необхідно визначити слабопрогнозовані комплексні чинники, які, з одного боку, суттєво впливають на розвиток країни, а з іншого – є взаємонезалежними (рис. 1).

До того ж необхідно враховувати вплив некерованих (слабокерованих) глобальних чинників. У цьому разі це такі чинники, як: ймовірна зміна демографічної ситуації в країнах регіону, прогноз розвитку ВВП країн і т. ін. За цими чинниками визначається співвідношення сил між основними регіональними суб'єктами. Цей підхід дає змогу розробити "опорний сценарій" розвитку ситуації. Він буде відповідати на запитання – як зміняться можливості країн щодо

просування своїх інтересів у регіоні у разі збереження їх поточної політики (див. рис. 1 – зелене коло).

Наступним кроком є врахування слабопрогнозованих впливових чинників через сфери впливу: економічну, демографічну, екологічну, культурну, технологічну тощо (див. рис. 1 – додаткові площини сфер). Це дає змогу конкретизувати уявлення експертів щодо окремих впливових сфер функціонування держави. Такий підхід дозволяє деталізувати оцінку важливих малопрогнозованих чинників: $N = 2n$, де N – кількість характеристик впливу важливих малопрогнозованих чинників; n – кількість врахованих сфер функціонування держави.

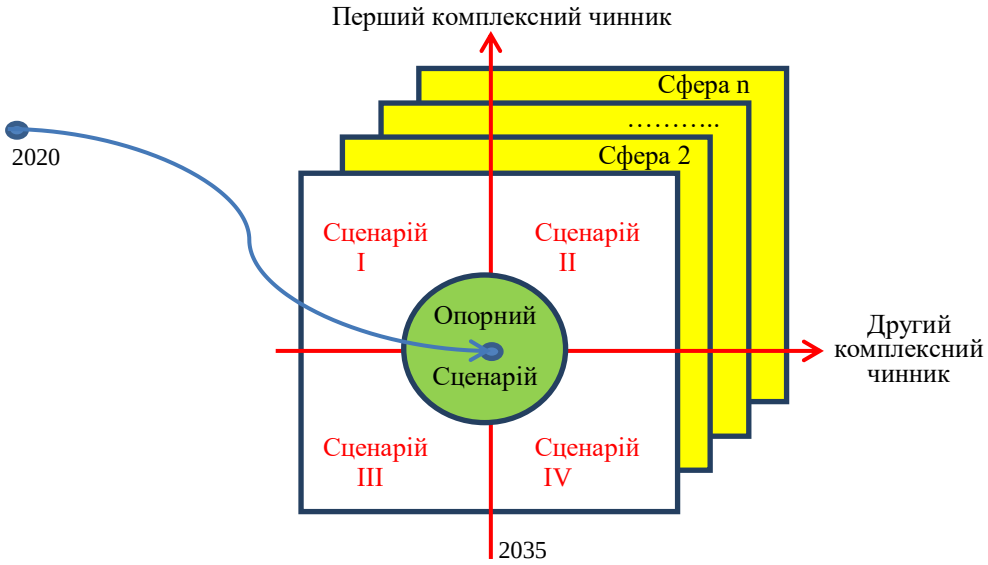


Рис. 1. Сценарії розвитку політичної ситуації в державі

3.1. Визначення ключових комплексних незалежних чинників. Під час прогнозування важливо визначитись з обмеженнями, у межах яких прогнози будуть актуальними. Стосовно поточного сценарію визначені такі обмеження:

Україна визначилась з європейським (євроатлантичним) вектором свого розвитку;

незмінний рішучій супротив з боку Російської Федерації, яка вважає Україну зоною своїх історичних інтересів;

підтримка з боку США стосовно прагнення України щодо приєднання до європейської (євроатлантичної) спільноти;

набуття Україною членства в ЄС (НАТО), або зміна політичного курсу України – докорінно змінює ланшафт ризиків і загроз та потребує перегляду сценаріїв.

Метод сценарного прогнозування передбачає визначення двох ключових комплексних незалежних чинників. Один з чинників стосується зовнішньополітичного вектора України. Вважається, що підтримання прагнення України щодо приєднання до західної спільноти з боку країн ЄС та США мають різну природу. Так, для США успіх України – це перемога над політичним конкурентом біля його кордонів. Для ЄС придбання України – це потенційне збільшення своїх економічних можливостей, розширення європейського внутрішнього ринку. Для ЄС Україна цікава не тільки як проєвропейська країна, але і заможня, самодостатня в економічному плані країна. Отже, підтримання України з боку ЄС залежить від успішності зміни ментального, економічного, технологічного станів держави. Країни ЄС є громадяниноцентричними країнами, а тому чутливо реагують на чинник добробуту та безпеки громадянина ЄС. Тому зовнішньополітичний чинник – *рівень зовнішньополітичної підтримки України країнами Європейського Союзу* визначається як один з впливових та неоднозначно прогнозованих.

З іншого боку, від успішності проведення реформ в Україні залежить ступінь консолідації суспільства в напрямі реалізації намагань щодо євроатлантичної інтеграції. Позитивні зрушення унаслідок реформ можливі в разі спільної консолідованої роботи всієї (переважної більшості) громадськості в державоутворюючих сферах діяльності: економічній, екологічній, технологічній, ідеологічній, науковій та ін. Саме тому, наступним впливовим чинником визначений – *рівень внутрішньополітичної стабільності в Україні.*

Можливі результати впливу чинника. Рівень внутрішньополітичної стабільності в Україні коливається в межах:

"максимально негативний рівень" (–1) – відсутність відчутних результатів реформ, затягнення вирішення питання збройного протистояння, численних жертв – у суспільстві присутні сумніви щодо доцільності обраного курсу на європейську (євроатлантичну) інтеграцію. На політичній арені з'являються політичні сили, які пропонують альтернативний шлях розвитку України. У певних регіонах країни збільшуються сепаратистські настрої, мають місце силові протистояння прибічників різних шляхів розвитку країни. Влада втрачає контроль над ситуацією в країні, але курс на євроінтеграцію залишається незмінним;

"максимально позитивний рівень" (+1) – консолідована підтримка суспільством курсу на європейську (євроатлантичну) інтеграцію. На політичній арені відсутні впливові політичні сили, що піддають сумніву доцільність обраного курсу. Найгострішою суперечкою в політичному секторі країни є дискусія вибору найефективнішого шляху досягнення поставленої мети.

Екстремальні варіанти впливу чинника Рівень зовнішньополітичної підтримки України країнами ЄС:

"максимально негативний рівень" (–1) – чинник вигоди економічної співпраці з РФ виявляється визначним у політиці країн ЄС. Європейський Союз розчарований динамікою подій в Україні, рівнем корупції, імітацією реформ. У ЄС не підтримується консолідована позиція стосовно економічних санкцій проти РФ. Ця позиція стає справою кожної окремо взятої країни Євросоюзу. Унаслідок подій в ЄС настає політична криза. Політична підтримка з боку країн ЄС залишається, але суто цивілізаційна. Основним меседжем для України з боку більшості країн ЄС є необхідність примирення з бунтівними регіонами на кшталт Придністровського питання;

"максимально позитивний рівень" (+1) – країни ЄС усіляко допомагають Україні на її шляху до євроінтеграції. Вони рішуче виступають на боці України в конфлікті з Росією, погрожуючи суттєвими економічними, трансєвроазійськими, фінансовими, політичними санкціями. Європейські країни повністю згортають свою економічну співпрацю з Російською Федерацією, відомі європейські концерни входять зі своїм капіталом в Україну, розбудовують економічний базис для розвитку країни.

Для перенесення константи прогнозу на визначений термін, необхідно вивчити сценарій, який розгорнеться довкола України в разі, якщо характер взаємного впливу на ситуацію з боку основних суб'єктів не зміниться. Це дасть змогу побудувати тренд, визначити динаміку якісної зміни ситуації як безпосередньо для України, так і для інших суб'єктів. Цей опорний сценарій розвитку ситуації довкола України авторами названий *"Рух у колії"* (див. рис. 1). За цим прогнозом: виконуються всі важливі прогнозовані (обмежувальні) чинники; визначальним чином на сценарій впливають впливові прогнозовані, але некеровані (повільно керовані) чинники; у певній сталій позиції залишаються впливові слабо прогнозовані комплексні чинники.

Загалом, з урахуванням можливих результатів впливу малопрогнозованих важливих комплексних чинників, можливо отримати один опорний і чотири похідних сценарії розвитку ситуації (див. рис. 1), які вербально можливо охарактеризувати таким чином:

0) *"Рух у колії"* – збереження внутрішньополітичної стабільності в Україні при збереженні нинішнього рівня підтримки України країнами ЄС;

1) *"Крізь терни до зірок"* – упевнений зріст внутрішньополітичної стабільності в Україні при збільшенні рівня підтримки України Заходом;

2) *"Добрий вечір владі"* – внутрішньополітична дестабілізація країни на тлі дієвої підтримки України на зовнішньополітичній арені з боку ЄС;

3) *"Колапс та байдужість"* – українська внутрішньополітична ситуація дестабілізується, країни ЄС скорочують підтримку України;

4) *"Київ самотужки"* – незважаючи на скорочення європейської підтримки, спостерігається зростання внутрішньополітичної стабільності в Україні.

3.2. Визначення ключових тенденцій і чинників. Для об'єктивного перенесення константи прогнозу на визначений термін (сценарій "Рух у колії"), необхідно вивчити впливові прогнозовані, але некеровані (повільно керовані) комплексні чинники, які за своєю сутністю є *"ресурсними чинниками"*. Результати аналізу чинників:

1. Динаміка росту населення в регіоні довкола України (демографічний чинник): кількість населення в Україні поступово зменшується; у разі збереження наявних тенденцій до 2025 року кількість населення в

Польщі та Україні зрівняється; у 2035 році населення Туреччини складе понад 100 млн осіб; процент населення України за звітні та прогнозовані роки відносно загальної кількості населення країн регіону поступово зменшується: від 15 % у 1980 р., до 11,5 % у 2019 р., з прогнозом до 8,2 % у 2035 р.

2. Обсяг валового продукту (економічний чинник): спадаючий тренд ВВП у регіоні мають Україна і Угорщина; у загальнорегіональному тренді (типові графіки ВВП) знаходяться: Болгарія, Польща, Словаччина, Румунія, Угорщина; певні проблеми в розвитку ВВП відмічаються в Україні, Росії (економічні санкції), Білорусі (країна-сателіт Росії); країна, яка стрімко зростає в економічному плані – Туреччина. Її економіка демонструє впевнене зростання.

3. Внутрішній валовий продукт на душу населення: менше, ніж в Україні, ВВП на душу населення тільки в Молдові, яка за динамікою очікувано поліпшує результати порівняно з Україною. Водночас, добре відстежується вплив санкцій на економічні можливості Росії – маючи другий показник ВВП на душу населення після Словаччини в регіоні у 2013 році, в 2016 році Росія вже мала шостий показник в регіоні.

Отже, порівняння загальнорегіонального тренду розвитку країн з трендом розвитку України вказує на поступовий порівняний спад показників розвитку України в регіоні. Ситуація, яка склалась у країні, сприяє зниженню економічних можливостей держави, відтоку робочої сили в інші країни регіону. Це призводить до поступової деградації країни. Тому загальний тренд є негативним, і потребує довгострокових програм комплексного розвитку країни, активного впливу на зміну тенденцій розвитку України.

4. Ідентифікація екстремумів можливих результатів впливу малопрогнозованих важливих комплексних чинників. Можливі екстремуми впливу чинників за сценарним методом прогнозування пропонуються в межах [–1...+1] залежно від реалізації відповідних чинників. На відміну від відомого методу сценарного прогнозування пропонується кожний імовірний сценарій розташовувати у куті чотирикутника. Відповідно, опорний сценарій є точкою всередині чотирикутника (див. рис. 1). Тоді інша поверхня чотирикутника відповідатиме певним комбінаціям запропонованих сценаріїв. Таким чином отримано область припустимих сценаріїв.

Крім того, кожний з імовірних сценаріїв має певні очікування щодо своєї реалізованості за визначеними сферами впливу. Цю реалізованість за сферами впливу пропонується оцінювати за шкалою від 0 до 1. За цим методом формується таблиця оцінювання відносної привабливості сценаріїв за сферами впливу (табл. 2).

Далі, експертні оцінки обробляються шляхом усереднення оцінок експертів із подальшим нормуванням на розмірність запропонованої осі (від –1 до +1) за формульним виразом $S(i)_{norm} = 2\,(S(i) - S_{min}) / (S_{max} - S_{min}) - 1$, де $S(i)$ – комплексна оцінка i-го сценарію; S_{max}, S_{min} – екстремальні значення комплексних оцінок сценаріїв; $S(i)_{norm}$ – нормована комплексна оцінка i-го сценарію. Інтегральна оцінка сценарію розраховується за аналогічним принципом, що і оцінка ваг суб'єктів регіональної політики.

Таблиця 2

Оцінювання відносної привабливості сценаріїв за сферами впливу

Сценарії	Влада	Економіка	Соціальна сфера	Міжнародні відносини	Військово-політична сфера	Прогнозні дії РФ	Інтегральна оцінка	Нормування
Рух в колії	0,7	0,6	0,8	0,5	0,5	0,6	3,7	**0,24**
Крізь терни до зірок	1	1	1	0,8	0,8	0,8	5,4	**1**
Добрий вечір владі	0,3	0,5	0,5	0,2	0,4	0,4	2,3	**-0,38**
Колапс та байдужість	0	0,2	0,3	0,1	0,1	0,2	0,9	**-1**
Київ самотужки	0,6	0,4	0,7	0,4	0,3	0,5	2,9	**-0,11**

Таким чином, оцінка відносної привабливості можливих сценаріїв розвитку подій за основними впливовими чинниками дала змогу співвіднести прийнятність сценаріїв для розвитку ситуації довкола України на період до 2035 року. З аналізу випливає, що в разі відсутності позитивної консолідації двох впливових слабопрогнозованих комплексних чинників: рівня внутрішньополітичної стабільності в Україні та рівня зовнішньополітичної підтримки України країнами ЄС, поліпшення ситуації для України не передбачається.

Якщо говорити про ймовірність виникнення того чи іншого сценарію розвитку ситуації довкола країни, необхідно сказати, що обрані впливові слабопрогнозовані чинники не є абсолютно самостійними – на практиці вони певною мірою залежать один від одного. З одного боку – стабільність у країні залежить від підтримання курсу України на Заході, з іншого боку – дієва підтримка України з боку країн ЄС залежить від успішності реформ, які проводяться владою всередині країни. Безумовно, на зазначені два чинники впливають інші важливі чинники. Отже, в реальності розгортатиметься деякий комбінований варіант з переважними ознаками одного із запропонованих сценаріїв. Найбільш вірогідними, з погляду домінантності, сценаріями будуть такі, що розташовані на цільовій осі *"Колапс та байдужість"* – *"Крізь терни до зірок"* з більш імовірним зосередженням комбінованого варіанта сценарію в районі сценарію *"Рух в колії"*. Сценарії на осі *"Добрий вечір владі"* – *"Київ самотужки"* є можливими, але вони будуть проміжними (короткочасними). Сценарій, у якому комбінуються два впливових малопрогнозованих чинників з різним ефектом є нестійкою комбінацією.

5. Побудова поля сценаріїв. Унаслідок застосування інтегральної оцінки сценаріїв (див. табл. 2), сценарний квадрат (див. рис. 1) деформується в "сценарний квазідельтоїд" (рис. 2).

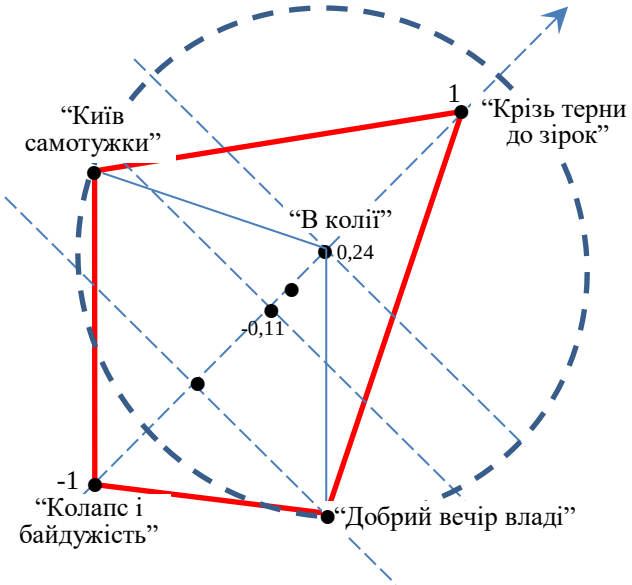


Рис. 2. Сценарний квазідельтоїд розвитку політичної ситуації в Україні

Алгоритм побудови поля сценаріїв: будується цільова вісь, яка єднає найбільш та найменш привабливі сценарії для держави; на цільовій осі відкладаються значення інтегральних оцінок основних сценаріїв. Після цього викреслюється коло одиничного радіусу довкола опорного сценарію; далі проводяться перпендикуляри від цільової осі на коло одиничного радіуса. На перехресті перпендикуляра та кола визначається просторове місцезнаходження сценаріїв; місця знаходження основних сценаріїв з'єднуються відрізками (див. рис. 2 – зона, що обмежена червоною лінією).

Отже, оцінювання сценаріїв дає змогу здійснити співвідношення сценаріїв за очікуваним ефектом; розташування ймовірних сценаріїв у вершинах сценарного квадрата визначає поле можливих сценаріїв; крім очікуваного ефекту від прогнозованих сценаріїв у майбутньому, авторами передбачено ймовірність виникнення ймовірних сценаріїв у полі сценарного квадрата розвитку політичної ситуації довкола України до 2035 року. Для більш якісного уявлення зони можливих сценаріїв, на цільовій осі сценаріїв побудуваний сценарний квазідельтоїд розвитку політичної ситуації довкола України до 2035 року (див. рис. 2).

6. Визначення пріоритетних завдань за сценаріями. На наступному етапі роботи експерти визначають перелік завдань, виконання яких сприятиме просуванню інтересів держави. Визначений перелік завдань ранжується експертами залежно від їх пріоритетності щодо досягнення поставленої мети.

7. Визначення пріоритетних заходів за завданнями. Після визначення пріоритетних завдань, будується пріоритетний ряд заходів, які мають бути виконані для реалізації визначених завдань для ефективного впровадження стратегії за поточним сценарієм. Ці заходи характеризуються, з одного боку, ступенем важливості (залежно від того, які завдання вони реалізовують і наскільки реалізовані завдання важливі (пріоритетні) для реалізації визначеної стратегії за поточним сценарієм), а з іншого боку – характеризуються ресурсоємністю.

Технологія роботи за двома останніми пунктами буде розкрита у подальшому.

Висновки. У статті удосконалено відомий метод сценарного прогнозування, який завдяки введенню до його складу аналітичної частини дав змогу збільшити ступінь об'єктивності під час оцінювання ймовірних сценаріїв розвитку подій на довгострокову перспективу.

Отримані такі результати: розроблено механізм визначення ступеня впливу держав, політичних блоків на розвиток подій у регіоні; запропоновано застосування "опорного сценарію", що дає змогу прогнозування деформації можливостей країн на вплив у регіоні через малокеровані впливові чинники; запропонований варіант модифікації сценарного квадрата, що дало змогу побудувати область припустимих сценаріїв.

Стаття висвітлює перший етап удосконалення методу сценарного прогнозування. Подальше удосконалення методу сценарного прогнозу спрямовано на вирішення таких завдань: визначення методу локалізації в області припустимих сценаріїв комбінованого сценарію, який розвивається; визначення пріоритетного переліку завдань, які мають бути виконані для поліпшення становища у сферах діяльності держави з урахуванням їх впливу на пару малопрогнозованих важливих чинників; розроблення алгоритму визначення необхідних обсягів ресурсів держави для реалізації пріоритетних завдань; створення алгоритму розподілу обмежених обсягів ресурсів між завданнями з урахуванням їх пріоритезації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Сиротенко А. М. Рекомендації щодо уточнення завдань і вдосконалення технологій моніторингу загроз національній та воєнній безпеці. *Наука і оборона.* 2018. № 2. С. 22–28.
2. Цілі сталого розвитку: 2016–2030. URL: http://www.un.org.ua/ua/tsili-rozvytku-tysiacholittia/tsili-staloho-rozvytku (дата звернення: 20.06.2021).
3. Future operating environment 2035. URL: https://www.cove.org.au/ wp-content/ uploads/ 2017/03/ Future-Operating-Environment-2035.pdf. (дата звернення: 22.06.2021).
4. Strategic Trends Programme. Future Operating Environment 2035. United Kingdom. URL: https://info.publicintelligence.net/UK-MoD-FutureEnvironment2035.pdf. (дата звернення: 22.06.2021).
5. Розвідка Міноборони визначила чотири ймовірні сценарії подальшої агресії Росії. URL: https://www.radiosvoboda.org/a/30105646.html. (дата звернення: 24.06.2021).
6. Війна Росії з Україною: чотири сценарії найближчого майбутнього. URL: http://www.icps.com.ua/viyna-rosiyi-z-ukrayinoyu-chotyry-stsenariyi-nayblyzhchoho-maybutnoho/ (дата звернення: 24.06.2021).
7. Вісім прогнозів агресії Росії від європейських експертів. URL: https://www.radiosvoboda.org/a/26807299.html. (дата звернення: 24.06.2021).
8. Jutta Brauers, Martin Weber. A new method of scenario analysis for strategic planning. Article. January, 1988. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/for.3980070104 (дата звернення: 24.06.2021).
9. Wright G., Goodwin P. Decision making and planning under low levels of predictability: Enhancing the scenario method. *International Journal of Forecasting.* October-December 2009. Vol. 25, Issue 4. P. 813–825.
10. Timothy Weaver W. The Delphy Forecasting Method. *The Phi Delta Kappan.* Vol. 52, No. 5 (Jan., 1971). P. 267–271.
11. Kosow H., Gaßner R. Methods of Future and Scenario Analysis: Overview, Assessment, and Selection Criteria. German Development Institute (DIE). Bonn, 2008, 133 p.
12. Bishop P., Hines A., Collins T. The current state of scenario development: an overview of techniques. *Emerald Group Publishing Limited.* 2007. Vol. 9, No. 1. P. 5–25. ISSN 1463-6689.
13. Биченков В. В. Етапи прогнозування поведінки складної інерційної системи з використанням розробленої моделі системи. *Сучасні інформаційні технології у сфері безпеки та оборони.* Київ, 2015. № 2 (23). С. 8–14.
14. Биченков В. В. Синтез системи підтримки прийняття рішень визначення рівня спроможностей ЗС України в ході оборонного планування. *Сучасні інформаційні технології у сфері безпеки та оборони.* Київ, 2015 № 3 (24). С. 9–17.
15. Биченков В. В., Заїка В. Ф. Розроблення системи критеріїв селекції формульних виразів для алгоритму побудови моделі складної системи з використанням комбінаторного методу з обмеженою базою аргументів. *Системи*

управління, навігації та зв'язку. Полтава, 2014. № 3 (31). С. 44–49.

Стаття надійшла до редакційної колегії 01.07.2021

Methodic for determining scenarios for the state development for the long-term

Annotation

The improved method of scenario forecasting solves the following tasks: determining the degree of influence of states, coalitions of states on the development of events in the region; formation of a reference scenario, which provides an opportunity to obtain information about the deformation in time of the ability of states to influence events in the region; taking into account the influence of important areas of state functioning on the assessment of poorly predicted important factors; determining the configuration of the area of acceptable scenarios, which allows to take into account a certain set of combined scenarios, which are not proposed by experts explicitly.

The goal of any state is sustainable development in the spheres of its activity: economic, political, demographic, technological, etc. The success of solving the problem of sustainable development of the state depends on the correctness of choosing the vector of its development, the ability to predict the impact of positive and negative factors under the influence of which the country will be, the ability to prepare adequate forces and means to solve problems. To solve this task, the state leadership is gained the experience used by the world's leading countries. It is a capability-based defense planning, based on which a number of long-term normative documents on the prospects of the country's development in the environment are formed. These are such documents as the National Security Strategy of Ukraine, sectoral strategies (for example, in the Ministry of Defense of Ukraine – the Strategy of Military Security of Ukraine is developed). For a high-quality development of these documents is carried out a comprehensive review of the security and defense sector, which includes defense review. The defense review at the main stage of its implementation contains four phases: assessment of the state and prospects of the security environment; review of capabilities by their functional groups and force planning; resource planning; formation of a perspective model of the Armed Forces and other components of the defense forces and their structure.

Keywords: capability-based defense planning; security environment; scenario forecast method; long-term forecasting; improving the objectivity of the forecast.

УДК 355.4 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/25-32

Свєшніков С. В., канд. техн. наук, ст. наук. співроб. (0000-0001-8924-4535)
Бочарніков В. П., д-р техн. наук, професор (0000-0003-4398-5551)
Прима А. М., д-р філос. (0000-0002-0776-6864)
Дергильова О. В., канд. техн. наук, ст. наук. співроб. (0000-0003-3916-1744)

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

Чинники безпекового середовища, важливі для розвитку сил оборони України

Резюме. У статті автори на основі розробленого на початку чергового циклу оборонного планування прогнозу майбутнього безпекового середовища виявляють його ключові аспекти, які можна розглядати визначальними чинниками і вимогами до розвитку сил оборони України. Пропонується визначити додаткову вимогу до опису безпекового середовища – виявлення та розгляд чинників, важливих для розвитку сил оборони України.

Ключові слова: безпекове середовище; воєнний конфлікт; оборона; оборонне планування; сили оборони.

Постановка проблеми. Відповідно до рішення першого заступника Міністра оборони України щодо виконання Плану підготовки проєкту опису майбутнього безпекового середовища “Майбутнє безпекове середовище 2030. Аналіз стратегічного передбачення”, протягом 2018–2019 років міжвідомчою робочою групою в рамках серії міжнародних семінарів було проведено дослідження і розроблено документ “Майбутнє безпекове середовище 2030. Стратегічне передбачення”. До міжвідомчої робочої групи було залучено фахівців багатьох міністерств і відомств, а також іноземних радників, які консультували групу щодо дотримання процедур дослідження, прийнятих у Північноатлантичному альянсі. Автори також брали участь у дослідженні і розробленні первинної версії зазначеного документа [1], який мав надати потрібні вихідні дані для чергового циклу оборонного планування.

Під час розроблення документа об’єктом дослідження було безпекове середовище, а предметом дослідження – його розвиток і визначення воєнно-політичних ризиків, викликів і воєнних загроз на середньострокову перспективу. Водночас, відповідно до наказу Міністра оборони України від 22.12.2020 № 484 “Про затвердження порядку організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони”, головною метою оборонного планування є “визначення пріоритетів і напрямів розвитку сил оборони, їх спроможностей ... з урахуванням реальних і потенційних загроз у воєнній сфері”. Як бачимо, об’єктом досліджень, що здійснюються в рамках оборонного планування, є сили оборони України, а предметом – їх розвиток з урахуванням воєнних загроз. Тобто, об’єкти дослідження в обох процесах є пов’язаними і, тому, потребують узгодження.

Дійсно, опис майбутнього безпекового середовища містить бачення багатьох його аспектів, викладених без проекції на визначення необхідних спроможностей сил оборони. До того ж, вимогу розгляду такої проекції містить п. 23 розділу 2 наказу Міністра оборони України № 484. Отже, є очевидними необхідність формування такої проекції і переломлення положень документа до головної мети оборонного планування.

Аналіз останніх досліджень і публікацій. Дослідження щодо визначення спроможностей сил оборони та їх розвитку проводились багатьма вітчизняними вченими. Зокрема, дослідження [2] аналізує базові категорії: спроможність, можливість, здатність. Огляд сучасного стану питань оборонного планування на основі спроможностей надано в дослідженні [3]. У роботі [4] запропоновано вдосконалення методології обґрунтування розвитку збройних сил. Концептуальні питання щодо визначення спроможностей сил оборони розглядаються в багатьох роботах, наприклад [5, 6]. Аналогічні питання також розглядаються стосовно окремих складових сил оборони, наприклад [7]. Найбільш наближеною до тематики, що розглядається в цій статті, є робота [8], де

аналізуються чинники, які впливають на розвиток сил оборони. Проте автори цієї роботи для визначення чинників спираються на наукові праці 2000–2012 років (переважно зі сфери зовнішньоекономічної діяльності) і на Воєнну доктрину України. Тобто, серед джерел визначення чинників відсутні джерела, що містять ґрунтовний аналіз безпекового середовища. Отже тема виявлення та розгляду чинників безпекового середовища, які є важливими для побудови перспективної моделі сил оборони України, залишається актуальним науковим завданням.

Мета статті полягає у переосмисленні результатів прогнозування розвитку майбутнього безпекового середовища і формуванні їх проекції на об'єкт оборонного планування – сили оборони України. Це дасть змогу зробити процедури оборонного планування ідеологічно більш цілісними і зрозумілими.

Виклад основного матеріалу. Загальний науково-методичний підхід до прогнозування розвитку безпекового середовища викладено раніше в роботах авторів, зокрема щодо поглядів на характер сучасних воєнних конфліктів [9], характерних рис воєнного конфлікту на території України [10] і технології аналізу воєнно-політичної обстановки [11]. Відповідно до цього підходу, будь-яка держава, зокрема Україна, розглядає безпекове середовище насамперед з погляду власних інтересів. Зважаючи на п. 3 ст. 3 Закону України "Про національну безпеку України", найбільш пріоритетними національними інтересами є:

відновлення суверенітету України в окремих районах Донецької та Луганської областей, а також в Автономній Республіці Крим (далі – АР Крим);

європейська та євроатлантична інтеграція України.

Відповідно до Стратегії воєнної безпеки України, затвердженої Указом Президента України від 25.03.2021 року № 121/2021 "Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України", Російська Федерація визначена воєнним противником України на національному рівні (далі – воєнний противник). З огляду на це, головними воєнно-стратегічними цілями сил оборони України, які витікають з її воєнно-політичних інтересів, мають бути:

змушення воєнного противника до відмови від збройної агресії проти України;

відновлення самостійності і верховенства державної влади в окремих районах Донецької та Луганської областей, а також в АР Крим;

протидія проявам сепаратизму на усій території України і забезпечення її територіальної цілісності та недоторканності;

запобігання збройній агресії проти України у майбутньому.

Зазначені воєнно-стратегічні цілі визначають вимоги до першого, найбільш узагальненого, рівня функціональних спроможностей сил оборони.

Нижче наведені важливі для побудови перспективної моделі сил оборони України ключові чинники майбутнього безпекового середовища визначені як результат переосмислення висновків [1] з прогнозу розвитку безпекового середовища.

Воєнно-політичні чинники

1. Прогнозована регіоналізація раніше глобального безпекового простору тягне за собою зростання воєнно-політичних ризиків, викликів і воєнних загроз, породжених на регіональному рівні, з боку впливових регіональних держав. Оскільки головна увага регіональних держав буде зосереджена насамперед на запровадженні елементів власного порядку в регіоні, найбільші суперечності виявлятимуться на територіях зіткнення їх інтересів. Звідси витікають характерні риси можливих загроз у сфері воєнної безпеки України. Зокрема, можна очікувати перманентної зацікавленості у схиленні України на той чи іншій бік. Одночасно, вибір Україною однієї зі сторін неминуче породжуватиме опір іншої сторони. До того ж не можна виключити ситуації, коли за певних умов (які залежать переважно від співвідношення економічних і воєнних потенціалів сторін) інтереси України виявлятимуться предметом компромісу між конкуруючими сторонами або предметом розділу впливу. Водночас із розгортанням процесів регіоналізації, не виключається, що Україна втрачатиме увагу з боку дружніх держав, розташованих в інших регіонах.

Це дуже жорстка головна властивість регіонального безпекового середовища довкола України, яка притаманна буферним геополітичним просторам [12] взагалі. Логіка буферного простору визначає, що у разі приблизно рівної сили протилежних сторін і незалежно від прихильності до однієї з них буферна держава має бути готовою до захисту з будь-якого напряму, особливо у той час, коли регіональні безпекові процеси

знаходяться в стадії біфуркації і можливість виникнення або активізації воєнного конфлікту постійно підвищується. Буферна держава є завжди предметом компромісу між великими геополітичними противниками. Ситуація з "Північним потоком-2" – наочне тому підтвердження. Саме на цій головній властивості має концентруватись увага під час планування розвитку і застосування сил оборони України.

2. У період до 2030 року очікується зростання кола безпекових проблем України, головною з яких залишиться збройна агресія Російської Федерації і окупація нею АР Крим. Останнім часом Російська Федерація значно підвищила рішучість до застосування воєнної сили. Регіональна частина її неядерного військового потенціалу перевищує відповідну частину військового потенціалу будь-якої європейської країни Північноатлантичного альянсу. З іншого боку, основу військового потенціалу Північноатлантичного альянсу складають США, швидкому збільшенню присутності яких в регіоні заважає у першу чергу величезне транспорте плече. Крім того, військова підтримка України з боку країн Північноатлантичного альянсу стримуватиметься загрозою переростання конфлікту до глобальної ядерної війни, результати якої знівелюють усі можливі воєнно-політичні ефекти.

3. Прогнозована тенденція на перманентне нарощування воєнної могутності впливових регіональних держав визначає необхідність відповідного нарощування спроможностей сил оборони України або вступу її до Північноатлантичного альянсу. Однак Україна не має потрібних для нарощування спроможностей безмежних фінансово-економічних ресурсів. Вступ України до Північноатлантичного альянсу в середньостроковій перспективі теж буде проблематичним. Це визначає потребу пошуку нових, нестандартних, можливо, асиметричних підходів до ідей забезпечення сил оборони ОВТ і власне організації оборони. Такі підходи мають бути спрямовані на стримування воєнного противника, примушення його до відмови від агресивних планів, зважаючи на неприпустимі матеріальні та нематеріальні втрати. З іншого боку, вони не мають вимагати від держави надвеликих витрат.

4. Руйнування міжнародних механізмів гармонізації інтересів підвищуватиме можливість того, що Україна буде змушена більшою мірою наодинці вирішувати власні проблеми безпеки. Є можливою переважно військово-технічна підтримка України з збоку дружніх держав, але вона не буде вирішальною. Розвиток сил оборони і планування їх застосування мають враховувати таку можливість, але не покладатись на неї.

5. Активний розвиток міжнародних транспортних шляхів "Схід-Захід" і значний транзитний статус України визначає нове завдання сил оборони – охорону транзитних комунікацій. Від успішності виконання цього завдання буде безпосередньо залежати реалізація транзитного потенціалу України та її поступальний економічний розвиток.

6. У період до 2030 року зростатиме геополітична важливість Чорного моря як головного шляху виходу до Середньої Азії та Середземноморського регіону, тому розвиток Військово-морських сил України має знаходитись серед головних пріоритетів розвитку сил оборони.

7. Оскільки інтереси провідних держав у світі та регіоні вже набули антагоністичного характеру, час для трансформації і досягнення необхідних спроможностей сил оборони України є незначним.

Військово-економічні та військово-технічні чинники

8. Складність безпекового середовища, велика чисельність і складність його елементів та зав'язків між ними, кореляція зав'язків у різних просторах (економічному, політичному, інформаційному тощо) потребує спеціального виокремлення в силах оборони аналітичної складової і побудови цілісної підсистеми стратегічного аналізу, заснованої на використанні сучасних аналітичних технологій, насамперед технологій штучного інтелекту. Водночас це підвищує вимоги до якості підготовки управлінського персоналу, оволодіння ним сучасними методами аналізу.

9. Гібридний характер сучасних воєнних конфліктів потребує аналогічних за характером відповідей. До вирішення завдань оборони мають залучатись усі державні інститути. Це означає кардинальне підвищення складності державного управління, вимог до його головних показників: оперативності, обґрунтованості, безперервності та повноти. Це також означає, що планування розвитку і застосування сил оборони має відбуватись у єдиній системі державного управління з належною міжвідомчою координацією.

10. Відповідно до принципів управління в ієрархічних системах, зростання

нестабільності безпекового середовища тягне за собою потребу посилення загального рівня централізації управління силами оборони і концентрування влади та відповідальності під єдиним керівництвом. Це дасть змогу підвищити оперативність реагування на несподівані ризики, виклики та загрози у сфері воєнної безпеки України. Поліпшення аналітичної складової має компенсувати недоліки, притаманні жорстко централізованим системам.

11. Зростання рівня біологічних загроз потребує створення в силах оборони України спеціальних елементів (підсистем), які забезпечуватимуть дії сил оборони в умовах епідемій і пандемій. Зважаючи на наявність на території України чисельних об'єктів хімічної та атомної промисловості, аналогічний висновок стосується умов радіаційного та хімічного забруднення. Крім того, у плануванні застосування сил оборони має враховуватись зростання рівня техногенних загроз, які можуть реалізовуватись у тому числі внаслідок терористичних актів, у результаті навмисного або випадкового застосування потенційним противником зброї проти екологічно небезпечних об'єктів.

12. Перманентна криза світової фінансово-економічної системи негативно відбиватиметься на стані державних фінансів і скорочуватиме можливості держави щодо фінансування потреб оборони, тому під час планування розвитку сил оборони слід орієнтуватись на брак і навіть зменшення реальних обсягів видатків на потреби оборони. Це також потребуватиме системних заходів щодо підвищення якості планування розвитку, запобігання непотрібним та неефективним витратам, кардинального підвищення рівня контролю витрат, реального обрахування ризиків розвитку і посилення боротьби з корупцією. Зі свого боку, це потребуватиме вдосконалення науково-методичного супроводження, розвитку аналітичних технологій і спроможностей системи управління силами оборони щодо контролю оборонних витрат.

13. Україна не має значущих запасів нафти, більшість потужностей її нафтопереробних заводів орієнтовані на переробку експортної нафти. В умовах прогнозованої нестабільності світової фінансової системи, зміни конфігурації світових і регіональних товарних шляхів, у критичні моменти часу зростатиме можливість зриву поставок нафти і паливно-мастильних матеріалів. З огляду на те, що моторизація сил оборони основана на двигунах внутрішнього згоряння, це може виявитись критичним елементом у забезпеченні боєздатності сил оборони, тому під час планування розвитку необхідно передбачити створення відповідних запасів нафти та/або паливно-мастильних матеріалів, консервування наявних родовищ нафти і резервування переробних потужностей. Загалом, оцінювання логістичних спроможностей має засновуватись на балансі можливості нормативного забезпечення потреб сил оборони, а також вартості створення, зберігання і оновлення запасів. Це також є одним з напрямів удосконалення науково-методичного супроводження в силах оборони.

14. Одним з факторів розвитку сил оборони України та підвищення їх бойових спроможностей є оснащення сучасними зразками озброєння та військової техніки, здатними протистояти застосуванню на полі бою потенційним противником високотехнологічних озброєнь. Україні бракує коштів для закупівлі за кордоном зразків ОВТ потрібної кількості та якості. Отже розвиток власного виробництва ОВТ залишається пріоритетним.

15. Ефективність зразків ОВТ вітчизняного виробництва визначається освоєнням оборонно-промисловим комплексом (ОПК) ключових технологій, насамперед, інформаційних і матеріалознавства. Сили оборони мають бути не просто замовником і споживачем пропонованої ОПК продукції. Вони повинні спільно з вітчизняним ОПК створити єдину систему розвитку, апробації та відпрацювання новітніх технологій, які будуть втілюватись не лише в новітніх зразках ОВТ, а й зможуть надати поштовх технологічному розвитку промисловості України, підвищити її експортний потенціал.

16. Зважаючи на збільшення ролі електронних компонентів у сучасних зразках ОВТ та їх електронної вразливості, у розвитку ОВТ пріоритет має бути відданий засобам технічної розвідки і радіоелектронної боротьби. Останні мають потенціал звести до нуля ефективність застосування на полі бою деяких систем озброєння потенційного противника.

17. Наукоємність сучасних зразків ОВТ постійно зростає, тому одним з пріоритетних напрямів розвитку сил оборони має стати розвиток наукового компоненту. У цьому контексті основна увага має приділятись

розвитку новітніх способів застосування сил оборони, технологій аналізу даних, управління складними системами у швидкоплинному зовнішньому середовищі, створення та виробництва озброєнь, навчання і тренування особового складу. Доцільно опрацювати питання щодо більшого залучення перспективної молоді до наукових підрозділів ОПК і сил оборони, програм підтримки молодих вчених, розвитку наукової та випробувальної бази. У цілому підготовка науковців має бути зосереджена на оволодінні системним підходом, сучасними математичними методами і технічними дисциплінами.

18. Комплектування сил оборони відбуватиметься в жорстких умовах. Загальна чисельність осіб призовного віку зменшуватиметься завдяки старінню населення, падінню народжуваності та зростанню міграції. Можна очікувати, що трудова міграція переростатиме до еміграції (зміни країни проживання), коли мігруватимуть переважно економічно активні громадяни, найбільш освічені та працьовиті. Загальний рівень освіти, знань і навичок призовного і контрактного контингенту зменшуватиметься, що вступатиме у суперечність зі складністю сучасних ОВТ і способів управління боєм. Моральні якості також погіршуватимуться, що загрожуватиме падінням духовного потенціалу сил оборони. Так комплектування сил оборони потребуватиме державної уваги і принципово нових підходів, спрямованих на злам ідеології "споживачів", яка не витримує критики в контексті захисту Вітчизни. Ці підходи мають торкатись усієї системи освіти, починаючи з дошкільного виховання, не зважаючи на те, що ці питання виходять за компетенцію органів управління силами оборони. Можливо, сили оборони мають виступити ініціаторами змін у вітчизняній системі освіти.

19. Україна – багатонаціональна, багатокультурна і багатоконфесійна країна. Це висуває дві вимоги до перспективної моделі сили оборони. По-перше, комплектування сил оборони відбуватиметься представниками різних національностей, культур і конфесій, тому виховна робота і навчання мають передбачати спеціальні заходи для забезпечення єдності військових колективів, їх вмотивованості на виконання бойових завдань щодо захисту Вітчизни. По-друге, підготовка сил оборони має враховувати особливості виконання бойових завдань на територіях України, де проживають національні, культурні та релігійні меншини. Це визначає особливе завдання щодо формування іміджу сил оборони як захисників справедливості.

20. Зважаючи на воєнно-політичну і військово-технічну підтримку України з боку країн Північноатлантичного альянсу, не можна втрачати можливість підвищення навченості особового складу сил оборони завдяки участі в спільних операціях альянсу, проведенню спільних навчань, участі в програмах навчання за кордоном. З іншого боку, треба подолати такі явища, коли військовослужбовець отримує якісну освіту за кордоном, але потім не реалізує отриманні знання у практиці військ. Отже такі заходи повинні мати єдиний вимір і контекст оцінки – підвищення ефективності дій сил оборони.

21. Трансформація сил оборони має відбуватись з урахуванням факту посилення тенденції на зростання інтенсивності та потенційної шкідливості кібернетичних атак, що вимагатиме забезпечення не лише захисту, але й активних дій в кібернетичному просторі. Рівень потенційної шкоди, яку можуть спричинити кібернетичні дії противника, змушує сили оборони приділяти цьому питанню пріоритетну увагу.

22. У сучасних воєнних конфліктах, особливо в гібридних і мережевих, головним об'єктом деструктивного впливу стає світосприйняття і світорозуміння населення, зокрема військовослужбовців. Так звана "війна в умах" усе більше набуває актуальності. Ця війна йде без пострілів, переважна її частина відбувається в мирний час. Сили оборони мають планувати і здійснювати не лише дії інформаційно-психологічного захисту, але й активні, наступальні дії, планувати і проводити цілісні інформаційно-психологічні кампанії в межах загальнодержавного і зарубіжного інформаційного простору. Вони мають бути спрямовані насамперед на формування думок і настроїв, сприятливих для виконання силами оборони бойових завдань.

Воєнно-стратегічні чинники

23. Наявні ресурсні обмеження України визначають потребу швидкого і надійного досягнення воєнно-стратегічних цілей України. Це потребує від сил оборони орієнтації на швидкоплинні дії і недопущення заморожування ситуації у разі ескалації збройної агресії або виникнення у майбутньому воєнного конфлікту. Заморожування ситуації або будь-яка інша затримка у досягненні воєнно-стратегічних цілей потягне значні матеріальні та

репутаційні втрати України і, як результат, гальмування її поступового соціально-економічного розвитку.

24. Воєнний противник України має значну ресурсну та військову перевагу. Безпосереднє зіткнення з ним загрожуватиме неприйнятними надвеликими втратами і знищенням України як самостійної держави, тому основним способом дій сил оборони України щодо досягнення її воєнно-стратегічних цілей під час протистояння проти переважаючого воєнного противника має бути змушення його до відмови від збройної агресії через демонстрацію можливості та/або спричинення неприпустимих збитків. Дії щодо останніх мають плануватись на усю глибину території воєнного противника і в усіх сферах безпеки, з використанням інших інструментів воєнної політики.

25. Головними, найбільш можливими сценаріями воєнно-політичних ситуацій, які потребуватимуть задіяння сил оборони, будуть:

масштабна збройна агресія воєнного противника проти України, яка супроводжуватиметься інформаційно-психологічними операціями, кібернетичними діями, спеціальними операціями, блокадами України;

підтриманий ззовні воєнний конфлікт усередині держави, який супроводжуватиметься міжнаціональною, міжконфесійною або соціально-політичною нестабільністю;

втягнення України в конфлікт між іншими державами, зокрема із застосуванням ядерної зброї;

воєнний конфлікт у прикордонному районі.

Іншими можливими сценаріями воєнно-політичних ситуацій, які потребуватимуть залучення сил оборони, будуть:

терористичні акти, зокрема із застосуванням зброї масового знищення;

масовий перехід державного кордону з території суміжних держав;

надання військової допомоги Україною іншим державам в межах міжнародних зобов'язань;

природна або техногенна катастрофа на території України або на території суміжної держави, зокрема пандемія.

Сили оборони повинні мати необхідні спроможності до ефективного виконання завдань в межах зазначених воєнно-політичних ситуацій. Критерій ефективного виконання завдань передбачає виконання завдань у повному обсязі за мінімальний або нормативний час та з мінімальними витратами ресурсів.

26. Під час визначення (уточнення) необхідних спроможностей сил оборони, визначення їх дислокації, навчання, планування застосування слід ураховувати рішучість воєнно-стратегічних цілей воєнного противника, серед яких можуть бути: знищення (розділ) України як держави, зміна її воєнно-політичного керівництва, знищення воєнного та економічного потенціалу, зміна конституційного ладу, відокремлення певних територій.

27. Спроможності воєнного противника, рішучість його воєнно-стратегічних цілей визначають складні умови застосування сил оборони у майбутньому, головними з яких є те, що воєнні дії можуть охоплювати всю територію України, а швидкоплинність дій воєнного противника не дасть часу для організації стратегічно відчутної військово-технічної допомоги Україні з боку дружніх держав.

28. Воєнний противник перспективними способами ведення воєнних дій розглядає мережеві дії, коли жертва агресії піддається інтенсивному впливу нібито не пов'язаних між собою різномасштабних дій різних військових і невійськових суб'єктів, які насправді діють за єдиним задумом і планом. Це потребує готовності сил оборони до дій в умовах мережевих конфліктів і передбачає спеціальні критерії оцінювання ефективності бойових дій, переосмислення організаційно-штатних структур, їх завдань, форм і способів підготовки тощо. Освоєння силами оборони мережевих технологій ведення бойових дій на тактичному і оперативному рівнях має бути пріоритетом у визначенні необхідних спроможностей.

29. У своєму арсеналі воєнний противник України має високоефективні неядерні засоби знищення центрів управління державою і силами оборони. Ця обставина змушує сили оборони шукати спеціальні (насамперед законодавчі, організаційні, технічні) шляхи збереження стійкості, оперативності, безперервності та повноти управління.

30. Дії сил оборони можуть супроводжуватись масштабними техногенними катастрофами, голодом і епідеміями серед населення. Це відволікатиме дефіцитні ресурси, потребуватиме додаткових зусиль з боку сил оборони, обмежувати

свободу маневру і вибору способу дій. Це також підвищуватиме вимоги до координованості дій складових сил оборони, підвищення якості планування операцій, пророблення усіх питань щодо спільного застосування, розмежування зон відповідальності тощо.

31. Слід ураховувати, що у разі подальшого розгортання внутрішніх соціально-економічних проблем не можна виключати зменшення патріотичних настроїв населення та його готовності захищати Вітчизну, бажання віддавати об'єкти приватної власності для задоволення потреб сил оборони, зростання міграції населення до сусідніх держав, що загрожуватиме оперативному і якісному проведенню мобілізації. Для уникнення несподіванок, сили оборони мають спостерігати за ситуацією і бути готовими до ініціювання заходів держави щодо її поліпшення.

32. Проведення військових операцій супроводжуватиметься гібридним (комплексним) застосуванням проти України усіх доступних більш-менш ефективних інструментів, які призвані ускладнити дії сил оборони і які потребуватимуть відповідних заходів протидії або утворення в силах оборони спеціальних організаційно-штатних одиниць. Насамперед, це кібернетичні дії та інформаційно-психологічні операції, політичні, економічні, фінансові санкції. Тому сили оборони мають знайти способи забезпечення ефективності дій у кібернетичному та інформаційному просторах, що може стати вирішальним чинником у справі досягнення перемоги.

33. Сили оборони мають бути всебічно підготовлені до дій проти непередбачених законом збройних формувань, які можуть комплектуватись як громадянами сусідніх держав, так і громадянами України. Непередбачені законом воєнізовані формування також можуть ускладнювати умови дій сил оборони. Їх нейтралізація потребує вдосконалення взаємодії між усіма елементами сил оборони.

34. Україна – багатонаціональна країна. Значна кількість національних меншин мешкає на прикордонних територіях. Завдяки демократичній національній політиці України ці меншини мають можливість свого культурного розвитку і підтримання зв'язків з представниками націй із суміжних країн. Проте іноді політичне керівництво суміжних країн ставить інтереси культурного розвитку споріднених національних меншин України вище за інтереси України, підживлюючи тим самим сепаратистські настрої. Не можна виключати виникнення умов їх ескалації на фоні воєнно-політичних невдач України, розвитку соціально-економічних негараздів, послаблення центральної влади тощо. Трансформація сил оборони, зокрема їх завдання, дислокація, навчання мають ураховувати таку можливість.

35. Україна є країною, яка завжди була донором безпеки. Політика України виходить з ідеї можливості забезпечення міцного миру та сприятливих умов справедливого соціально-економічного розвитку за допомогою створення багатонаціональних безпекових організацій. Саме тому Україна прагне участі в ЄС і НАТО. З огляду на це, не залишаючи в стороні нагальні завдання, пов'язані з протидією агресії воєнного противника, сили оборони мають розвивати спроможності щодо забезпечення належного внеску до загальноєвропейського безпекового простору, а також у спільні операції ЄС і НАТО.

Висновок. З погляду оборонного планування, прогноз розвитку безпекового середовища потребує інтерпретації з метою переломлення його ключових положень до питань розвитку сил оборони. Є доцільним запропонувати визначити додаткову вимогу до опису безпекового середовища – виявлення та розгляд чинників, важливих для розвитку сил оборони України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Бочарніков В. П., Свєшніков С. В. Безпекове середовище 2030 : монографія. Київ : Майстер книг, 2019. 76 с.
2. Марко І. Аналіз понять "спроможність", "можливість" і "здатність" та пропозиції щодо їх застосування у документах сектору безпеки і оборони України. *Social development & Security*. 2018. Vol. 5, No. 3. P. 76–86.
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*. Київ, 2020. № 3 (70). С. 54–61.
4. Загорка О.І. Планування розвитку (реформування) збройних сил: методологічний аспект. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2020. № 3 (70). С. 40–46.
5. Сурков О. О. Концептуальний підхід до вибору пріоритетних напрямів розвитку спроможностей Збройних Сил України та інших складових сил

оборони. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2018. № 2 (63). С. 39–45.
6. Устименко О. В., Білик В. І. Планування розвитку спроможностей сил оборони України щодо протидії загрозам у ході гібридної війни. *Вісник НАДУ при Президентові України. Державне управління*. 2018. № 2. С. 48–52.
7. Коробкін В. Ф., Слюсар А. А. Спроможності у сфері цивільного захисту: пошук категоріально-понятєвого апарату. *Науковий вісник: Цивільний захист та пожежна безпека*. Київ, 2020. № 2 (10). С. 61–68.
8. Іваницький М. Г., Саганюк Ф. В., Мудрак Ю. М., Пальчик А. В. Підходи до аналізу чинників, які впливають на розвиток Збройних Сил України та інших складових сил оборони. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2019. № 3 (67). С. 54–58.
9. Бочарніков В. П., Свєшніков С. В. Погляди на характер сучасних воєнних конфліктів. *Наука і оборона*. 2017. № 1. С. 3–8.
10. Бочарніков В. П., Свєшніков С. В. Воєнні аспекти протидії гібридній агресії: досвід України : монографія. Київ : НУОУ імені Івана Черняховського, 2020. С. 5–35.
11. Бочарніков В. П., Свєшніков С. В., Тимошенко Р. І., Павленко В. І. Технологія аналізу воєнно-політичної обстановки. Київ : НУОУ імені Івана Черняховського, 2019. 384 с.
12. Mohammad Reza Hafeznia, Syrus Ahmadi, Bernard Hourcad. Explanation of the Structural and Functional Characteristics of Geographical Buffer Spaces. Geopolitics Quarterly. Winter 2013. Vol. 8, No 4. P. 1–40. URL: https://www.sid.ir/EN/VEWSSID/J_pdf/108020132801.pdf (дата звернення: 02.04.2021).

Стаття надійшла до редакційної колегії 13.05.2021

Factors of a safe environment important for the development of Ukraine's defense forces

Annotation

In accordance with the decision of the First Deputy Minister of Defense of Ukraine on the implementation of the Project Plan for the draft description of the future security environment "Future Security Environment - 2030. Strategic Forecast Analysis", during 2018-2019 an interagency working group conducted a series of international seminars and developed a document security environment 2030". The object of the study was the security environment, and the subject of the study was its development and identification of military-political risks, challenges and military threats in the medium term.

The purpose of the article is to rethink the results of forecasting the development of the future security environment and forming their projection on the object of defense planning - the defense forces of Ukraine. This will make defense planning procedures ideologically more coherent and understandable. In accordance with the Strategy of Military Security of Ukraine, approved by the Decree of the President of Ukraine, the Russian Federation is defined as a military adversary of Ukraine at the national level.

The main military-strategic goals of Ukraine's defense forces, which stem from its military-political interests, have been identified. The key factors of the future security environment, military-political, military-economic and military-technical, which are important as a result of rethinking the conclusions from the forecast of the security environment development, are important for building a perspective model of Ukraine's defense forces.

From the point of view of defense planning, the forecast of the development of the security environment needs to be interpreted in order to refract its key provisions on the development of the defense forces. It is expedient to propose to define an additional requirement for the description of the security environment - identification and consideration of factors important for the development of the defense forces of Ukraine.

Keywords: security environment; military conflict; defense; defense planning; defense forces.

УДК 355.45(477) DOI: https://doi.org/10.33099/2304-2745/2021-2-72/33-39

Богданович В. Ю., д-р техн. наук, професор[1] (0000-0003-0481-9454)
Ільяшов О. А., д-р військ. наук, професор[2] (0000-0002-8099-5057)
Комаров В. С., д-р військ. наук, професор[2] (0000-0003-2873-8261)
Олексіюк В. В., канд. військ. наук[2] (0000-0002-9577-4257)

[1] – Центральний науково-дослідний інститут Збройних Сил України, Київ;
[2] – Військова частина А1906, Київ

Підхід до оцінювання безпекового середовища в сучасних умовах ведення збройної боротьби

Резюме. У статті викладені результати досліджень щодо оцінювання безпекового середовища в сучасних умовах ведення збройної боротьби. Запропонований підхід є практичною реалізацією методики оцінювання безпекового середовища. У його основу покладено модель застосування військової сили проти України. Зазначена модель побудована як система координат з відповідними осями, на яких відображені: модель гібридної війни РФ (за етапами виникнення, нарощування і реалізації воєнної загрози для нашої держави), ознакове поле та сфери прояву моніторингових ознак.

Ключові слова: національна безпека; безпекове середовище; моніторинг безпекового середовища; інформаційно-аналітичне забезпечення; моніторингова ознака.

Постановка проблеми. Однією з особливостей розвитку безпекового середовища на початку XXI століття є перенесення ваги у збройних конфліктах на асиметричне застосування військової сили. Усе частіше акцент методів протиборства, які застосовуються, зміщується у бік комплексного використання військових і невійськових заходів (політичних, економічних, інформаційно-психологічних, гуманітарних тощо), що принципово змінює характер збройної боротьби та ставить більш високі вимоги до системи забезпечення воєнної безпеки (СЗВБ).

За таких умов важливим для національної безпеки (НБ) є питання своєчасного виявлення викликів і загроз воєнній безпеці держави, яке здійснюється за результатами аналізу безпекового середовища, а також оцінювання їх характеру, рівня, масштабу та прогнозування можливого від них збитку у разі їх реалізації.

Аналіз останніх досліджень та публікацій. На теперішній час можна виділити підходи вітчизняних і зарубіжних дослідників, що викладені у [1–7] та використовуються для оцінювання стану НБ у цілому та окремих її складових.

Зазначені методи, методичні підходи мають загальнонауковий характер у галузі забезпечення воєнної безпеки (ВБ) держави та не можуть бути використані безпосередньо через те, що в них не враховані особливості, пов’язані з асиметричними діями, які широко застосовуються в сучасних збройних конфліктах.

Особливу увагу привертає праця [8], яка присвячена розробленню методологічного інструментарію забезпечення ВБ України в умовах сучасних загроз комплексним, зокрема асиметричним, використанням військових та невійськових сил і засобів сектору безпеки. У контексті зазначеної роботи розроблена методика оцінювання зовнішнього безпекового середовища, для її реалізації авторами пропонується практичний підхід, який дає змогу оцінювати безпекове середовище в умовах ведення сучасних збройних конфліктів.

З огляду на зазначене, **метою статті** є викладення результатів досліджень щодо практичної реалізації процесу оцінювання безпекового середовища в сучасних умовах ведення збройної боротьби.

Виклад основного матеріалу. Проблемні питання у сфері НБ досліджують державні науково-дослідні установи та навчальні заклади, вітчизняні та закордонні фахівці з питань оборони, але дефініція “безпекове середовище” у нормативно-правових актах нашої держави не визначена. Авторами пропонується використовувати визначення, сформульоване у [8]: *безпекове середовище* – геополітична, політико-дипломатична, воєнна, інформаційна та інші сфери, де зароджуються, існують, накопичуються або проявляються сприятливі умови або небезпечні явища, потенційні та реальні загрози реалізації національних інтересів, у яких держава реалізує свою політику національної безпеки, взаємодіє з міжнародними структурами безпеки,

стратегічними партнерами, союзниками, військово-політичними та іншими інститутами та організаціями в інтересах забезпечення свого сталого розвитку в певному часовому інтервалі.

Для оцінювання безпекового середовища у системі забезпечення НБ організовується й проводиться комплексний моніторинг викликів і загроз. Під моніторингом викликів і загроз (небезпек) слід розуміти постійне, спеціально організоване, систематичне спостереження для виявлення явищ і чинників, які утруднюють або роблять неможливою реалізацію національних інтересів у певних сферах НБ держави [8].

Для інформаційного забезпечення ефективної імплементації національних інтересів даних моніторингу недостатньо. Необхідна кваліфікована аналітична обробка інформації, яка циркулює у безпековому середовищі, але не фіксується під час моніторингу. Для обробки цієї інформації необхідний відповідний методичний інструментарій, в основу якого покладена Методика оцінювання зовнішнього безпекового середовища [8], структурна схема якої наведена на рис. 1. Методика складається з 14 основних блоків, у яких викладено порядок здійснення аналітичних, логічних, експертних, порівняльних та інших процедур з інформацією, отримуваною з аналізу безпекового середовища, стосовно умов, у яких відбувається імплементація національних інтересів, деструктивних процесів, явищ, небезпек, загроз тощо. Однак у зазначеній методиці висвітлено лише порядок проведення процедур, практична їх реалізація залишилась поза увагою.

У контексті вирішення зазначеного питання авторами пропонується, на основі проведеного аналізу дій Російської Федерації (РФ) під час анексії Автономної республіки (АР) Крим та подій на сході України, новий підхід, який дає змогу:

своєчасно виявляти виклики та загрози на основі проявлення відповідних моніторингових ознак певних подій і процесів у відповідних сферах НБ;

оцінювати їх характер, рівень і масштаб;

відстежувати глобальні та локальні процеси, тенденції розвитку обстановки в окремих регіонах та у світі в цілому;

виявляти явища і чинники, які утруднюють або роблять неможливою реалізацію національних інтересів у певних сферах НБ держави;

прогнозувати сценарії реалізації виявлених загроз і небезпек.

Для розроблення зазначеного підходу були проаналізовані погляди воєнно-політичного керівництва провідних країн світу щодо ведення гібридних війн, досвіду застосування нетрадиційних форм і методів ведення війн такого формату, характерних ознак технологій їх застосування, а також досвід ведення збройного конфлікту під час російської агресії [9–13].

У контексті збройної агресії РФ на сході України особливу увагу привертає бачення воєнно-політичного керівництва РФ щодо нових форм і способів застосування збройних сил у сучасних збройних конфліктах. Офіційні погляди на базові принципи сучасної стратегії і тактики за російською Моделлю гібридної війни були сформульовані начальником Генерального штабу Збройних сил РФ генералом армії В. Герасимовим у 2013 році [9].

Серед ключових складових цієї моделі необхідно відмітити збільшення ролі невоєнних методів впливу на противника, передусім за допомогою політичних (дипломатичних), економічних, інформаційних, гуманітарних заходів тощо. При цьому інформаційна складова визначається як основа діяльності на всіх етапах конфлікту – від його підготовки до постконфліктного періоду. Належна увага в ній також приділяється асиметричним заходам, якими є діяльність підрозділів спеціального призначення, підтримка внутрішньої опозиції і колабораціоністів, а також збільшення цілеспрямованого інформаційного впливу на об’єкт нападу.

Саме на основі цих принципів були сплановані та реалізовані агресія проти України, операція з анексії АР Крим та конфлікт на сході України.

Етапами російської Моделі гібридної війни визначені:

інноваційна агресія (кібервійна, економічний тиск, інформаційно-психологічні атаки та ін.);

дестабілізація обстановки – виникнення збройного конфлікту (застосування нерегулярних збройних формувань, приватних військових компаній, партизанських рухів, терористів);

переростання збройного конфлікту у воєнний конфлікт (офіційні воєнні дії або демонстрація сили).

Проведений аналіз російської Моделі гібридної війни вказує на те, що події під час операції з анексії АР Крим та збройної агресії на сході України повністю відповідають її етапам.

Для врахування всіх відомих особливостей гібридної війни РФ проти України розроблена Модель застосування військової сили проти України (табл. 1).

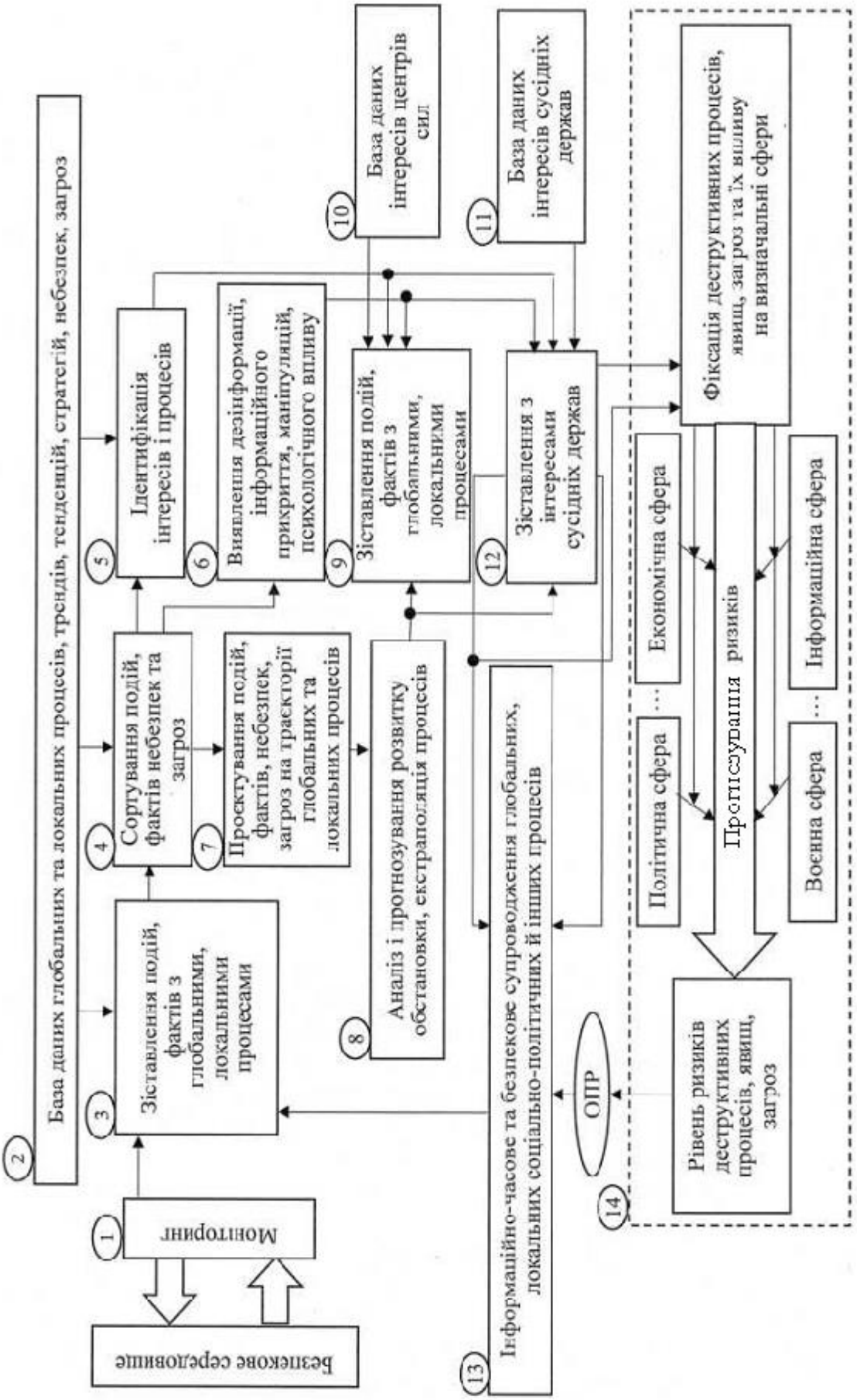


Рис. 1. Структурна схема методики оцінювання безпекового середовища.

Таблиця 1

Модель застосування військової сили проти України

<table>
<tr><td colspan="2" rowspan="2">Вісь “А”
Вісь “В”</td><td colspan="13">Етапи застосування військової сили</td></tr>
<tr><td colspan="4">“Прихований” (у гібридному варіанті)</td><td colspan="2">“Гуманітарна інтервенція”</td><td colspan="7">“Відкритий”</td></tr>
<tr><td></td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td></tr>
<tr><td rowspan="4">Сфери прояву моніторингових ознак</td><td rowspan="4">Приховане зародження конфлікту.

ВПО стає небезпечною, хоча безпосередньої воєнної загрози внутрішнього вибуху немає і стратегічна стабільність зберігається.</td><td rowspan="4">Загострення напруженості і наявність ознак початку конфронтації, яка супроводжується різкими політичними заявами і демонстрацією воєнної сили.</td><td rowspan="4">Поглиблення конфронтації, сторони переходять до провокацій, але від прямого застосування військової сили утримуються. Наростання протиріч, хоча воєнно-стратегічна обстановка може в цілому бути ще відносно стабільною.</td><td rowspan="4">Кризовий стан, безпосередня воєнна загроза (внутрішній вибух), що в більшості випадків веде до втрати стратегічної стабільності.</td><td>Миротворча операція “Розділення протиборчих сторін”</td><td>Миротворча операція “Примушення до миру”</td><td colspan="7">Відкрита агресія.
Наступальна операція</td></tr>
<tr><td>За мандатом ООН, ЄС ОБСЄ</td><td>За мандатом СНД, ОДКБ</td><td rowspan="3">Вищі органи державного і військового управління</td><td>Стратегічні ядерні сили (компоненти ЗС)</td><td colspan="5">Сили загального призначення (угруповання ЗС)</td></tr>
<tr><td>Пропозиції від країн-постійних членів РБ ООН</td><td>Країни-ініціатори</td><td>ВПС/ПКС</td><td>ВМС/ВМФ</td><td>РВСП</td><td>СВ</td><td>ВПС/ПКС</td><td>ВМС/ВМФ</td></tr>
<tr><td>Росія, Китай, Франція</td><td>Росія, Білорусь, Вірменія</td><td>Функціонують в режимі воєнного стану</td><td>Проводять заходи з демонстрації військової сили поблизу ДКУ</td><td colspan="5">Переходять від провокаційних акцій до превентивних дій проти ЗС України</td></tr>
<tr><td colspan="7">Заходи Росії зі створення “антиукраїнської” коаліції</td><td></td><td></td><td colspan="5"></td></tr>
<tr><td>Політична</td><td></td><td></td><td></td><td></td><td colspan="2" rowspan="5">Ознакове поле</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Економічна</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Інформаційна</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Воєнна</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Інші</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

Її побудова здійснювалась на основі аналізу, систематизації та трансформації наявної інформації:

вивчались та аналізувались офіційні погляди російського воєнно-політичного керівництва на базові принципи сучасної стратегії і тактики гібридної війни;

відбиралась та систематизувалась за сферами прояву достовірна інформація стосовно заходів з підготовки РФ до розв'язання гібридної війни;

визначались моніторингові ознаки з підготовки до розв'язання гібридної війни проти України.

Розроблена Модель застосування військової сили проти України передбачає створення єдиного інформаційного простору, подібного до системи координат (з осями "А" і "В"), яка відображає російську Модель гібридної війни (за етапами виникнення, нарощування і реалізації воєнної загрози для нашої держави), ознакове поле, яке складається із нумерованих сегментів для кожного етапу, сфер прояву моніторингових ознак.

На осі "А" розміщені етапи гібридної війни:

перший – "Прихований" і передбачає ескалацію конфлікту до стану кризи (розділи 1–4);

другий – "Гуманітарна інтервенція". На цьому етапі передбачена загроза поширення конфлікту від локального рівня до регіональної війни, для запобігання яким послідовно започатковуються миротворчі операції "Розділення протиборчих сторін" та "Примушення до миру" (розділи 5–6). У цих розділах припускається можливість започаткування офіційної військової присутності на території України, а саме: розгортання пунктів примирення ворогуючих сторін за участю військовослужбовців і команд від ЗС держави агресора, діяльність яких також будуть забезпечувати приватні військові компанії. Така форма застосування військ розглядається як елемент гуманітарних операцій, зокрема в Сирії, а реально це додатковий спосіб започаткування і поширення російської військової присутності в зонах конфліктів на іноземних територіях;

третій – "Відкритий". Найбільш ймовірний у разі відсутності результатів миротворчих операцій, які проводитимуться на території держави-мішені. Цей етап деталізований у розділах 7–13, головним змістом яких є підготовка і проведення ЗС класичної наступальної операції на території держави-мішені.

На осі "В" розміщені сфери прояву моніторингових ознак: економічна, політична, воєнна, інформаційна.

На пересіченні осей "А" та "В" сформовано ознакове поле.

Як вихідні дані для оцінювання безпекового середовища застосовуються активовані сегменти ознакового поля з усіх сфер прояву моніторингових ознак.

У кожному сегменті відображаються моніторингові ознаки (деструктивні явища, чинники і загрози воєнного та гібридного характеру), які раніше вже були отримані та можливі потенційні (прямі, опосередковані, комплексні, загальні та індивідуальні), які вже проявилися чи можуть проявитися у відповідних сферах і характеризуватимуть наміри (дії) протилежної сторони за відповідними етапами (розділами) застосування військової сили проти України згідно з моделлю.

Формат моніторингової ознаки передбачає обов'язкове визначення конкретних суб'єктів (об'єктів моніторингу), від яких отримана ця ознака, або про яких згадується в ній за поточним часом і відміткою про належність до протилежної сили за відповідним індексом. Моніторингові ознаки формуються на основі параметрів (характеристик) об'єктів моніторингу, які можна визначити (виміряти) і використовувати для їх розпізнавання, визначення стану, характеру діяльності, а також прогнозування напряму розвитку (прогнозування) подій.

У всіх сегментах суб'єкти і об'єкти моніторингу розглядаються як "об'єкти моніторингу", а в активованих сегментах вони вже вважаються як "виявлені". Окрім цього, шляхом позиціонування сегментів ознакового поля, які активовані за певний період часу або у поточному режимі, відповідно до осей "А" і "В" створюються два сектори (рис. 2): "С" (ліворуч лінії проєкції на вісь "А" і вище лінії проєкції на вісь "В") та "D" (праворуч лінії проєкції на вісь "А" і нижче лінії проєкції на вісь "В").

Призначення зазначених секторів наступне: за кількістю активованих сегментів ознакового поля у секторі "С" оцінюється стан виконання завдань моніторингу та проводиться аналіз ефективності дій сил і засобів моніторингу. Сегменти ознакового поля, які не активовані у зазначеному секторі, визначають завдання з моніторингу. Відсутність активації сегментів ознакового

поля в секторі “С” свідчить про те, що противник проводить заходи підготовки до застосування військової сили проти України приховано і досить вдало або організація їх моніторингу має певні недоліки. Суб’єкти (об’єкти моніторингу) у сегментах ознакового поля сектору “D” застосовуються під час визначення завдань моніторингу і оцінювання (прогнозування) обстановки.

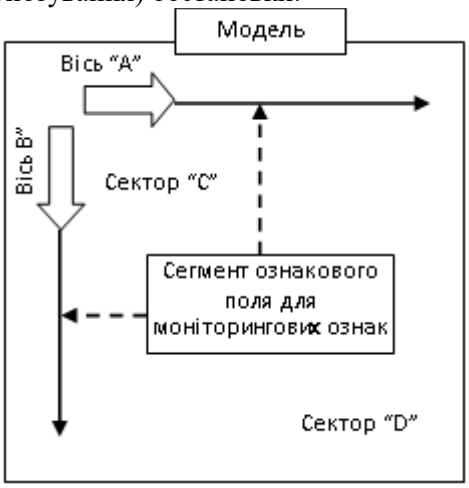


Рис. 2. Формування секторів “С” і “D”

Оцінювання (прогнозування) обстановки здійснюється за такими показниками (намірами (діями) протилежної сторони): масштаб, тривалість, об’єкт і наслідки.

Масштаб впливу визначається обсягом (розмахом) негативного впливу на національні інтереси України, який виникає (може виникнути) внаслідок їх реалізації.

Тривалість впливу – період (час), протягом якого наміри та дії протилежної сторони негативно впливатимуть на національні інтереси України.

Об’єкт впливу – оцінюється за важливістю об’єкта впливу, на який спрямовуються наміри (дії) протилежної сторони, визначається місцем та роллю цього об’єкта для забезпечення національних інтересів України.

Можливі наслідки впливу намірів (дій) протилежної сторони визначаються результатом (заподіяною шкодою, завданими збитками), який може бути.

Використовуючи відповідну шкалу, аналітик, на основі наявної інформації, надає кожному наміру (дії) числове значення за показниками масштабу, тривалості, об’єктів і наслідків впливу.

Висновок. Використання розробленої Моделі застосування військової сили проти України, як практичної реалізації Методики оцінювання зовнішнього безпекового середовища, дає змогу:

виявляти ознаки підготовки до застосування військової сили проти України з боку іноземних країн (воєнно-політичних блоків) у *прихованій* та відкритій формах в усіх сферах на основі проявлення відповідних моніторингових ознак;

у поточному режимі оцінювати рівень воєнної загрози;

відстежувати глобальні та локальні процеси, тенденції розвитку обстановки в окремих регіонах та у світі в цілому;

виявляти явища і чинники, які ускладнюють або роблять неможливою реалізацію національних інтересів у певних сферах НБ держави;

прогнозувати сценарії реалізації виявлених викликів і загроз.

Напрямом подальших досліджень є розвиток (удосконалення) методів (методик) та способів щодо пошуку та виявлення (ідентифікації) джерел гібридних загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Богданович В. Ю., Свида І. Ю., Скулиш Є. Д. Теоретико-методологічні основи забезпечення національної безпеки України : монографія у 7 т. Т. 1 : Теоретичні основи, методи й технології забезпечення національної безпеки України / за заг. ред. Є. Д.Скулиша. Київ : НА СБ України, 2012. 548 с.
2. Методика оцінювання зовнішнього безпекового середовища / В. Ю. Богданович, А. М. Сиротенко, О. В. Дублян, О. В. Дейнега // Збірник наукових праць ЦНДІ ЗС України. Київ, 2019. № 2 (88). С. 30–37.
3. Богданович В. Ю., Дублян А. В., Передрий А. В., Прима А. М. Граф-модель гибридной агрессии государства-инициатора против выбранного государства-мишени // SDirect24 : межд. науч. журнал. Варшава, 2020. № 1 (12).
4. Леонов В. В., Ворович Б. О. Парадокс асиметрії в сучасних міжнародних збройних конфліктах. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2016. № 1. С. 29–34.
5. Богданович В. Ю., Висідалко А. Л. Методика автоматизованого моделювання експертно-аналітичних сценаріїв виявлення та усунення загроз реалізації національних інтересів. *Наука і техніка Повітряних сил Збройних Сил України*. Харків, 2015. № 3 (20). С. 21–29.
6. Кобко Є. В. Моніторинг загроз національній безпеці держави: зарубіжний досвід та українські реалії публічно-правового забезпечення. *Науковий вісник Національної академії внутрішніх справ*. Київ, 2018. № 1 (106). С. 122–133.
7. Балик І. В. Удосконалення математичного апарату визначення рівня воєнної загрози. *Наука*

і техніка Повітряних Сил Збройних Сил України. Харків, 2020. № 3 (40). С. 7–12.
8. Методологія комплексного використання військових і невійськових сил та засобів сектору безпеки та оборони для протидії сучасним загрозам воєнній безпеці України : монографія ; вид. 2-ге, розширене та доповнене / В. Ю. Богданович, І. С. Романченко, І.Ю. Свида, А. М. Сиротенко, О.В. Дублян. Київ : НУОУ імені Івана Черняховського, 2021. 364 с.
9. Герасимов В. В. Основные тенденции развития форм и способов применения ВС, актуальные задачи военной науки по их совершенствованию: доклад. *Военно-промышленный курьер*. Київ, 2013. № 8 (476).
10. Бертош А. Гибридные войны в стратегии США и НАТО. *Независимая газета – 2014*. URL: http://nvo.ng.ru/concepts/2014-10-10/1_nato. html. (дата звернення: 10.10.2020).
11. Арзумян Р. В. Кромка хаоса. Сложное мышление и сеть: парадигма нелинейности и среда безопасности XXI века. Москва : Регнум, 2012. 600 с.
12. Євген Магда. Майбутнє безпекове середовище 2030. URL: http://fpp.com.ua/majbutnye-bezpecove-seredovyshhe-2030/ (дата звернення: 16.11.2020).
13. Максименков И. А., Богданов А. С. Современные подходы к информационно-аналитической деятельности по выявлению гибридных угроз. *Военная мысль*. 2021. № 5. С. 42–49.

Стаття надійшла до редакційної колегії 29.07.2021

The approach to estimate security environment in modern conditions of armed struggle

Annotation

One of the special features of the development of the security environment at the beginning of the 21st century is the shifting the focus in armed struggle to the asymmetric use of military force. More and more frequently, the focus of struggle methods is shifting to the complex usage of political, economic, informational-psychological, humanitarian and other non-military methods, which are provoking the changes in the nature of armed struggle and making higher demands to the military security system.

There is an important issue for national security, in such conditions. For instance, timely manner identification of challenges and threats to the military security of state, which is carried out by results of analyzing the security environment and by estimating their characters, levels, scale and by predicting of possible loss (damage) in case of their realization.

The paper reports on research results on how to estimate the security environment in modern conditions of conducting armed struggle. The proposed approach is a practical realization of estimating the external security environment methodic. It based on the Model of applying of military force against Ukraine. It designed as a system of coordinates with certain axes, on which are represented: the Model of hybrid warfare of the Russian Federation (for the stages of emergence, build-up and realization of military threats against our state of Ukraine), field of signs threats and manifestation of monitoring signs threats.

The usage of the developed Model allows: to identify signs of preparation for the application of military force against Ukraine by other states (military-political blocks) in covert and overt forms in all areas based on manifestation of monitoring signs threats; in a current situation to estimate the level of military threats; to monitor global and local operational environment, trends in the development of the operational environment in unstable regions and in the world in general; to monitor the level of military threat in all areas that complicate or make impossible the realization of national interests in certain areas of national security; to predict scenario of the military threats.

Keywords: national security; security environment; monitoring of security environment; information and analytical support; monitoring signs threats.

УДК 355/359.07 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/40-50

Сніцаренко П. М., д-р техн. наук, ст. наук. співроб. (0000-0002-6525-7064)
Саричев Ю. А., канд. техн. наук, ст. наук. співроб. (0000-0003-1380-4959)
Ткаченко В. А., канд. військ. наук (0000-0002-9625-2434)
Зубков В. П. (0000-0003-1616-2795)

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

Досвід збройних сил провідних країн світу в інтересах удосконалення інформаційного забезпечення Збройних Сил України

Резюме. У статті аналізується досвід упровадження інформаційних систем для управління збройними силами провідних країн, особливості їх організації та здійснення в арміях держав – членів НАТО. За результатами цього аналізу пропонуються підходи до визначення шляхів удосконалення інформаційного забезпечення систем управління Збройних Сил України.

Ключові слова: інформаційні системи; системи управління; мережецентрична війна.

Постановка проблеми. Сучасні збройні конфлікти характеризуються посиленням ролі політичних, економічних, екологічних та особливо інформаційних засобів під час підготовки і воєнного протистояння, перетворенням сухопутного, повітряного, космічного, морського та інформаційного просторів у єдиний театр воєнних дій. До того ж постерігається швидкоплинність воєнних дій, які можуть поширюватися на всю територію держав-суперниць. Набирає обертів тенденція до "безконтактних" та асиметричних бойових дій, зосередження зусиль на виведенні з ладу "критичних центрів" противника, насамперед, органів політичного та військового керівництва, об'єктів, які мають стратегічне значення для економіки та безпеки держави.

Усе це створило передумови докорінного перегляду характеру майбутніх операцій (бойових дій), які все більше набувають інформаційно-технологічного характеру в усіх сферах воєнних дій та змусило керівництво провідних держав світу переглянути теорію і практику військового будівництва. Саме тому, із врахуванням змін характеру війн і воєнних конфліктів, продовжується масштабне реформування збройних сил провідних країн світу, спрямоване, зокрема, на структурні та функціональні зміни в системах їх управління, що тісно пов'язане з удосконаленням процесів інформаційного забезпечення.

Аналіз публікацій показує, що на сьогодні активно досліджується проблематика формування майбутнього обрису Збройних Сил України (ЗС України) за досвідом держав – членів Альянсу. Зміст концепцій і планів будівництва та розвитку збройних сил країн світу показує, що удосконалення системи управління військами (силами) відноситься до пріоритетних напрямів [1, 2]. Водночас, досвід участі збройних сил провідних країн світу в операціях кінця XX – початку XXI століття визначив основною тенденцією розвитку теорії і практики управління військами – розроблення та впровадження концепції мережецентричних війн (Net-Centric Warfare – NCW) [3–9]. У цих публікаціях стверджується, що мережецентрична війна – війна, у якій досягнення успіху забезпечується на основі інформаційної переваги над противником за допомогою об'єднання військових об'єктів у *єдину інформаційну мережу* [10].

У наведених виданнях досліджуються в основному принципові завдання побудови автоматизованих систем управління для реалізації концепції мережецентричних війн [9]. Водночас, у них не достатньо уваги приділяється саме інформаційному забезпеченню таких систем. Без актуальної інформації будь-яка автоматизована система не спроможна виконати функціональні завдання за призначенням. До того ж інформаційна перевага може бути досягнута своєчасним інформаційним забезпеченням процесу прийняття рішень та дій на всіх рівнях системи управління військами (силами). Отже питання інформаційного забезпечення сучасних систем управління у воєнній сфері набуває найважливішого значення.

Метою статті є обґрунтування підходів до визначення напрямів (шляхів)

удосконалення інформаційного забезпечення системи управління ЗС України на підставі досвіду побудови та використання інформаційних систем для управління збройними силами провідних країн світу. У статті позначені лише основні контури розвитку систем в умовах підготовки до ведення принципово нових війн XXI століття.

Виклад основного матеріалу. Наприкінці XX століття американськими військовими аналітиками було проведено дослідження характеру воєн і воєнних конфліктів у світі, починаючи з XVI століття. Війна майбутнього видається не тільки як високотехнологічна війна, а, насамперед, як "мережева" війна, що потребує об'єднання всіх учасників бойових дій, надання точних і своєчасних даних про обстановку на полі бою в реальному масштабі часу для забезпечення упереджувального ураження об'єктів противника [11].

Водночас, однією з найбільш поширених помилок є думка про те, що механічне об'єднання органів управління військових формувань усіх рівнів інформаційною мережею дасть змогу вирішити проблеми стійкості та надійності керівництва військами (силами). Такі мережі, як і всі комп'ютерні системи, працюють за принципом "сміття на вході – сміття на виході", тобто це принцип програмування, відповідно до якого невірні вхідні дані не можуть привести до правильного кінцевого результату. Отже, без точних об'єктивних даних актуальної інформації, якими наповнюють мережі, самі собою ці мережі залишаються не більше ніж високошвидкісними цифровими трактами обміну інформацією між об'єктами.

Саме для мережевого принципу забезпечення військ (сил) точною та своєчасною інформацією і проводиться реформування збройних сил провідних країн світу, а також реалізуються нові принципи управління і ведення бойових дій, передбачені перспективними "мережецентричними" концепціями.

На сьогодні поняття інформації має багато визначень. Для воєнної сфери доцільно вважати, що узагальнено під *інформацією* розуміються оброблені та осмислені дані (відомості), тобто їх змістовність, значення (сутність), знання або висновки, отримані на їх основі незалежно від форми подання [12]. При цьому цінність інформації визначається корисністю та її здатністю забезпечити певного суб'єкта необхідними умовами для досягнення ним поставленої мети.

Слід зауважити, що за законами кібернетики [13] будь-яка функція управління в системах реалізується виключно інформаційним шляхом, а тому зрозуміло, що процес всякого управління, а у воєнній сфері особливо, потребує реалізації низки інформаційних процесів, що мають вплив на усі елементи механізму управління. Сукупність цих інформаційних процесів власне і об'єднується поняттям *інформаційного забезпечення*, яке пронизує замкнений контур управління, а його сутність полягає, з одного боку, у формування завдань та їх донесення від органу управління до суб'єктів системи, а з іншого – у можливості отримання органом управління зворотної інформації для контролю процесу управління та коригування інформаційного впливу. Зазначене узагальнюється доречними визначеннями, наведеними у Військовому стандарті [12].

Інформаційне забезпечення (у воєнній сфері) – сукупність заходів органів військового управління усіх рівнів, дій військ (сил) та інших суб'єктів інформаційної діяльності з метою створення (формування) і використання в інформаційному просторі воєнної сфери необхідних інформаційних ресурсів для реалізації процесів управління в інтересах оборони держави.

Інформаційний простір воєнної сфери – частина інформаційного простору держави: середовище, у якому відбуваються інформаційні процеси та інформаційні відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації (інформаційних продуктів, інформаційних ресурсів) воєнного характеру.

Невід'ємними складовими інформаційного середовища є інформаційні ресурси, інформаційна інфраструктура та інформаційні технології, що становлять сутність національного інформаційного потенціалу.

Інформаційний ресурс – дані та знання, відмінною і невід'ємною характеристикою яких є їхня прагматична цінність, що визначається практичними потребами в інтересах вирішення певних завдань.

Інформаційна інфраструктура – сукупність різноманітних інформаційних (автоматизованих) 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.

Нині саме рівень інформаційного потенціалу, в основі якого лежить інформаційний ресурс, що продукується елементами інформаційної інфраструктури, та можливість його ефективного, зокрема автоматизованого, використання, все більшою мірою зумовлює високу оперативність та якість прийняття рішень, необхідні структуру і характеристики органів управління, зразків озброєнь, оцінку рівня їх достатності, у цілому з великою ймовірністю визначає результат збройного протистояння.

Принципи ведення воєнних дій, будівництва збройних сил і управління бойовими формуваннями в XX столітті, в епоху "індустріальної ери", серед військових фахівців отримали найменування "платформоцентричні" (Platform-Centric Warfare). Тим часом успіх операцій (боїв) залежав, здебільшого, від індивідуальних можливостей бойових засобів, а об'єднання мережами, хоча і передбачалося, але не давало змоги домогтися ефекту, який дають нові інформаційні технології [9].

У сучасну епоху "інформаційної ери" (*Information Age, Digital Age, Computer Age*) на перше місце виходять нові інформаційні технології. Їх впровадження у військову сферу також спрямовано на підвищення бойових можливостей формувань, але вже не тільки через підвищення розвідувальних, вогневих, маневрених та інших характеристик індивідуальних зразків (платформ), але, насамперед, завдяки наявності кращого інформаційного забезпечення та можливості скорочення циклу бойового управління в операції (бою) [14].

Об'єднання мережею охоплює не тільки системи бойового управління, зв'язку, обчислювальної техніки, розвідки і спостереження, а й бойові платформи, і насамперед такі, як носії засобів вогневого ураження. Це і визначає формування нової системи поглядів на форми і способи ведення збройної боротьби. Тому найімовірніше, що у 2020-х збройні сили провідних країн світу повністю перейдуть від "платформоцентричних" до "мережецентричних" операцій, що передбачають отримання нових можливостей формувань від об'єднання різноманітних платформ в єдиний бойовий інформаційно-комунікаційний простір.

Поняття "мережецентрична війна", або "ведення бойових дій в єдиному інформаційно-комунікаційному просторі", розглядає елементи збройних сил як пристрої, підключені до мережі. Залежно від вибору мережевої архітектури і її типу засобами мережі можуть бути військові частини та підрозділи, кораблі, літаки, засоби ураження, органи управління, зв'язку, розвідки, а також комбінація і тих, і інших. Можливості таких бойових одиниць визначаються не стільки індивідуальними характеристиками, скільки можливостями всієї групи підключених до мережі засобів, як єдиного цілого.

За розрахунками спеціалістів, автоматизація процесів збору, оброблення, узагальнення, передавання (приймання), використання інформації може сприяти підвищенню бойових можливостей військ (сил) на 15–20 % і водночас на 50 % скоротити час, який витрачають органи військового управління всіх рівнів на прийняття рішень і доведення завдань до підлеглих [15].

Забезпечення всебічної інтеграції, підвищення рівня взаємодії завдяки реалізації принципів нових мережецентричних концепцій та інтеграції систем управління, зв'язку, розвідки і ураження стає все більш актуальним і пріоритетним напрямом реформування збройних сил більшості країн світу.

Загалом, заходи з питань упровадження мережецентричних концепцій в основному здійснюються в трьох ключових напрямах:

розроблення систем отримання, обробки, аналізу і розподілу інформації, що використовують уніфіковані інструментарії її обробки і формати передання;

розгортання сучасних систем зв'язку і передання даних;

оптимізації організаційних структур органів управління, обробки та аналізу інформації, підготовка особового складу та перегляд доктринальних документів.

Відомо, що у ***НАТО*** реалізується концепція "Комплексні мережеві можливості" (NATO Network Enabled Capabilities – NNEC), яка призначена для організації взаємодії високотехнологічних формувань національних збройних сил у збройних конфліктах [9, 16, 17]. Її реалізація дасть змогу здійснювати ефективне інформаційне забезпечення операцій всього можливого спектру, починаючи від миротворчих операцій зі встановлення миру до великомасштабних бойових дій високої інтенсивності. Водночас, військові фахівці НАТО підкреслюють, що NNEC – це не тільки інтеграція систем управління і зв'язку,

а й можливість підвищити рівень інформаційної взаємодії всіх учасників операції (бойових дій), зокрема і засобів ураження, органів і пунктів матеріально-технічного забезпечення.

У ***США*** сутність поняття "мережецентрична війна", "ведення бойових дій у єдиному інформаційно-комунікаційному просторі", зважаючи на досвід застосування військ (сил) у сучасних конфліктах, набула найбільшого практичного наповнення у єдиній системі розвідувально-інформаційного забезпечення і бойового управління ЗС США – "Мережецентрична війна" (Network Centric Warfare – NCW) [9, 16].

Тим часом у ***Великобританії*** формується власна інформаційна інфраструктура (Network Enabled Capability), що являє собою єдину інформаційно-керуючу мережу, зі спеціалізованими системами забезпечення безпеки і єдиним сімейством програмного інструментарію. У майбутньому можливості інформаційної інфраструктури планується розширити для організації взаємодії та забезпечення доступу до інформаційних ресурсів збройних сил союзників: США, Канади, Австралії та Нової Зеландії [9, 16, 17].

У ***Франції*** такі заходи реалізуються також у межах мережецентричної концепції (Інформаційно-центрична війна (Guerre Infocentre), яка, здебільшого, акцентує увагу на інформаційних потоках, а не самих мережах, як прийнято у США [16]. Розгорнуті командно-інформаційні системи рівня С2: у сухопутних військах – для дивізій, полків, артилерії, протиповітряної оборони, ВПС – для управління повітряними операціями, у ВМС тактичні системи встановлені на авіаносцях та фрегатах [9, 17].

У ***ФРН*** також працюють над створенням перспективної системи "Піхотник майбутнього" (Infanterist der Zukunft), для реалізації нових принципів інформаційного забезпечення та зв'язку між бойовими формуваннями і вищими органами управління. Заходи включають розроблення перспективних засобів розвідки, комп'ютерних систем, військових систем управління та зв'язку типу "тактичний інтернет", що дасть змогу організувати взаємодію між аналоговими засобами зв'язку та цифровими системами передавання даних [9, 17, 18].

Крім того, вперше в світовій історії дві держави, ФРН і Нідерланди, домовилися щодо об'єднання в єдине ціле своїх оборонних інформаційних мереж. Нова єдина система стане називатися "Tactical Edge Networking" (TEN). Вона буде пробною версією для об'єднання в подальшому оборонних інформаційних мереж інших держав Північноатлантичного Альянсу [19].

Ізраїль також розглядає впровадження інформаційних технологій як невід'ємний і обов'язковий атрибут сучасних і майбутніх операцій [16].

Китай серйозно ставиться до мережецентричної концепції інформаційного забезпечення управління і ведення бойових дій. У документах Національно-визвольної армії Китаю (НВАК) зустрічається термін "інтегрована мережева і електронна війна" (Integrated Network-Electronic Warfare- INEW) [9, 20].

В ***Австралії*** в межах концепції "Мережецентрична війна" (Network Centric Warfare) розробляються нові засоби добування інформації, впроваджуються перспективні інформаційні технології, проводяться випробування безпілотних і роботизованих комплексів і систем для того, щоб зробити свої нечисленні збройні сили більш ефективними. Проводиться тестування перспективних мережевих засобів зв'язку і передавання даних, які повинні дати змогу одному оператору здійснювати управління угрупованням робототехнічних засобів, здатних також виходити з мережі і діяти самостійно в цілях збору розвідувальної інформації або нанесення ударів по виявлених об'єктах і цілях [16].

Керівництво збройних сил ***Російської Федерації*** розробляє практичні заходи переходу до управління військами за "мережецентричним" принципом, розглядаючи міжвидове (об'єднане) угруповання військ (сил) як набір елементів мережі, а її застосування, залежно від обраного варіанта дій, як багатоваріантна комбінація дій елементів мережі (бойових формувань). Вважається, що можливості таких бойових формувань визначатимуться не стільки індивідуальними характеристиками, скільки можливостями всієї групи підключених до мережі засобів як єдиного цілого, а успіх у таких умовах залежатиме від ступеня об'єднання всіх учасників операції (бойових дій) у єдиний інформаційно-комунікаційний простір [9, 21].

Очевидно, що головними принципами реалізації заходів щодо широкого впровадження інформаційних складових у

воєнну сферу в межах концепції мережецентричних операцій є:

забезпечення реальної інформаційної об'єднаності угруповань;

застосування відкритої архітектури і модульної побудови сучасних систем і комплексів збройної боротьби;

здійснення вертикальної і горизонтальної інформаційної інтеграції та взаємодії всіх учасників операції (бойових дій).

Аналітиками стверджується [9], що війни наступного покоління – це, насамперед, війни розвідок, де володіння необхідною інформацією про противника є ключем до досягнення успіху в таких війнах. В сучасних умовах у провідних країнах світу проглядається стійка тенденція щодо акцентування уваги на здобуванні та інтеграції різноманітної інформації про стан політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших відносин між державами, групами держав та й у світі в цілому.

Отже, такий вид інформаційного забезпечення як моніторинг противника, в основі якої процес всебічної розвідки, є домінуючим у загальній системі інформаційного забезпечення військ (сил). До того ж, будь-яку мережецентричну систему неможливо використовувати за призначенням без актуальної інформації у реальному масштабі часу. Залежно від рівня мережецентрична система за наявністю повної, достовірної, своєчасної, потрібної розвідувальної інформації спроможна наочно відображати обстановку, оцінювати місцевість, стан противника і своїх військ (сил), моделювати розвиток бойових дій, виробляти рекомендації, варіанти рішень, проєкти бойових документів, доводити завдання до підлеглих пунктів управління.

З цією метою військові експерти США [9, 22] вважають за доцільне мати розгалужену структуру збору та постачання розвідувальної інформації для ефективного функціонування мережецентричної системи. Саме тому найбільш розвинута система добування розвідувальної інформації була створена у Сполучених Штатах Америки. Розвідувальне співтовариство Сполучених Штатів включає в себе 16 суб'єктів, серед яких, зокрема, військові структури:

розвідувальне управління міністерства оборони (РУМО) – головний орган, який здійснює свою діяльність в інтересах інформаційного забезпечення прийняття рішень військово-політичним керівництвом країни, а також надає розвідувальну інформацію міністру оборони, комітету начальників штабів (КНШ), об'єднаним командуванням, командуванням видів збройних сил;

агентство національної безпеки – організовує, координує та безпосередньо веде радіо- і радіотехнічну розвідку в глобальному масштабі, а також забезпечує безпеку своїх систем управління та зв'язку;

національне управління геопросторової розвідки – надає своєчасні і точні дані видової розвідки, метеорологічної, океанографічної та іншої інформації, керує силами і засобами видової розвідки національного рівня;

національне управління повітряно-космічної розвідки – здійснює розроблення та управління розвідувальними системами космічного базування, збір і обробку видобутої такими системами розвідувальної інформації;

органи розвідки Сухопутних військ (Army), ВПС (Air Force), ВМС (Navy) – у межах компетенції здійснюють розвідувальне забезпечення бойових дій, управління силами і засобами розвідки, участь у розробленні, оснащення підлеглих структур розвідувальної технікою, навчання особового складу.

Невійськові члени співтовариства: центральне розвідувальне управління, управління розвідки і досліджень державного департаменту, федеральне бюро розслідувань, управління аналізу інформації та захисту інфраструктури міністерстві внутрішньої безпеки, органи розвідки Берегової охорони, відділ розвідки і інформаційно-аналітичної діяльності міністерства фінансів, розвідувальний відділ міністерства енергетики здійснюють за своїми напрямами добування інформації, аналіз та формування висновків для керівництва держави, інших державних органів.

Така потужна структура розвідувальних органів США дає змогу вирішувати весь спектр стратегічних, оперативних і тактичних завдань з розвідки, забезпечувати надання своєчасної і достовірної інформації з політичних, військових, технічних, економічних та інших питань не тільки керівництву держави, міністерству оборони та військовим формуванням, але й іншим державним органам країни.

Зауважимо, що поряд із перевагами мережецентричної концепції ведення бойових дій виявлено і низку проблем щодо її

реалізації. Зокрема, гостро постає питання раціонального розподілу та обробки великих обсягів інформації, що надходять до споживачів.

Для ліпшого розуміння цієї проблеми вважаємо за доцільне зупинитися на розподілі класів мережецентричних систем залежно від ступенів автоматизації керованих процесів і потоків інформації, яка в них циркулює.

Досвід розроблення, впровадження та експлуатації мережецентричних систем у США свідчить [9, 23], що сучасні автоматизовані системи управління, які за своєю сутністю є інформаційними, поділяються на декілька класів відповідно від функцій, що виконуються системами – командування, управління, зв'язок, комп'ютери (інформатизація), загальна розвідка, спостереження, розвідка в режимі реального часу (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance).

До того ж, системи різняться за ступенем автоматизації керованих процесів відповідно до цієї класифікації. Кожна система відноситься до конкретного класу відповідно до рівня *автоматизації управлінських функцій.*

Так, якщо система управління в автоматизованому режимі має лише дві функції, наприклад, командування і управління (Command and Control), то відповідатиме класу "СС" (С2).

Якщо в системі автоматизовані чотири функції – командування, управління, зв'язок, інформатизація (Command, Control, Communications, Computers), то таку систему відносять до класу "СССС"(С4).

До того ж, функції, починаючи з буквами "С" використовуються як базові, а інші – додаткові.

З погляду автоматизованих управлінських функцій (завдань), система управління, яка містить у своїй абревіатурі більше букв "С", є більш досконалою. Так, система класу C2SR (Command, Control, Surveillance, Reconnaissance) буде поступатися системі класу С4 за спектром завдань, які використовуються в автоматизованому режимі.

Системи, у яких автоматизовані функції Command and Control (С2), вирішують такі завдання:

відображення та передання бойових завдань підлеглим органам управління (об'єктам управління) у формалізованому текстовому та графічному форматі з використанням єдиної мережі;

визначення положень власних об'єктів управління та оповіщення своїх органів управління і сусідів про їх місцезнаходження з відображенням на електронних картах;

відображення на електронних картах і обмін даними про виявлені об'єкти противника, елементи інфраструктури на полі бою;

відбір і розрахунки маршрутів руху за відомими даними про дорожню мережу та відображення пройденого шляху.

Система С2 дає змогу командиру лише швидко довести прийняте рішення до підлеглих і контролювати хід його виконання. До того ж функції оцінювання обстановки і прийняття рішення повною мірою покладається саме на людину.

Деякі системи, що відносяться до класу С2, можуть виконувати взаємне розпізнавання об'єктів, які знаходяться в системі, за принципом "свій-чужий", а також виконувати ідентифікацію цілей та надавати в автоматичному режимі цілевказівки засобам вогневого ураження, що входять до системи.

Системи управління, у яких автоматизовані такі функції, мають додаткові літери "SR" (Surveillance, Reconnaissance) і позначаються як C2SR (або С2+).

До того ж комп'ютери, які використовуються в системах класу С2, розглядаються тільки як засоби первинної обробки та відображення інформації. Хоча системи С2 і містить у своєму складі ПЕОМ, але слово "Computers" і відповідну літеру в абревіатурі свого класу не мають.

Загалом, система класу С2 лише допомагає командирам доводити до підлеглих завдання, збирати та відображати поточну інформацію про противника та стан своїх об'єктів управління. При цьому, про інтелектуальну підтримку прийняття рішень та про вироблення варіантів рішень на бій і їх моделювання поки ще не йдеться.

Такі завдання, як автоматична організація зв'язку та локальних обчислювальних мереж – це вже відмінність системи, яка має у назві свого класу абревіатуру слова Communications (С3).

Наявність в абревіатурі класу системи четвертої літери "С" (Computers), а також літери "I" (Intelligence) означає, по-перше, повну автоматичну обробку даних, отриманих під час реалізації перших двох "С" – Command and Control, по-друге, вироблення на підставі обробки первинних даних варіанта

ситуаційного рішення командира та його представлення у найзручнішій для людини формі, відповідно.

Системи класу С4 (крім виконання функцій, реалізованих в системах класу С2 і С3), мають бути здатні вирішувати такі завдання:

повна автоматизація збору і обробки інформації;

інформаційна підтримка вироблення командиром варіантів рішення (наявність програм типу "Sketch in the decision" – замисел рішення);

моделювання бойових дій за обраними варіантами виконання бойових завдань з графічним відображенням їх ходу і результатів на електронних картах, зокрема з використанням засобів тривимірного відображення поля бою;

інформаційна підтримка розроблення плануючих документів (програма "Sketch in the plan" (начерк до плану), що здійснює перетворення графічних і аудіоматеріалів у плануючі документи;

інформаційна підтримка прийняття рішень під час виконання бойового завдання (оновлення оцінок і висновків на підставі інформації, отриманої під час бою).

Принципова відмінність систем класу С4І від класу С2 полягає в більш високому ступені автоматизації інформаційних та управлінських завдань.

У збройних силах навіть розвинених технологічно країн системи класу С4І і С4SR за рівнем управління відносяться до систем *оперативної або оперативно-стратегічної ланки.*

Наявні на озброєнні іноземних держав системи тактичної ланки відносяться до класу С2 або С2+ і розрізняються між собою лише невеликим розширенням спектру розв'язуваних завдань. До того ж, усі системи тактичного призначення принципово не досягають навіть класу С3.

На думку військових експертів [22], основними перешкодами на шляху розвитку систем тактичної ланки з класу С2 до класу С3 і С4 є:

відсутність математично коректних алгоритмів оцінки дій військ на тактичному рівні, зважаючи на величезну різноманітність застосовуваних ними способів і прийомів виконання бойових завдань;

складність створення автоматизованої системи збору та оцінки даних тактичної обстановки, з огляду на велику різноманітність її параметрів і швидкоплинність змін (порівняно з оперативною ланкою управління);

необхідність обробки великої кількості даних в одиницю часу, які за своїми обсягами на сьогодні перевищують можливості машинного забезпечення, що використовується в тактичної ланці управління;

складність створення мереж зв'язку і надійних локальних мереж (систем передачі даних) між великою кількістю високомобільних об'єктів управління.

На теперішній час вагомий розвиток систем класу С+ в інтересах реалізації концепції мережецентричних операцій здійснено фахівцями США.

Найбільш відомою з усіх існуючих систем тактичної ланки є американська система класу "C2SR" FBCB2 – Force XXI Battle Command Brigade and Below ("Система управління бригадою та підпорядкованими підрозділами в бою (битві) двадцять першого століття") – один з основних компонентів автоматизованої системи управління сухопутних військ США ABCS (Army Battle Command System), яка зіграла ключову роль в операціях в Іраку і Афганістані [23].

Слід зауважити, що на цьому етапі розвитку ЗС України стан автоматизації управлінських процесів неможливо назвати задовільним. Відповідно до [24] автоматизація діяльності органів військового управління становить лише 10-30 % від потреб, наявні засоби не складають цілісних систем, існуючі інформаційно-розрахункові ресурси відповідають потребам органів управління лише на 12-15 %. До того ж рівень інформатизації систем управління суб'єктів оборони держави порівняно зі збройними силами провідних країн світу становить 2-2,5 %. Водночас слід зауважити, що наявність на пункті управління великих екранів зі значками різних кольорів на електронній топографічній карті не є ознакою високого рівня автоматизації системи управління військами. За роки незалежності в ЗС України, незважаючи на низку спроб, не було створено жодної завершеної інформаційної системи як управління військами (силами), так і оборонними ресурсами [25]. Виявилося, що таке завдання постало надто складним.

Тим часом у цьому контексті вищим військовим керівництвом України визначено бачення щодо розвитку системи управління військами (силами): "… Необхідно побудувати у Збройних Силах України надійну систему зв'язку, автоматизації,

розвідки та спостереження (C4ISR), стійку до зовнішнього впливу, захищену від засобів РЕБ, яка буде мати альтернативні канали зв'язку. Засоби зв'язку повинні бути поєднані із засобами зв'язку країн – партнерів. Необхідно створити інформаційну мережу в інтересах сектору безпеки і оборони держави, яка забезпечуватиме набуття інформаційних спроможностей для отримання, опрацювання, зберігання, передавання, контролю та надання інформації на вимогу командувачів (командирів) та штабів (тактичного, оперативного, стратегічного рівнів) об'єднаних сил" [26].

На нашу думку, робити спробу на створення одразу системи C4ISR – це завдання, яке не відповідає ресурсним можливостям держави. Як приклад, для оптимізації проведених заходів реалізації концепції НАТО "Комплексні мережеві можливості" (NATO Network Enabled Capabilities – NNEC) сформовано спеціальний консорціум NCOIC (96 компаній з 32 країн, 26 з яких є членами НАТО), призначений забезпечити єдність протоколів обробки інформації та координацію зусиль промисловості у виконанні вимог щодо досягнення необхідного рівня взаємодії і інтеграції перспективних систем стосовно забезпечення реалізації мережецентричних принципів управління військовими формуваннями.

Так, за висновками американських аналітиків, жоден з європейських союзників у найближчому майбутньому, швидше за все, не зможе створити повністю мережеву армію. Найбільшим обмеженням для європейських інвестицій у C4ISR є загальні обмеження оборонних бюджетів, а не відсутність адекватної технології [17].

Може бути запозичений також і досвід Китаю, де військові фахівці усвідомлюють, що створити мережецентричну систему, адекватну американській, незважаючи на наявність значного воєнного бюджету, в найближчому майбутньому їм не вдасться. Тому ставка робиться на створення сил, систем і засобів, що забезпечують асиметричну дію на противника – вогнева і електронна поразка елементів інформаційних структур (командних пунктів, вузлів зв'язку, орбітального угруповання супутників розвідки та управління і т. ін.) [27].

З огляду на зазначене, в Україні розроблення С-подібної системи доцільно починати з рівня С2+, з подальшим еволюційним нарощуванням до С3 і вище, зважаючи на результати випробувань, досвіду експлуатації та ресурсних можливостей. Однак слід пам'ятати, що інформаційне забезпечення органів управління є пріоритетним завданням – без інформації будь-яка система управління працює неефективно. Лише за наявністю актуальної інформації система спроможна виконати функціональні завдання за призначенням.

На наш погляд, рівень інформаційного забезпечення військ (сил) в інтересах ситуаційної обізнаності має забезпечувати:

для *тактичного рівня (взвод, рота, батальйон, бригада)* – за допомогою системи типу С2+, з вирішенням таких завдань:

обмін інформацією про положення, виявлені об'єкти противника та його дії в автоматизованому режимі у реальному масштабі часу з відображенням на електронних картах зверху вниз і знизу вгору;

передання бойових завдань підлеглим у формалізованому текстовому та графічному форматі та контроль їх виконання;

визначення положень власних об'єктів управління та оповіщення своїх органів управління і сусідів про їх місцезнаходження з відображенням на електронних картах;

взаємне розпізнавання об'єктів, що знаходяться в системі, за принципом "свій-чужий";

ідентифікація цілей та надання в автоматизованому режимі цілевказівки засобам вогневого ураження;

для *оперативного та стратегічного рівнів* – за допомогою системи типу С3 (надалі – С4 з додатками), яка має бути здатною вирішувати такі завдання:

повна автоматизація збору і оброблення інформації у реальному (близькому до реального) масштабі часу про противника, положення та стан своїх військ (сил);

інформаційна підтримка вироблення варіантів рішень на застосування Збройних Сил, військ (сил), з'єднань та військових частин;

моделювання операцій (бойових дій) за обраними варіантами з графічним відображенням їх ходу і результатів на електронних картах, у тому числі, з використанням засобів тривимірного відображення;

інформаційна підтримка розроблення плануючих документів, перетворення графічних і аудіо матеріалів в плануючі документи;

інформаційна підтримка уточнення рішень у ході операцій (бойових дій).

Отже, досвід провідних країн світу переконливо свідчить, що під час впровадження мережецентричної концепції для систем управління ЗС України головна увага має бути зосереджена на питаннях збору, обробки, аналізу, ототожнення та безпеки інформації для підтримки прийняття рішень керівниками усіх рівнів. До того ж, надання своєчасної актуальної достовірної (релевантної) інформації для систем управління військового призначення постає головним завданням в загальному процесі інформаційного забезпечення ЗС України.

Висновки

1. Діяльність щодо побудови та використання інформаційних систем для управління збройними силами провідних країн світу, насамперед, досвід держав – членів НАТО, викликає нагальну потребу для подальшого пошуку підходів до удосконалення *інформаційного забезпечення* систем управління ЗС України. Мережеву війну можна виграти тільки мережевими засобами, адаптувавши до власних умов і цілій ефективні технології.

2. Концепція мережецентричних війн являє собою систему поглядів на ведення бойових дій та військово-технічне забезпечення в умовах повної комп'ютеризації сил і засобів збройної боротьби. При цьому функціональна сумісність автоматизованих систем розвідки, управління військами та зброєю, а також забезпечення стійкої взаємодії між ними розглядаються як ключові компоненти, необхідні для досягнення *інформаційної переваги* і, як наслідок, переваги у виробленні та прийнятті рішення з метою рішучого упередження противника за всім циклом бойового управління (за принципом "першим побачив – першим вистрілив").

3. Інформаційне забезпечення мережевих структур стає головною і необхідною умовою ефективного функціонування систем управління. Для створення такої структури та єдиного інформаційного простору для користувачів у реальному (близькому до реального) масштабі часу необхідно об'єднання автоматизованими системами всіх сил і засобів добування та генерування інформації.

4. Належне та своєчасне інформаційне забезпечення систем управління військового призначення, як необхідна умова втілення мережецентричних принципів ведення бойових дій, може бути реалізоване в ЗС України впровадженням С-подібної системи автоматизованого управління шляхом її еволюційного розвитку, починаючи з побудови системи класу С2+. У цьому разі, враховуючи великий досвід, набутий збройними силами США щодо розвитку інформатизації воєнної сфери, впровадження у практику теорії мережецентричних операцій, а також той факт, що Україна знаходиться у стані війни, вважаємо за доцільне:

узяти за приклад для впровадження у ЗС України існуючу американську автоматизовану систему управління тактичної ланки класу C2SR – Force XXI Battle Command Brigade and Below (FBCB2) або іншу перспективну автоматизовану систему управління іноземного виробництва;

на першому етапі, як невідкладний захід, розглянути питання щодо закупівлі бригадного комплекту автоматизованої системи управління тактичної ланки для проведення випробувань для визначення доцільності щодо подальшого впровадження у ЗС України;

у разі отримання позитивних результатів порушити питання щодо поетапного оснащення військових частин та підрозділів Сухопутних військ ЗС України перспективними автоматизованими системами управління тактичної ланки іноземного виробництва;

одночасно набутий досвід спрямувати на розроблення вітчизняних (з урахуванням можливостей науки і промисловості України) С-подібних перспективних адаптивних систем управління різних рівнів, сумісних з автоматизованими системами управління збройних сил країн – членів НАТО.

Подальші дослідження доцільно спрямувати на розвиток інформаційного забезпечення ЗС України за допомогою більш чіткого визначення складу, структури та обсягів потоків інформації, які циркулюють у системах управління, обґрунтуванні функціональних складових інформаційного процесу в таких системах, що дасть змогу оптимізувати перелік завдань, які мають виконуватися на кожному етапі циклу управління.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Пащетник О. Д. Аналіз світових тенденцій розвитку автоматизованих систем управління військами і зброєю. *Наука і техніка Повітряних Сил Збройних Сил України*. Харків, 2015. № 2 (19). С. 64–68.
2. Короленко В. А., Синявский В. К., Верещагин С. И. Автоматизация системы управления войсками: на пути от идеи к

решению. URL: https://docplayer.ru/56089435-Avtomatizaciya-sistemy-upravleniya-voyskami-na-puti-ot-idei-k-resheniyu.html. (дата звернення: 28.06.2021).
3. Ільяшов О. А. Тенденції розвитку збройної боротьби у війнах четвертого – шостого поколінь. *Наука і оборона*. 2009. № 3. С.43–48.
4. Савин Л. В. Сетецентричная и сетевая война. Введение в концепцию. Москва : Евразийское движение, 2011. 130 с. URL: https://www.geopolitica.ru/sites/default/ files/ncw.pdf. (дата звернення: 28.06.2021).
5. Гаврилов А. Автоматизированная система сбора, обработки и распределения разведывательной информации СВ США DCGS-A. *Зарубежное военное обозрение*. 2010. № 7. С. 32–40. URL: http://pentagonus.ru/publ/ 122-1-0-1596 (дата звернення: 25.06.2021).
6. Кондратьев А. Реализация концепции “Сетецентрическая война” в ВВС США. *Зарубежное военное обозрение*. 2009. №5. С. 44–49. URL: http://pentagonus.ru/publ/24-1-0-1159 (дата звернення: 25.06.2021).
7. Баулин В., Кондратьев А. Реализация концепции “Сетецентрическая война” в ВМС США. *Зарубежное военное обозрение*. 2009. № 6. С. 61–67. URL: http://pentagonus.ru/publ/26-1-0-811 (дата звернення: 27.06.2021).
8. Кондратьев А. Е. Борьба за информацию на основе информации. *Независимое военное обозрение*. 2008. № 10. URL: https://nvo.ng.ru/concepts/ 2008-10-24/1_info.html. (дата звернення: 27.06.2021).
9. 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 ім. Івана Черняховського, 2020. 248 с.
10. Воєнна доктрина США “Joint Vision 2020”. URL: http://pentagonus.ru/doc/JV2020.pdf. (дата звернення: 28.06.2021).
11. Балахонцев Я., Кондратьев А. Влияние концепции “сетецентрическая война” на эффективность разведывательного обеспечения Вооружённых сил США. *Зарубежное военное обозрение*. 2011. № 2. С. 14–20.
12. Військовий стандарт ВСТ 01.004.004 – 2014 (01) “Інформаційна безпека держави у воєнній сфері. Терміни та визначення” [затверджено наказом начальника Центрального управління метрології і стандартизації Збройних Сил України Озброєння Збройних Сил України – головного метролога Збройних Сил України від 27.02.2014 р. № 1].
13. Винер Н. Кибернетика или управление и связь в животном и машине. Москва : Сов. Радио, 1968. 328 с.
14. Кондратьев А. Е. Общая характеристика сетевых архитектур, применяемых при реализации перспективных сетецентрических концепций ведущих зарубежных стран. *Военная мысль*. 2008. № 12. С. 63–73.
15. Фролов В. С. Структурно-логічна схема Єдиної автоматизованої системи управління Збройних Сил України. *Наука і оборона*. 2012. № 1. С. 15.
16. Молитвин А.О реализации концепции единого информационного пространства НАТО. *Зарубежное военное обозрение*. 2008. № 1. С. 23–27.
17. Adams G., Ben-Ari G., Logsdon J., Williamson R. (2004). European C4ISR Capabilities and Transatlantic Interoperability. The George Washington University.
18. Корчагин С. Автоматизированные системы управления Сухопутных войск Бундесвера. *Зарубежное военное обозрение*. 2013. № 7. С. 47–53. URL: http://factmil.com/publ/strana/germanija/ 41-1-0-266 (дата звернення: 28.06.2021).
19. MILITARYEXP.COM. URL: https:// militaryexp.com/v-evrosoyuze-vpervye-v-istorii-dogovorilis-o-sozdanii-voennoy-vsemirnoy-pautiny (дата звернення: 25.06.2021).
20. Thomas T. L. (2005). Chinese and American network warfare // Joint Force Quarterly, July, 2005.
21. Долгополов А. И еще раз о сетецентрических войнах. *Армейский сборник*. Февраль 2015. № 2. URL: https://sc.mil.ru/files/morf/military/archive/ ac_5_02_2015.pdf. (дата звернення: 25.06.2021).
22. Разведывательное сообщество США // ВПК. 2009. № 22. URL: vpk-news.ru/sites/default/ files/pdf/issue_288.pdf. (дата звернення: 27.06.2021).
23. Американська АСУ військами FBCB2. URL: http://dragon-first-ru.livejournal.com/33339.html; http://defense-update.com/; http: // pentagonus.ru / (дата звернення: 25.06.2021).
24. Гаценко С. С. Аналіз вимог до систем управління військами та шляхи їх удосконалення. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2015. № 2. С. 85–90.
25. Галаган В. І., Полішко С. В., Бондарчук С. В. Пропозиції щодо удосконалення процесу впровадження інформаційних систем іноземного виробництва в діяльність Збройних Сил України. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2019. № 2. С. 62–68.
26. Візія Генерального штабу ЗС України щодо розвитку Збройних Сил України на найближчі 10 років. URL: https://www.mil.gov.ua/news/ 2020/01/11/viziya-generalnogo-shtabu-zs-ukraini-shhodo-rozvitku-zbrojnih-sil-ukraini-na-najblizhchi - 10-rokiv/ (дата звернення: 28.06.2021).
27. Буренок В. А., Кравченко А. Ю., Смирнов С. С. Сетецентричные войны “Воздушно-космическая оборона”. URL: https://www. Мережецентричні війни\ВКО-03-06-11.mht. (дата звернення: 26.06.2021).

Стаття надійшла до редакційної колегії 30.07.2021

The experience of the armed forces of the world's leading countries in the interests of improving the information support of the Armed Forces of Ukraine

Annotation

The experience of the armed forces of the world's leading countries in the operations of the late twentieth and early twenty-first centuries identified the main trend in the development of the theory and practice of troop management - the introduction of the concept of network-centric wars.

The purpose of the article is to substantiate the approaches to determining the directions (ways) of improving the information support of the control systems of the Armed Forces of Ukraine on the basis of the experience of using information systems to manage the armed forces of leading countries.

It is estimated that automation of the processes of collecting, processing, summarizing, transmitting (receiving) information can increase the combat capabilities of troops (forces) by 15-20% and reduce by 50% the time spent on decision-making and bringing tasks to subordinates.

Modern automated control systems, which are essentially informational, are focused on "network-centric actions". The article presents key areas for the implementation of network-centric concepts, the distribution of classes of network-centric systems depending on the degree of automation of controlled processes and the flow of information circulating in them.

The level of automation of military administration at this stage of development of the Armed Forces of Ukraine is only 10-30% of the needs. During the years of independence, the Armed Forces of Ukraine has not created any complete information system for both the management of troops (forces) and defense resources.

The article offers recommendations for the implementation of a network-centric concept (for example C-control system by Armed Forces of USA with an evolution since S2 to S4ISR) for control systems of the Armed Forces of Ukraine. From the experience of the world's leading countries in implementing a network-centric concept for the control systems of the Armed Forces of Ukraine, the main focus should be on the collection, processing, analysis, identification and security of information to support decision-making by managers at all levels. Providing timely up-to-date reliable (relevant) information for military management systems is the main task in the overall process of information support of the Armed Forces of Ukraine.

Keywords: information systems; control systems; network-centric war.

УДК 355.45.02 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/51-56

Саганюк Ф. В., канд. юрид. наук, доцент (0000-0002-9516-0562)
Мудрак Ю. М. (0000-0002-1159-5746)
Мазуренко І. М. (0000-0003-2233-7563)
Піщанський Ю. А. (0000-0003-4392-3318)

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

Тероризм та інші протиправні дії у російській гібридній війні

Резюме. Розглянуто наявні способи та методи гібридної російської війни проти України та інших суверенних держав світу з позиції чинного законодавства України та міжнародного права.

Ключові слова: збройна агресія; збройні сили; міжнародне право; міжнародне гуманітарне право; міжнародний тероризм; тероризм; російська гібридна війна.

Постановка проблеми. Головним сучасним безпековим аспектом у воєнній сфері на національному рівні залишається розв'язана Російською Федерацією (РФ) гібридна війна проти України, яка ведеться у формі комбінації різноманітних агресивних протиправних дій, застосування регулярних військ (сил), незаконних збройних формувань і терористичних організацій, використання пропаганди, саботажу, терору, вчинення диверсій, умисного завдавання шкоди громадянам та об'єктам державної власності України [1].

Окупація РФ частини території України – Автономної Республіки Крим, Донецької і Луганської областей, розпалювання в східних регіонах збройної агресії та відвертих терористичних діянь, руйнування системи світової та регіональної безпеки і міжнародного та міжнародного гуманітарного права зумовлюють переглянути та оновити наявні підходи щодо забезпечення незалежності та державного суверенітету України, відновлення її територіальної цілісності, протидії агресії Російської Федерації для реалізації сучасної Стратегії зовнішньополітичної діяльності України, затвердженої Указом Президента України від 26.08.2021 № 448/2021. Відповідно до цієї Стратегії досвід, набутий за роки протидії агресії Російської Федерації, зокрема щодо протистояння її гібридним загрозам, має бути використаний для розвитку безпекового та політичного співробітництва з іншими державами.

Аналіз останніх досліджень і публікацій. У сучасній літературі [2–8] йдеться про те, що тероризм – це злочин відверто насильницького характеру, який у сучасних умовах характеризується широким розмахом, відсутністю чітко виражених державних кордонів, наявністю зв'язку і взаємодії з міжнародними терористичними центрами та організаціями, суворою конспірацією і ретельним відбором кадрів, надсучасним технічним оснащенням і озброєнням, використанням найбрутальніших і найнесподіваніших прийомів і способів.

Протиправні дії РФ проти України, які наведені в табл. 1, набули саме такого характеру і терористичних ознак, що потребує нових підходів до їх правової оцінки та протидії.

Характерні ознаки тероризму, як обґрунтовано у [2–4], притаманні агресивним гібридним діям РФ, угруповань її збройних сил і створених нею терористичних структур, що здійснюються не тільки проти України. Росія використовує тероризм як стратегію і тактику у терористичних агресивних гібридних діях і проти інших сусідніх держав (табл. 2) [2].

У [3] йдеться про акт тероризму за участю представників ФСБ РФ у Чехії, пов'язаний з підривом підпорядкованими керівництву Росії військовослужбовцями складів боєприпасів у чеському селі Врбетіце у 2014 році.

Нещодавно керівництво РФ схвально оцінило скоєний нинішнім керівництвом Білорусі фактично терористичний акт проти іноземного пасажирського авіалайнера та насильницьке поневолення кількох його пасажирів [4].

Окупаційна адміністрація РФ на окупованих територіях розграбовує майно місцевого населення, здійснює насильницьку русифікацію, репресії та інші суспільно небезпечні діяння, катування та вбивства полонених, інші воєнні злочини; системно і масово користується репресивними методами та способами, залякуваннями; порушує права людини та свободи місцевого населення на окупованих територіях. Критична ситуація у сфері прав людини в окупованому Криму засуджена Резолюцією ГА ООН 71/205 від 19.12.2016.

Таблиця 1

Протиправні дії РФ проти України

Період	Вчинені протиправні дії
29.09.2003	Самочинне протиправне будівництво всупереч нормам міжнародного права переправи (дамби) до о. Тузла (Україна)
04.03.2014	Блокування та захоплення незаконними групами РФ та військовослужбовцями без пізнавальних знаків (“зеленими чоловічками”) будівель місцевої влади АР Крим, Донецької та Луганської областей, військових частин та портів
03–27.03.2014	Блокування військово-морської бази та захоплення 13 кораблів ВМС ЗС України (Донузлав)
26.05.2014–22.01.2015	Збройний напад, захоплення та знищення групами російських спецпризначенців та терористичних найманців проросійських бойовиків Донецького міжнародного аеропорту
06–09.2014	Масоване застосування регулярними військами РФ залпового вогню БМ-21 з території РФ по населеним пунктам та підрозділам ЗС України; вчинення насильницьких діянь, пов’язаних із загрозою життю і здоров’ю та вбивством невинних людей, руйнуваннями важливих народногосподарських об’єктів, систем життєзабезпечення, комунікацій, унаслідок чого загинуло 30 військовослужбовців ЗС України, 6 прикордонників та значна кількість цивільного населення
28.02–22.03.2014	Терористичне блокування і захоплення незаконними терористичними формуваннями РФ аеропорту “Бельбек” в АР Крим та літаків ВВС ЗС України і поневолення командира в/частини ЗС України
11.06.2014	Обстріли російськими терористами снарядами РСЗВ “Град” населених пунктів та невійськових об’єктів України з території РФ
01.06.2014	Збройне захоплення терористичними угрупованнями РФ та знищення українського телецентру на горі Карачун Донеччини
06–08.2014	Збройне захоплення російськими терористичними угрупованнями кургану “Савур-Могила” на Донеччині
14.06.2014	Збройний теракт та збиття підрозділами російської диверсійної терористичної групи ПВК “Вагнер” літака Іл-76 ПС ЗС України поблизу аеропорту “Луганськ”
17.07.2014	Збиття над Донецьком терористичним формуванням РФ із ЗРК “Бук” міжнародного пасажирського літака Boeing 777 компанії “Malaysia Airlines”, що виконував рейс МН17, унаслідок чого загинуло 298 пасажирів з кількох іноземних держав та екіпаж
08.2014	Збройне оточення та розстріл регулярними підрозділами РФ українського угруповання під Іловайськом унаслідок чого загинули 366, поранені 429, полонені 300 осіб та знищено 125 одиниць військової техніки ЗС України
01–02.2015	Збройне захоплення російськими угрупованнями населеного пункту Дебальцево з нещадним артобстрілом з установок “Град” по житловим кварталам, знищенням та підпалом житлових будинків, обстрілами та окупацією прилеглої території
22.01.2015	Артобстріл російськими найманцями зупинки “Донецькгірмаш” у Донецьку; мінометний обстріл транспортної розв’язки в Ленінському районі Донецька внаслідок чого загинуло 8 невинних осіб та 13 отримали важкі поранення
01.2016 – 06.2020	Самочинне будівництво Керченського мосту на території окупованої АР Крим
25.11.2018	Збройний напад військових кораблів РФ і захоплення у нейтральних водах Чорного моря військових катерів і моряків ВМС ЗС України, поранено 6 військовослужбовців, узято в полон і засуджено РФ усі екіпажі захоплених катерів ВМС ЗС України
02.2010 – 03.2020	Погрози РФ застосовувати проти інших держав ядерну та іншу зброю масового ураження згідно з указом президента РФ “Основи державної політики Російської Федерації в галузі ядерного стримування”
1917 до т. ч	Насильницьке нав’язування РФ іншим державам та просування на їх територіях проголошеної керівництвом РФ ідеї “руського міру” та захисту “руськоязичного” населення, що ґрунтуються на твердженні про надособливості російської душі, місії, російської людини та руської мови
20.03.2021	Чергові агресивні утиски та переслідування українців і кримських татар на території окупованого півострова Крим на підставі указу президента Росії про заборону “іноземним громадянам” володіти землею в незаконно окупованому Криму
14.04.2021 до т. ч.	Агресивна та суперечлива міжнародно-правовим договорам концентрація військ РФ поблизу кордонів України та в окупованому Криму (понад 150 тис. військових і озброєння)

Таблиця 2

Міжнародні злочинні дії РФ проти суверенних держав світу

Грузія, Абхазія	1992-1993 збройний конфлікт з 8 тисячами загиблих	1999 незаконний «референдум» про незалежність	1994, 1999 проголошена псевдонезалежність т.зв. «Республіки Абхазія»	2021 **невизнання у світі** порушення прав людини, щонайменше 4,5 тисяч російських військових на території
Грузія, Цхінвальський район	1991-1992, 2008 2 війни, щонайменше 2 тисячі загиблих	1992, 2006 незаконні «референдуми» про незалежність і «возз'єднання з Росією»	1992, 2006 проголошена псевдонезалежність т.зв. «Республіки Південна Осетія»	2021 **невизнання у світі** порушення прав людини, до 4,5 тисяч російських військових на території
Молдова, Придністров'я	1992 збройний конфлікт з 1 тисячею загиблих	2006 незаконний «референдум» про незалежність від Молдови і приєднання до Росії	2017 Придністров'я використовує прапор Росії як другий «державний»	2021 **невизнання у світі** порушення прав людини, щонайменше 3 тисячі російських військових на території

Для диверсійної роботи вербуються члени терористичних організацій та спецслужб РФ, які інструктують, навчають, фінансують та озброюють терористів. Надання Російською Федерацією ПЗРК терористам підтверджує факт прямого втручання РФ у внутрішні справи України та підтримання тероризму [2, 5].

Найочевидніша характерна ознака згаданих терористичних діянь РФ – насильство. За даними Уповноваженого верховного комісара ООН з прав людини загальна кількість людських жертв, пов'язаних з агресією РФ проти України, з 14.04.2014 по 31.01.2021 становить 42 000–44 000 осіб: 13 100–13 300 загиблих (щонайменше 3 375 цивільних осіб, приблизно 4 150 українських військових і 5 700 членів озброєних РФ груп); 29 500–33 500 поранених (7 000–9 000 цивільних осіб, 9 700–10 700 українських військових та 12 700–13 700 членів озброєних РФ груп) [5].

У сучасних ЗМІ [5, 6] йдеться про безпрецедентну за масштабами передислокацію військ РФ до українських кордонів з погрозами широкомасштабною війною та значне загострення ситуації вздовж лінії розмежування і в окупованому Криму, а також про самочинне протиправне обмеження на півроку судноплавства в трьох районах Чорного моря, зокрема й поблизу Керченської протоки. МЗС України розцінило ці дії РФ як ескалацією країною-агресором ситуації в Азово-Чорноморському регіоні, що свідчить про відсутність будь-яких намірів Росії відмовлятися від продовження гібридної війни проти України.

Метою статті є пошук правових підходів до належного оцінювання наявних агресивних гібридно-терористичних збройних та інших діянь Російської Федерації проти України й інших суверенних держав світу відповідно до чинного законодавства України та міжнародного і міжнародного гуманітарного права.

Викладення основного матеріалу. На сучасному етапі розвитку не існує загальноприйнятих кодексів, які б давали чітку оцінку протиправним діям РФ проти України та інших суверенних держав світу як тероризму чи міжнародному тероризму. Факт існування такого виду світових проблем потребує зосередження на законодавстві кожної держави на ознаках таких діянь відповідно до кримінального та процесуального кодексів з урахуванням міжнародно правової практики щодо таких найнебезпечніших злочинів.

Зокрема, злочини проти людства (англ. – Crimes against humanity) або злочини проти миру та безпеки людства визначені в Римському статуті Міжнародного кримінального суду, як "найбільш ненависні злочини, оскільки уособлюють цілком серйозний і руйнівний вплив на людську гідність, принижують і спричиняють деградацію особистості". Як видно з табл. 1 та 2, саме такі протиправні дії є основою політики нинішніх правителів РФ з широким розповсюдженням звірств, яке замовчується чи виправдовується ними. Вбивства, масове знищення людей, тортури, зґвалтування, політичне, расове або релігійне

переслідування та інші нелюдські акти поведінки досягають критичного рівня.

Іншими словами, протиправні дії РФ, які відобразились у масових злочинах проти України та інших сусідніх держав, мають певні ознаки й злочинів проти людства, бо вони несуть загрозу не лише конкретній особі, а людській спільноті, довкіллю, порушують правила людського співіснування. Отже такі злочини мають каратися не тільки за законами окремої країни, а й засуджуватися світовою спільнотою загалом.

Першоджерелами характеристики таких злочинів за міжнародним правом є статути військових трибуналів таких, як Нюрнбергський (1945 р.), Токійський (1946 р.), міжнародних кримінальних трибуналів по Югославії (1993 р.), Руанді (1994 р.) та Римський Статут Міжнародного кримінального суду (1998 р.), а також численні конвенції та резолюції ООН.

Законом України "Про боротьбу з тероризмом" від 20.03.2003 № 638-IV (ст. 1) міжнародний тероризм визначений як "здійснювані у світовому чи регіональному масштабі терористичними організаціями, угрупованнями, зокрема за підтримки державних органів окремих держав, для досягнення певних цілей суспільно небезпечні насильницькі діяння, пов'язані з викраденням, захопленням, вбивством невинних людей чи загрозою їх життю і здоров'ю, зруйнуванням чи загрозою зруйнування важливих народногосподарських об'єктів, систем життєзабезпечення, комунікацій, застосуванням чи загрозою застосування ядерної, хімічної, біологічної та іншої зброї масового ураження". У Росії "тероризм" визначається як "диверсійна діяльність" і як складова гібридної війни [7].

Вторгнення або напад збройних сил РФ на територію України та іншої держави чи будь-яка військова окупація, який би тимчасовий характер вона не носила, є результатом такого вторгнення чи нападу, або будь-яка анексія із застосуванням сили території іншої держави чи її частини, Генеральною Асамблеєю ООН ще в 1974 році визнані як агресія, а Законом України "Про оборону України" від 06.12.1991 № 1932-XII (ст. 1) – як збройна агресія.

Аналогічно визнані бомбардування збройними силами держави території іншої держави чи застосування будь-якої зброї державою проти території іншої держави, блокада портів чи берегів держави збройними силами іншої держави, напад збройними силами держави на сухопутні, морські чи повітряні сили або морські та повітряні флоти іншої держави; застосування збройних сил однієї держави, що знаходяться тимчасово на території іншої держави за згодою з приймаючою державою, у порушенні умов, передбачених в угоді, чи будь-яке продовження їхнього перебування на такій території після припинення дії угоди; дія держави, яка дає змогу, щоб її територія, яку вона надала в розпорядження іншої держави, використовувалася цією іншою державою для здійснення акта агресії проти третьої держави; засилання державою чи від імені держави збройних банд, груп і регулярних сил чи найманців, які здійснюють акти застосування збройної сили проти іншої держави, що носять настільки серйозний характер, що це рівнозначно зазначеним вище актам, або його істотна участь у них.

Водночас, усі ці діяння Росії проти України, яка розпочалася 20.02.2014 з військової операції збройних сил РФ і окупації ними частини території України, з вчиненням її терористичними організаціями та угрупованнями суспільно небезпечних насильницьких діянь (див. табл. 1, 2), пов'язаних з викраденнями та захопленнями і вбивствами невинних людей чи загрозою їх життю і здоров'ю, руйнуваннями важливих народногосподарських об'єктів, систем життєзабезпечення, комунікацій, застосуванням чи загрозою застосування ядерної, хімічної, біологічної та іншої зброї масового ураження і подальших її агресивних терористичних діянь на окупованих територіях, так званих тренувань біля кордону України та на окупованих агресором територіях військ (сил) Південного військового округу РФ та на морських акваторіях доводить подальше вдосконалення нею гібридних агресивно-терористичних способів і методів гібридної війни проти України та інших держав світу.

Відповідно до ст. 1 Закону України "Про боротьбу з тероризмом" усі такі дії РФ належить визнати Україною, а відтак і міжнародною спільнотою, передусім ООН, ОБСЄ, ЄС, НАТО, відповідно до міжнародного права, як міжнародний тероризм, тобто злочинами, що охоплюють:

планування, організацію, підготовку та реалізацію терористичних актів;

підбурювання до вчинення терористичних актів, насильства над фізичними особами або організаціями, знищення матеріальних об'єктів;

організацію незаконних злочинних збройних формувань та організацій і організованих злочинних груп для вчинення терористичних актів, так само як і участь у таких актах;

вербування, озброєння, підготовку та використання терористів;

пропаганду і поширення ідеології тероризму на кшталт "руського міру";

проведення навчання тероризму;

в'їзд в Україну громадян РФ та угруповань, зокрема "Вагнер" з терористичною метою;

фінансування в Криму та на Сході України терористичних організацій й інше сприяння тероризму, що включає надання чи збір будь-яких активів прямо чи опосередковано для їх використання для будь-яких цілей окремим терористом чи терористичною групою (організацією) чи для організації, підготовки або вчинення терористичного акту, втягнення до вчинення терористичного акту, публічних закликів до вчинення такого акту, створення терористичної групи (організації), сприяння вчиненню терористичного акту, навчання тероризму, виїзду з України та в'їзду в Україну з терористичною метою, провадження будь-якої іншої терористичної діяльності, а також навіть спроби вчинення таких злочинних діянь.

Для активнішої протидії злочинним міжнародним діянням РФ наряду з примушуванням її до виконання Мінських домовленостей (Протокол від 05.09.2014, Меморандум від 19.09.2014 та Комплекс заходів від 12.02.2015) у [2–8] рекомендується:

по-перше, зосередити увагу усіх інституцій України та міжнародного співтовариства на ефективній реалізації міжнародно-правових норм і правил, передбачених, зокрема, Глобальною контртерористичної стратегією Організації Об'єднаних Націй (*UN Global Counter-Terrorism Strategy*), яка визначає загальні стратегічні підходи до боротьби з тероризмом у світовому масштабі.

Цей міжнародно-правовий документ спрямований на посилення національних, регіональних та міжнародних підходів до боротьби з тероризмом. Держави – члени ООН погодилися не тільки оголосити про те, що тероризм є неприйнятним у всіх його формах і проявах, але й висловили рішучість зробити практичні кроки на рівні окремих держав, так і колективно для запобігання тероризму і боротися з ним. Ці підходи включають широке коло заходів від зміцнення потенціалів окремих держав у боротьбі з терористичними загрозами до забезпечення координації контртерористичної діяльності в системі ООН;

по-друге, на виконання вимог чинної Стратегії національної безпеки України, державний суверенітет, територіальна цілісність, демократичний конституційний лад та інші життєво важливі національні інтереси мають бути захищені не тільки від воєнних загроз з боку РФ, а і від невоєнних, які продукуються нею проти України та деяких інших суверенних держав світу;

по-третє, на виконання Стратегії воєнної безпеки України [1] необхідно посилити боротьбу на дипломатичному рівні в інтересах захисту суверенного права України на активну всеохоплюючу оборону від нападу агресора як міжнародного терориста, зокрема в ООН та Раді Безпеки, міжнародних судах, Інтерполі тощо, до яких Росія активно апелює. Її дії не узгоджуються з принципами міжнародного гуманітарного права і мають зустріти адекватну протидію міжнародних інституцій та й міжнародної спільноти, зокрема з посилення санкцій проти польотів військових літаків у міжнародному просторі та походів у міжнародних водах військових кораблів ВМС РФ, передусім з так званими гуманітарними вантажами тощо. Окрім цього, як пропонується у [6], запровадити бойкот РФ на світовій арені та міжнародну ізоляцію її вищого керівництва, введення повного ембарго на експорт енергоносіїв (газу, нафти і вугілля); суттєво посилити санкційний тиск ЄС, заборонити будівництво та введення в експлуатацію газогону "Північний потік-2"; заморозити російські активи та вжити інші ефективні заходи.

Висновки

1. Сучасні дослідження [2, 7, 8] наявних підходів до боротьби з російським міжнародним тероризмом і збройною агресією, що здійснюється Росією проти України та інших суверенних держав світу переконують, що такі діяння РФ є насильницькими та особливо небезпечними, пов'язаними з масовими вбивствами, захопленнями та викраденнями невинних людей, руйнуваннями чисельних населених пунктів, важливих народногосподарських об'єктів, систем життєзабезпечення, комунікацій, застосуванням зброї масового ураження. Україною та міжнародним співтовариством належить розцінити як

міжнародний тероризм вжити ефективніших заходів відповідно до національного законодавства та Глобальної контртерористичої стратегії Організації Об'єднаних Націй (*UN Global Counter Terrorism Strategy)*, яка визначає загально стратегічні підходи до боротьби з тероризмом у світовому масштабі.

2. Здійснювані вже восьмий рік Російською Федерацією та її правителями і збройними формуваннями, терористичними організаціями й найманцями гібридні агресивні злочинні терористичні діяння на території України та інших суверенних держав світу без оголошення війни та з відвертим цинічним нехтуванням норм міжнародного та міжнародного гуманітарного права належить розцінювати не як війну в межах міжнародного права, а як збройну агресію з наявними ознаками міжнародного тероризму.

3. Нарощення з боку РФ, як держави-агресора, проти України та інших суверенних держав світу злочинно-терористичних діянь потребує посилення санкцій проти польотів її військових літаків у міжнародному просторі та походів у міжнародних водах військових кораблів ВМС РФ, передусім з так званими гуманітарними вантажами, запровадити бойкот її на світовій арені та міжнародну ізоляцію вищого її керівництва, введення повного ембарго на експорт енергоносіїв, замороження активів та вжиття інших ефективних підходів до протидії її злочинній діяльності.

Напрям подальших досліджень. Проведення більш детального аналізу сутності діянь РФ проти України порівняно з міжнародним тероризмом на основі норм національного та міжнародного законодавства і міжнародного гуманітарного права, які регулюють правовідносини у цій сфері, пошук правових підходів до вдосконалення загальнодержавної системи боротьби з цією злочинною діяльністю відповідно до чинного законодавства України і вимог міжнародного та міжнародного гуманітарного права.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стратегія воєнної безпеки України: воєнна безпека – всеохоплююча оборона : затв. Указом Президента України 25.03.2021 № 121/2021.
2. Міжнародний тероризм у сучасному світі. URL: https://osvita.ua/vnz/ reports/world_ history/ 31752/; Крим – головні заяви до семиріччя окупації півострова. URL: https://nv.ua/ ukraine/politics/krym-glavnye-zayavleniya-k-semiletiyu-okkupacii-poluostrova-novosti-ukrainy-50148020.html. (дата звернення: 03.04.2021).
3. Фактично відбулася терористична атака РФ на країну – члена НАТО. URL: https://gordonua.com/news/worldnews/fakticheski-proizoshla-terroristicheskaya-ataka-rf-na-stranu-chlena-nato-posol- ukrainy-v-chehii-1549779.html. (дата звернення: 04.04.2021).
4. Європейська правда. 2021. 24 травня; Українська правда. 2021. 25 травня.
5. Радіо Свобода, 2021. 30 травня.
6. Офіційний вебсайт Посольства України у ФРН. URL: https://germany.mfa.gov.ua/news/posol-ukrayini-u-frn-andrij-melnyk-publichno-zaklikav-federalnogo-kanclera-angelu-merkel-negajno-vtrutitisya-u-situaciyu; РБК Україна. 2021. 28 травня; 10 фактів про збройну агресію Росії проти України. URL: https://mfa.gov.ua/ 10-faktiv-pro-zbrojnu-agresiyu-rosiyi-proti-ukrayini (дата звернення: 03.04.2021).
7. Україна і Росія. Чим відрізняється тероризм від гібридної війни / Радіо Свобода. 2017. 24 квітня.
8. Воєнні аспекти протидії "гібридній" агресії: досвід України : монографія / колектив авторів ; за заг. ред. А. Сиротенка. Київ: НУОУ, 2020. 176 с.

Стаття надійшла до редакційної колегії 02.05.2021

Terrorism and other illegal actions in the Russian hybrid war

Annotation

The main modern security aspect in the military sphere at the national level is the hybrid war against Ukraine unleashed by the Russian Federation (RF), which is conducted in the form of a combination of various aggressive illegal actions, the use of regular troops (forces), illegal armed groups and terrorist organizations, sabotage, terror, intentional harm to citizens and state property of Ukraine.

The aim of the article is to find legal approaches to the proper assessment of the existing aggressive hybrid terrorist armed and other actions of the RF against Ukraine and other sovereign states of the world in accordance with current legislation of Ukraine and international and international humanitarian law.

Modern studies of existing approaches to combating Russian international terrorism and armed aggression show that such actions of the RF are violent and especially dangerous, associated with mass killings, hostage-taking and abductions of innocent people, destruction of numerous settlements, important economic facilities, systems life support, communications, use of weapons of mass destruction.

The hybrid aggressive terrorist acts committed by the RF for the eighth year in a row on the territory of Ukraine and other sovereign states of the world without declaring war and with outright cynical disregard for international humanitarian law should be regarded not as a war within international law but as armed aggression.

Keywords: armed aggression; armed forces; international law; international humanitarian law; international terrorism; Russian hybrid war.

УДК 351.746.1 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/57-63

Торічний В. О., д-р наук з держ. упр. (0000-0003-3336-6386)
Братко А. В., канд. військ. наук, доцент (0000-0001-5503-3318)
Захарчук Д. О., канд. військ. наук (0000-0001-6051-305X)

Національна академія Державної прикордонної служби України імені Богдана Хмельницького, Хмельницький

Збройні конфлікти як дестабілізуючий фактор прикордонної безпеки

Резюме. У статті проаналізовано природу, характер та особливості сучасних збройних конфліктів. Визначено завдання та дії прикордонних підрозділів Державної прикордонної служби України в разі їх виникнення та ескалації. Розглянуто нові виклики та загрози національній безпеці України на сучасному етапі загалом та у сфері безпеки державного кордону зокрема.

Ключові слова: збройний конфлікт; регіональний збройний конфлікт; гібридна війна; національна безпека; Державна прикордонна служба України; прикордонний загін.

Постановка проблеми. На сьогодні Україна протистоїть найсерйознішому безпековому виклику за всі роки своєї незалежності та є державою, що зазнала зовнішньої агресії з боку Російської Федерації. Наслідком цих дій для українського суспільства стали значні людські, територіальні, економічні втрати, дестабілізація ситуації на Донбасі та найближчих до нього регіонів.

Актуальність дослідження зумовлена тим, що українська держава, маючи збройний конфлікт на ділянці Луганської та Донецької областей, опинилася перед викликом загрози її територіальної цілісності. Недостатня вивченість природи сучасних збройних конфліктів, зміни їх характеру та трансформація у так звані локальні "малі" чи "гібридні" війни позначається на функціональній ефективності дій Державної прикордонної служби (ДПС) України та результативності її структурних підрозділів у питаннях забезпечення прикордонної безпеки як складової національної безпеки України.

Зважаючи на це, потребує подальшого вивчення та більш глибокого аналізу сутність і характер сучасних збройних конфліктів та оцінювання спроможностей прикордонних загонів ДПС України виконувати завдання захисту державного кордону.

Аналіз останніх досліджень і публікацій. Сутність сучасних збройних конфліктів, їх особливості та характер аналізують у своїх наукових доробках західні науковці у сфері політології, філософії, міжнародного права, державного управління, а саме З. Бжезінський, Г. Кіссінджер, Г. Маккіндер, П. Сорокін, Ф. Фукуяма, Е. Тофлер. Комплексні дослідження сучасних збройних конфліктів, зокрема, так званої "гібридної війни", під час окупації АР Крим та збройного конфлікту на Донбасі здійснено вітчизняними дослідниками В. Горбуліним, Ю. Климчуком, М. Требіним, Г. Яворською та ін.

Чималим є доробок військових спеціалістів у сфері аналізу сучасних збройних конфліктів. Зокрема, доктор військових наук, професор І. Руснак представив серйозний аналіз специфіки оборонного будівництва в умовах "гібридної війни", обґрунтовує варіанти своєчасного і адекватного реагування на її виклики [1]. Привертає увагу серія публікацій у збірниках наукових праць Національної академії Державної прикордонної служби України [2–3] та Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського [4–7].

Діям прикордонних підрозділів у контексті забезпечення національної безпеки України присвячене колективне монографічне дослідження, автори якого презентують теоретичні та практичні рекомендації з організації прикордонного контролю [8]. Питання ефективності системи інформаційно-аналітичного забезпечення процесів охорони державного кордону досліджено у роботах В. Городнова, М. Литвина, Д. Іващенко, В. Кириленка [9], О. Фаріона [3].

Дослідженням проблем військових конфліктів загалом, і збройних зокрема в Україні займається низка науково-дослідних інституцій, серед них: Національний університет оборони України імені Івана Черняховського, Інститут історії України НАН, Український інститут воєнної історії, Національний інститут стратегічних досліджень, Центр досліджень армії, конверсії та роззброєння, Національна академія

Державної прикордонної служби України імені Богдана Хмельницького тощо.

Незважаючи на достатній доробок досліджень у сфері військової конфліктології, потребує подальшого вивчення питання трансформації сучасних збройних конфліктів, їх сутнісних характеристик, ретельний аналіз наслідків та розроблення механізмів їх урегулювання для вдосконалення системи охорони державного кордону та визначення завдань і алгоритму дій прикордонних підрозділів в умовах збройних конфліктів.

Метою статті є аналіз природи сучасних збройних конфліктів як дестабілізуючих факторів порушення територіальної цілісності України та визначення завдань і дій прикордонних підрозділів ДПС України у разі їх виникнення та ескалації.

Виклад основного матеріалу. Більшість дослідників розглядають збройний конфлікт у розрізі його макро- та мікрорівнів. Так, у широкому розумінні, під *збройним конфліктом* розглядають будь-яку військову акцію із застосуванням військової сили. У вузькому, він являє собою відкрите збройне протистояння, частіше за все на державному кордоні, пов'язане з його порушенням, утиском суверенітету тієї чи іншої держави або ж те, що виникло на ґрунті політичних протиріч всередині держави [2].

Досить часто у науковій літературі можна зустріти використання поняття "воєнний конфлікт", "війна" та "збройний конфлікт". Так А. Нікітін [10] надає певні визначення цих понять.

Війна – це соціально-політичне явище, що є найбільш гострою формою розв'язання суспільно-політичних, економічних, ідеологічних, національних, релігійних, територіальних та інших суперечностей між державами, народами, націями, класами і соціальними групами засобами збройного насильства.

Воєнний конфлікт – доволі поширене поняття, яке використовується і у повсякденні та в офіційних документах, наукових працях, публіцистичній літературі. Воно вживається з різними предикатами:

"обмежений", "локальний", "регіональний", "етнічний", "територіальний", "релігійний", "ракетно-ядерний" тощо.

Вважаємо, що в широкому розумінні "збройний конфлікт" – це вид воєнного конфлікту між державами, який полягає в односторонньому або взаємному прояві агресивних сил через використання озброєння чи бойової техніки тощо.

Однак не кожен збройний конфлікт можна називати війною, оскільки між ними існує суттєва відмінність, зокрема, війна має такі ознаки: акт оголошення війни; розірвання дипломатичних відносин між воюючими державами, що є наслідком оголошення війни; анулювання двосторонніх договорів, особливо політичних, та вживається для позначення збройного протистояння між двома або декількома суверенними державами. Натомість, коли відбувається громадянська війна або народ чи нація борються за незалежність, застосовують термін "збройний конфлікт". Війна спричиняє зміну усього суспільства, зокрема, державні інститути починають виконувати специфічні функції,зумовлені нею. Під час збройного конфлікту не відбувається докорінна зміна усього державного механізму на військовий лад. Збройний конфлікт – це збройна боротьба між державами або між державою та антиурядовими військовими формуваннями.

Під час аналізу збройних конфліктів на ділянках державного кордону вважаємо доречним використання поняття регіональний збройний конфлікт, тобто, збройний конфлікт між двома і більше державами, який стосується обстановки в конкретному регіоні та найчастіше відбувається з прямою або опосередкованою участю великих держав або залучення воєнно-політичних об'єднань міжнародного характеру. Розпочинається він, як правило раптово, без офіційного оголошення про військові дії, ведеться невеликими силами та засобами. Їх досить часто використовують для здійснення силового тиску на ймовірного та потенційного противника (як приклад, можемо навести дії Російської Федерації щодо впровадження так званого "русского мира") [2].

Аналізуючи сучасні збройні конфлікти, відзначимо, що можливими районами їх виникнення є прикордонні території суміжних держав. Характерні особливості таких конфліктних протистоянь:

посилення інтернаціоналізації збройних конфліктів (залучення міжнародних терористичних чи злочинних організацій, що виступають воюючою стороною, найманців з третіх країн);

застосування незаконних збройних формувань;

політичний (державний) тероризм;

залучення мирного населення до протистоянь, збільшення його жертв під час терористичних актів чи етнічних чисток;

використання методів ведення "партизанської війни";

застосування широкого спектру озброєнь, зокрема, новітні технології;

залучення до конфлікту угруповань кримінального характеру;

трансформація методів управління конфліктами, що зумовлює різкі переходи від ескалації конфлікту до його деескалації тощо.

Низка дослідників доповнюють цей перелік такими характеристиками:

мережева структура бойових дій (шляхом проведення локальних воєн, диверсійних операцій);

відсутність класичної лінії фронту;

відсутність чітко розрізнюваних комбатантів (однакова військова форма, зброя, техніка, військові відзнаки);

якісна відмінність засобів і методів боротьби у сторін, які протистоять, за умови точкового характеру бойових дій (як з боку терористів, так і збройних сил держав);

якісна відмінність сил у сторін, які протистоять, оскільки військовий потенціал терористичних чи повстанських організацій на декілька порядків нижчий за потенціал регулярних військових формувань, що зумовлює використання різних тактичних операцій (терористичних акцій, диверсій, точних авіаційних ударів, спеціальних операцій, масових облав та обшуків);

спрямованість дій обох сторін на досягнення максимального інформаційного ефекту від здійснення диверсійних чи контртерористичних операцій [11].

На останню особливість збройних конфліктів сучасності звертає увагу інший дослідник Е. Гугнін та підкреслює, що глобалізація визначила їх нові особливості: насильство змістилося з міжкордонного простору на внутрішньосоціальний та культурний простори, зокрема інформаційний та кіберпростір. Вони відбуваються всередині однієї держави з підключенням транснаціональних акторів та обставин розмивання відмінностей між внутрішніми і зовнішніми діями, між інтервенціями і контрінтервенціями, між національними і глобальними рівнями соціальної організації [12].

Через це, останнім часом суттєво розширився спектр потенційних учасників збройних конфліктів, окрім держав, їх суб'єктами стають різні опозиційні угруповання – примирення з ними не можливе, отже і повноцінне врегулювання конфліктів матиме місце лише після повного знешкодження.

Участь загонів (підрозділів) охорони державного кордону у збройних конфліктах визначається в основному через залучення їхніх сил і засобів у заходах із територіальної оборони та у боротьбі з незаконними збройними формуваннями в тісній взаємодії з іншими правоохоронними органами та Збройними Силами України, але не як сили, спроможні самостійно вести бойові дії. Події на південному сході України наглядно продемонстрували необхідність перегляду деяких механізмів забезпечення прикордонної безпеки саме під час збройного конфлікту [13].

Ураховуючи сумний досвід збройного конфлікту на ділянці Луганської та Донецької областей, відзначимо, що у тих умовах підрозділам охорони державного кордону довелося виконувати непритаманні їм завдання: вони змушені були переходити до оборони своїх об'єктів, залишившись сам на сам із незаконними збройними формуваннями. Особливо вразливими у цьому контексті виявилися пункти пропуску, розташовані на лінії державного кордону. Крім того, мали місце провокації з боку місцевого населення на відділах прикордонної служби для дестабілізації їх роботи.

Ще одним суттєвим аспектом цих подій, як підкреслюють О. Суботін та О. Ананьєв стала слабка організація взаємодії з прикордонними підрозділами з боку керівництва інших міністерств і відомств сектору безпеки і оборони [13]. Таку взаємодію не ватро недооцінювати, особливо в умовах ескалації збройного конфлікту, що супроводжується відкритими спробами незаконного перетину державного кордону та захоплення територій. Слушною у цьому контексті виглядає пропонована Ю. Івашковим модель дій сил і засобів ДПС України в період ускладнення воєнно-політичної обстановки та в загрозливий період. Останню він визначає як опис процесу оперативно-службової діяльності, що відображає його призначення, складений для вивчення його властивостей, особливостей функціонування у взаємодії з внутрішніми та зовнішніми елементами [4]. Така модель відображає сукупність процедур, сил і засобів, які залучаються до оперативно-службової діяльності і порядок взаємодії учасників процесу.

Отже, сутність пропонованої моделі полягає у тому, що з метою підсилення підрозділів, що безпосередньо здійснюють охорону державного кордону, з органів охорони державного кордону залучатимуться бойові резерви (оперативно-бойові прикордонні комендатури швидкого реагування), які використовуватимуться як безпосередньо для охорони державного кордону, так і на ділянках, де можливі збройні конфлікти. Можливе залучення також загонів підтримки чисельністю до посиленого механізованого батальйону. Такі підрозділи посилення братимуть участь у веденні пошукових дій у районах можливого знаходження диверсійних груп, інших озброєних формувань з метою їх виявлення, затримання або знищення; розчленуванні та видворенні великих мас цивільного населення, заходах із припинення провокаційних дій проти органу охорони державного кордону та його структурних підрозділів; знищенні невеликих груп противника, який вторгся на територію України [4].

Отже, якщо основними завданнями прикордонного загону залишається охорона цілісності та недопущення незаконного перетину державного кордону із використанням традиційних форм оперативно-службової діяльності, то в умовах розвитку збройного конфлікту прикордонники можуть виконувати низку додаткових завдань:

ведення розвідки, з метою своєчасного виявлення лідерів, активістів екстремістських організацій;

встановлення осіб, які розповсюджують неправдиві, панічні чутки;

посилення охорони на ділянках, де потенційно можливі прецеденти збройних сутичок і конфліктів;

посилення охорони кордонів, місць компактного поживання сімей прикордонників;

виявлення та ліквідація місць незаконного збереження зброї, боєприпасів, вибухівки, токсичних речовин;

організація та ведення цілодобового спостереження за районами, що наближені до державного кордону, де можливі масові виступи та порушення державного кордону;

завчасне планування заходів, можливих дій прикордонного загону в умовах збройного конфлікту;

проведення оперативних, військових режимних дій із запобігання ліквідації масових виступів, порушень перетину кордону, проявів тероризму та бандитизму.

Визнаємо, що пропонований перелік заходів є не повним, адже будь-який збройний конфлікт розвивається за своїм сценарієм, з властивими лише йому суб'єктно-об'єктними характеристиками та специфікою динаміки. До того ж, існує низка факторів, які ускладнюють врегулювання збройних конфліктів у сучасних умовах, серед них вплив на хід конфлікту недержавних акторів і міжнародних організацій та інтернаціоналізація більшості з них. До того ж варто враховувати нові виклики та загрози національній безпеці України на сучасному етапі загалом, та у сфері безпеки державного кордону зокрема. Серед таких:

намагання деяких країн вирішити питання щодо зміни проходження лінії державного кордону або здійснення політики з відторгнення частини українських територій. Так, загрози з питань територіальних претензій існують не лише з боку Російської Федерації, але і інших держав, зокрема Румунії, яка неодноразово декларувала територіальні претензії на Бессарабію та Північну Буковину, прагнення румунської влади обмежити судноплавство в українській частині гирла р. Дунай, конфлікти за острів Зміїний, намагання надати частині українського населення прикордонних районів України румунського громадянства з видачею румунського паспорта. Мають місце також приховані територіальні претензії до України з боку Угорщини на окремі райони Закарпатської області та Польщі на окремі райони Львівської та Волинської областей;

загроза виникнення прикордонного конфлікту із застосуванням сили або погроза застосування сили для вирішення територіальних претензій щодо України;

імовірність незаконного перетину державного кордону значною кількістю населення прикордонних територій або біженцями через виникнення регіональних або прикордонних конфліктів поблизу державного кордону України;

загроза нападу на персонал та об'єкти ДПС України для оволодіння зброєю, технікою чи майном або під час здійснення персоналом своїх функціональних обов'язків;

створення злочинних угрупувань, що здійснюють свою діяльність на державному кордоні та в межах прикордонних районів і спроби втягування персоналу ДПС України у протиправну діяльність;

озброєні та неозброєні провокації на державному кордоні, для втягнення України в регіональні конфлікти тощо [14].

Усе це варто враховувати, обираючи стратегію, місце і роль органів охорони державного кордону в процесі забезпечення державної безпеки в умовах збройного конфлікту.

Загалом, у конфліктології виокремлюють дві форми вирішення збройних конфліктів, що відрізняються мірою завершення цього процесу:

урегулювання конфлікту – максимально повне усунення невійськовими (зокрема політико-дипломатичними) засобами протиріч, які детермінували початок бойових дій, за мінімізації ризику їх відновлення;

управління або регулювання конфліктами – можливість контролю над ходом збройних конфліктів для недопущення його необмеженого розвитку та досягнення швидкого завершення, мінімізація стадії ескалації [15].

Як підкреслює С. Стасюк, остання чверть ХХ ст. продемонструвала ще один "силовий спосіб" врегулювання конфліктів – односторонні, короткотермінові військові акції держав – лідерів у царині міжнародних відносин. Так, США періодично здійснюють повітряні напади на об'єкти в інших країнах з використанням високоточної зброї, а також інтервенції до деяких країн (Афганістан, Сомалі, колишня Югославія та Ірак). Особливий тип збройного насильства становить інтервенція – насильницьке втручання у внутрішні справи інших держав через введення військ або іншим чином, однієї або декількох держав у внутрішні справи інших держав і спрямоване проти їх суверенітету, територіальної цілісності, політичної незалежності. Розрізняють збройні інтервенції – гуманітарну, економічну, дипломатичну. Найнебезпечнішою формою інтервенції для сучасного світового порядку слід вважати збройну, яку важко диференціювати від неспровокованої агресії [16].

З оперативно-тактичного погляду, дії прикордонних підрозділів в умовах збройного конфлікту також мають свої особливості. Для них характерними є поєднання військових і невійськових форм протистояння, створення для вирішення конфлікту тимчасових позаштатних формувань, до яких залучаються також представники різних силових структур та правоохоронних відомств.

Одним із найбільш складних завдань прикордонного підрозділу в умовах збройного конфлікту є створення єдиної, уніфікованої системи зв'язку та інформації між самостійно діючими прикордонними підрозділами та допоміжними групами на різних ділянках кордону, координація спільних зусиль та узгодження окремих дій з органами місцевої адміністрації в питаннях дотримання надзвичайного стану в регіоні.

Погоджуємося із позицією О. Суботіна та О. Ананьєва щодо класичних принципів формування оборони, які не завжди можуть бути прийнятні під час деескалації збройного конфлікту. Отже під час побудови оборони безпосередньо поблизу державного кордону в першому ешелоні не має сенсу розміщувати війська (сили) Збройних Сил України з їх тяжким озброєнням та засобами ураження великої потужності. Натомість у першому ешелоні оборони разом з підрозділами ДПС України доцільно розміщувати підрозділи Національної гвардії та їхні сили швидкого реагування. Угруповання Збройних Сил України як мобільні резерви та підрозділи з важким озброєнням та авіацією (вертольоти, вогнева підтримка) мають перебувати в другому ешелоні, щоб у разі ескалації конфлікту, вони були спроможні надати необхідну збройну підтримку прикордонним підрозділам та Національній гвардії. Та найголовнішим завданням органів охорони державного кордону в процесі забезпечення прикордонної безпеки під час збройного конфлікту є формування ефективного балансу між військовими та невійськовими формами і способами боротьби [17]. За умов відсутності останнього, ймовірність ескалації та затягування збройного конфлікту є досить високою.

Висновки та напрями подальших досліджень. Теоретико-методологічний аналіз сутності сучасних збройних конфліктів продемонстрував недостатню наукову оцінку цього явища, особливо в контексті зміни його характеру, суб'єктів в умовах глобалізаційних процесів. Державна прикордонна служба України, ключовим завданням якої є забезпечення національної безпеки держави на державному кордоні опинилася перед новими викликами, пов'язаними з російською агресією, анексією АР Крим тощо. Ці події засвідчили нагальну потребу в доопрацюванні механізмів захисту державного кордону та оцінюванні спроможностей підрозділів прикордонних загонів виконувати свої завдання. Досвід, який отримала ДПС України на початку та під час розгортання АТО/ООС є на сьогодні тим базисом, який варто використовувати для формування моделі

реагування та захисту державного кордону в умовах збройного конфлікту.

Володіючи знаннями про історичні детермінанти виникнення, природи та динаміки сучасних збройних конфліктів, можна спрогнозувати ймовірність їх виникнення у майбутньому та потенційні осередки їх розгортання. Водночас, зважаючи на швидкоплинність геополітичної ситуації, потребують надалі більш детального вивчення вплив ключових та другорядних міжнародних акторів на розвиток збройного конфліктного протистояння, а також проблеми терористичних угруповань та найманства (діяльність приватних військових компаній) як складових сучасних збройних конфліктів. Окремих наукових досліджень потребують питання дій, спроможностей і механізмів вирішення збройних конфліктів прикордонними підрозділами Державної прикордонної служби України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Руснак І. С. Підсумки та перспективи оборонного будівництва України в контексті реалізації воєнної політики держави. *Стратегічні пріоритети*. 2015. № 4. С. 35–44.
2. Трембовецький О. Г., Лазоренко О. В. Аналіз умов виникнення регіональних збройних конфліктів та завдання прикордонного відомства у разі їх виникнення. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки*. 2015. № 4. С. 248–261.
3. Фаріон О. Б. Методика оцінки ефективності системи інформаційного забезпечення відділу прикордонної служби типу «В». *Збірник наукових праць Національної академії Державної прикордонної служби України*. 2009. № 49. С. 97–115.
4. Івашков Ю. Б. Модель дій сил і засобів Державної прикордонної служби України в період ускладнення воєнно-політичної обстановки та загрозливий період. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.* Київ, 2017. № 2 (60). С. 116–120.
5. Леонов В. В., Ворович Б. О., Сівоха І. М. Війни XXI століття: технології "гібридної війни". *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2015. № 1 (53). С. 24–30.
6. Фролов В. С., Саганюк Ф. В., Лобко М. М. Деякі підходи щодо стратегії протистояння та протидії агресору. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2017. № 1 (59). С. 5–11.
7. Фролов В. С., Саганюк Ф. В. Стратегія переходу в умовах гібридної війни до нового формату стратегічного керівництва сектором безпеки і оборони України. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.* Київ, 2017. № 2 (60). С. 6–12.
8. Назаренко В. О., Серватюк В. М., Ставицький О. М. Теорія і практика організації та здійснення прикордонного контролю (у контексті забезпечення національної безпеки України в прикордонній сфері) : монографія. Хмельницький : НАДПСУ, 2013. 360 с.
9. Городнов В. П., Литвин М. М., Іщенко Д. В., Кириленко В. А. Теоретичні основи інформаційно-аналітичного забезпечення процесів охорони державного кордону (у контексті завдань національної безпеки України в прикордонній сфері) : монографія. Хмельницький : НАДПС України, 2009. 473 с.
10. Нікітін А. А. Збройний конфлікт як вид воєнного конфлікту. *Науковий вісник Львівського державного університету внутрішніх справа*. 2018. Вип. 2. С. 52–59.
11. Bratko A., Zaharchuk D., Zolka V. Hybrid warfare – a threat to the national security of the state. *Revista de Estudios en Seguridad Internacional*. 2021. 7, 1. P. 147–160. URL: http://dx.doi.org/10.18847/1.13.10 (дата звернення: 02.08.2021).
12. Гугнін Е. А. Гібридна війна як технологія зовнішнього впливу (на прикладі анексії Криму). *Грані.* 2020. Вип. 20. С. 13–19.
13. Суботін В. О., Ананьїн О. В. Забезпечення прикордонної безпеки України в умовах збройного конфлікту. *Наука і оборона*. 2014. № 4. С. 30–36.
14. Цевельов О. Є. Державне реагування на загрози національній безпеці у сфері безпеки державного кордону України : дис… канд. наук з держ. упр. : 25.00.05 / Хмельницький університет управління та права. Хмельницький, 2017. 330 с.
15. Torichnyi V., Biletska T., Rybshchun O., Kupriyenko D., Ivashkov Y., Bratko A. Information and propaganda component of the Russian Federation hybrid aggression: conclusions for developed democratic countries on the experience of Ukraine. *TRAMES*. 2021. Vol. 25 (75/70), № 3. P. 355–368.
16. Луцишин Г. Особливості сучасних збройних конфліктів в умовах глобалізації. *Українська національна ідея: реалії та перспективи розвитку*. 2014. Вип. 26. С. 128–133.
17. Братко А. В., Мисик А. Б. Роль Державної прикордонної служби України в системі воєнної безпеки в умовах гібридної війни. *Честь і закон*. 2021. № 1 (76). С. 5–10.

Стаття надійшла до редакційної колегії 01.09.2021

Armed conflicts as a destabilizing factor for the state border guard service of Ukraine

Annotation

The authors analyze the nature, essence and characteristics of contemporary armed conflicts and identify the main tasks of the State Border Guard Service of Ukraine if the armed conflicts arise or escalate. It was found, that the frontier zone of the bordering countries and the small individual localities considering their affiliation are the areas of potential armed conflicts. The author emphasizes that the range of potential participants of armed conflicts has been significantly increased in recent times. In addition to the states, oppositional groups also become the actors in conflict. Given that reconciliation with these groups may not be possible, conflict resolution could be only after their annihilation. The author analyzes the emerging challenges and threats to Ukraine's national securities in general and in particular in the sphere of border security control.

The author claims that in terms of tactical and operational activities, the action of the border detachments in situations of armed conflict has its own specificity. It is characterized by the combination of military and non-military forms of confrontation, establishment of the temporary non-staff groups that involve security forces, including law enforcement agencies, in order to resolve the conflict. Author also stresses that the main tasks of border guard detachments are ensuring inviolability of state borders and preventing illegal cross-border movements with the traditional operational methods, and, if the conflict is developing, border guards may do a number of additional missions.

The author concludes that one of the most difficult tasks of border guard detachments in armed conflict is the establishment of unified information communication system between the independent border guard detachments and the subsidiary groups in different areas of the border, the coordination of common efforts, and consultation with the local administration regarding compliance with the martial law.

Keywords: armed conflict; regional armed conflict; hybrid warfare; national security; the State Border Guard Service of Ukraine; border guard detachment.

УДК 355:327.7:НАТО DOI: https://doi.org/10.33099/2304-2745/2021-2-72/64-69

Андріянова Н. М., канд. політ. наук [1] (0000-0002-7115-2445)
Голопатюк Л. С., канд. військ. наук [2] (0000-0003-4153-532X)
Коваленко Г. А. [3] (0000-0002-7256-2665)
Шпура М. І., канд. військ. наук, ст. наук. співроб.[2] (0000-0002-3350-6003)

[1] – Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ;
[2] – Головне управління військового співробітництва та верифікації Збройних Сил України, Київ;
[3] – Стратегічне командуванняя НАТО з Трансформації, Норфолк, штат Вірджинія, США

НАТО та світова пандемія: від невизначеності до плану дій

Резюме. Стаття присвячена аналізу наявних напрямів реагування НАТО на новітні виклики і загрози спричинені світовою пандемією COVID-19 та визначення подальших напрямів політики Альянсу, враховуючи складну епідеміологічну ситуацію.

Ключові слова: НАТО; пандемія; реагування НАТО; COVID-19.

Постановка проблеми. Світова пандемія, викликана вірусом COVID-19 вже майже два роки продовжує вирувати в країнах світу, не зважаючи на різні підходи до її приборкання. Без сумніву, пандемія стала безпрецедентним викликом для усього світу і її наслідки ще довго матимуть вплив та відображатися як на сферах життя окремих країн, так і напрямах політики, яка реалізовуватиметься міжнародними організаціями, зокрема Організацією Північноатлантичного договору.

Хоча наразі ще досить складно говорити про вплив вірусу COVID-19 на діяльність та плани Альянсу, певних висновків вже можна дійти, а також розглянути напрями подальшої діяльності НАТО на короткострокову та середньострокову перспективу. Такі висновки будуть неодмінно враховані в державах – членах Альянсу та знайдуть своє відображення в документах стратегічного рівня вже найближчим часом.

Аналіз основних досліджень і публікацій. Варто наголосити, що питання дослідження впливу світової пандемії на діяльність НАТО є абсолютно новим як в сучасній вітчизняній, так і зарубіжній науковій літературі, але водночас необхідно відмітити роботи [1–5], які заклали основи дослідження з цієї тематики. Так, у роботі [1] автори роблять спробу передбачити можливі наслідки впливу пандемії, а також кризових явищ у світових фінансах і економіці, робота [2] присвячена дослідженню впливу світової пандемії COVID-19 на глобальну систему безпеки, у [3] – аналізу проблеми підвищення ефективності кризисного реагування на виклик світової пандемії COVID-19, у роботі [4] проведено аналіз наративів пов'язаних з пандемією, інформаційні кампанії, які проводяться Китаєм та Росією щодо відображення цієї проблеми, а у [5] – дослідження питань ролі та місця науково-технічної мережі НАТО в протидії виклику світової пандемії COVID-19. Проте аналізу напрямів реагування НАТО на наслідки світової пандемії COVID-19 та визначення напрямів подальшої політики Альянсу присвячено не достатньо уваги.

Метою цієї публікації є аналіз напрямів реагування НАТО на нові виклики і загрози, а саме, на наслідки світової пандемії COVID-19 та визначення напрямів подальшої політики Альянсу, враховуючи складну епідеміологічну ситуацію.

Виклад основного матеріалу. Беручі до уваги безпрецедентність такого рівня пандемії, більшість експертів погоджується з оцінкою, що НАТО, як і інші міжнародні організації (включаючи ООН та Світову організацію охорони здоров'я), виявилося не готове до абсолютно нового виклику всесвітньої пандемії та оперативної протидії спричиненим нею наслідкам. Але неготовність не слід плутати з розгубленістю.

На користь НАТО свідчить той факт, що керівництву Альянсом знадобився короткий термін для реагування на новий виклик та започаткування відповідної політики на стратегічному рівні [6–8] (Генеральний секретар НАТО не зайняв позицію вичікування, а, навпаки, постійно комунікує: виступає із заявами, коментарями та інформаційними брифінгами [9]).

З початку розповсюдження вірусу світом, Альянсом (за провідної ролі Стратегічного командування НАТО з

Трансформації) було оперативно визначено такі пріоритети діяльності [10]:

забезпечення зниження рівня ризику зараження вірусом персоналу, який задіяний до планування і реалізації заходів НАТО;

збереження (підтримання) належного рівня ефективності роботи як організації загалом, так і окремих її компонентів (головним чином системи управління та контролю (С2);

поступова, але наполеглива адаптація до нових умов діяльності Організації Північноатлантичного договору з урахуванням чіткого розуміння своєї ролі на всіх щаблях прийняття рішень.

Водночас, акцент було зроблено на збереженні постійного тісного (робочого) зв'язку як між структурними елементами штабів стратегічного та оперативного рівнів, так і між стратегічними командуваннями та навчальними закладами НАТО, центрами вивчення передового досвіду, центрами освіти та підготовки держав – членів НАТО, а також агенціями й індустріально-виробничими структурами, які працюють з Альянсом.

Основні заходи, що проводяться та сплановані в НАТО на боротьбу з пандемією, новим світовим викликом, доцільно розділити на такі основні напрями (складові):

інституційний, який пов'язаний зі змінами у процедурах прийняття рішень стратегічного рівня, і потребує прийняття консенсусних рішень на рівні голів держав та урядів;

організаційний напрям, який стосується змін у практичній площині діяльності Альянсу, включаючи заходи освіти та підготовки, спільні військові навчання, проведення операцій та здійснення планових ротацій розгорнутих контингентів;

інформаційний, який охоплює як заходи, спрямовані на оперативне й неупереджене інформування широкого загалу стосовно пандемії, так і на протидію пропаганді, розгорнутій певними країнами з метою дискредитації НАТО, як єдиної міжнародної організації, здатної забезпечити колективну оборону для держав – членів.

Така класифікація прийнята в штаб-квартирі Альянсу і в обох стратегічних командуваннях НАТО – з Операцій (м. Монс, Королівство Бельгія) та з Трансформації (м. Норфолк, Сполучені Штати Америки).

Більш детально зупинимося на змістовному наповненні цих напрямів.

Отже, на ***інституційному напрямі*** наразі здійснюється ретельний аналіз можливого впливу пандемії на поточну діяльність Організації Північноатлантичного договору. Основним завданням такого аналізу є виявлення та мінімізація впливу факторів, які значно зменшують інституційну єдність держав – членів НАТО.

Хоча радикальних змін у процесі прийняття рішень в Альянсі очікувати не варто, більшість експертів погоджуються з думкою, що повернення до ведення справ так, як було раніше (business as usual), є неможливим.

На *перспективу*, в *інституційному напрямі* слід очікувати ініціювання керівництвом Альянсу та проведення державами – членами НАТО змін, пов'язаних із адаптацією національних законодавств до потреб Організації Північноатлантичного договору. Водночас, кількість рішень, до прийняття яких залучатимуться топ-посадовці керівництва Альянсом, буде поступово зменшуватися.

Також можна передбачити збільшення ролі засобів обміну інформацією (у тому числі інформацією з обмеженим доступом) під час обговорення та прийняття рішень Альянсом. Зокрема, одночасно з розширенням спектру використання каналів зв'язку, буде вжито заходів, спрямованих на їх всебічний захист, у тому числі і від кібернетичних атак.

Водночас, у середньостроковій перспективі керівництво НАТО вживатиме заходів, спрямованих на запобігання окремими країнами скорочення витрат на оборону на користь необхідності боротьби з вірусами. Наразі існують певні побоювання, що політики в окремих столицях держав – членів НАТО можуть використати пандемію як підставу для перерозподілу ресурсів з оборонних питань на користь заходів охорони здоров'я.

Керівництвом Альянсу наразі вживаються такі ***організаційні заходи*** з боротьби із розповсюдженням вірусу:

створено досить життєздатну та ефективну систему залучення військових до надання допомоги. Зокрема, Верховний головнокомандувач НАТО в Європі генерал Тед Волтерс тепер координує військову підтримку для боротьби з кризою. Він визначає необхідні військово-транспортні можливості повітряних перевезень медичних матеріалів і обладнання, координує надлишкові спроможності і запаси та узгоджує запити на допомогу з пропозиціями союзників і партнерів;

налагоджено оперативну взаємодію з Агенцією ЄС з контролю за повітряним рухом, іншими структурними підрозділами ЄС, оперативними командуваннями НАТО в Неаполі, Нортвуді, Брюнссумі та Рамштайні, а також створено спільний інформаційний портал (захищений) для координації всіх заходів, спрямованих на боротьбу з вірусом;

розгорнуто низку польових шпиталів (понад 100) на території країн – членів НАТО, які найбільше постраждали від епідемії;

здійснюється оперативне переміщення пацієнтів, які знаходяться в критичному стані до медичних закладів з вищим рівнем надання медичної допомоги. НАТО використовує можливості з авіаперевезень для транспортування критично важливих медичних виробів. Йдеться, зокрема, про Міжнародну програму забезпечення стратегічних авіаперевезень (Strategic AirLift Interim Solutions – SALIS), яка надає можливості оренди комерційних транспортних літаків;

введено режим обмеженого пересування для військовослужбовців і цивільних представників, які працюють у штабах НАТО всіх рівнів. Такі заходи супроводжуються також широким використанням відповідного програмного забезпечення (GoToMeeting, Zoom, Skype та інші). Також системою контролю за виконанням завдань запроваджено систему під назвою "Tasker Tracker";

запроваджено систему інформування особового складу органів управління НАТО щодо поточної ситуації в світі з розповсюдженням та боротьбою із зазначеним вірусом;

скориговано план заходів на друге півріччя 2020 та на 2021 рік у бік зменшення заходів із залученням значної кількості персоналу, а також пов'язаних з необхідністю здійснювати подорожі;

запроваджено заходи обмеженого перебування в штабах (закритих приміщеннях); штаби та приміщення обладнано додатковими засобами гігієни та самоізоляції.

Станом на початок липня 2020 року, до заходів, пов'язаних з протидією світовій пандемії залучається більше 500 000 військовослужбовців країн – членів НАТО, включаючи 14 000 осіб медичного персоналу та 6 000 наукових працівників у галузі медицини.

НАТО також працює над інноваційними рішеннями, зокрема, виробництво (друк) респіраторів на 3D-принтерах, і масок для апаратів штучної вентиляції легенів, переобладнаних з приладдя для дайвінгу. А ще в штаб-квартирі Альянсу було запущено платформу "Челендж від головного науковця НАТО" із запрошенням науковців держав – членів Альянсу до пошуку рішень для виявлення вірусів, покращення інформування та майбутнього відновлення після COVID-19.

Протягом останніх місяців з боку Організації Північноатлантичного договору було надано суттєву допомогу й іншим країнам, зокрема – Боснії та Герцеговині, Грузії, Іраку, Колумбії, Молдові, Сербії та Україні.

У короткостроковій та середньостроковій перспективі слід очікувати продовження адміністративних та організаційних заходів. Серед них слід відмітити поступове відновлення роботи штабів усіх рівнів до алгоритму перед-вірусного часу. Таке відновлення планується у декілька етапів.

Відтак, такий поступовий підхід дасть змогу з одного боку уникнути переможної ейфорії у разі зниження рівня захворюваності, а з іншого – здійснювати аналіз ефективності заходів кожного етапу відновлення від світової пандемії. Також у планах Альянсу більш широке застосування засобів програмного забезпечення, спрямованих на організацію та проведення заходів дистанційного характеру. Зокрема, планується до кінця 2020 року в повсякденній діяльності застосовувати програмні продукти Skype, GoToMeeting, Zoom тощо для організації та проведення спільних заходів (конференцій, семінарів, нарад тощо).

Протягом найближчого часу буде закінчено перегляд переліку навчальних програм, які пропонуються Коледжем НАТО в Римі та Школою НАТО в Обераммергау у напрямку збільшення курсової підготовки за дистанційною формою (Advanced Distant Learning – ADL). Аналогічний підхід застосовується і в інших військових навчальних закладах держав – членів НАТО, зокрема, Балтійського оборонного коледжу (м. Тарту, Естонія).

Водночас протягом найближчих півроку діятимуть обмеження на пересування військового та цивільного персоналу НАТО. Це стосується проведення ротацій (їх перенесення на 2021 рік) як в операціях, так і в командних структурах Альянсу. Проте додатковою проблемою стане дотримання вимог національних обмежень на пересування

під час ротацій у складі багатонаціональних контингентів.

Для розуміння складності проблеми слід звернути увагу на обсяг пересування та розгортання військ. Тільки протягом січня-березня 2020 року до Європи зі Сполучених Штатів Америки було переміщено більше 6 000 осіб персоналу, 9 000 зразків озброєння було транспортовано та розгорнуто, включаючи 3 000 зразків, переміщених з території США [7].

Зазначені обмеження напряму також торкнуться й проведення спільних військових навчань. Одночасно зі скороченням кількості навчань та персоналу для участі в цих навчаннях, фокус поступово буде змінюватися на користь залучення цивільних компаній. Уже сьогодні комерційними компаніями здійснюється близько 90 % перевезень під час проведення навчань. Відсоток інформації, яка надходить з комерційних супутників вже сягнула 70 %, а 99 % інтернет-трафіку надається цивільними (комерційними) провайдерами [7].

У середньостроковій перспективі планується переглянути ставлення Альянсу до медичної безпеки та захисту від зброї масового ураження, зокрема біологічної зброї. Нині визначаються завдання з вивчення питань реагування на пандемії Центрам вивчення передового досвіду НАТО (COE – Centres of Excellences) (зокрема у Португалії та Норвегії), в планах також залучити до цієї діяльності Партнерські центри навчання та підготовки (PTEC – Partner Training and Education Centres).

Поряд з інституційними та організаційними заходами, воєнно-політичне керівництво Альянсу проводить комплекс ***заходів інформаційного характеру***. Особлива увага і зусилля зосереджуються, зокрема, на протидії кампанії дезінформації і звинувачень з боку Російської Федерації.

Серед основних російських міфів (табл. 1) і контрпропагандних наративів Альянсу можна виділити такі [4, 11].

У цьому контексті поняття вживаються у значенні: міф – щось вигадане, неіснуюче, фантастичне. Наратив – викладення фактів, подій [12], які відображають існуючу реальність.

Таблиця 1

№	Міф	Наратив
1	COVID-19 зруйнує НАТО	Альянс створений 70 років тому, неодноразово доводив свою ефективність у вирішенні значної кількості завдань життєвої важливості. Відтак пандемію слід розглядати в контексті ще одного виклику Альянсу, хоча вона й має нову форму та зміст
2	НАТО не змогло допомогти країнам – членам у боротьбі з вірусом	Альянс надає всі наявні спроможності для боротьби з вірусом. Зокрема це стосується перевезення медичних працівників і вантажу та працівників до країн, які найбільше потерпають від такої пандемії. Також медичний персонал залучається до процесу розроблення вакцини, використовуючи новітні інноваційні підходи
3	Вірус є біологічною зброєю, розробленою саме в НАТО	Світова організація охорони здоров'я має всі докази про природнє походження вірусу (вірус тваринного походження). Немає жодних підстав стверджувати, що вірус має штучне походження, тим більше, походження з території будь-якої країни НАТО
4	НАТО розповсюджує вірус COVID-19 під час своїх навчань	Альянсом вживаються всі вичерпні заходи, спрямовані на запобігання та розповсюдження захворювання персоналу НАТО (військового і цивільного) на коронавірус. Здебільшого, план навчань до кінця 2020 року було скориговано у напрямі зменшення кількості навчань і скорочення кількості персоналу, який бере участь у зазначених навчаннях
5	НАТО закликає збільшити витрати на оборону за рахунок зменшення витрат на охорону здоров'я в країна – членах	Військовий персонал НАТО навпаки, надає допомогу медичному персоналу та медичним представникам країн – членів Альянсу у їх боротьбі з вірусом

Серед *перспективних напрямів інформаційної* протидії світовій пандемії, слід очікувати нарощування кампанії, спрямованої на інформування суспільства в країнах – членах НАТО, а також в інших державах. Створення прошарку добре поінформованого суспільства дасть змогу ефективно протистояти намаганням певних країн спекулювати на вірусі та розповсюджувати фейкові новини та міфи.

До планування та проведення таких заходів, наразі активно залучається й експертна спільнота, зокрема Центр вивчення передового досвіду НАТО з питань стратегічних комунікацій (м. Рига, Латвійська Республіка).

Висновки. У статті проаналізовано основні напрями реагування НАТО на нові виклики і загрози, а саме, на наслідки світової пандемії COVID-19, такі як інституційний, організаційний та інформаційний напрями,

відповідно. У межах цих напрямів відбулася спроба визначити поточну і подальшу політику Альянсу в умовах складної епідеміологічної ситуації.

Проведене дослідження доводить, що не зважаючи на масштабність і наслідки пандемії COVID-19, НАТО внесло свій вклад у її приборкання і продемонструвало здатність діяти в кризових умовах, відіграло суттєву роль під час врятування людських життів і поширення найсмертоноснішої пандемії за останнє століття.

Фахівці Альянсу і експертні кола на сьогодні єдині у своєму висновку: Альянс вже ніколи не буде таким, як до весни 2020 року.

Перспективним напрямом подальших досліджень є комплексний аналіз шляхів реагування НАТО на нові виклики і загрози, зокрема і на наслідки світової пандемії COVID-19 та дослідження напрямів подальшої політики Альянсу враховуючи зміни безпекового середовища.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Свєшніков С. В., Бочарніков В. П., Полякова О. В. Коронавірус і безпекове середовище: спроба неупередженого аналізу. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2020. № 2 (69). С.22–29.
2. Lord Campbell of Pittenweem. *COVID-19 and Transatlantic Security.* Draft special report, June, 2020. URL: https://www.nato-pa.int/document/2020-covid-19-and-transatlantic-security-105-pc-20-e-campbell-pittenweem (дата звернення: 25.07.2021).
3. Mesterhazy A. The Role of NATO's Armed Forces in the COVID-19 Pandemic. Draft Special Report", June, 2020. URL: https://www.nato-pa.int/download-file?filename=sites/default/files/2020-06/091%20DSC%2020%20E%20-%20COVID-19%20SPECIAL%20REPORT_1.pdf. (дата звернення: 25.07.2021).
4. Bentzen N. COVID-19 Foreign Influence Campaigns: Europe and Global Battle of Narratives. European Parliamentary Research Service. April 2020. URL: www.europarl.europa.eu/RegData/etudes/BRIE/2020/649367/EPRS_BRI(2020)649367_EN.pdf (дата звернення: 25.07.2021).
5. Jones K. COVID-19, International Security, and the Importance of NATO's Science and Technology Network. Draft special report. June 2020. URL: https://www.nato-pa.int/download-file?filename=/sites/default/files/2020-12/090%20STC%2020%20E%20rev%202%20fin%20-%20COVID-19%2C%20INTERNATIONAL%20SECURITY%2C%20AND%20THE%20IMPORTANCE%20OF%20NATO%E2%80%99S%20STO.pdf. (дата звернення: 25.07.2021).
6. NATO HQ Declaration by NATO Foreign Ministers issued following their meeting of 2nd April 2020. URL: https://www.nato.int/cps/en/natohq/official_texts_174855.htm. (дата зверненн: 25.07.2021).
7. NATO Review – Exercise Defender-Europe 20: enablement and resilience in action. URL: https://blog.act.nato.int/wordpress/2020/06/nato-review-exercise-defender-europe-20-enablement-and-resilience-in-action/ (дата звернення: 25.07.2021).
8. COVID-19 AND TRANSATLANTIC SECURITY URL: https://www.nato-pa.int/download-file?filename=/sites/default/files/2020-12/105%20PC%2020%20E%20rev.2%20fin%20-%20COVID-19%20AND%20TRANSATLANTIC%20SECURITY.pdf. (дата звернення: 25.07.2021).
9. NATO HQ NATO and Allied response to COVID-19 by the numbers, June 2020. URL: https://www.youtube.com/watch?v=nIlJfzRgvVc&feature=youtu. (дата звернення: 25.07.2021).
10. Supreme Allied Command Transformation HQ (SACT HQ, 2020) "Food for Thought" (FFT) Paper on Post COVID-19 Global Security Landscape, pp. 14-15. Distributed 16.06.20 in SACT HQ. URL: https://www.act.nato.int/application/files/6716/1915/3701/20200623_fft-covid.pdf. (дата звернення: 25.07.2021).
11. NATO HQ Russia's Top Five Myths about NATO & COVID, April 2020. URL: www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/2004-Factsheet-Russia-Myths-COVID-19_en.pdf. (дата звернення: 25.07.2021).
12. Словник. Портал української мови та культури. URL: https://slovnyk.ua/ (дата звернення: 25.07.2021).

Стаття надійшла до редакційної колегії 30.07.2021

NATO and the global pandemic: from uncertainty to an action plan

Annotation

The global pandemic caused by the COVID-19 virus been raging in the world for almost two years. Undoubtedly, the pandemic has become an unprecedented challenge to the world and its consequences will continue to impact on life spheres of individual countries and policies pursued by international organizations, including the North Atlantic Treaty Organization.

The issue of researching the impact of the global pandemic on NATO activities is absolutely new for both foreign and domestic scientists.

Given the unprecedentedness of this level of pandemic, NATO was not ready to promptly counter the spread of this virus. However, it took Alliance leadership a short time to begin responding to the new challenge, led by NATO's Strategic Command Transformation.

In the article, based on the analysis carried out, the following were determined:

1. Priorities of the Alliance:

the first is to ensure that the level of risk of virus infection of personnel is reduced;

second, maintaining (maintaining) an appropriate level of work efficiency;

third, gradual but persistent adaptation to new conditions;

2. The main activities carried out and planned in NATO to combat the global challenge:

institutional, related to changes in the procedures for making decisions at the strategic level at the level of heads of state and government;

organizational, concerning changes in the practical plane of the Alliance's activities, including measures of education and training, joint military exercises, conducting operations and implementing planned rotations of deployed contingents;

informational, covering both measures aimed at promptly and impartially informing the general public about the pandemic, and at countering the propaganda deployed by certain countries in order to discredit NATO as a single international organization capable of providing collective defense for its member countries. Particular attention and efforts are focused, in particular, on countering the campaign of disinformation and accusations on the part of the Russian Federation.

The study proves that, despite the scale and impact of the COVID-19 pandemic, NATO has contributed to curbing it and has demonstrated its ability to respond to crises.

Keywords: NATO; pandemic; NATO response; COVID-19.

УДК 358.211 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/70-77

Ворович Б. О., канд. військ. наук, доцент (0000-0002-4083-3707)

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

Управління ризиками розроблення та імплементації основних концептуальних документів оборонного планування

Резюме. У статті розглянуті можливі шляхи вирішення питань управління ризиками імплементації основних концептуальних документів оборонного планування в України.

Ключові слова: імплементація документів; ризики; ризикостворюючі фактори; оцінювання та управління ризиками.

Постановка проблеми. Різноманітність та значна чисельність проєктів основних концептуальних документів оборонного планування, які на сьогодні розробляються, їх відповідність сучасним вимогам, підвищена складність реалізації внаслідок існуючих політичної, економічної, соціальної ситуацій в Україні та недостатня підготовленість фахівців до законотворчої діяльності ініціює чисельні ризики, які суттєво впливають на результативність та ефективність програмного документа, підвищують витрати та час на реалізацію цілей і визначених завдань. Отже питання управління ризиками імплементації основних концептуальних документів оборонного планування Україні є пріоритетною і актуальною задачею, яка передбачає науково обґрунтовану діяльність у процесі управління ризиками для кожного його елемента: ідентифікація, оцінювання, оброблення, моніторинг і вплив на нього.

Зважаючи на реальні умови виникнення ризиків імплементації основних концептуальних документів оборонного планування в України та їх вплив на виконання визначених завдань, виникає необхідність щодо пошуку шляхів вирішення проблемних питань та розроблення більш ефективних засобів і методів для їх уникнення.

Аналіз останніх досліджень і публікацій. У публікаціях дослідників [1–7, 13, 14], присвячених управлінню програмними проєктами, наведені переліки ідентифікованих ризиків. Переліки акцентують увагу керівників (розробників) програмних документів на чинниках, які є типовими та не стосуються ризиків проєктів концептуальних документів оборонного планування. Відсутній також системний аналіз управління ризиками імплементації програмних документів і не розглянуті можливі шляхи управління ними та реагування на них. Унаслідок цього вже проведені дослідження потребують розроблення зручних для практичного застосування методів управління ризиками імплементації основних концептуальних документів оборонного планування.

Мета статті – обґрунтування шляхів управління ризиками імплементації основних концептуальних документів оборонного планування та заходів з управління ризиками для підвищення ефективності імплементації документів оборонного планування.

Виклад основного матеріалу. Основоположні документи, які охоплюють усі сфери національної безпеки і оборони, є підґрунтям для розроблення детальних планів і їх імплементації. Документи стратегічного та оборонного планування, які наведені в табл. 1, є основою для розроблення або внесення змін до цілої низки законодавчих актів у сфері безпеки і оборони.

Правовою основою діяльності Збройних Сил (ЗС) України є Конституція України, Законодавчі акти, акти Президента України та Кабінету Міністрів (КМ) України, міжнародні договори, які регулюють відносини у сфері оборони.

Процес оборонного планування містить стандартний набір дій, зокрема оцінювання ризиків, пов’язаних з виконанням завдань (заходів), та план управління ризиками.

Оскільки у статті розглядаються ризики імплементації основних концептуальних документів оборонного планування та заходи з управління ними, для підвищення ефективності імплементації документів оборонного планування, доцільно надати визначення основних понять.

Під *ризиком імплементації* основних концептуальних документів оборонного планування (далі – документів) розуміється подія або умова, яка може статися в майбутньому під час імплементації програмного документа (ПД) і негативно вплинути на виконання ПД, та може привести до недосягнення цілей і завдань визначених у ньому.

Таблиця 1

Документи оборонного планування у сфері національної безпеки і оборони

Нормативний документ	Часовий горизонт
Стратегія національної безпеки і оборони України	Документи довгострокового планування
Стратегія воєнної безпеки України (розроблятиметься за результатами проведення оборонного огляду)	
Стратегія громадської безпеки та цивільного захисту України (розроблятиметься за результатами огляду громадської безпеки та цивільного захисту)	
Стратегія розвитку оборонно-промислового комплексу України на період до 2028 року	
Стратегія кібербезпеки України	
Національна розвідувальна програма	Середньо- та довгострокова перспектива
Стратегія сталого розвитку	
Аналітична доповідь до щорічного Послання Президента України до Верховної Ради України “Про внутрішнє та зовнішнє становище України”	
Стратегічний оборонний бюлетень	Середньо- та довгострокова перспектива
Державні програми розвитку ЗС України	
Державні програми розвитку озброєння та військової техніки	

Не можна сказати заздалегідь, чи відбудеться ця подія, але відомо, що її виникнення позначиться на функціоналі, якості, вартості або терміні виконання проєкту ПД.

Ризики розроблення проєктів ПД знаходяться в безпосередньому зв’язку з ризиками імплементації ПД, тісно пов’язані та витікають один з одного, тому можливо припустити однаковий підхід щодо управління ризиками, але потрібно враховувати, що управління ризиками імплементації є більш складним через більшу невизначеність і терміни реалізації проєктів.

До основних показників (індикаторів) імплементації концептуальних документів оборонного планування у сфері оборони і безпеки можна віднести:

1. Відсутність або невідповідність концептуального документа: нормативно-правовій базі; вимогам, принципам, що ставляться до законодавчого документа; цілям і завданням довгострокової перспективи концептуального документа оборонного планування; сучасним Євроатлантичним підходам та стандартам армій держав – членів НАТО; політичним, економічним, військовим, науковим, організаційним заходам щодо захисту і оборони держави.

2. Невизначення: реальних термінів для виконання вимог законодавчого документа; пріоритетних напрямів розвитку порушених питань і завдань; основних орієнтовних показників забезпечення матеріальними, фінансовими та людськими ресурсами для реалізації концептуальних документів оборонного планування.

3. Нецілеспрямованість, неефективність, нереальність, необґрунтованість, неконкретність, негнучкість, нединамічність, некомплексність, несистемність.

Поява кожного з ризиків можлива за наявності причин (процесів або явищ), що сприяють його виникненню і пояснюють, чому наступ ризику неминучий. Такі явища називають ризикостворюючими факторами [9].

Для стандартизації та уніфікації термінології ризикостворюючими факторами, оцінювання їх впливу на конкретні цілі проєкту концептуального документа оборонного планування України та його подальшої імплементації необхідна систематизація та класифікація факторів за певними ознаками. Так під час виконанні аналізу ризиків необхідно визначити такі якісні та кількісні оцінки ризиків і ризикостворюючих факторів:

ймовірність появи ризикостворюючих факторів і рівень їх впливу на цілі (завдання) ПД;

часовий діапазон прояви ризикостворюючих чинників;

ризикостворюючі фактори, що мають критичний вплив на результати документа оборонного планування та потребують якомога найшвидшого реагування;

ймовірність досягнення цілей (завдань) ПД.

З огляду на явний логічний взаємозв’язок між цілями проєкту і можливими ризиками, можна припустити, що під час розроблення ПД можуть виникнути чотири типи (категорії) ризиків [6, 8, 9]:

зрив планових термінів проєкту;

перевищення вартості (бюджету) проєкту;

критичні відхилення за складом і змістом проєкту (невиконання функціональних вимог);

критичне відхилення за показниками якості проєкту (невиконання функціональних вимог).

Розглядати ризик імплементації документів пропонується з трьох точок зору [7]:

ризик як можливість загрози реалізації (виконання) ПД;

ризик як негативна подія, що не дає змоги досягти повною мірою мети та завдань, що визначені в документі;

ризик як невизначеність між виникаючими несприятливими ситуаціями і можливими діями щодо їх усунення.

Для класифікації факторів ризику рекомендовано використовувати ієрархічний метод класифікації, під час якого безліч ризикостворюючих факторів послідовно відповідно до обраних ознак класифікації розбивається на певні рівні [7].

На першому рівні класифікатора у якості підстави класифікації використовується модель життєвого циклу проєкту ПД: ініціація – розроблення – просування – впровадження (табл. 2).

Таблиця 2

Співвідношення цілей і ризиків ПД

Етапи ЖЦ	Цілі	Ризики
Ініціація	Розроблення концепції майбутнього ПД	Помилки у виборі функціоналу і, як наслідок, незатребуваність ПД, порушення термінів його виконання
Розроблення	Розроблення проєкту ПД з необхідним функціоналом при обмеженні на терміни і бюджету	Критичні відхилення за термінами і бюджету проєкту ПД
Просування	Забезпечення визначеному інтервалу часу заданого обсягу розроблення проєкту ПД при обмеженні виділеного бюджету	Невідповідність між бажаними і фактичними обсягами розроблення проєкту ПД. Наявність критичних відхилень за бюджетом програми просування
Впровадження (імплементація)	Забезпечення процесу впровадження ПД відповідно до вимог нормативно-правових актів та відносин між розробниками ПД і виконавцями його впровадження	Критичні відхилення за термінами і бюджету впровадження (імплементації)

На другому рівні для кожного етапу життєвого циклу ПД можна виділити зовнішні та внутрішні фактори. Зовнішні фактори – це події, які лежать за межами контролю та впливу розробників проєкту ПД. Внутрішні фактори визначають здатність самої організації успішно реалізувати ПД (табл. 3).

Таблиця 3

Склад зовнішніх і внутрішніх первинних факторів ризику імплементації ПД

Класифікація	Первинні фактори ризику
Внутрішні фактори ризику	
Програмний документ	Невизначеність вимог, часті зміни цілей і завдань документа. Нереальні терміни розроблення проєкту документа та його реалізації. Можлива зміна розробників (виконавців) ПД. Недостатня підтримка та допомога з боку замовника виконавців ПД. Нестабільне фінансування робіт щодо впровадження (реалізації) документа. Низька готовність замовників щодо впровадження (реалізації) документа
Персонал	Часта зміна виконавців ПД. Некомпетентність та відсутність досвіду щодо розроблення ПД та його імплементації. Небажання або ігнорування виконавців (розробників) документа сумлінно виконувати обов'язки
Управління розробленням та реалізацією ПД	Відсутність у розробника ефективної методології управління розробленням та імплементацією ПД. Помилки у розрахунках фінансових витрат на розроблення та імплементацією ПД. Помилки в оцінці трудомісткості та термінів виконання робіт. Невиконання стандартів і вимог до розроблення та імплементації ПД. Відсутність ефективної взаємодії із замовником
Зовнішні первинні фактори ризику	
Держава	Зміни нормативно-правових механізмів розроблення та імплементації ПД. Зміни економічної ситуації в державі, воєнній сфері
Споживачі (виконавці ПД)	Неповнота і неточність оцінювання ПД. Невідповідність функціональних характеристик ПД потребам споживачів. Незатребуваність, несвоєчасність, застарілість ПД. Приховане протистояння фахівців-споживачів упровадженню ПД. Низький рівень підготовки користувачів ПД. Поява нових документів, що конфліктують з розробленим концептуальним ПД
Фінансовий ринок	Коливання курсу валют. Зміна ставок по кредитах

На третьому рівні прояв зовнішніх факторів обумовлюється як політикою держави щодо концептуальних ПД, так і різними ситуаціями в державі, воєнній сфері. Набір внутрішніх факторів визначається складом системної моделі діяльності: засобами діяльності, предметами діяльності, кадрами, технологією.

Четвертий рівень являє собою набір первинних факторів ризику. До того ж допускається можливість належності того ж самого фактора різними підставами класифікації.

Вплив ризикостворюючих факторів на цілі (завдання) ПД відображає міру негативних наслідків (зміни вартості, термінів виконання, змісту, якості) під час реагування на конкретний ризикостворюючий фактор. Втрати можуть оцінюватися у вигляді можливого збільшення бюджету проєкту ПД, перегляду (зриву) термінів, невідповідності вимогам та змісту, додатковим витратам на запобігання ризиків і таке інше.

Оцінювання ймовірності появи факторів ризику імплементації ПД та впливу на цілі (завдання) ПД може бути проведене за кожним ризикостворюючим фактором окремо для кожної цілі ПД: вартості, часу, змісту і якості. До того ж імовірність має бути більше нуля (інакше ризикостворюючий фактор не впливає) і менше одиниці (інакше прояв фактора не містить невизначеності та являє собою відому проблему).

Оцінювання може проводитися на підставі результатів опитувань розробників проєкту ПД і експертів (фахівців, які мають широкі пізнання в питаннях, що оцінюються).

Значення показників імовірності та впливу можуть оцінюватися як у кількісних, так і у якісних шкалах. Для визначення ймовірності та впливу виникнення конкретного ризику, застосовують метод експертних оцінок, при якому можливо використовувати рейтингову шкалу від 1 до 5 балів.

Серед кількісних методів оцінювання ймовірності ризикостворюючих факторів і їх впливу на цілі (завдання) проєкту ПД найбільш часто використовується метод PERT-аналізу (Project Evaluation and Review Technique) [2]. Сутність його полягає в тому, що для кожної характеристики експерту необхідно вказувати три оцінки – оптимістичну, найбільш імовірну (реалістичну) і песимістичну.

Тоді ймовірність настання ризикостворюючих факторів можна обчислити за формулою

$$P\left(x_j\right)=\frac{p_1x_j+4\left(p_2x_j\right)+p_3x_j}{6},$$

де p_1, p_2, p_3 – оптимістична, реалістична і песимістична ймовірності настання ризикостворюючого фактора x_j-го ризику відповідно.

Однак з огляду на сформульовані особливості ПД, оцінки ризикостворюючих факторів не завжди можна описати за допомогою числових значень. У такому випадку для цих цілей доцільно використовувати якісну шкалу з градаціями: низька, середня, висока вірогідності. Крім того, за відсутності достовірних статистичних даних про ПД, оцінки ризикостворюючих факторів формуються, як правило, шляхом проведення опитування експертів. У цьому разі доцільно використовувати математичний апарат нечіткої логіки [10].

Для оцінювання ймовірності прояви ризиків і ступеня їх впливу на цілі проєкту пропонується такий зміст градацій ймовірностей:

низька – цілі ПД і вимоги добре зрозумілі та документовані, масштаб і рамки задані чітко, ресурси доступні у повному обсязі, під час реалізації проєкту не потрібно освоєння нових інструментальних засобів розробки;

середня – цілі ПД визначені більш-менш чітко, масштаб і рамки задані добре, ресурси в основному доступні, під час реалізації проєкту використовуються нові, але добре освоєні інструментальні засоби;

вище середнього – цілі ПД недостатньо чіткі, вимоги викладені нечітко і можуть змінюватися, масштаб і рамки проєкту визначені недостатньо чітко, ресурси сильно обмежені, ПД реалізується з використанням нових інструментальних засобів;

висока – цілі проєкту нечіткі, вимоги не визначені, масштаб і рамки незрозумілі, ресурси практично відсутні, під час реалізації ПД використовуються нові, але недостатньо освоєнні інструментальні засоби.

Експерти під час оцінювання ймовірності мають аналізувати причини і умови, які можуть привести до прояву ризику або ризикостворюючих факторів.

Для оцінювання ймовірності прояву ризику проєкту ПД та якісної інтерпретації умов його прояву пропонується використовувати шкалу, представлену в табл. 4 [11].

Таблиця 4

Шкала оцінювання ймовірності прояву ризикостворюючих факторів

Якісна оцінка	Низька	Середня	Вище середньої	Висока
Інтервал кількісної оцінки	0,01–0,24	0,25–0,49	0,5–0,74	0,75–1,0

У табл. 5 з урахуванням рекомендацій [9] представлена можлива шкала оцінювання впливу ризикостворюючих факторів на реалізацію мети та заходів ПД.

Таблиця 5

Шкала оцінювання впливу факторів на цілі (заходи) ПД

Мета ПД	Вплив фактора				
	Незначний: < 0,15	***Помірний 0,16-0,3***	***Високий 0,4-0,6***	***Критичний 0,7–0,8***	***Катастрофічний > 0,8***
Вартість	Незначне збільшення вартості	Збільшення вартості < 10 %	збільшення вартості 10-20 %	Збільшення вартості 20-40 %	Збільшення вартості > 40 %
Терміни	Незначне збільшення часу	Збільшення часу < 5 %	Збільшення часу 5-10 %	Збільшення часу 10-20 %	Збільшення часу > 20 %
Зміст	Ледь помітне зменшення змісту	Зачеплені другорядні області змісту	Порушені основні області змісту	Зменшення вмісту неприйнятно для замовника	Проєкт ПД практично некорисний
Якість	Ледь помітне зниження якості	Порушено не самі трудомісткі завдання	Для зниження якості потрібні схвалення змін до мети та завдань проєкту ПД	Зниження якості неприйнятно для проєкту ПД	Кінцевий продукт – проєкт ПД практично не потрібен

За результатами ідентифікації та аналізу зазначених показників можливо виділити множину ризикостворюючих факторів, які мають критичний вплив на реалізацію ПД і потребують якнайшвидшого реагування на них. Ця процедура може бути реалізована за допомогою побудови і аналізу матриці: ймовірність появи – вплив (табл. 6) [12].

Таблиця 6

Матриця ймовірності появи та впливів ризикостворюючих факторів

Ймовірність появи	Вплив				
	0,01–0,15	**0,16–0,3**	**0,4–0,6**	**0,7–0,8**	**> 0,8**
0,75–1,0	0,0075–0,15	0,075–0,4	0,15–0,6	0,375–0,9	0,6–0,99
0,5–0,74	0,005–0,111				
0,25–0,49					
0,01–0,24					

Для побудови матриці використовуються отримані раніше оцінки ймовірності появи ризикостворюючих факторів і рівень їх впливу на цілі ПД. Множення цих величин визначає єдину інтегральну оцінку критичності ризикостворюючого фактора. Чим вище ймовірність прояву ризикостворюючих факторів, тим вище його вплив на розроблення та імплементацію ПД. Залежно від значення впливу визначається ранг та близькість настання ризику (табл. 8).

Однією з важливих характеристик ризиків і ризикостворюючих факторів є близькість їх настання. Природно, що за інших рівних умов ризиків, які можуть здійснитися вже завтра, слід своєчасно і негайно приділяти більше уваги, ніж тим, які можуть відбутися не раніше ніж через півроку.

Можлива шкала оцінювання близькості ризику представлена в табл. 7.

Інтегральна оцінка критичності і характеристика близькості настання ризикостворюючого фактора є основою для його ранжирування. Ранг визначає його порядковий номер у повній сукупності ризиків проєкту. Чим вище ранг, тим небезпечніший ризик (табл. 8).

Таблиця 7

Відносна шкала вимірювання наближення ризику

Кількісне значення наближення ризику	Більше ніж через ...	Від ... до	Менше ніж через ...
Якісне значення наближення ризику	Нескоро	Не дуже скоро	Дуже скоро

Таблиця 8

Матриця рангів виявлених ризиків проєкту ПД

Основні фактори	Імовірність	Вплив	**Ранг** **Близькість настання ризику**
Відсутність у розробників необхідного досвіду з розроблення ПД	Висока	Катастрофічний (**>0,8)**	9 Дуже скоро
Поява нових аналогічних (додаткових) проєктів ПД	Висока	Критичний **(0,4-0,8)**	6 Не дуже скоро
Зміна нормативного регулювання процесів (завдань), що визначені в ПД	Низька	Мало критичний **(0,01-0,3)**	4 Нескоро

Ранжирування факторів ризику дасть змогу розробникам проєктів ПД розподілити їх за категоріями небезпеки наслідків під час імплементації ПД [11], а саме:

потребують негайного реагування;

реагування можна виконати пізніше;

потребують додаткового розгляду (включаючи кількісний аналіз);

надалі має проводитися спостереження.

Процеси планування заходів з реагування на ризики імплементації і їх моніторинг припускають вибір стратегії зниження загроз для кожної з цілей проєктного плануючого документа і розроблення планів заходів щодо їх реалізації. Згідно з [13] можливі чотири види дій: ухилення від ризику, передача ризику, зниження ризику, прийняття ризику.

Ухилення від ризику передбачає розроблення комплексу заходів з нейтралізації критичних ризикостворюючих чинників, тобто зміна плану управління проєктом під час імплементації документів таким чином, щоб виключити вплив негативних чинників на цілі проєкту або скорегувати цільові показники, що знаходяться під загрозою, наприклад, відмовитися від реалізації ризикованої функціональної вимоги.

Передача ризику має на увазі перекладення негативних наслідків від прояву ризикостворюючого фактора на “іншу сторону” (але ризик при цьому залишається). Ці дії ефективні для нейтралізації критичних ризикостворюючих факторів, які впливають на бюджет проєкту ПД.

Зниження ризику передбачає зниження ймовірності та/або наслідків негативного прояву ризикостворюючого фактора до прийнятних меж, наприклад, збільшити терміни розроблення проєкту ПД, знизити значення низки показників якості ПД. Вжиття запобіжних заходів щодо зниження вірогідності настання фактора або його наслідків часто виявляється більш ефективним, ніж дії щодо усунення негативних наслідків, що вживаються після настання події.

Прийняття ризику передбачається у разі, коли через усунення прояву ризикостворюючого фактора малоймовірно і розробники проєкту ПД не знайшли ефективних заходів реагування на ризики. Реалізація цієї стратегії можлива у двох варіантах: активному або пасивному.

Пасивне прийняття цієї стратегії не передбачає проведення будь-яких запобіжних заходів, залишаючи розробникам ПД право діяти на власний погляд в разі настання негативних подій. Найбільш поширеною формою активного прийняття цієї стратегії є створення резерву на непередбачені обставини у вигляді можливості залучення додаткових фінансових і/або інших ресурсів, або коригування термінів реалізації ПД.

Одним з можливих математичних апаратів прийняття рішень щодо вибору стратегії зниження загроз є апарат таблиць рішень.

Складання планів заходів якісного і кількісного аналізу ризикостворюючих факторів проводиться відповідно до їх рангів.

За кожним із заходів призначають одного або декілька відповідальних осіб (відповідальних за реагування на ризики), визначаються бюджет і терміни виконання заходу. Затверджений план заходів, пройшовши експертизу, має бути включений у загальний процес управління змінами ПД [1].

Нижче наводиться опис заходів, спрямованих на зниження низки ризикостворюючих факторів (табл. 9).

Для встановлення відкритих і довірливих відносин із розробниками та замовниками ПД необхідно здійснювати такі заходи: постійна взаємодія та узгодження з питань пошуку взаємоприйнятних рішень щодо виконання проєкту ПД для їх тестування і оцінки та подальшої імплементації.

Таблиця 9

Перелік основних заходів, спрямованих на зниження низки ризикостворюючих факторів

Назва фактора	Зміст фактора	Заходи	Результат, що очікуються
Негативний вплив	Неповні або нечіткі вимоги до програмного продукту	Знизити завдяки зміні вартості та строків реалізації проєкту ПД під час коригування вимог; використання моделей ЖЦ	Дозволить періодичне уточнення вимог; ведення робіт з відповідним ресурсом і тривалістю виконання
	Зміна ситуації на фінансовому ринку	Знизити шляхом урахування умов	Коригування вартості проєкту ПД у разі кризових явищ (наприклад, зміна курсу валют)
Негативні наслідки	Недостатні навички володіння виконавцями засобами розроблення ПД	Зменшити завдяки залученню експертів-консультантів на початкових етапах розроблення проєкту ПД та врахуванню під час оцінювання трудомісткості виконавців додаткового часу на навчання розробників ПД	Поліпшення якості ПД, уточнення трудомісткості виконавців (розробників) ПД

Моніторинг та управління ризиками імплементації – є процес ідентифікації, аналізу ризиків та ризикостворюючих факторів, планування заходів з реагування на нові ризики, відстеження раніше ідентифікованих ризиків, а також перевірки та виконання заходів з реагування на ризики і оцінки ефективності їх виконання. До того ж необхідно постійно вирішувати такі завдання: перегляд ризиків, аудит ризиків, аналіз відхилень і трендів.

Перегляд ризиків передбачає регулярну, згідно з прийнятими регламентами, ідентифікацію, аналіз і планування реагування на нові ризики. Управління ризиками проєкту ПД має бути під постійним контролем.

Аудит ризиків – це вивчення і надання в документальному вигляді результатів оцінювання ефективності виконання заходів з реагування на ризики, що потребують негайного реагування, аналізу основних причин їх виникнення.

На підставі аналізу відхилень і трендів проєкту ПД можна прогнозувати на плановий період вплив негативних наслідків прояву ризикостворюючих факторів на цілі (завдання) ПД. Контроль і аналіз трендів може спричинити за собою вибір альтернативних стратегій, прийняття коректив, перепланування проєкту ПД для досягнення його цілей і завдань.

Висновок. Використання запропонованих шляхів управління ризиками імплементації основних концептуальних документів оборонного планування враховують імовірність впливу, зменшують суб'єктивність результатів, дають змогу розробникам ПД оборонного планування та керівникам (виконавцям) запланованих заходів зменшити ризики або їх уникнення, скоротити вплив ризику імплементації на проєкт ПД до прийнятного рівня завдяки науково обґрунтованому способу реагування та своєчасного прийняття вірних управлінських рішень.

За результатами дослідження запропоновано метод оцінювання ризиків імплементації як окремих ризикостворюючих факторів проєктів концептуальних документів оборонного планування. Цей метод дає змогу підбирати спосіб управління (реагування) на кожний ідентифікований ризик.

Подальші дослідження доцільно продовжити в напрямі застосування запропонованих рекомендацій щодо імплементації документів оборонного планування в секторі безпеки і оборони.

СПИСОК ВИКОРИСТАННОЇ ЛІТЕРАТУРИ

1. Руководство к своду знаний по управлению проектами (PMBOK). 4-е изд. Москва : Project Management Institute, 2010. 496 с.
2. Фатрелл Роберт Т., Шафер Дональд Ф., Шафер Линда И. Управление программными проектами. Достижение оптимального качества при минимуме затрат. Москва : Вильямс, 2004. 1136 с.
3. Ньюэлл Майкл В. Управление проектами для профессионалов. Руководство по подготовке к сдаче сертификационного экзамена / пер. с англ.

А. К. Казакова. 3-е изд. Москва : КУДИЦ-ОБРАЗ, 2006. 416 с.
4. Хэлдман Ким. Управление проектами. Быстрый старт / пер. с англ. Ю. Шпаковой ; под ред. С.И. Неизвестного. Москва : ДМК Пресс; Академия АйТи, 2008. 352 с.
5. Математические основы управления проектами : учеб. пособ. для вузов / С. А. Баркалов и др. ; ред. В. Н. Бурков. Москва : Высшая школа, 2005. 421 с.
6. Основы управления проектами. URL: http://www.e-college.ru (дата звернення: 12.05.2021).
7. Ехлаков Ю. П. Классификация и описание рискообразующих факторов при создании программных продуктов : доклады ТУСУРа. 2013. № 4 (30). С. 142–147.
8. Липаев В. В. Экономика производства программных продуктов. 2-е изд. Москва : СИНТЕГ, 2011. 352 с.
9. Авдошин С. М., Песоцкая Е. Ю. Информатизация бизнеса. Управление рисками. Москва : ДМК Пресс, 2011. 176 с.
10. Заде Л. Понятие лингвистической переменной и ее роль в принятии приближенных решений. Москва : Мир, 1976. 168 с.
11. Архипенков С.Я. Лекции по управлению программными проектами. URL: http://www.arkhipenkov.ru/resources/sw_Droject_management.pdf. (дата звернення: 12.05.2021).
12. Евланов Л. Г. Теория и практика принятия решений. Москва : Экономика, 1984. 176 с.
13. Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS). 12 February 2015. Joint Staff, 2015. 416 p.
14. Comprehensive Political Guidance Endorsed by NATO. Heads of State and Government on 29 November 2006. Riga. Latvia. Part 3. § 11.

Стаття надійшла до редакційної колегії 17.06.2021

Risk management of the development and implementation of the main conceptual documents of defense planning

Annotation

Diversity and significant number of drafts of the main conceptual documents of defense planning; the need for their compliance with modern requirements, the increased complexity of implementation, due to the existing political, economic, social situations in Ukraine and the insufficient preparedness of specialists for lawmaking activities initiates numerous risks that significantly affect the effectiveness and efficiency of the program document, increase the costs and time for achieving goals. So the issue of risk management in the implementation of the main conceptual documents of defense planning in Ukraine is a priority and urgent task, which provides for scientifically based activities in the risk management process for each of its elements: identification, assessment, processing, monitoring and impact on it.

The *risk of implementation* of the main conceptual documents of defense planning is understood as an event or condition that may occur in the future during the implementation of the program document (PD), adversely affect the implementation of the PD and lead to failure to achieve the goals and objectives defined in it.

The use of the proposed ways of managing the risks of the implementation of the main conceptual documents of defense planning takes into account the likelihood of impact, reduces the subjectivity of the results, allows developers of defense planning PDs to reduce or avoid risks, reduce the impact of the implementation risk on the PD project to an acceptable level, thanks to a scientifically grounded response method and timely adoption of adequate management decisions.

Based on the results of the study, a method is proposed for assessing the risks of implementation as individual risk-forming factors of draft conceptual documents for defense planning. This method allows you to select a management (response) method for each identified risk.

Keywords: implementation of documents; risks; risk generating factors; risk assessment and management.

УДК 355.45.02 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/78-83

Поляєв А. І. (0000-0002-6710-5144)

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

Підходи щодо розроблення методики імплементації концептуальних документів стратегічного та оборонного планування

Резюме. У статті на основі аналізу вітчизняного і зарубіжного досвіду розглянуто можливі підходи щодо розроблення методики імплементації концептуальних документів стратегічного та оборонного планування у процесі оборонного менеджменту в Міністерстві оборони України та Збройних Силах України.

Ключові слова: методика імплементації концептуальних документів стратегічного та оборонного планування; державний менеджмент; спроможність; оборонне планування на основі спроможностей.

Постановка проблеми. Державна політика у сфері оборони спрямовується на створення сучасних, мобільних і боєздатних сил оборони, які спільно з іншими інституціями держави забезпечуватимуть всеохоплюючу оборону України, захист її суверенітету, територіальної цілісності та недоторканності.

Базовими документами у цих сферах є Закон України "Про національну безпеку України" від 21.06.2018 № 2469-УП, Укази Президента України "Про затвердження Стратегії національної безпеки України" і "Про затвердження Стратегії воєнної безпеки України", Постанова Кабінету Міністрів України "Про затвердження Порядку проведення оборонного огляду Міністерством оборони" від 31.10.2018 № 941, наказ Міністерства оборони України "Про затвердження Порядку організації та здійснення оборонного планування в Міністерстві оборони України, Збройних Силах України та інших складових сил оборони" від 22.12.2021 № 484 [1–5].

Одним із важливих пріоритетів реалізації державної політики у сфері оборони є виконання завдання з імплементації концептуальних нормативно-правових актів взаємоузгоджених з іншими документами оборонного планування в системи оборонного менеджменту Міністерства оборони України та Збройних Сил України [3].

Саме тому, вважається актуальним і невідкладним завдання щодо визначення підходів до розроблення методики імплементації концептуальних документів стратегічного та оборонного планування в Міністерстві оборони України та Збройних Силах України з урахуванням досвіду держав – членів НАТО.

Аналіз останніх досліджень і публікацій, у яких висвітлювалися питання імплементації документів стратегічного планування, свідчить про те, що в сучасних умовах розвитку методології оборонного планування в Україні імплементація стає невід'ємною частиною діяльності центральних органів виконавчої влади [7].

Протягом останніх кількох років провідними вітчизняними науковцями здійснюється пошук шляхів удосконалення системи оборонного планування, впровадження оборонного менеджменту в діяльність Міністерства оборони України та Збройних Сил України. Цій проблематиці присвячено низку наукових досліджень, зокрема І. С. Руснака, А. Г. Петренка, П. В. Щипанського, С. О. Кириченка, І. М. Романюка, Ф. В. Саганюка та ін. [6, 7, 11, 12].

Водночас у цих наукових працях недостатньо уваги приділяється питанням розроблення методики імплементації концептуальних документів стратегічного та оборонного планування як невід'ємного елемента системи оборонного менеджменту.

Отже, виникає потреба у пошуку нових підходів до розроблення методики імплементації концептуальних документів стратегічного та оборонного планування в процесі оборонного менеджменту в Міністерстві оборони України та Збройних Силах України.

Мета статті полягає у визначенні підходів щодо розроблення методики імплементації концептуальних документів стратегічного і оборонного планування в системі оборонного менеджменту в Міністерстві оборони України та Збройних Силах України з використанням вітчизняного

досвіду і принципів та підходів, прийнятих в державах – членах НАТО.

Виклад основного матеріалу. На сьогодні остаточно не розроблена модель імплементації законів та інших нормативно-правових актів яка могла б послужити базовою основою процесу їх реалізації, тому перед вченими і практиками оборонної сфери постало складне завдання – розроблення теоретико-методологічних основ імплементації, термінологічного тлумачення її базових понять, а також рекомендацій і методики її здійснення.

Так, нині в Міністерстві оборони України та Збройних Силах України вживаються лише перші кроки щодо розроблення науково-методологічної бази імплементації, зокрема і методики імплементації концептуальних документів стратегічного та оборонного планування в системі оборонного менеджменту.

На теперішній час відсутнє однозначне розуміння єдиного методичного підходу до формування поняття концептуальні документи стратегічного та оборонного планування. Хоча окремі автори у своїх статтях робили спроби до формалізації цього визначення [7, 11]. А. І. Семенченко [13] вважає, що поряд з визначеними концептуальними документами національної безпеки та оборони України до їх складу має входити також сукупність концептуальних документів, що визначають розвиток сил оборони та її складових тощо.

З огляду на зазначене можна визначити, що *концептуальні документи* стратегічного та оборонного планування – це нормативно-правові акти (концепції, доктрини, стратегії, напрями, засади, основи, принципи, декларації тощо), у яких сформована система поглядів щодо організації та здійснення оборонного планування в Міністерстві оборони України та Збройних Силах України. Їх умовно можна класифікувати за термінами дії як концептуальні документи на довгострокову, середньострокову та короткострокову перспективу.

У сучасній науковій літературі достатньо широко розкриті поняття імплементації міжнародних нормативно-правових актів [7–9]. Однак у них не чітко визначені поняття імплементації державних нормативно-правових актів. Зокрема, у [10] йдеться про імплементацію як форму дій для досягнення бажаного результату. В інших публікаціях тільки фрагментарно розглядаються теоретичні засади імплементації, що не дає змоги комплексно оцінити способи імплементації і сформулювати відповідні підходи до її реалізації.

Автори [7] виклали підходи до можливої імплементації норм чинного Закону України “Про національну безпеку України”, пов’язані з формуванням сучасної системи планування та розвитку сектору безпеки і оборони, розробленням довго- та середньострокових документів стратегічного та оборонного планування з розвитку Міністерства оборони України та Збройних Сил України на основі спроможностей, з урахуванням досвіду імплементації норм законів держав – членів НАТО у підзаконні акти.

У дослідженнях [8, 9] висвітлюються деякі шляхи та підходи до імплементації основних норм Стратегічної концепції НАТО в Комплексній політичній директиві НАТО, прийнятій державами – членами у НАТО, яка забезпечує єдність підходів усіх членів Альянсу для досягнення спільної мети. У директиві визначаються пріоритети трансформації НАТО, спрямовані на ефективне виконання операцій, вдосконалення потенціалів, трансформацію сил і засобів, конкретні вимоги щодо сил і засобів. Закладені директивою підходи до імплементації в державах – членах НАТО відображаються в послідовній розробці документів оборонного планування на довгострокову, середньострокову і короткострокову перспективу.

Зважаючи на результати проведених досліджень, доцільно вважати, що *імплементація* (від англ. implementation, латин. impleo – здійснення, впровадження, досягнення, виконання) – це сукупність цілеспрямованих організаційно-правових та інституційних заходів, які здійснюються органами державної влади та іншими державними органами (зокрема Міністерством оборони України), організаціями (військовими організаційними структурами) і спрямовані на забезпечення виконання (реалізацію) ними прийнятих на себе зобов’язань (програм, планів).

Під *імплементацією концептуальних документів стратегічного та оборонного планування* у цій статті розуміється сукупність цілеспрямованих організаційно-правових та інституційних заходів, які здійснюються в Міністерстві оборони України та Збройних Силах України, і спрямованих на реалізацію державної політики у сфері оборони, що визначена законами, стратегіями, концепціями, доктринами, засадами, основами, деклараціями для ефективного розвитку Збройних Сил України.

Аналіз публікацій [7–12] свідчить про те, що імплементація положень та вимог концептуальних документів стратегічного та оборонного планування в процесі оборонного менеджменту може бути реалізована різними способами. Найбільш доцільними способами імплементації концептуальних документів стратегічного та оборонного планування можуть бути: інкорпорація; трансформація; відсилання [10].

Спосіб інкорпорації полягає у тому, що положення концептуальних документів без будь-яких змін дослівно відтворюються в проєктах нормативно-правових актів.

Під час застосування способу трансформації відбувається певна переробка норм відповідних концептуальних документів під час перенесення їх положень та вимог у проєкти нормативно-правових актів, що розробляються.

У разі застосування способу відсилання норми концептуальних документів безпосередньо не включаються в текст проєкту нормативно-правового акта, в якому міститься лише згадка про них.

Підходи до розроблення методики імплементації концептуальних документів стратегічного та оборонного планування можна уявити як поетапний процес, який наведено на рис. 1.

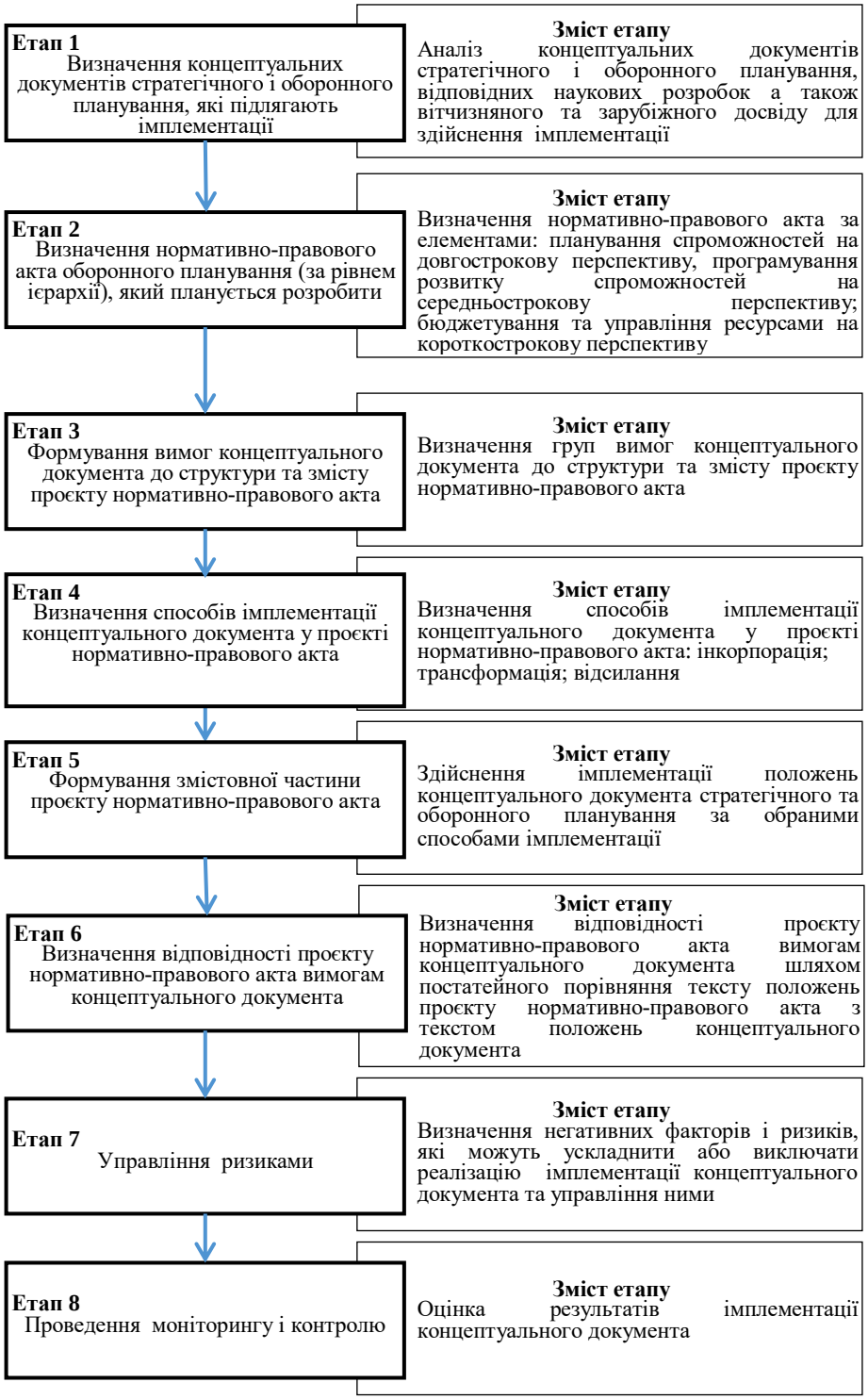


Рис. 1. Порядок імплементації концептуальних документів стратегічного і оборонного планування

На *першому етапі* імплементації стратегічного і оборонного планування та їх визначаються концептуальні документи основні положення, які підлягають

імплементації за напрямом розроблення проєкту нормативно-правового акта. Під час цього етапу проводиться аналіз законодавчих та нормативно-правових актів у сфері безпеки і оборони, відповідних наукових розробок, а також вітчизняного та зарубіжного досвіду щодо визначення документів стратегічного і оборонного планування та їх основних положень, які підлягають імплементації.

До основних концептуальних документів стратегічного і оборонного планування відносяться Закон України "Про національну безпеку України", Укази Президента України "Про затвердження Стратегії національної безпеки України" та "Про затвердження Стратегії воєнної безпеки України".

На *другому етапі* імплементації визначається нормативно-правовий акт оборонного планування (за рівнем ієрархії), який планується розробити, оскільки він забезпечуватиме найвищу ефективність імплементації концептуального документа.

Категорія нормативно-правового акта для здійснення імплементації концептуального документа визначається за елементами оборонного планування:

планування спроможностей на довгострокову перспективу;

програмування розвитку спроможностей на середньострокову перспективу;

бюджетування та управління ресурсами на короткострокову перспективу;

виконання програм і планів.

Основними нормативно-правовими актами оборонного планування є: Об'єднана оперативна концепція сил оборони, Державна (цільова) програма розвитку Збройних Сил України, Державна (цільова) програма розвитку ОВТ, План утримання та розвитку Збройних Сил України.

Під час *третього етапу* імплементації формуються вимоги концептуального документа до структури та змісту проєкту нормативно-правового акта.

На *четвертому етапі* імплементації визначаються способів імплементації концептуального документа (документів) в проєкт нормативно-правового акта.

Способи імплементації концептуального документа (документів) у проєкт нормативно-правового акта визначаються відповідно до його мети, структури та змісту. Найбільш доцільними способами імплементації концептуального документа (документів) є: інкорпорація, трансформація, відсилання.

На *п'ятому етапі* формування змістовної частини проєкту нормативно-правового акта, здійснюється імплементація положень концептуального документа (документів) стратегічного та оборонного планування за обраними способами імплементації за кожною визначеною статтею.

Імплементація концептуальних документів у проєктах нормативно-правових актах, які розробляються на відповідних рівнях оборонного планування (планування спроможностей, програмування розвитку спроможностей, бюджетування та управління ресурсами, виконання програм і планів) забезпечує ефективну реалізацію державної політики щодо досягнення спроможностей Збройних Сил України.

Для досягнення найбільш прийнятного (доцільного) варіанта імплементації концептуальних документів у проєкті нормативно-правового акта можуть розроблятися декілька їх варіантів.

На *шостому етапі* здійснюється визначення відповідності проєкту нормативно-правового акта вимогам концептуального документа.

Відповідність проєкту нормативно-правового акта вимогам концептуального документа здійснюється шляхом порівняння тексту положень проєкту нормативно-правового акта з текстом положень концептуального документа. Під час оцінювання відповідності положень проєкту нормативно-правового акта вимогам концептуального документа можуть застосовуються таки варіанти відповідності:

"відповідає вимогам" – якщо визначені основні завдання імплементації концептуального документа виконані у повному обсязі;

"частково відповідає вимогам" – якщо більшість визначених завдань імплементації концептуального документа виконані;

"не відповідає вимогам" – якщо мета імплементації концептуального документа не досягнута.

На етапі управління ризиками визначаються негативні фактори і ризики, які можуть ускладнити або виключати реалізацію імплементації концептуального документа.

Основними сферами виникнення ризиків під час реалізації імплементації концептуального документа можна визначити: соціально-економічні, організаційно-технологічні, нормативно-правові, кадрові.

Під час проведення моніторингу і контролю визначаються результати імплементації концептуального документа. На цьому етапі здійснюється:

аналіз та оцінювання стану реалізації положень нормативно-правового акта, у якому імплементовані концептуальні документи щодо досягнення стратегічних цілей (завдань) державної політики у сферах національної безпеки і оборони;

забезпечення виконання спланованих заходів у визначений термін;

досягнення визначених спроможностей (кількісних і якісних показників) оборонного планування у встановлені терміни;

забезпечення використання фінансових, матеріально-технічних та інших ресурсів за призначенням та їх ефективного розподілу.

Кожний із зазначених етапів імплементації концептуальних документів може супроводжуватися окремо розробленими моделями, які у сукупності дають змогу об'єктивно обґрунтувати перспективу імплементації концептуальних документів стратегічного та оборонного планування.

Висновки. У статті здійснено аналіз вітчизняного та зарубіжного досвіду держав – членів НАТО щодо імплементації нормативних документів у сфері оборони.

За результатами аналізу визначені підходи до розроблення методики імплементації концептуальних документів стратегічного та оборонного планування. Ці підходи є логічною послідовністю виконання її процедур, елементів та зв'язків між ними.

Таки підходи до імплементації нормативних документів можуть слугувати теоретико- методичною базою для розроблення методики імплементації концептуальних документів стратегічного та оборонного планування в Міністерстві оборони України та Збройних Силах України.

Напрямом подальших наукових досліджень є розроблення методики імплементації концептуальних документів стратегічного та оборонного планування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018.
2. Стратегія національної безпеки України : Указ Президента України від 14.09.2021 р. № 392/2020.
3. Стратегія воєнної безпеки України : Указ Президента України від 25.03.2021 р. № 121/2021.
4. Про затвердження Порядку проведення оборонного огляду Міністерством оборони : Постанова Кабінету Міністрів України від 31.10.2018 р. № 941.
5. 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 22.12.2021 р. № 484.
6. Руснак І. С., Петренко А. Г., Яковенко А. В., Романюк І. М., Кохно В. Д. Оборонне планування на основі спроможностей: особливості та перспективи впровадження. *Наука і оборона*. 2017. № 2. С. 3–10.
7. Тютюнник В. П., Горовенко В. К. Як імплементувати Закон України "Про національну безпеку України". *Defense Express*. URL: https://old.defence-ua.com/index.php/statti/publikatsiji-partneriv/5277-yak-implementuvaty-zakon-ukrayiny-pro-natsionalnu-bezpeku-ukrayiny (дата звернення: 23.07.2021).
8. Пальчик А. В. Деякі підходи до імплементації вимог концептуальних оборонних документів в НАТО. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2020. № 3 (70).
9. Брежнєва Т. В. Імплементація "Комплексної політичної директиви НАТО" як нового стратегічного документа. *Стратегічні пріоритети* : наук.-аналіт. зб. Київ, 2009. № 1 (10).
10. Клименко О. Базові засади імплементації міжнародних нормативних документів у діяльності наукових бібліотек України: термінологічний аспект. URL: http://nbuviap.gov.ua/ index.php? option=com (дата звернення: 23.07.2021).
11. Саганюк Ф. В., Кириченко С. О. Підходи до формування моделі для імплементації концептуальних документів у сфері оборони. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2020. № 3 (70).
12. 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*. Київ, 2021. № 1 (71).
13. Семенченко А. І. Розробка категорійно-понятійного апарату стратегічного планування з державного управління забезпеченням національної безпеки. URL: http://academy.gov.ua/ej/ej6/txts/07saiznb.htm. (дата звернення: 23.07.2021).

Стаття надійшла до редакційної колегії 20.08.2021

Approaches to developing methodic for implementing conceptual documents of strategic and defense planning

Annotation

One of the important priorities for the implementation of state policy in the field of defense is to implement the task of implementing conceptual regulations consistent with other defense planning documents in the defense management system of the Ministry of Defense of Ukraine and the Armed Forces of Ukraine. Therefore, it is considered relevant and exigent to determine approaches to the development of methods for implementing conceptual documents of strategic and defense planning in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine, taking into account the experience of NATO member-states.

The *implementation of conceptual documents of strategic and defense planning* in this article means a set of targeted organizational, legal and institutional measures implemented in the Ministry of Defense of Ukraine and the Armed Forces of Ukraine and aimed at implementing state policy in the field of defense, defined by laws, strategies, concepts, doctrines, principles, bases, declarations for effective development of the Armed Forces of Ukraine.

Approaches to the development of methods for implementing conceptual documents of strategic and defense planning can be represented as a step-by-step process:

definition of conceptual documents of strategic and defense planning which are subject to implementation;

determination of the normative-legal act of defense planning (according to the level of hierarchy), which is planned to be developed;

formation of requirements of the conceptual document to structure and the maintenance of the project of the regulatory legal act;

definition of ways of implementation of the conceptual document in the project of the regulatory legal act;

formation of the substantive part of the draft normative legal act and determination of compliance of the draft normative legal act with the requirements of the conceptual document;

risk management and monitoring and control.

Keywords: methodic of implementation of conceptual documents of strategic and defense planning; state management; capability; capability-based defense planning.

УДК: 355.45 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/84-89

Попельський М. І. (0000-0002-2425-756X)

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

Погляди щодо організації національного спротиву з урахуванням вимог Закону України “Про основи національного спротиву”

Резюме. У статті розглянуто складові національного спротиву, погляди на формування нового окремого роду сил Збройних Сил України – Сил територіальної оборони Збройних Сил України. Запропоновано потребу в подальшому удосконаленні та розвитку організаційно-штатної структури військових частин (підрозділів) Сил територіальної оборони, опрацювання та внесення змін в нормативно-правову базу, керівні документи.

Ключові слова: національний спротив; рух опору; територіальна оборона України; організаційно-штатна структура частин та підрозділів територіальної оборони; добровольче формування територіальних громад.

Постановка проблеми. Аналіз локальних війн і збройних конфліктів останнього десятиріччя свідчить про те, що поряд з безпосереднім застосуванням сил військової організації, держави активно проводять комплексне застосування за єдиним замислом і планом сил спеціальних операцій, формувань збройної опозиції та інших незаконно утворених антидержавних озброєних формувань.

Основною метою діяльності цих формувань є забезпечення в стислі строки підриву економічного, політичного, воєнного і морального потенціалів держави, істотного впливу противника на хід та результати як перших операцій, так і війни (конфлікту) загалом. До того ж об’єктами особливої уваги стають підприємства військово-промислового комплексу, об’єкти на комунікаціях, електростанції, водосховища та інші важливі державні та військові об’єкти. Підтвердженням цьому стали воєнні конфлікти в Перській затоці, на Балканах, в Центральній Азії.

Отже, в особливий період значна увага має приділятися утриманню території держави, забезпеченню спроможності підприємств, у визначені строки в необхідній кількості забезпечити потребу складових Сил оборони всім необхідним для відбиття агресії, розміщенням військових частин Сил територіальної оборони Збройних Сил України в межах відповідних адміністративно-територіальних одиниць, сприянню підготовки та виконанню завдань національного спротиву, створенню добровольчих формувань територіальних громад [1], які будуть здійснюватися органами державної влади та місцевого самоврядування при активній участі частин (підрозділів) Сил територіальної оборони Збройних Сил України, Національної Гвардії України, Національної поліції України, Служби безпеки України, Державної прикордонної служби України, Державної служби спеціального зв’язку та захисту інформації України, Державної спеціальної служби транспорту, Управління державної охорони України, центральних органів виконавчої влади, що реалізує державну політику у сфері цивільного захисту.

З набранням чинності та подальшим введенням у дію Закону України “Про основи національного спротиву” збільшується обсяг завдань, які виконують військові частини та підрозділи територіальної оборони. Державні органи влади та місцевого самоврядування набувають нових повноважень з питань підготовки та виконання завдань національного спротиву в мирний час та в особливий період.

Зважаючи на нестабільну і недоброзичливу зовнішньополітичну, економічну, соціальну, інформаційну обстановку навколо України виникає об’єктивна потреба подальшого удосконалення організаційно-штатної структури частин (підрозділів) територіальної оборони, пошуку ефективних методів їх застосування, враховуючи обстановку, яка склалася на сьогодні, удосконалення заходів щодо планування і ведення територіальної оборони.

Аналіз основних досліджень і публікацій. Слід зазначити, що протягом останніх років в Україні питанням територіальної оборони приділяється значна увага, свідченням чого є перелік основних нормативно-правових актів, прийнятих в Україні, що регламентують діяльність центральних органів виконавчої влади в особливий період та під час виконання

завдань територіальної оборони.

Визначенню складу сил і засобів, які залучаються до виконання завдань територіальної оборони, порядку їх формування, підготовки, зокрема і бойового злагодження, всебічного забезпечення, застосування їх за призначенням, основам взаємодії присвячено багато вітчизняних і зарубіжних видань [5, 7, 10, 11], у яких викладені принципи, вимоги, умови, мобілізаційні, організаційні, економічні можливості підготовки і здійснення територіальної оборони, погляди авторів на невирішені проблеми, аналізуються прорахунки і позитивні моменти минулого і сучасного досвіду, наводяться різноманітні напрями і шляхи його вирішення.

З набранням чинності та подальшим введенням в дію Закону України "Про основи національного спротиву" виникають питання щодо внесення змін до законодавчих актів, опрацювання положень про Командування Сил територіальної оборони, регіональні органи військового управління Сил територіальної оборони, визначення ролі та місця Сил територіальної оборони Збройних Сил України в загальній системі оборони України, їх складу та організаційно-штатної структури військових частин (підрозділів) територіальної оборони, місць їх розміщення та питання всебічного забезпечення Сил територіальної оборони Збройних Сил України, узагальнення порядку виконання завдань територіальної оборони у взаємодії з іншими складовими Сил безпеки та сил оборони держави, інші питання, які потребують негайного вирішення.

Ці питання нові та потребують наукового підходу та вирішення.

Мета статті – аналіз складових національного спротиву, обґрунтування пропозицій щодо удосконалення організаційно-штатної структури військових частин (підрозділів) територіальної оборони Збройних Сил України, порядку формування добровольчих формувань територіальних громад та їх застосування під час планування і ведення територіальної оборони у взаємодії з іншими складовими сектору безпеки і оборони держави.

Виклад основного матеріалу. Аналіз досвіду виконання завдань територіальної оборони у 2014–2019 роках свідчить, що на ефективність їх виконання істотно впливала ціла низка факторів політичного, воєнного, економічного, організаційного, соціального, нормативно-правового, морально-психологічного та інформаційного характеру, обумовлених поглядами на підготовку і ведення територіальної оборони, можливостями вірогідного противника, своїх військ (сил), рівня розвитку економіки держав і збройних сил протиборчих сторін, рівня морально-психологічного стану військ (сил) територіальної оборони і населення країни (регіону), станом інфраструктури, рівнем підготовки держави до оборони, у тому числі, і станом підготовки території держави до оборони та її оперативного обладнання тощо.

Актуальність сучасних гібридних викликів і загроз, насамперед таких, як триваюча збройна агресія Російської Федерації проти України, анексія окремих територій нашої держави, збройні чи незбройні провокації спонукають до пошуку консолідованих заходів щодо забезпечення незалежності та територіальної цілісності нашої держави. Одним з ефективних механізмів підтримання на належному рівні обороноздатності держави є система територіальної оборони України, яка включає в себе комплекс загальнодержавних воєнних і спеціальних заходів, що здійснюються в особливий період на всій території України або в окремих її місцевостях, крім зон (районів) проведення бойових дій [5].

У Законі України "Про основи національного спротиву" визначено, що складовими національного спротиву є територіальна оборона, рух опору та підготовка громадян України до національного спротиву, тобто: національний спротив – *комплекс заходів*, які організовуються та здійснюються з метою сприяння обороні України шляхом максимально широкого залучення громадян України до дій, спрямованих на забезпечення воєнної безпеки, суверенітету і територіальної цілісності держави, стримування і відсічі агресії та завдання противнику неприйнятних втрат, з огляду на які він буде змушений припинити збройну агресію проти України [1].

Для залучення громадян до відповідних дій із захисту суверенітету і територіальної цілісності держави під час їх ведення, необхідно в мирний час організувати систему відбору та навчання громадян до майбутніх дій у складі підрозділів – добровольчих формувань територіальних громад, тобто створити систему зарахування зі складу залишків вільних мобілізаційних ресурсів громадян України, які знаходяться на обліку в територіальних центрах комплектування та соціальної підтримки, які за станом здоров'я, з інших причин, визначених у керівних

документах, не можуть бути призваними під час мобілізації, але можуть бути зараховані до складу добровольчих формувань територіальних громад за їх бажанням.

Отже, Положення про добровольчі формування територіальних громад, а також визначення порядку їх обліку територіальними центрами комплектування та соціальної підтримки потребує опрацювання.

Для комплектування органів військового управління, військових частин, підрозділів Сил територіальної оборони Збройних Сил України призначений територіальний резерв, якій включає резервістів і військовозобов'язаних та здійснюється в особливий період. Водночас потребує уточнення порядок їх комплектування, терміни подачі мобілізаційних ресурсів та порядок формування підрозділів і добровольчих формувань територіальних громад.

Потребує вирішення питання підготовки громадян України до національного спротиву, тобто сприянню обороні України. Якщо в минулому підготовка здійснювалася в загальній системі підготовки допризовної молоді до служби в збройних силах, та за час існування незалежної України цим питанням приділялося мало уваги (у школах предмет військова підготовка та наявна матеріальна база в класах була знищена, занять з матеріальної частини не проводилося, в кращому разі все зводилося до викладання предмету захист Батьківщини, зв'язок зі Збройними Силами України був забутий).

Заняття з військовозобов'язаними, які були в мирний час приписані до військових частин, через брак коштів увійшли в минуле.

Події на сході та півдні України в наші дні диктують необхідність формувати свідому, вмотивовану та фізично підготовлену молодь, яка зможе відстоювати національні інтереси, і якщо треба, то й зі зброєю в руках. Як відомо, мотиваційний набір людина не отримує з народженням, він формується впродовж її життя. Для цього відповідна політика держави має бути спрямована на цільове мотивування співгромадян до співпраці з органами державної безпеки та іншими державними установами. Під час реалізації спеціальних програм молодь слід залучати до вивчення історії та культури України, подвигів борців за її незалежність, суверенітет та територіальну цілісність; до фізичних тренувань; до занять з вогневої, парашутної, автомобільної підготовки тощо. Заходи з національно-патріотичного виховання необхідно проводити у закладах загальної середньої, спеціалізованої позашкільної освіти, музеях, бібліотеках, клубах та інших закладах культури.

Нині одним із таких заходів є Всеукраїнська дитячо-юнацька військово-патріотична гра "Сокіл" ("Джура"), метою якої є виховання в молодого покоління України патріотизму, національної гідності, високої самосвідомості та активної громадянської позиції, прищеплення навичок здорового способу життя, розвиток духовно багатої та фізично загартованої особистості. Гра проводиться під егідою Міністерства освіти і науки України за сприяння Міністерства оборони України [12]. Пропонується використовувати можливості Товариства сприяння обороні Україні, головною метою якого є підготовка його членів до суспільно-корисної праці й захисту України [4].

Підготовка молоді передбачає її навчання в освітніх закладах України та в навчальних центрах Збройних Сил України. Звісно, не всі, хто навчався у школах чи пройшов підготовку в гуртках (клубах, секціях), виявлять бажання стати до лав захисників держави. Хтось вступатиме до закладів професійної (професійно-технічної) чи вищої освіти, а хтось захоче пов'язати своє життя зі службою у Збройних Силах України, однак вчасно посіяні зерна патріотизму в юнацьких головах вже почнуть давати сходи.

Відродити патріотичне виховання молоді на прикладах боротьби України за її недоторканість, Революції гідності, героїзму під час проведення антитерористичної операції. Для цього нашій державі доцільно мати удосконалену програму патріотичного виховання молоді та загальновійськової підготовки громадян України, з урахуванням вимог сьогодення, визначиться з відповідальними органами за їх підготовку та здійснення контролю, у найближчий час впровадити в дію.

У новому законі збільшено кількість завдань територіальної оборони, замість п'яти їх визначено аж дванадцять. Новим завданням є *своєчасне реагування та вжиття необхідних заходів щодо оборони території та захисту населення на визначеній місцевості до моменту розгортання в межах такої території угруповання військ (сил) або/чи угруповання об'єднаних сил, призначених для ведення воєнних (бойових) дій з відсічі збройній агресії проти України* [1]. Раніше задачу щодо оборони території

покладалася на визначений комплект сил та засобів зі складу військових частин оперативних командувань в їх зоні відповідальності, які відносилися до основних сил оборони, та в мирній час були укомплектовані до 80-90 % від штату мирного часу. Нині це питання потребує вирішення складом (військ) сил Командування Територіальної оборони.

Якщо раніше *посилення та охорона державного кордону* покладалася на визначений комплект військових частин, які розміщувалися поблизу кордону та загони Державної прикордонної служби України, то на сьогодні до цих питань залучатимуться військові частини та підрозділи Сил Територіальної оборони Збройних Сил України в своїх зонах відповідальності до моменту розгортання в межах такої території угруповання військ (сил) або/чи угруповання об'єднаних сил, призначених для ведення воєнних (бойових) дій з відсічі збройній агресії проти України, які братимуть участь у посиленні охорони та захисті державного кордону [1].

Крім того, новими завданням територіальної оборони визначена участь у:

участь у захисті населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій, ліквідації наслідків ведення воєнних (бойових) дій;

участь у підготовці громадян України до національного спротиву;

участь у здійсненні заходів щодо тимчасової заборони або обмеження руху транспортних засобів і пішоходів поблизу та в межах зон/районів надзвичайних ситуацій та/або ведення воєнних (бойових) дій;

участь у забезпеченні заходів *громадської безпеки* і порядку в населених пунктах;

участь в інформаційних заходах, спрямованих на підвищення рівня обороноздатності держави та на протидію інформаційним операціям агресора (противника).

Структура існуючих штатів підрозділів територіальної оборони була визначена під задачі, які покладалися на той час для виконання п'яти задач територіальної оборони. З набранням чинності новим Законом України "Про основи національного спротиву" та збільшенням кількості та різноманітності завдань, виникає потреба в негайному перегляді штатів частин (підрозділів) територіальної оборони та внесенні змін в організаційно-штатну структуру бригад (батальйонів) територіальної оборони, збільшення кількості особового складу, переопрацювання табелів до штатів, визначення місць розміщення військових частин (підрозділів) територіальної оборони, Положень про військові частини (підрозділи) Сил територіальної оборони, з визначенням нових завдань та порядку їх виконання.

Створення нового окремого роду сил Збройних Сил України – Сил територіальної оборони Збройних Сил України [1], дасть змогу більш якісно виконувати завдання територіальної оборони, звільняючи Збройні Сили України від виконання невластивих завдань, що потребує значного збільшення кількості військових частин, і підрозділів територіальної оборони.

Усе це потребує часу та злагоджених дій створеного Командування Сил Територіальної оборони з апаратом Головнокомандувача Збройними Силами України та Генерального штабу, структурними підрозділами Міністерства оборони України, органами державної влади та місцевого самоврядування.

Відповідно до вимог Закону для розміщення військових частин Сил територіальної оборони Збройних Сил України в межах відповідних адміністративно-територіальних одиниць використовується інфраструктура (фонди) Збройних Сил України, а також інфраструктура (фонди) складових сил безпеки та сил оборони, органів місцевого самоврядування у порядку, визначеному Кабінетом Міністрів України.

На превелику жаль, протягом тридцяти років вносилися зміни в кількісні показники складу та місць розміщення складових сектору безпеки і оборони. Наявна інфраструктура (фонди) розміщення військових частин та інших складових сил оборони прийшла в негідність через їх скорочення та ліквідацію. Охорона об'єктів здійснювалась неякісно, що призвело до їх знищення, проте їх відновлення буде потребувати значних коштів та часу для відновлення або до нового обладнання військових містечок.

Доцільно звернути увагу на одну зі складових національного спротиву – рух опору.

Рух опору – система воєнних, інформаційних і спеціальних заходів, організація, планування, підготовка і підтримка яких здійснюється з метою відновлення державного суверенітету і територіальної цілісності під час відсічі збройної агресії проти України [1].

Завданнями руху опору є:

формування осередків руху опору та набуття ними відповідних спроможностей;

перешкоджання діям військ (сил) агресора (противника);

участь у проведенні спеціальних (розвідувальних, інформаційно-психологічних) операцій.

участь у підготовці громадян України до національного спротиву.

Крім завдань визначених Законом під час захисту та недоторканості Батьківщини від агресору, пропонується виконання таких завдань:

добування розвідувальної інформації;

порушення системи управління, комунікацій і зрив військових перевезень противника;

знищення живої сили, військової техніки та матеріальних засобів противника;

протидія використанню противником місцевих ресурсів;

сприяння підрозділам Збройних Сил України (переховування і супроводження на свою територію екіпажів збитих повітряних суден чи військовослужбовців, які втекли з полону);

пропаганда спротиву окупаційній або чинній владі (військам) серед населення;

виявлення баз підготовки, складу, озброєння, районів розташування диверсійно-розвідувальних сил і незаконних озброєних формувань та намірів їх дій;

встановлення бойового складу, стану (положення), можливостей, намірів і характеру дій військових формувань, що прибули з території агресора;

викриття (дорозвідка) об'єктів (цілей) для ураження, а також визначення результатів ураження;

наведення та цілевказання артилерії (по скупченню сил ворога, його вогневих позиціях тощо);

проведення силових операцій (знищення особового складу (командирів), воєнної техніки та об'єктів ворога, об'єктів інфраструктури тощо).

Слід зазначити, що лише у 2016 році змінами у деякі законодавчі акти було врегульовано на державному рівні питання організації руху опору. Так, Законом України "Про оборону України" заходи з планування та підготовки руху опору включено до складових елементів підготовки держави до оборони, Законом України "Про Збройні Сили України" – функцію щодо організації та ведення руху опору покладено на Збройні Сили України.

Питання організації руху опору потребує подальшого вивчення та наукового обґрунтування.

Для більш наочного сприйняття пропозиції, які наведені в статті, доцільно звести у табл. 1.

Таблиця 1

№	Напрям застосування	Зміст пропозиції	Відповідальні органи та виконавці
1	Подальший розвиток складових національного спротиву	Опрацювати: Положення про добровольчі формування територіальних громад; визначити порядок їх обліку територіальними центрами комплектування та соціальної підтримки; визначити робочу групу з напрацювання змін в нормативно-правові акти, підготувати проєкт Положення Про Командування Сил територіальної оборони, визначити функції та завдання, які плануються покласти на частини (підрозділи) Сил територіальної оборони та інші складові Сил оборони держави	Командування Сухопутних військ, Генеральний штаб Збройних Сил України, Міністерство оборони України, органи державної влади та місцевого самоврядування
2	Удосконалення організаційно-штатної структури	Опрацювати штати, табелі до штатів підрозділів територіальної оборони, зважаючи на завдання територіальної оборони, відповідно до Закону України "Про основи національного спротиву"	Командування Сухопутних військ, Генеральний штаб Збройних Сил України
3	Пошуку і визначення найбільш ефективних загальних типових форм застосування складових національного спротиву	Визначити склад, порядок формування, підготовки складових національного супротиву як у мирній час, так і особливий період. Призначити відповідальні органи військового командування та органи державної влади щодо організації виконання Закону України "Про основи національного спротиву"	Командування Сил спеціальних операцій, Генеральний штаб, Командування Сухопутних військ Збройних Сил України, органи державної влади
4	Підготовка молоді	Вирішити питання підготовки громадян України до національного спротиву. Опрацювати програму підготовки молоді для служби в Збройних Силах України, відновити в школах, вищих навчальних закладах II-III ступенів викладання довійськової підготовки молоді	Міністерство освіти і науки України, Міністерство оборони України, Товариство сприяння оборони України
5	Організація, планування та підготовка руху опору	Опрацювати схему організації руху опору, його складові, відповідальних за його організацію та підготовку, План підготовки руху опору в мирний та воєнний час, розробити проєкт Положення про рух опору	Командування Сил спеціальних операцій, Генеральний штаб ЗС України, органи державної влади

Висновки та напрям подальших досліджень. Зважаючи на погляди, які були запропоновані для врахування під час розгляду складових національного спротиву, опрацювати зміни в нормативно-правові акти, організаційно-штатні структури військових частин (підрозділів) Сил територіальної оборони Збройних Сил України, підготувати проєкт Положення про Командування Сил територіальної оборони, визначити функції та завдання, які плануються покласти на військові частини (підрозділи) територіальної оборони та інші складові сектору безпеки і оборони держави, проєкт Доктрини територіальної оборони, Типового положення про штаб зони (району) територіальної оборони, Положення про добровольчі формування територіальних громад, удосконалити програму патріотичного виховання молоді та загальновійськової підготовки громадян України.

Пропозиції, які надані у статті, можуть бути використані органами: військового управління, державної влади та місцевого самоврядування.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про основи національного спротиву : Закон України від 29.07.2021 р. № 406/2021.
2. Про оборону України : Закон України від 06.12.1991 р. № 1932-XII.
3. Про заходи щодо поліпшення національно-патріотичного виховання дітей та молоді : Указ Президента України від 12.06.2015 р. № 334.
5. Положення про територіальну оборону України : Указ Президента України від 23.09.2016 р. № 406/2016. 2016. С. 2. п. 3.
6 Про національну безпеку України : Закон України від 2018 р. *Відомості Верховної Ради*. 2018. № 31. ст. 241.
7. Про оборону України : Закон України від 1991 р. № 1932-XII. р. III.
8. Товариство сприяння обороні України (ТСО України) : Статут громадської організації. Київ, 2016. 36 с.
9. Фрунзе М.В. Единая Военная доктрина и Красная Армия. *Военная наука и революція*. (июль-август 1921 г.).
10. Про військовий обов'язок і військову службу : Закон України від 25.03.1992 р. № 2232- XII (зі змінами).
11. Лавніченко О.В., Тробюк В.І. Аналіз підготовки і ведення територіальної оборони. *Університетські наукові записки*. Хмельницький, 2002. № 22. Ч. II.
12. Про затвердження Положення про Всеукраїнську дитячо-юнацьку військово-патріотичну гру "Сокіл" ("Джура") : наказ Міністра освіти і науки, молоді та спорту України від 43.06.2012 р. № 687.

Стаття надійшла до редакційної колегії 16.08.2021

Views on the organization of national resistance taking into account the requirements of the Law of Ukraine "On the basis of national resistance"

Annotation

Analysis of local wars and armed conflicts of the last decade shows that along with the direct use of military forces, states are actively pursuing a comprehensive plan and plan of special operations forces, armed opposition and other illegally formed anti-state armed groups.

Despite the unstable and hostile foreign policy, economic, social, information situation around Ukraine, there is an objective need to further improve the organizational and staffing structure of units (bases) of territorial defense, finding effective methods of their application, given the current situation, improving measures to planning and conducting territorial defense.

With the entry into force and subsequent entry into force of the Law of Ukraine "On the basis of national resistance" there are questions about amendments to legislation, elaboration of provisions on the Command of the Territorial Defense Forces, regional military authorities of the Territorial Defense Forces. Requires definition: the role of the Territorial Defense Forces of the Armed Forces of Ukraine in the overall defense system of Ukraine, the composition and organizational structure of military units of territorial defense, issues of comprehensive support, the procedure for territorial defense in cooperation with other components of the Security and Defense Forces.

The bodies of can use the suggestions given in the article: military administration, state power and local self-government.

Keywords: national resistance; resistance movement; territorial defense of Ukraine; organizational and staff structure of units and subdivisions of territorial defense; voluntary formation of territorial communities.

УДК 351.863 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/90-96

Шапталенко М. І., канд. техн. наук, доцент (0000-0001-8343-694X)

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

Напрями удосконалення організаційно-штатної структури органів технічного забезпечення підрозділів і частин тактичного рівня у єдиній системі логістики

Резюме. У статті обґрунтовано необхідність удосконалення організаційно-штатної структури органів технічного забезпечення підрозділів і частин тактичного рівня Сухопутних військ Збройних Сил України, враховуючи досвід збройних сил США, ФРН та інших провідних країн НАТО. Запропоновано необхідні рекомендації для вирішення визначених проблем.

Ключові слова: озброєння; військова техніка; відновлення; технічне обслуговування; логістика; тилове та технічне забезпечення.

Постановка проблеми. Уже понад шість років Збройні Сили (ЗС) України ведуть бойові дії з відстоювання суверенітету та територіальної цілісності України. За цей час відбулися радикальні зміни у політичному житті, економіці держави і ЗС України. Для укомплектування військ озброєнням та військовою технікою (ОВТ) були залучені всі зразки ОВТ, які були в наявності, зокрема з центрів зберігання надлишкового майна.

Постала проблема неповної відповідності можливостей сил і засобів ремонтно-відновлювальних органів (РВО) підсистеми технічного забезпечення (ТхЗ) цілям і завданням функціонування системи матеріально-технічного забезпечення (МТЗ) Сухопутних військ (СВ) у єдиній системі логістики [1]. Це, зі свого боку, призводить до того, що підсистема ТхЗ не повністю забезпечує своєчасність відновлення та повноту технічного обслуговування (ТО) ОВТ, що вийшли з ладу, як у разі бойових пошкоджень, так і за технічними причинами.

Отже, постає завдання удосконалення організаційно-штатної структури (ОШС) РВО на основі системного підходу, що дасть змогу удосконалити ОШС сил і засобів МТЗ СВ ЗС України [2].

Аналіз останніх досліджень і публікацій. У роботі показано, що аналіз досвіду застосування військ країн НАТО в локальних конфліктах свідчить про те, що існує певна пропорція між загальною кількістю особового складу підрозділів, частин і з'єднань та кількістю особового складу підрозділів і частин логістики, зокрема і ТхЗ, які займаються безпосереднім відновленням і ТО ОВТ. Наприклад, в арміях США і ФРН доля підрозділів і частин логістики складає 50-70 % від загальної чисельності особового складу об'єднань (їх відповідних підрозділів, частин та з'єднань). Це означає, що одного солдата забезпечують 2-3 військовослужбовця. У ЗС України цей показник не перевищує 35-40 % [3]. Це свідчить про те, що провідні країни НАТО зосередили переважну більшість сил і засобів МТЗ в з'єднаннях, частинах і підрозділах тактичного рівня, тобто максимально наблизили сили і засоби МТЗ до військ, які вони забезпечують [4–6].

Мета статті – обґрунтування рекомендацій зі створення ОШС єдиної системи МТЗ тактичного рівня, яка б максимально відповідала вимогам сучасності.

Для досягнення мети враховано досвід провідних країн НАТО [4–6], останніх війн і локальних конфліктів. До того ж основна увага зосереджена на елементах загальної проблеми, які не були висвітлені в попередніх публікаціях на цю тему.

Аналіз проводиться на основі системного підходу для вироблення єдиних підходів, як до удосконалення Міжвидової єдиної системи МТЗ у системі логістики, так і її елементів у підрозділах, частинах та з'єднаннях, застосовуючи єдині методологічні погляди [1, 7, 8]. Це надалі дасть змогу обґрунтовано запропонувати шляхи та форми удосконалення ОШС РВО тактичного рівня СВ ЗС України [3].

Викладення основного матеріалу. Загальновідомо [9], що в арміях провідних країн світу, зокрема НАТО, на їх забезпечення МтЗ, зокрема ОВТ, виділяється не менше 50-70 % фінансових ресурсів від оборонного бюджету цих країн. Це дає змогу забезпечити і підтримувати матеріально-технічну основу їх боєздатності на досить високому рівні. Розглянемо, які головні завдання вирішує

система МТЗ та основні принципи організації відновлення ОВТ в арміях США і ФРН.

Головні завдання МТЗ в арміях США і ФРН:

визначення потреби, забезпечення, приймання, розосередження, утримання, розподіл і видача МтЗ військам (у тому числі ОВТ);

адміністративний і технічний моніторинг щодо організації постачання, проведення технічного обслуговування, ремонту і модернізації усіх видів ОВТ;

керівництво технічною і спеціальною підготовкою особового складу військ;

підготовка особового складу частин і підрозділів системи МТЗ зі спеціально-технічних питань;

евакуація, збір, відновлення ОВТ і постановка до строю під час бойових дій;

транспортне забезпечення військ (перевезення військових вантажів, особового складу) як у мирний, так і воєнний час.

Основні принципи організації відновлення ОВТ в арміях США і ФРН [6]:

суворий розподіл функцій з обсягу і переліку робіт між рівнями та ланками системи;

відповідність технічного оснащення, кваліфікації і спеціалізації особового складу РВО та забезпечення необхідною кількістю запасних частин і агрегатів відповідно до обсягу і переліку робіт, які виконуються;

виконання ремонту ОВТ на місцях виходу із ладу або на пунктах збору пошкоджених бойових машин, зважаючи на найменший час, який витрачається на евакуацію пошкодженого ОВТ;

тісна взаємодія усіх сил і засобів ТхЗ із виконання необхідних робіт;

виконання ремонту агрегатним методом.

Відповідно до цих принципів побудована структура підрозділів і частин, які відновлюють ОВТ у польових умовах. Основна увага приділяється відновленню ОВТ на місцях виходу з ладу, тому переважна більшість сил і засобів, які призначені для ремонту ОВТ знаходиться у РВО тактичного рівня. Окремо слід зазначити, що 90 % виробничих потужностей з відновлення ОВТ в арміях США і ФРН зосереджені у РВО тактичного рівня [10].

Це забезпечує мінімальний час їх відсутності в бойових порядках і, як наслідок, високий рівень боєздатності підрозділів, частин і з'єднань тактичного рівня.

Для забезпечення високої живучості та рухомості засобів евакуації і ремонту, особливо у ланках рота – батальйон – бригада, які працюють під впливом вогневих засобів противника, як база для ремонтно-евакуаційних сил і засобів використовуються сучасні танки та інші типи бронетанкової техніки.

Головним військовим засобом евакуації, який діє безпосередньо за підрозділами, що ведуть бойові дії, є броньована ремонтно-евакуаційна машина (БРЕМ). Оснащення військ БРЕМ дало змогу суттєво збільшити обсяг ремонтно-відновлювальних робіт, які виконуються безпосередньо за бойовими порядками частин, прискорює повернення ОВТ до строю. У ланках, починаючи з дивізії, де необхідно евакуйовувати пошкоджену техніку на велику відстань, переважно застосовуються великовантажні автомобілі (трейлери).

Для забезпечення боєздатності цих ОВТ, як у мирний час, так і в усіх видах бою, в системі логістики тактичного рівня створена підсистема ТхЗ.

Для початку необхідно розглянути підсистеми ТхЗ системи логістики тактичного рівня армії США та інших провідних країн – членів НАТО. Розглянемо їх на основі теорії систем, що дасть змогу розрахувати кількість особового складу РВО всіх ланок підсистеми ТхЗ тактичного рівня.

Як і в більшості провідних країн світу, в армії США всі функції з підтримання високої боєздатності ОВТ зосереджені в єдиному органі – командуванні тилу. Обмежимося розглядом органів тилу тільки тактичного рівня, тобто командуванням тилу дивізії і бригади.

Командування тилу здійснює функції постачання з'єднанням та частинам всіх видів МтЗ, організовує і здійснює транспортне і військове перевезення [4] [5].

Командування тилу дивізії і бригади є ланками системи логістики, які найбільше наближені до бойових підрозділів. Вони призначені для всіх видів МТЗ частин і підрозділів, що діють у смузі відповідальності з'єднання, а також для вирішення завдань з охорони та оборони дивізійного тилового району. Керівництво ТхЗ дивізії здійснює безпосередньо начальник технічної служби.

Слід відзначити, що на тактичному рівні розподілу по службах, а саме: службу ракетно-артилерійського озброєння, бронетанкову, автомобільну тощо, немає. Розподіл проходить за функціональним принципом: технічна служба, матеріально-технічного

забезпечення, служба постачання, транспортна служба, медична служба тощо.

Начальник ремонтної служби дивізії, старший офіцер ремонтної служби дивізії (бригади) є радником командира дивізії (бригади) з питань бойової готовності ОВТ, ТО і ремонту, а також з питань, які стосуються експлуатації і відновлення ОВТ. Усі РВО дивізії належать до системи МТЗ. Завдання на їх застосування в бою та операції ставиться в наказі з матеріально-технічного забезпечення.

На сьогодні існують 2 типи ОШС командування тилу дивізії – для "важких" і для "легких" з'єднань. Схема організації командування тилу "важкої" дивізії (механізована, бронетанкова) наведена на рис.1.

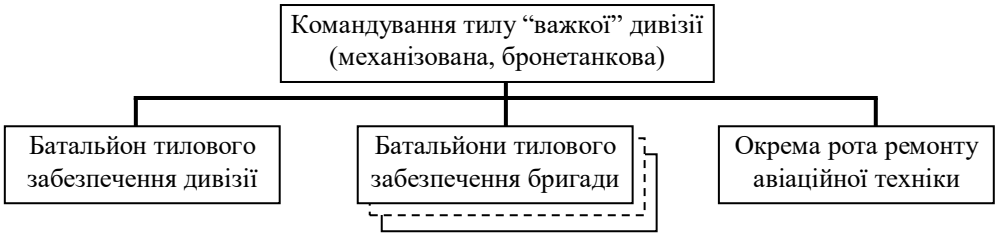


Рис. 1. Схема організації командування тилу "важкої" дивізії (механізована, бронетанкова)

Вважається, що подібна організація в умовах централізованої дії дає змогу частинам і підрозділам такої дивізії підвищити гнучкість використання всіх тилових органів і звільняє командирів бригад і батальйонів від безпосереднього управління тилом, щоб зосередити їх зусилля на вирішенні тільки бойових завдань.

Схема організації командування тилу "легкої" дивізії (легка піхотна, повітрянодесантна, повітряно-штурмова) наведена на рис. 2.

Рис. 2. Схема організації командування тилу "легкої" дивізії (легка піхотна, повітрянодесантна, повітряно-штурмова)

Це дає змогу використовувати сили і засоби переважно децентралізовано (побригадно і побатальйонно), а також створити тимчасові формування МТЗ, склад яких визначатиметься конкретним бойовим завданням тактичної групи.

ТхЗ в армії США здійснюють підрозділи і частини, які організаційно входять до штату частин і з'єднань, а також частин, що знаходяться у розпорядженні Командування СВ на ТВД.

Штатні ремонтно-відновлювальні та евакуаційні засоби є у ротах, батальйонах, дивізіях.

Схема організації ремонтної секції танкової роти наведена на рис. 3.

БРЕМ – 1 од.; автомобілі – 2 од.; причепи – 2 од.; радіостанції – 3 од.

Рис. 3. Схема організації ремонтної секції танкової роти "важкої" дивізії

Ремонтна секція призначена для надання кваліфікованої технічної допомоги екіпажам при ТО ОВТ, засобів зв'язку та іншого обладнання, яке встановлено на зразках ОВТ і для евакуації пошкодженого ОВТ в укриття.

Схема організації ремонтного взводу танкового батальйону наведена на рис. 4.

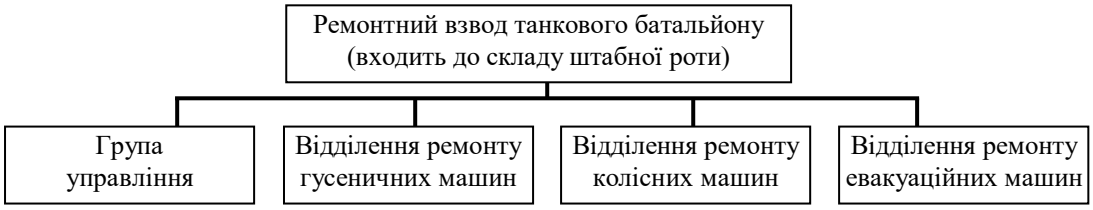


Рис. 4. Схема організації ремонтного взводу танкового батальйону "важкої" дивізії

Ремонтний взвод призначений для виконання військового ремонту, надання допомоги екіпажам в обслуговуванні ОВТ та евакуації пошкодженого ОВТ. За добу ремонтний взвод може відремонтувати до трьох бронеоб'єктів. Можливості ремонтного взводу дають змогу ремонтувати й інші види ОВТ, що знаходиться на озброєнні батальйону. Керує роботою ремонтного взводу офіцер технічного обслуговування і ремонту батальйону, який одночасно є і командиром ремонтного взводу [4].

Схема організації ремонтного батальйону дивізії наведена на рис. 5.

Рис. 5. Схема організації ремонтного батальйону "важкої" дивізії

Ремонтний батальйон призначений для ТО і ремонту ОВТ, майна штатних і приданих дивізії частин і підрозділів. Технологічна оснащеність, возимі запаси МтЗ, як і рівень кваліфікації особового складу батальйону дає змогу комплексно виконувати середній ремонт ОВТ (у тому числі ракетного) і майна тилу, за виключенням медичного.

Рота штабна і ремонту легкого озброєння і техніки обслуговує та ремонтує тільки ОВТ окремих частин і підрозділів бойового і тилового забезпечення дивізії.

Рота ремонту важкого озброєння і техніки призначена для ремонту озброєння і бронеоб'єктів частин дивізії, які не входять до складу бригад. За необхідності з цієї роти можуть виділятися групи (секції) для підсилення рот з ремонту ОВТ бригад.

Аналіз структури ремонтного батальйону показує, що характерною особливістю є наявність у його складі ремонтних підрозділів широкого профілю, які забезпечують відновлення більшості зразків ОВТ дивізії і ремонтні підрозділи, які спеціалізуються на відновленні тільки певних видів ОВТ.

ОШС батальйону відповідає розподілу ОВТ по частинах дивізії та елементах бойового порядку. Характерно, що у той час, коли загальна чисельність дивізії порівняно з дивізією існуючої організації в середньому збільшилася на 9,3 %, то чисельність командування тилу дивізії збільшилася на 32,8 %, тобто на третину [4]. Масштаби ремонтно-відновлюваних робіт з відновлення ОВТ у сучасному бою і операції залежать від потреби в силах і засобах відновлення, принципів і способів їх використання та визначатимуться рівнем втрат ОВТ, умовою їх формування і характером дій.

Аналіз бойових втрат ОВТ у локальних війнах показує, що величина середньодобових втрат складає 9-12 %, але переважна більшість із них – результат застосування високоточної зброї (табл. 1).

Таблиця 1

Втрати БТОТ від високоточної зброї, які потребують:	
поточного ремонту	10-15 %
середнього ремонту	20-25 %
капітального ремонту	10-15 %
безповоротні втрати	40-45 %

Отже війська (сили) повинні мати значні можливості щодо поповнення втрат бойових засобів у бою і операції завдяки їх відновленню РВО. Для вдосконалення ОШС

підсистеми РВО використовуються основи системного підходу. На основі логічної схеми процесу розроблення типових ОШС бойових сил пропонується вдосконалена структурно-логічна схема розроблення та визначення структури і чисельності особового складу РВО військ (сил).

Під структурою системи мається на увазі склад сил і засобів, що виконують часткові завдання для досягнення цільової функції. Цільовою функцією (головним завданням) підсистеми відновлення в бойових умовах є тривала підтримка боєздатності частин і підрозділів на заданому рівні шляхом своєчасної евакуації і ремонту всього штатного ОВТ, які вийшли з ладу.

Аналіз функціонування розподілу особового складу по ланках структури ремонтних підрозділів і частин існуючої системи відновлення дає змогу визначити загальну чисельність особового складу ремонтного органу:

$$R_{заг} = R_{вир} + R_{доп} + R_{забез} + R_{упр}, \quad (1)$$

де $R_{заг}$ – загальна чисельність особового складу;

$R_{вир}$ – чисельність виробників;

$R_{доп}$ – чисельність допоміжного особового складу;

$R_{забез}$ – чисельність особового складу забезпечення;

$R_{упр}$ – чисельність особового складу управління.

Структура організації, створеної на основі рекомендацій теорії систем, має чіткий розподіл сил і засобів по ланках, що виконують у процесі функціонування основну і допоміжну функції, функції забезпечення, а також функцію управління. Таким чином, твердження теорії систем щодо наявності в структурі будь-яких організацій певного співвідношення в розподілі сил і засобів по ланках, що виконують в процесі функціонування основну і допоміжну функції, функції забезпечення, а також функцію управління, є справедливим для усіх ланок організаційної структури рухомих ремонтних засобів. Насправді, від того, наскільки вірно вибрані співвідношення між основними, допоміжними і забезпечуючими підрозділами, значною мірою залежить ефективність організації в цілому [11, 12].

Структурно-логічна схема розроблення ОШС ремонтно-відновлювальних органів тактичного рівня на основі системного підходу дає змогу обґрунтувати як загальну чисельність особового складу, так і ремонтних засобів, як РВО тактичного рівня в цілому, так і його підрозділів. Позитивним є те, що їх розподіл по підрозділах РВО проводиться з урахуванням призначення складових, які виконують функції управління, основну, допоміжну і забезпечення (табл. 2, 3).

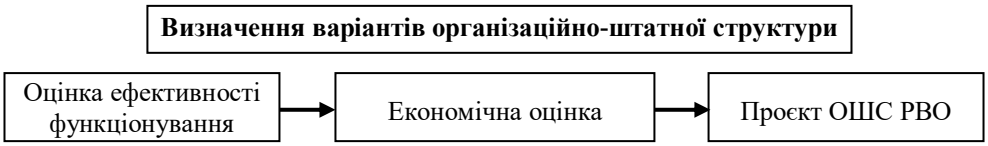


Рис. 6. Структурно-логічна схема розроблення ОШС ремонтно-відновлювальних органів тактичного рівня на основі системного підходу

Таблиця 2

Визначення розрахункової чисельності ремонтних засобів та особового складу підрозділів ремонтно-відновлювальних органів з'єднань, частин та підрозділів			
Визначення номенклатури підрозділів, що виконують функції			
Основна	Допоміжна	Забезпечення	Управління
ремонт (виробничий процес)	технічна розвідка; евакуація; транспортування; ремонт устаткування	постачання військово-технічного майна	координація дій
Визначення чисельності особового складу у ремонтних органах підрозділів, частин			
85 – 90 %	6 – 10 %	–	3 – 5 %
Визначення чисельності особового складу у ремонтних органах з'єднань			
62 – 83 %	6 – 22 %	5 – 17 %	3 – 11 %
Визначення засобів технічного оснащення підрозділів ремонтних органів			
рухомі ремонтні майстерні; БРЕМ; машини техдопомоги	тягачі; трейлери тощо	склади; транспорт тощо	засоби пересування і управління

Таблиця 3

Визначення чисельності і спеціальностей особового складу	
$R_{вир} = N \cdot m,$ де N – чисельність бригад; m – чисельність ремонтників в бригаді для рухомих ремонтних засобів: з'єднань – 62-83 %; частин – 85-90 %	$R_{спец} = R_{вир} \cdot f / 100,$ де f – обсяг робіт (%): демонтажно-монтажні роботи – 68-81 %; теплові – 8-13 %; слюсарно-механічні – 4-5 %; ремонт електрообладнання – 4-7 %; ремонт озброєння, оптики – 1-3 %; інші – 2-4 %

Висновки. Проведені дослідження підсистеми ТхЗ показують, що питання ОШС РВО військ (сил) тактичного рівня необхідно переглянути з погляду не тільки ефективності функціонування, а також економічної оцінки. Найкращі вирішення проблем в складних ситуаціях, зазвичай, знаходять завдяки раціональній побудові організаційної структури системи та її окремих ланок, чіткого розподілу функцій між ними в типових ситуаціях роботи, достатнього резервування виробничих потужностей і матеріальних засобів на кожному рівні, а також стійкого управління.

Удосконалення ОШС РВО частин і підрозділів СВ ЗС України тактичного рівня необхідно проводити з урахуванням процентного складу підрозділів, що виконують функції основні, допоміжні, забезпечення та управління, з урахуванням визначення чисельності і спеціальностей особового складу.

Метою **подальших досліджень** є визначення за класифікацією видів ремонту, обсягу, часу виконання робіт, структури РВО механізованої (танкової) бригади СВ ЗС України. Визначенню їх раціональної ОШС буде присвячена наступна стаття.

ПЕРЕЛІК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Доктрина "Об'єднана логістика" – ВКП 4.00 (01). 01 від 19.09.2020 р.
2. Ковалішин С. С., Халтурин Р. В. Напрями удосконалення організаційно-штатної структури органів технічного забезпечення у військовій ланці в єдиній системі матеріально-технічного забезпечення. *Збірник наукових праць Військової академії.* Одеса, 2014. С. 70–76.
3. Романченко І. С., Шуєнкін В. О. Погляди на розвиток системи матеріально-технічного забезпечення Збройних Сил України. *Наука і оборона.* 2007. № 4. С. 22–27.
4. AJP-4 (B) – Allied Joint Doctrine for Logistics, Edition B Version 1, December 2018 (Доктрина НАТО з логістики).
5. JP-4 – JOINT LOGISTICS February 2019, INCORPORATING CHANGE May 2019 (Доктрина об'єднана логістика, МО США).
6. MC 319/3 – NATO Principles and Policies for Logistics (Принципи та політика НАТО щодо логістики).
7. Доктрина "Сили логістики" – ВКП 4.32 (41). 01 від 08.02.2021 р.
8. Доктрина "Застосування сил логістики" – ВКП 4.32 (03). 01 від 04.02.2021 р.
9. Проєкт Держбюджету на 2020 рік. Розподіл видатків за напрямами фінансування (діаграма "світова практика").
10. Система технического обеспечения Сухопутных войск : военно-теоретический труд. Москва : Военная академия БТВ, 1985.
11. Гуляев А. В. Руководство и управление производственным процессом в подвижных ремонтных средствах танковых войск. Москва : Военная академия БТВ, 1977.
12. Тихонов В. П. Основы организации ремонта БТТ. Москва : Военная академия БТВ, 1975.
13. Хазанович О. І. Система матеріально-технічного забезпечення: Ретроспектива розвитку та напрями удосконалення. *Наука і оборона*. 2007. № 1. С. 27–31.
14. Доктрина "Забезпечення МтЗ, роботами та послугами" – ВКП 4–160 (03).01 від 21.01.2021 р.
15. Доктрина "З організації переміщень та перевезень (транспортувань) у Збройних Силах України" – ВКП 4.00 (03).01 від 19.08.2020 р.

Стаття надійшла до редакційної колегії 25.11.2020

Directions of improvement of organizationally-staff structure of organs of technical support of subdivisions, units and forces of tactical level in the single system of logistic

Annotation

The necessity of improvement of organizationally-staff structure of bodies of technical support of subdivisions, units and forces of tactical level of Land Forces of Armed Forces of Ukraine is reasonable in the article, taking into account experience of armed forces of the USA, German Federal Republic and other leading countries of NATO. A necessary apparatus is offered for the decision of certain problems.

Already more than six years Armed Forces of Ukraine conduct the warfare under defending of sovereignty and territorial integrity of Ukraine. For this time, radical changes took place in political life, economy of the state and Armed Forces of Ukraine.

The problem of the complete falling short of possibilities of forces and facilities of repair-restoration organs of subsystem of hardware appeared to the aims and tasks of functioning of the system of logistical support of Land forces in the single system of logistic. It, in turn, results in a volume, that the subsystem of technical support provides the timeliness of renewal and plenitude of technical maintenance of armament and military technique not fully, that broke ranks, both because of battle damages and after technical reasons.

The best decisions of these tasks in difficult situations, usually, find by the rational construction of organizational structure the systems and her separate sections, clear distribution of functions between them in the typical situations of work, sufficient redundancy of production capacity and material resources at each level, as well as sustainable management.

Therefore, exactly consideration of this problem on principles of approach of the systems allowed to offer the ways of rational construction of organizationally-staff structure of both forces and facilities of repair-restoration organs of tactical level on the whole and him separate sections, clear distribution of functions between them in the typical situations of work, sufficient redundancy of production capacities and material facilities at every level, and also proof management forces and facilities of logistic, in particular hardware of Land Forces of Armed Forces of Ukraine.

Keywords: armament; military technique; renewal; technical service; logistic; logistic and technical providing.

УДК 005.5: 004.41: 004.453: 623.618.3 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/97-106

Беляченко В. В. (0000-0003-3938-5158)
Бобров С. В., канд. техн. наук, доцент (0000-0002-9647-9700)
Закалад М. А. (0000-0002-0624-4140)
Утюшев М. К. (0000-0002-7386-7831)

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

Обґрунтування функціональних вимог до програмної компоненти системи управління життєвим циклом автоматизованих систем у Збройних Силах України

Резюме. У статті розглянуто підхід до розв'язання проблеми неузгодженості проєктної діяльності у сфері інформатизації органів військового управління Збройних Сил України шляхом створення системи управління життєвим циклом автоматизованих систем. Досліджено приклади неузгодженості проєктної діяльності під час створення автоматизованих систем у сфері управління оборонними ресурсами, функціональність програмних компонентів окремих зразків систем управління життєвим циклом програмних засобів та запропоновано базовий перелік функціональних вимог до програмного компонента перспективної системи "Управління життєвим циклом автоматизованих систем управління Збройних Сил України".

Ключові слова: автоматизована система військового призначення; система управління життєвим циклом програмних засобів; система управління життєвим циклом систем; функціональні вимоги; інформаційна інфраструктура.

Постановка проблеми. Актуальним документом щодо діяльності МО України у сфері інформатизації залишається Концепція галузевих програм створення ЄАСУ ЗС України, єдиної інформаційної системи управління оборонними ресурсами та інформаційної інфраструктури на період до 2020 року, затверджена Міністром оборони України від 12.05.2018. Концепція в частині обґрунтування містить відомості про низку систематичних проблем, що не вирішуються довгий час і потребують розв'язання, зокрема неузгодженість розробок, які не становлять єдиної системи, що призвело до стану розпорошеності, за якого "створені окремі компоненти інформаційної інфраструктури та інформаційних систем різняться між собою за часом створення, ступенем завершеності, масштабом розгортання та використаними технологіями, обсягом охоплених процесів та наповненням даними" [1]. Розробки, які мали б бути підсистемами ЄАСУ ЗС України, у разі механічного об'єднання не створюють єдиної АСУ, а є об'єднанням АСУ, які не здатні підтримувати цикли управління оборонними ресурсами, військами і зброєю у реальному часі у єдиному інформаційному просторі [2].

Згідно з ДСТУ 24748-1:2018 типові етапи життєвого циклу системи охоплюють концепцію, розроблення, виробництво, використання, підтримання й утилізацію, під час яких виконуються проєктні процеси, технічні процеси, процеси угод та організаційного забезпечення, які підлягають комплексній автоматизації для інформаційного забезпечення, зокрема координації заходів проєктної діяльності. На сьогодні в Україні процеси управління ЖЦ АСУ ЗС України в цілому, та проєктні процеси зокрема, під час створення ЄАСУ не автоматизовані. Розв'язання проблем неузгодженості розробок потребує координації заходів проєктної діяльності учасників створення ЄАСУ ЗС України на основі розроблення та впровадження системи комплексної автоматизації процесів управління життєвими циклами програмних засобів (ЖЦ ПЗ) та життєвих циклів систем, до складу яких входять розроблені ПЗ. Формування функціональних вимог, які згідно зі стандартом ISO/IEC/IEEE 29148:2018 "*описують функцію або завдання системи або системних елементів, які необхідно виконати"*, до програмного компонента перспективної системи "Управління життєвим циклом автоматизованих систем управління Збройних Сил України" є нагальним завданням.

Аналіз останніх досліджень та публікацій. У публікаціях щодо проєктів інформатизації в МО США у 2000–2019 рр. зафіксовано систематичні проблеми проєктної

діяльності, зокрема у звіті Офісу урядової підзвітності США (ОУП США) в 2010 році вказано, що шість з дев'яти проєктів з упровадження АСУ перевищили графік від двох і більше років, а п'ять потребували збільшення витрат. Про проблеми свідчить той факт, що в жодній з програм інформатизації не було повністю розроблено основний інтегрований графік упровадження (*Integrated Master Schedule*), який мав містити відомості про ієрархічну, багатошарову структуру проєктних процесів з врахуванням взаємозалежностей, часових і ресурсних обмежень, та основний інтегрований план (*Integrated Master Plan*) про порядок трансформації процесів з конкретними цілями, заходами та шаблонами підзвітності для моніторингу [3]. Інститут оборонного аналізу США в публікації 2011 року вказав типові проблеми, що виникли внаслідок неузгодженості проєктної діяльності та незадовільної комунікації учасників проєктів, зокрема нереалістичні графіки і бюджети проєктів інформатизації [4]. ОУП США у звіті 2011 року зазначив, що МО США неефективно керувало придбанням АСУ на базі ERP-систем і не досягало очікуваних спроможностей вчасно та в межах бюджету [5]. Завдання синхронізації інвестиційної діяльності всіх компонентів МО США шляхом "*ефективного управління портфелем проєктів та управління інвестиціями і забезпечення інновацій в архітектурі організації, стандартах та технологіях процесів*" указано в Стратегічному плані МО США на 2015–2018 рр. і Стратегії цифрової модернізації МО США на період 2019–2023 рр., що свідчить про актуальність проблеми неузгодженості проєктної діяльності [6, 7]. Важливою особливістю сучасної проєктної діяльності в МО США є застосування набору принципів, практик і технологій DevSecOps, яка є сучасним стандартом придбання СПЗ згідно з Інструкцією 5000.02 МО США щодо сценаріїв діяльності з адаптивних закупівель та Інструкцією 5000.82 МО США щодо закупівель інформаційних технологій.

Більшість сучасних досліджень щодо управління життєвим циклом АС, під час якого здійснюється управління проєктною діяльністю під час технічних процесів і процесів угод, технічного управління і організаційного забезпечення, зосереджені на: окремих аспектах функціонування і підходах, зокрема на **оптимізації процесів** з погляду досягнення вищої безпеки, продуктивності, якості та інтеграції з процесами життєвого циклу продукту (PLM) і процесами життєвого циклу сервісів (SLM) [8]; **застосування і комбінації практик** ITIL, COBIT та міжнародного стандарту ISO/IEC 27002 щодо заходів інформаційної безпеки до процесів програмної інженерії в напрямі вищого рівня керованості життєвого циклу кожного програмного компонента АС, що входять в інформаційну інфраструктуру (ІнфІС) організації [9]; **розробленні нових моделей** життєвого циклу систем, у яких передбачається використання технологій машинного навчання, алгоритмів обробки даних, які моделюють роботу штучного інтелекту (ШІ), технологій машино-машинної взаємодії в мережевому середовищі, що загалом динамічно змінює характеристики та стан життєвого циклу АС [10] тощо.

Дослідники проблем інформатизації ЗС України розглядають різні аспекти процесу створення ЄАСУ і, зокрема, сходяться на думці, що проблеми фрагментарності АСУ ЗС України, неузгодженості проєктної діяльності, досі марнотратних спроб об'єднання у єдиному інформаційному середовищі сукупності автономно функціонуючих АСУ, замість створення від початку єдиної АСУ ЗС України, **мають розв'язуватись під час комплексу організаційних, економічних, нормотворчих і технологічних заходів**, спрямованих на забезпечення узгодженого функціонування АС, ІАС та електронних інформаційних ресурсів (ЕІР) усіх об'єктів управління в інформаційному просторі ЗС України [11–18]. Проте систематизованих формулювань функціональних вимог до програмної компоненти системи управління життєвим циклом автоматизованих систем управління ЗС України, в доступній для аналізу літературі не знайдено, лише вимоги до окремих аспектів систем управління життєвим циклом ПЗ і АС без акцентування на синхронізації та координації проєктної діяльності під час управління програмами інформатизації. Формування базових функціональних вимог до програмного компонента перспективної системи під робочою назвою АС "УЖЦ АСУ ЗС України" започатковують процес наукового обґрунтування фінальної специфікації функціональних вимог, які є підставою для підготовки технічного завдання на АС, до функціонального складу якої входитиме функція координації заходів проєктної діяльності зі створення ЄАСУ.

Метою статті є формування основних функціональних вимог до програмної компоненти перспективної системи "УЖЦ АСУ ЗС України" з урахуванням досвіду інформатизації (автоматизації) процесів ведення проєктної діяльності.

Виклад основного матеріалу. Проєктна діяльність щодо створення ЄАСУ ЗС України продовжує здійснюватись в умовах обмеженого ресурсного і кадрового забезпечення, незначного досвіду учасників проєктів і фундаментальної проблеми суб'єкта про неможливість самостійно досягти несуперечності та повноти вимог щодо об'єкта проєктування, доки не залучити суб'єктів вищого рівня ієрархії. Дієвим технологічним заходом розв'язання проблеми є комплексна автоматизація усіх груп процесів управління ЖЦ АС, зокрема процесів управління проєктом на кожному етапі ЖЦ АС, що дасть змогу перейти від "ручного" управління проєктами до автоматизованого управління проєктами, програмами та портфелями проєктів зі створення АС та узгодженому функціонуванню програмних компонентів ЄАСУ ЗС України у єдиному інформаційному просторі.

Складність формулювання вимог обумовлена необхідністю дотримання і врахування:

загальносистемних принципів побудови інформаційних систем;

існуючої сукупності АС;

обсягів фінансування на утримання і розвиток ЗС України;

чинних і перспективних державних і відомчих нормативних документів.

До того ж, мають бути враховані:

перспективна доктрина "Зв'язок та інформаційні системи", гармонізована з доктриною НАТО щодо вимог до комунікаційно-інформаційних систем AJP-06 (A);

чинні та перспективні ВСТ щодо військового зв'язку та інформаційних систем;

перспективний Технічний регламент щодо управління життєвим циклом інформаційних систем;

низка ДСТУ щодо ЖЦ АС, ПЗ та проєктів (ДСТУ 15288:2016, 12207:2018, 16326:2015);

низка ДСТУ щодо забезпечення якості інформатизованих процесів, процесів проєктування, якості ПЗ та систем (комплект ДСТУ 330**, комплект ДСТУ 15504-*, комплект ДСТУ 250**);

низка ДСТУ, гармонізованих з такими угодами країн – членів НАТО як STANAG 4107:2018 "Додаткові вимоги НАТО до AQAP 2110 або AQAP 2310 щодо забезпечення якості програмного забезпечення", STANAG 4107:2019 "Політика НАТО щодо інтегрованого системного підходу до якості протягом життєвого циклу (STANAG 4107 Ed:11/AQAP-2000 Ed. 3)", STANAG 4107:2018 "Вимоги НАТО щодо проєктування, розроблення та виготовлення (STANAG 4107 Ed:10/AQAP-2110" та внутрішні документи МО України щодо розвідки, контррозвідки та відповідних процедур (STANAG 2190, AJP 2, STANAG 2191, AJP-2.1);

угоди країн – членів НАТО (STANAG 4728, AAP-20, AAP-48) у частині моделей і процесів управління ЖЦ, операцій у кіберпросторі (STANAG 6514, AJP 3.20), публікації НАТО щодо вимог до якості ПЗ упродовж життєвого циклу (AQAP-160) і керівництво AQAP-169 із застосування AQAP-160.

Перед формуванням базового переліку функціональних вимог до програмного компонента АС "УЖЦ АСУ ЗС України" доцільно прийняти положення щодо особливостей створення і експлуатації АС.

1. Концепція побудови АС "УЖЦ АСУ ЗС України" має враховувати вимогу сумісності з програмними компонентами гетерогенної інформаційної інфраструктури (ІнфІС) ЗС України для досягнення адаптивності (через стандартизацію та уніфікацію) і відповідати вимогам до кібербезпеки і кіберстійкості.

2. Як типову модель для здійснення проєктної діяльності під час створення АС у сфері управління зброєю доцільно обрати каскадну модель з послідовним виконанням етапів створення від задуму і концепції і до введення в експлуатацію готового продукту. Для здійснення проєктної діяльності під час створення програмних компонентів ЄАСУ має бути обрана інкрементна (нарощування спектру можливостей в функціональних сферах), спіральна (створення АС шляхом ітераційного прототипування з оцінюванням ризиків при кожній ітерації) та водночас еволюційна модель ЖЦ АС (гнучка IEC-модель) для здійснення циклічних заходів безперервного удосконалення функціональності або модернізації АС у зв'язку з появою нових вимог або інформаційних технологій.

3. Проєктна діяльність має відбуватись відповідно до етапів життєвого циклу АС, що

створюється, та етапів ЖЦ ПЗ (множини програмних компонентів, які входять в АС). До того ж слід ураховувати чинні відомчі нормативні документи, рекомендації національних і міжнародних стандартів та знання про проєктний і експлуатаційний досвід ЗС України та інших оборонних організацій.

4. Під час планування проєктних заходів у сфері інформатизації мають застосовуватись стратегії забезпечення кібербезпеки щодо придбання інформаційних технологій та підходи до організаціїі створення програмних компонентів згідно з набором принципів, практик і технологій DevSecOps. Суть DevSecOps у частині проєктної діяльності полягає у фокусуванні на забезпеченні кібербезпеки із самого початку проєктування (конструювання шляхом автоматизації тестування, інтеграції та розгортання) під час якого кібербезпекові характеристики програмних компонентів та їх функціональні можливості розробляються і тестуються одночасно, що зменшує ймовірність ризику колапсу АС ЗС України внаслідок кібератак і спростить досягнення інтероперабельності без втрати кіберстійкості.

5. Управління життєвими циклами програмних компонентів інформаційної інфраструктури ЗС України має здійснюватись через інтеграційну платформу із сервісною інтеграційною шиною даних з використанням ієрархічного класифікованого переліку сервісів комунікаційно-інформаційних систем на базі моделі NATO C3 Classification Taxonomy, що дасть змогу обґрунтуванню розподілу і синхронізації витрат ресурсів на досягнення інтероперабельності між системами завдяки стандартизованому опису інформаційних сервісів та їх взаємодії.

6. Результати функціонування АС "УЖЦ АСУ ЗС України" у вигляді інформації про поточний і перспективний стан програмних компонентів АСУ, які входять в ІнфІС ЗС України, мають надаватись в реальному часі учасникам проєктної діяльності щодо створення ЄАСУ.

Наступний крок – це огляд і фіксація сценаріїв використання сучасних програмних рішень автоматизації процесів проєктної діяльності, які дадуть змогу окреслити коло програмних рішень обмежено придатних для інформатизації в цілому процесів управління ЖЦ АС та ЖЦ ПЗ і придатних за окремими функціональними сферами. Розробники ПЗ для АСУ організаційного типу, як правило, окреслюють обсяг функцій на основі міжнародних стандартів, бібліотек кращих практик та вимог клієнтів згідно з такими моделями управління процесами:

управління життєвим циклом розроблення програмних засобів (Software Development Lifecycle Management, SDLC-система) на основі ISO/IEC/IEEE 12207:2017 "Інженерія систем і програмних засобів. Процеси життєвого циклу програмних засобів", сімейства ISO/IEC/IEEE 24748 "Інженерія систем і програмного забезпечення. Керування життєвим циклом" та рекомендацій бібліотеки з управління застосунками впродовж ЖЦ ПЗ (Application Services Library (ASL);

управління життєвим циклом програмних засобів (Application Lifecycle Management System, ALM-система) на основі ISO/IEC/IEEE 15288:2015 "Інженерія систем і програмного забезпечення. Процеси життєвого циклу систем" і стандартів сімейства ISO/IEC 19770-1:2017 "Вимоги до систем управління програмним забезпеченням як активом";

управління проєктною діяльністю (Project Management System, PMS-система) на основі PMBoK та інших бібліотек проєктних практик (PRINCE2, P2M) та ISO/IEC/IEEE 16326:2019 "Інженерія програмного забезпечення і систем. Процеси життєвого циклу. Управління проєктом";

управління портфелем проєктів (Project Portfolio Management System, PPMS-система) на основі ISO 21505:2017 "Управління програмами, проєктами і портфелями проєктів";

управління життєвим циклом інформації (Information Lifecycle Management, ILM-система) на основі вимог стандартів ISO/TR 22957:2018 "Управління документами. Аналіз, вибір та впровадження систем управління корпоративною інформацією", ISO 16175-1:2020 та ISO/TS 16175-2:2020 "Інформація та документація. Процеси та функціональні вимоги до програмного забезпечення для керування записами", ISO 15489-1: 2016 "Інформація та документація. Управління документами. Ч. 1: Концепції та принципи" та моделей і рекомендацій з управління діловою інформацією (Business Information Services Library (BISL);

управління життєвим циклом продукту (Product Lifecycle Management (PLM) на основі сімейства ISO 10303-***:2021 "Системи промислової автоматизації та

інтеграції. Подання даних щодо виробів та обміну даними";

управління життєвим циклом інформаційних сервісів (Service Lifecycle Management, SLM-система) на основі стандартів сімейства ISO/IEC 2000*-*:2018 "Інформаційні технології. Управління сервісами", зокрема 11 та 12 частинами, які встановлюють зв'язок стандарту із моделями управління і поліпшення інформаційних сервісів по ITIL (Information Technology Infrastructure Library, Бібліотека інформаційних технологій інфраструктури) та моделями удосконалення процесів управління сервісами (CMMI-SVC);

управління архітектурою організації (Enterprise Architecture Management System, EAM-система), з використанням уніфікованої мови моделювання (UML), згідно зі стандартами ISO/IEC 19505-1 "Інформаційні технології. Уніфікована мова моделювання OMG (OMG UML). Інфраструктура" та ISO/IEC 19505-2:2012 "Інформаційні технології. Уніфікована мова моделювання OMG (OMG UML). Суперструктура";

управління та використання корпоративних інформаційних технологій (IT governance system) згідно зі стандартом ISO/IEC 38500:2015 "Інформаційні технології. Управління IT в організації" та бібліотекою принципів застосування та аудиту інформаційних технологій (COBIT);

управління сервісами організації (Enterprise Service Management System, ESM-система) на основі застосування принципів управління IT-сервісами до підтримки і поліпшення сервісів організації загалом.

Аналіз функціональності представлених моделей управління свідчить, що жодна з них наразі не відповідає повною мірою процесам управління життєвим циклом АС. Завдання створення системи управління життєвим циклом автоматизованих систем у ЗС України, у якій були б присутні повністю або частково функціональні можливості розглянутих моделей управління і досягнуто принципово нові можливості управління створенням ЄАСУ ЗС України, потребує інтегрованого підходу та додаткових досліджень щодо визначення цілей, функцій, складу АС "УЖЦ АСУ ЗС України" і її місця в архітектурі ІнфІС ЗС України.

Для визначення змісту вимог щодо інформаційної підтримки проєктних завдань, найуразливіших з погляду виникнення проблем і вагомих з погляду економічного ефекту, було виокремлено чотири групи проєктних завдань під час інформатизації процесів управління (табл. 1).

Таблиця 1

Проєктні завдання та зміст вимог щодо інформаційної підтримки проєктних завдань

Проєктні завдання	Вимоги щодо інформаційної підтримки проєктних завдань
Реалістичні графіки і бюджети	Під час управління портфелем проєктів та програмами інформатизації має здійснюватись управління вимогами до програмних компонентів АС з метою створення календарно-ресурсних планів проєктів та планів витрат, формування ієрархічної структури проєктних робіт, які зі свого боку узгоджуються та синхронізуються на рівні керівників програм інформатизації, а на рівні керівників інвестиційних програм з орієнтовним Планом утримання і розвитку ЗС України
Комунікація та передавання знань	Під час ЖЦ програмних компонентів АС, користувачі АС "УЖЦ АСВП ЗС України" (керівники портфелю проєктів, програм, уповноважені представники учасників окремих проєктів, експерти та представники НДО, що здійснюють НТС) мають отримувати інформацію про хід проєктів та результати оцінок характеристик створюваного програмного компонента, брати участь в оцінюванні рівнів технологічної, інженерної, організаційної, експлуатаційної та інших видів готовності, ініціювати або здійснювати коригувальні заходи, ухвалювати рішення щодо подальшого фінансування розроблень
Управління змінами та удосконаленням задля досягнення цілей проєкту	Користувачі АС "УЖЦ АСВП ЗС України" для досягнення результатів проєктів здійснюють управління змінами та удосконалення операційних процесів і процесів експлуатації програмних компонентів АС, що полегшує подальший моніторинг, аудит і підтвердження довіри до АС
Забезпечення кібербезпеки і кіберстійкості	Автоматизація, моніторинг та застосування вимог і процедур кібербезпеки та забезпечення кіберстійкості згідно з набором принципів, практик і технологій DevSecOps має застосовуватись на всіх стадіях ЖЦ програмних компонентів АС ЗС України

Для визначення базової функціональності програмного компонента АС "УЖЦ АСУ ЗС України", було проаналізовано відомості про функціональні можливості трьох зразків програмних рішень для створення ALM-систем (ALM Octane Enterprise компанії MicroFocus, SAP Solution Manager 7.2 компанії SAP та сімейство застосунків для спільного управління життєвим циклом систем на платформі IBM Jazz Team Server компанії IBM). Вибір програмних рішень для створення ALM-

систем як основи для першої черги перспективної АС "УЖЦ АСУ ЗС України" пояснюється широким спектром функціональності, яка потрібна для подолання неузгодженості проєктної діяльності. Усі досліджені зразки підтримують "каскадну", "еволюційну", "інкрементну", "спіральну", "гнучку" та змішану "інкрементно-еволюційну" моделі ЖЦ АС, що дає змогу зформувати адаптивний інформаційний простір для учасників проєктів, які зі свого боку можуть локально використовувати програмні рішення для управління ЖЦ АС від інших постачальників.

Зважаючи на потреби управління ЖЦ АС ЗСУ вагомими недоліками наведених програмних рішень для створення ALM-систем є обмеженість інформаційної підтримки процесів управління та удосконалення компонентів архітектури організації та ІнфІС. Потреби управління ЖЦ АС ЗС України і водночас проєктною діяльністю потребує ширшої функціональності програмних компонентів у складі АС "УЖЦ АСУ ЗС України", тому варто розглянути *сценарій інтеграції функціональності* ALM-систем з компонентами EAM-систем та ESM-систем в одному програмному комплексі та інтеграцією на рівні обміну даними із системами управління інформаційними сервісами. Базові функціональні вимоги до програмної компоненти АС "УЖЦ АСУ ЗС України" можна структуризувати за напрямами, кожний з яких охоплює процеси, які підлягають автоматизації, властиві одному, або декільком етапам життєвого циклу системи згідно з орієнтовною схемою розподілу (Схема 1).

Схема 1

Структура базових функціональних вимог до програмної компоненти АС "УЖЦ АСУ ЗС України"

Етапи ЖЦ АС	**Напрями базових функціональних вимог до АС "УЖЦ АСУ ЗС України"**								
Концепція	Управління процесами	Управління випробуваннями	Управління проєктом			Моніторинг та управління змінами		Управління ЖЦ СПЗ власного розроблення	
Розроблення									
Виробництво									
Використання				Виконання операційних процесів	Експлуатація АС		Управління інформаційними сервісами		Управління інформаційною інфраструктурою
Підтримка									
Утилізація									

1. У сфері "Управління процесами" має бути можливість документувати існуючі процеси і зберігати їх версії, моделювати майбутні процеси як з погляду цілей організації так і з погляду використання ІТ для їх підтримки. Результати документування мають бути доступні для використання учасниками ЖЦ АС ЗС України під час процесів управління проєктами згідно з IEC-моделі.

2. У сфері "Управління випробуваннями" має бути можливість автоматизованого тестування наборами тестових сценаріїв відповідності компонентів АС технічному завданню та забезпечення вимог щодо кібербезпеки згідно з принципами DevSecOps на етапах концепції, розроблення та удосконалення функціональних можливостей як окремих складових АС, так і в інтеграції з іншими компонентами ІнфІС. Має бути забезпечена синхронність між оновленням документації на АС та здійсненням автоматизованого тестування впливу змін на АС, зокрема:

оцінювання та оптимізація обсягу тестувань і попереднє оцінювання ризиків розгортання;

набори прикладів (кейсів) для ручного і автоматизованого тестування;

план і послідовність випробувань на кіберстійкість, відповідність ТЗ та призначення наборів тестових сценаріїв функціональним сферам;

управління виявленими невідповідностями;

відображення на інформаційних панелях відхилень від очікуваних показників, поточного статусу та динаміки змін процесів.

Виконання комплексу заходів із запобігання невідповідностям на ранньому етапі сприятиме поліпшенню якості АС і продуктивності процесів, зменшенню втрат ресурсів на виявлення та виправлення помилок на етапі експлуатації, точнішому оцінюванню потреби у додаткових ресурсах.

3. У сфері "Управління проєктом" має бути підтримка створення інтегрованих проєктних документів за допомогою інформаційного обміну з результатами інших функціональних сфер. Наприклад, з "Управління вимогами" отримувати дані про пріоритетність вимог, з "Управління процесами" – які процеси мають бути реалізовані, з "Управління випробуваннями" – дані моніторингу виконання змінюваних процесів, з "Управління інформаційними сервісами" – дані про невідповідності, з "Управління змінами" – дані про хід змінюваних процесів і їх ресурсне забезпечення, а також відповідність активностей в інших функціональних сферах АС.

4. У сфері "Виконання операційних процесів" має бути підтримання завдань:

виявлення проблем, які впливають на якість, ефективність, швидкість, продуктивність, результативність процесів;

виявлення потенціалу удосконалення процесів з урахуванням залежностей та обмежень;

моніторинг операційних процесів за допомогою ергономічного інтерфейсу, заснованому на ролях;

набір сценаріїв реагування на позанормові відхилення від планованих показників;

превентивне уникнення чи виявлення невідповідностей даних про хід операційних процесів;

надання даних і знань, що накопичились під час управління проєктом для аналізу з використанням алгоритмів штучного інтелекту.

5. У сфері "Експлуатація АС" має бути підтримання завдань:

здійснення централізованого моніторингу систем і підсистем та стану інтеграції усіх компонентів ІнфІС, у контурах якого експлуатуються сукупності АС;

аналітична обробка даних з виведенням ключових показників їх стану на інформаційні панелі ситуаційних центрів та оброблення оповіщень;

управління обсягом даних (аналіз потенціальних та фактичних відхилень) та відповідна звітність для учасників проєктів;

сценарії реагування на відхилення від нормативних показників;

реалізація сценаріїв підтримки ПЗ, що входять в програмні компоненти АС ЗС України, зокрема відповідності прав користування умовам ліцензування і аналіз автоматично зібраних даних про використання;

моніторинг статусів та активності користувачів, зокрема діагностика та аналіз першопричин проблем користувачів з найпоширенішими технологіями та досягненням інтероперабельності між компонентами ІнфІС ЗС України;

моніторинг статусів виконання напівавтоматичних та автоматичних завдань, які виконуються у розподілених системах;

технічне адміністрування ПЗ із застосуванням централізовано керованих сценаріїв типових процедур з використанням даних аналізу першопричин інцидентів;

управління знаннями та неструктурованою інформацією щодо компонентів ІнфІС ЗС України;

конфігурування та валідація компонентів ІнфІС на відповідність вимогам користувачів;

6. У сфері "Моніторинг та управління змінами" має бути можливість контролювати зміни конфігурацій компонентів ІнфІС, перевіряти ризики для стабільності та безпеки, спричинені змінами, підтримувати вимоги щодо вжиття заходів із захисту інформації згідно з ДСТУ 27001, зокрема способів організації безпеки інформації, розподілу обов'язків, цілісності систем та їх компонентів, принципів керування інцидентами згідно з ДСТУ 27035. Методи та інструменти АС "УЖЦ АСУ ЗС України" мають підтримувати прозорість та постійне поліпшення якості процесів змін протягом усього ЖЦ АС шляхом охоплення усіх платформ та технологій.

7. У сфері "Управління інформаційними сервісами" має бути можливість підтримки управління життєвим циклом інформаційних сервісів та реалізовані основні процеси ITIL, зокрема управління інцидентами безпеки, проблемами, зверненнями користувачів, рівнем сервісу, релізами та розгортанням, змінами, конфігуруванням, каталогом і портфелем сервісів, доступністю, подіями, ємністю, безперебійністю та виконанням запитів.

8. У сфері "Управління ЖЦ СПЗ власного розроблення" має надаватись авторизований доступ до кодів власних розробок для оптимізації, контролю впровадження, моніторингу використання та показників якості, що дає змогу зберігати контроль над власними розробками при реорганізаціях та реінжинірингу процесів. Власні розробки доповнюють придбані АС функціями, які сторонній розробник не мав можливості додати чи передбачити.

9. У сфері "Управління інформаційною інфраструктурою" опис компонентів ІнфІС має бути доступним адміністраторам та архітекторам систем та давати змогу керувати процесом інвентаризації, введення нових та змінювання або заміни чи утилізації існуючих програмних компонентів інформаційної інфраструктури через зміни технологій та процесів. Зміни процесів (порядку, змісту, рівня залученості учасників процесу) зумовлюють необхідність централізованого управління компонентами ІнфІС, що сприяє попередженню невідповідностей на всіх етапах ЖЦ АС.

10. Програмні компоненти АС "УЖЦ АСУ ЗС України" також мають взаємодіяти в інформаційній інфраструктурі ЗС України з іншими ІС, зокрема:

ІС управління оборонним плануванням у завданні визначення напряму розвитку архітектури військової організації та формування дорожньої карти трансформації від стану архітектури "як є" до стану "як має бути" з врахуванням доктрин та стратегій розвитку ЗС України, обмежень існуючої архітектури та прогнозованих загроз майбутнього;

ІС управління портфелем проєктів у завданні управління напрямами і обсягами інвестицій та оцінювання ризиків, планування портфелю проєктів і програм інформатизації, спрямованих на застосування проривних інформаційних технологій і виконання проєктів у сфері побудови і удосконалення архітектури інформаційної інфраструктури ЗС України;

ІС управління інформаційною інфраструктурою у завданні інформаційного забезпечення користувачів та досягнення і утримання технологічної переваги перед потенційним агресором, підтримки успадкованих систем;

іншими ІС управління компонентами архітектури ЗС України, які входять до складу компонентів DRMIS та C4ISR і утворюють ЄАСУ ЗС України.

Результатом взаємодії цих ІС з АС "УЖЦ АСУ ЗС України" є можливість **узгодження** архітектури ЗС України та архітектури інформаційної інфраструктури ЗС України з місією, цілями та стратегією досягнення і утримання переваги під час збройної агресії чи конфлікту.

Експлуатація АС "УЖЦ АСУ ЗС України" дасть змогу оцінювати стан і управління ЖЦ усіх АС з управління оборонними ресурсами та військами, використання ЕІР у режимі реального часу, поліпшення інформаційного забезпечення інформаційно-аналітичних систем і СППР у ситуаційних центрах, обґрунтованого підходу до удосконалення інформаційної інфраструктури ЗС України завдяки:

ліпшому розумінню існуючих процесів через застосування єдиних підходів до документування і розроблення пропозицій щодо змін процесів, зокрема внаслідок інформатизації, автоматизації і роботизації;

ліпшому розумінню всіх шарів і контурів інформаційної інфраструктури і спрощенню завдань з удосконалення та інтеграції компонентів ІнфІС, що зі свого боку полегшує завдання адміністрування, забезпечення кібербезпеки та актуалізації в режимі реального часу даних про стан ЕІР МО України відповідно до рівнів доступу;

унормування порядку управління життєвим циклом АС у вигляді технічних регламентів та настанов;

зменшення витрат ресурсів на дослідження об'єктів інформатизації та розроблення програмно-технічних рішень під час проєктного етапу ЖЦ АС.

Висновки. Розв'язання проблеми неузгодженості проєктної діяльності у сфері інформатизації органів військового управління Збройних Сил України пропонується за допомогою створення системи управління життєвим циклом автоматизованих систем з робочою назвою АС "УЖЦ АСУ ЗС України".

Сформульовано базові функціональні вимоги до програмної компоненти АС "УЖЦ АСУ ЗС України", яка може бути використана для:

управління життєвим циклом програмного забезпечення на основі використання ALM-систем;

управління архітектурою організації на основі EAM-систем;

управління сервісами організації на основі ESM-систем;

реалізації функції обміну даними із системами управління інформаційною інфраструктурою на основі процесів, описаних в ITIL.

АС “УЖЦ АСУ ЗС України” має підвищити якість управління усіма аспектами ЖЦ програмних компонентів АС ЗС України та дасть змогу:

1) управляти проєктними та експлуатаційними процесами;

2) інформаційно підтримувати учасників проєктів створення та супроводження експлуатації ЄАСУ ЗС України;

3) формувати обґрунтовані рішення щодо використання компонентів ЄАСУ.

Напрямами подальших досліджень є виявлення, аналіз, документування та підготовка проєкту специфікації функціональних вимог до АС “УЖЦ АСУ ЗС України” та проведення випробувань зразків програмних рішень для створення ALM-систем, EAM-систем, ESM-систем на базі науково-випробувальних комплексів ВВНЗ і НДО системи МО України для отримання скоригованої оцінки придатності до створення програмного компонента АС “УЖЦ АСУ ЗС України”.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Концепція галузевих програм створення ЄАСУ ЗСУ, єдиної інформаційної системи управління оборонними ресурсами та інформаційної інфраструктури на період до 2020 року : затв. Міністром оборони України від 12.05.2018 р.
2. Морозов А. О., Косс В. А. Управління розробкою Єдиної АСУ Збройних Сил. *Математические Машины и Системы*. 2007. № 2. С. 1–11. URL: http://www.immsp.kiev.ua/publications/files/5_syst_proekt.pdf (дата звернення: 25.06.2021).
3. U.S. GAO. Dod Business Transformation. Improved Management Oversight of Business System Modernization Efforts Needed. URL: https://www.gao.gov/products/GAO-11-53 (дата звернення: 25.06.2021).
4. Institute for Defense Analyses. Assessment of DoD Enterprise Resource Planning Business Systems. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a563798.pdf (дата звернення: 25.06.2021).
5. U.S. GAO. Critical Factors Underlying Successful Major Acquisitions. P. 38–39. URL: https://www.gao.gov/assets/gao-12-7.pdf (дата звернення: 25.06.2021).
6. U.S. DoD. Agency Strategic Plan. Fiscal Years 2015-2018. 28 p. URL: https://cmo.defense.gov (дата звернення: 25.06.2021).
7. U.S. DoD. DoD Digital Modernization Strategy. P. 11–12. URL: https://media.defense.gov (дата звернення: 25.06.2021).
8. Peruzzini M., Germani M., Marilungo E. Product-service lifecycle management in manufacturing: An industrial case study. In IFIP International Conference on Product Lifecycle Management; Springer: Berlin/Heidelberg, Germany, 2014. P. 445–454. URL: https://hal.inria.fr/hal-01386551/document (дата звернення: 25.08.2021).
9. Sahibudin S., Sharifi M., Ayat M. Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. 2-nd Asia International Conference on Modelling & Simulation, Malaysia, 13–15.05.2008. URL: https://www.researchgate.net (дата звернення: 25.08.2021).
10. Ashmore R., Calinescu R., Paterson C. Assuring the machine learning lifecycle: Desiderata, methods, and challenges. Arxiv 2019. URL: https://dl.acm.org/doi/pdf/10.1145/3453444 (дата звернення: 25.08.2021).
11. Пропозиції щодо формування вимог під час розроблення (вдосконалення) інформаційних систем військового призначення Збройних Сил України / В. І. Галаган, С. В. Полішко, С. В. Бондарчук, А. В. Фатальчук // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ, 2020. № 1 (68). С. 74–80.
12. Визначення технологічних рішень щодо створення Єдиної інформаційної системи управління оборонними ресурсами / Ю. А. Кірпічніков, О. В. Андрощук, О. В. Головченко, М. В. Петрушен // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ, 2019. № 1 (65), С. 86–91.
13. Кірпічніков Ю. А., Андрощук О. В., Петрушен М. В. Аналіз поняття інтеграційної платформи та методів інтеграції даних інформаційних систем управління оборонними ресурсами. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2017. № 2 (60). С. 73–78.
14. Теоретичні підходи до побудови архітектури інформаційної системи управління оборонними ресурсами на основі сервісно-орієнтованої моделі. / Ю. А. Кірпічніков, О. В. Андрощук, М. В. Петрушен, С. І. Васюхно // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ, 2018. № 1 (62). С. 80–85.
15. Особливості розроблення технічного регламенту щодо управління життєвим циклом інформаційних систем у воєнному відомстві / А. А. Рибидайло, А. М. Турейчук, О. С. Прокопенко, О. Д. Розумний // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ, 2017. № 2 (60). С. 79–85.

16. Кучеренко Ю. Ф., Демидов Б. А., Науменко М. В. Системно-концептуальные основы построения единой автоматизированной системы управления вооруженными силами государства. *Системи озброєння і військова техніка*. Харків, 2013. С. 72–76.
17. Забезпечення кібероборони держави : матеріали наук.-практ. Вебінару. (м. Київ, 16 квіт. 2020 р.) Київ, 2020. С. 30–32 URL: https://elib.nuou.org.ua/katalog/zabezpechennya-k%D1%96beroboroni-derzhavi.html (дата звернення: 25.06.2021).
18. Бобров С. В., Беляченко В. В., Утюшев М. К. Управління ризиками створення елементів автоматизованих систем управління. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2020. № 3 (70), С. 101–106.

Стаття надійшла до редакційної колегії 16.06.2021

Substantiation of functional requirements to the software component of the life cycle management of automated systems of the Armed Forces of Ukraine

Annotation

The current document of the Ministry of Defense of Ukraine in the field of Informatization is the "Concept of industry programs to create a Unified Automated Management System of the Armed Forces of Ukraine (UAMS of AFU), a single information management system of defense resources", which identifies a number of issues to be addressed, namely:

Inconsistency of developments that do not constitute a single system;

Achieving technical and information compatibility;

State of dispersion, in which separate components of information infrastructure and information systems are created.

Some of them differ in terms of creation time, degree of completion, scale of deployment and technologies used, scope of processes covered and data content.

Developments, which should be subsystems of the UASU of the Armed Forces of Ukraine, do not create an UAMS of AFU by mechanical association, but are an association of UAMS that are not able to support management cycles of defense resources, forces and weapons in real time in a single information space.

The solution to the problem of inconsistency of project activities in the field of Informatization of the military administration of the Armed Forces of Ukraine is proposed by creating a life cycle management system (LCMS) of automated systems of the Autonomous Systems of the "LCMS of UAMS of AFU".

The basic functional requirements to the software component of the "LCMS of UAMS of AFU" are already formulated, and can be used for the next tasks:

software lifecycle management based on the use of ALM-systems;

organization architecture management - based on EAM-systems;

organization services management based on ESM-systems;

implementation of the data exchange function with information infrastructure management systems based on the processes described in ITIL.

Keywords: automated military system; software lifecycle management system; system lifecycle management system; functional requirements, information infrastructure.

УДК 004.056.53 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/107-113

Федорієнко В. А. (0000-0002-0921-3390)
Кульчицький О. С. (0000-0002-4901-0192)
Розумний О. Д. (0000-0003-3225-8375)

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

Особливості спеціального програмного забезпечення управління подіями безпеки для системи DRMIS

Резюме. У статті визначено особливості спеціального програмного забезпечення управління подіями безпеки SIEM для єдиної інформаційної системи управління оборонними ресурсами (DRMIS) у рамках функціонування центру управління інформаційною безпекою в інформаційних системах SOC. Запропонована система обробки даних та експертних оцінок дасть змогу визначити захищеність інформаційної системи під час побудови програмної компоненти системи захисту інформації. Розкрито особливості найбільш застосованих моделей оцінювання захищеності за визначеними метриками.

Ключові слова: спеціальне програмне забезпечення SIEM; обробка даних; кібернетичний простір; інформаційна безпека; події інформаційної безпеки.

Постановка проблеми. Проведення злочинних заходів щодо втручання у функціонування роботи державних інформаційних систем для їх блокування та витоку інформації зумовлюють перегляд та уточнення основних принципів і підходів до захисту інформаційної інфраструктури Міністерства оборони (МО) України в умовах загроз у кібернетичному просторі.

Першим кроком захисту інформаційної інфраструктури вважається використання спеціально програмного забезпечення (СПЗ) системи менеджменту інформаційною безпекою та моніторингу подій (Security Information and Event Management, SIEM). *Другим кроком* – розгляд цієї системи як програмної складової центру управління інформаційною безпекою (Security Operation Center – SOC), що є досить поширеним рішенням для великих організацій, підприємств, урядових та оборонних відомств. Центр безпеки або SOC виконує функції вчасного і швидкого реагування на події під час спроби впливу на працездатність і цілісність системи управління. Такі кроки є доцільними для забезпечення функціонування єдиної інформаційної системи управління оборонними ресурсами (DRMIS) Міністерства оборони України.

Програмна компонента SIEM, яка є ключовим СПЗ SOC базується на принципах своєчасного оповіщення щодо змін стану інформаційної безпеки на основі менеджменту подій. Тут під *подією* розуміється потенційний результат певних дій, які за допомогою впливу на інформацію або інші компоненти інформаційної системи можуть прямо або опосередковано призвести до заподіяння шкоди даним, а також ставлять під загрозу захищеність інформаційних ресурсів того чи іншого об’єкта чи суб’єкта інформаційної діяльності. Залежно від величини ризику інформаційній безпеці, за своїм наслідком події можна кваліфікувати, як ті, що призводять до загрози інформаційній безпеці, порушення цілісності, конфіденційності та доступності інформації.

У статті зосереджено увагу на дослідженні особливостей СПЗ менеджменту інформаційної безпеки та моніторингу подій під час побудови програмної компоненти системи захисту інформації центру безпеки у DRMIS у складі інформаційної інфраструктури МО України.

Аналіз останніх досліджень і публікацій. Дослідженням особливостей роботи запропонованих систем управління подіями під час захисту інформаційних систем присвячені роботи [1–5], у яких розкриті застосовані моделі оцінки захищеності за визначеними метриками.

Питання застосування методів експертного оцінювання моніторингу подій у процесі побудови програмної компоненти

системи захисту інформації центру безпеки під час підтримки прийняття рішення стосуються досліджень І. Котенко [2]. У джерелах наукових праць [6–8], процес експертного оцінювання якості захисту інформаційних систем описується за визначеними критеріями з урахуванням сфери компетентності експертів та ваг кожного з експертів. У роботі [3] задачу щодо підбору системи управління подіями та визначення якості захищеності інформаційних систем пропонується вирішити на основі узагальненої ієрархічної моделі. Проте питання щодо особливостей СПЗ для управління подіями безпеки для системи DRMIS інформаційної інфраструктури МО України досліджені поверхнево.

Метою статті є аналіз особливостей системи управління подіями безпеки технології SIEM у складі SOC для обґрунтування рекомендацій щодо їх реалізації у системі DRMIS Міністерства оборони України.

Виклад основного матеріалу. Уперше поняття управління інформаційною безпекою та моніторингу подій (SIEM) було введене Марком Ніколетта та Амріта Вільямсом з компанії Gartner у 2005 році. Вони описали функціональність збору, аналізу та подання інформації від мережевих пристроїв і пристроїв безпеки, додатків ідентифікації (управління обліковими даними) та доступу, інструментів підтримки політики безпеки і відстеження вразливостей, операційних систем, баз даних і журналів додатків, а також відомостей про зовнішні загрози для здійснення раціонального управління інформаційною безпекою та підтримки прийняття рішень.

Технологія SIEM складається з двох сегментів. *Перший* – сегмент систем управління безпекою (SEM) – здійснює моніторингом у реальному часі та управлінням подіями шляхом співставлення їх відповідності (кореляції), повідомленням для відображення результатів на кінцевих пристроях. *Другий* – сегмент управління інформаційною безпекою (SIM) – забезпечує довготривале зберігання, аналіз і звітність за накопиченими даними. У міру зростання потреб у додаткових можливостях функціональність технології SIEM безперервно розширюється і доповнюється. Узагалі, SIEM-система – це програмна компонента технології захисту, яка виконує такі функції:

аналіз події та створення попередження за певних аномаліях: мережевого трафіку, несподіваних дій користувача, невпізнаних пристроях тощо;

перевірка системи захисту на відповідність стандартам захищеності;

створення гнучких інформативних звітів (наприклад, щоденний звіт про інциденти, щотижневий звіт порушників, звіт щодо працездатності пристроїв і т. ін.);

проведення моніторингу подій від пристроїв, серверів, критично важливих систем і створення відповідних оповіщень для визначених осіб;

проведення збору доказової бази за інцидентами;

за наявності сканера вразливостей, SIEM-система частково впливає на зміну ризиків.

Відповідно до звіту світової аналітичної компанії Gartner до лідерів виробників технології SIEM увійшли системи: IBM, Splunk, LogRhythm і McAfee. Ринок SIEM продовжує домінувати порівняно небагатьма постачальниками – Micro Focus, IBM, McAfee і Splunk, які дають понад 60 % доходу від ринку. Інші постачальники SIEM, як правило, орієнтовані на певні сегменти ринку. Огляд ринку та загальні тенденції розвитку технології SIEM наведені у роботі [9].

Технологія SIEM покладена в основу SOC, який, зі свого боку, відповідальний за виконання завдання щодо підтримки прийняття рішення стосовно інформаційної та кібербезпеки на організаційному та технічному рівнях. Центр безпеки є об’єктом, де корпоративні інформаційні системи (вебсайти, додатки, бази даних, центри обробки даних, сервери, активне мережеве обладнання, комп’ютери та інше кінцеве обладнання) контролюється, оцінюється та захищається. Тобто, SOC є комплексом програмно-технічних засобів, кваліфікованого персоналу та процесів їхньої взаємодії.

Передумовами щодо можливості використання організаційно SOC на основі СПЗ SIEM стали появи різного роду загроз інформаційній безпеці. Зокрема, найбільша з них – масштабна хакерська атака з боку Росії проти України у 2017 році з компрометації системи оновлення програмного забезпечення для подання звітності до контролюючих органів та обміну юридично значущими первинними документами між контрагентами в електронному вигляді (M.E.Doc) з використанням різновиду вірусу “Petya”. Ця атака спричинила порушення роботи

українських державних підприємств, установ, банків, медіа тощо. Унаслідок атаки було заблоковано діяльність таких підприємств, як аеропорт "Бориспіль", ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця та низки інших великих підприємств. Зараженню піддалися інформаційні системи Міністерства інфраструктури, Кабінету Міністрів, сайти Львівської міської ради, Київської міської державної адміністрації, кіберполіції та Служби спецзв'язку України.

Зазвичай SOC базуються на СПЗ системи безпеки інформації та SIEM, яка агрегує та корелює дані із системних каналів безпеки, мережевого каналу передачі даних та системи оцінювання вразливостей і складається з:

підсистеми управління, ризику та дотримання (Governance, Risk and Compliance, GRC);

підсистеми оцінки та моніторингу вебсайтів, прикладних програм і сканерів баз даних;

інструментів тестування проникнення;

підсистеми виявлення вторгнень (Intrusion Detection System, IDS);

підсистеми запобігання вторгненню (Intrusion prevention system, IPS);

підсистеми управління журналами;

аналітичної підсистеми поведінки в мережі та налагодження інтелектуальної безпеки Cyber threat;

підсистеми бездротового запобігання вторгненню;

брандмауерів, корпоративних антивірусних баз та уніфікованого управління загрозами (Unified Threat Management, UTM).

Основна увага приділяється управлінню повноваженнями користувачів і служб, сервісів директорій та іншим змінам конфігурації, а також забезпеченню аудиту та моніторингу журналів, реакцій на інциденти.

Загальна технологічна схема проходження подій, які призвели до порушення інформаційної безпеки із попередженням пріоритету події та її впливу на систему захисту за їх функціональними рівнями наведена на рис. 1.

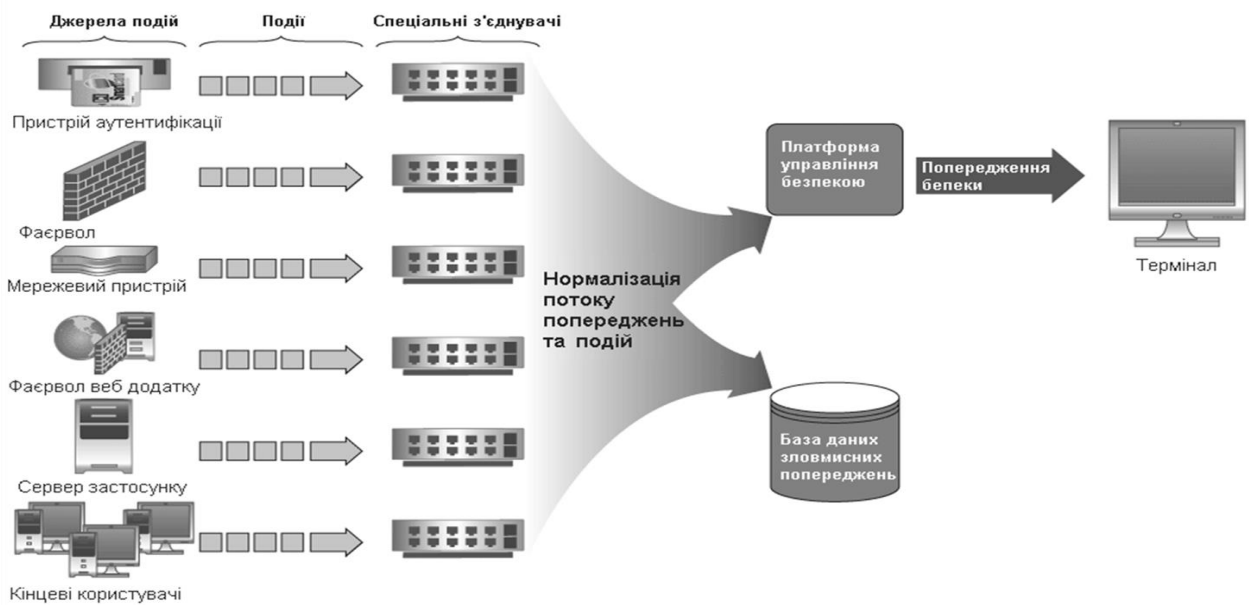


Рис. 1. Технологія SIEM, як основа програмних рішень SOC

Збір даних про події з боку порушників здійснюється від джерел різних типів. Приклади можливих джерел даних про події, які впливають на безпеку інформаційної системи наведено на рис. 1. *Джерела подій* представлені пристроями захисту входу в систему, записами у системних журналах та діями користувачів. Через зазначені джерела подій можливі вторгнення порушника (фізичної особи чи зловмисного програмного коду) в інформаційну систему. Джерела фіксують події, які дають змогу виявити ознаки порушення інформаційної безпеки та завдяки спеціальним з'єднувачам нормалізувати потік попереджень і подій. Наприклад, порушники намагаються ввійти в інформаційну систему в обхід стандартних процедур входу. На такі події технологія SIEM формує базу даних порушників (база даних зловмисних попереджень) для аналітиків безпеки та для моніторингу установи (організації) загалом.

Під час створення інформаційних систем нормативно-правовою базою [4]

передбачено виконання комплексу заходів щодо захисту інформації. Одним із таких заходів є розроблення моделі загроз і моделі порушника. Після аналізу потенційних загроз безпеці, використання системи SIEM та обраного способу захисту з'являється можливість щодо автоматичного використання зазначених моделей за допомогою моніторингу попереджень подій Як наслідок, система дасть змогу ідентифікувати порушників за встановленими сценаріями. Пропонується класифікувати таких порушників інформаційної безпеки на внутрішніх і зовнішніх.

Зовнішні порушники підрозділяються на дві категорії: категорія I (особи, які не мають права доступу до контрольованої зони інформаційної системи) і категорія II (особи, які мають право постійного або разового доступу до контрольованої зони інформаційної системи). До зовнішніх порушників категорії I відносяться колишні співробітники та сторонні особи, які діють в ініціативному порядку. До зовнішніх порушників категорії II відносяться представники злочинних організацій.

До *внутрішніх порушників* відносяться співробітники з різними правами доступу до компонентів системи, персонал, який не має легітимного доступу до компонентів системи, і особи зі сторонніх організацій, які мають прямий або непрямий доступ до компонентів інфраструктури.

Зважаючи на визначені загрози та розроблені моделі порушника розроблюються вимоги до системи захисту інформації в інформаційних системах МО України.

Під час дослідження були визначені завдання, структура та шляхи побудови системи захисту інформації в інформаційній інфраструктурі МО України на основі запропонованого концептуального програмного технологічного рішення SIEM.

Рекомендовані заходи, які визначають можливість упровадження системи захисту інформації в інформаційній інфраструктурі МО України слід вважати:

забезпечення побудови максимально деталізованих ланцюжків та схем взаємозв'язку між подіями;

визначення фізичного і логічного поділу даних за різними сховищами з поділом повноважень за доступом;

визначення достатньої кількості інтеграційних механізмів до зовнішніх систем інцидент-менеджменту, звітності та візуалізації для отримання даних;

забезпечення стабільної роботи унаслідок зростання навантаження в потоці подій, під час роботи великої кількості кореляційних правил та здійсненні ретроспективних пошуків і формування звітності.

Як правило, SIEM-система має архітектуру "агенти – сховище даних – сервер додатків", яка розгортається поверх захищеної інформаційної інфраструктури. Це дає підстави в SIEM-системі виділити три основні функціональні рівні в її побудові – збір, обробка та аналіз даних (рис. 2):

На першому рівні збір даних здійснюється від джерел різних типів. До таких належать: файлові сервери, сервери баз даних, Windows-сервери, міжмережеві екрани, робочі станції, системи протидії атакам (Intrusion Prevention Systems, IPS), антивірусні програми тощо.

На другому рівні здійснюється обробка даних про події безпеки, які зберігаються в репозиторію. Дані, що зберігаються в репозиторію видаються за шаблонними запитами, які вбудовані в аналітичний інструментарій системи. Запити можуть бути сформовані користувачем та виконуватися інтерактивно або в автоматичному фоновому режимі виконання програм.

На третьому рівні результатами обробки даних у SIEM-системі є звіти у стандартній чи довільній формі, оперативна (on-line) кореляція даних про події, а також попередження, що виробляються в режимі on-line і (або) передаються електронною поштою.

Реалізація зазначених функціональних рівнів SIEM-системи здійснюється на основі виконання комплексу різних механізмів функціонування, а саме серверів, робочих станцій, антивірусу тощо. У SIEM-системах першого покоління до таких механізмів, як правило, відносяться нормалізація, фільтрація, класифікація, агрегація, кореляція і пріоритезація подій, а також генерація звітів і попереджень. У SIEM-системах нового покоління до їх числа додані – аналіз подій, інцидентів та їх наслідків, а також процес підтримки прийняття рішень із його візуалізацією.

Розподіл зазначених механізмів за трьома рівнями ієрархії SIEM-системи наведено на рис. 2.

Рис. 2. Узагальнена ієрархічна модель SIEM-системи (за трьома рівнями)

З рис. 2 видно, що відносна величина складності обробки даних є пропорційна кількості подій. Тобто, зі зростанням кількості подій зменшується якість їх моніторингу, а саме, на *якість* моніторингу подій безпеки SIEM впливають правила нормалізації, способи налаштування джерел, пакети з правилами виявлення загроз, інструкції з активації джерел, описів правил детектування, рекомендації про реагування, у разі спрацювання правил. Це пояснюється застосуванням більшої кількості механізмів (інструментів) на кожному наступному (вищому) рівні обробки, що виокремлює найбільш значущі події, які достатні для проведення різних типів аналізу, візуалізації, прийняття рішення тощо.

На рис. 3 наведено підсистеми функціональної моделі SIEM, які відповідають трьом функціональним рівням: збору даних (охоплює підсистему збору даних, може охоплювати підсистему сховища), обробку даних (охоплює підсистему обробки) та аналізу даних (охоплює підсистеми аналізу, сховища та вигляду).

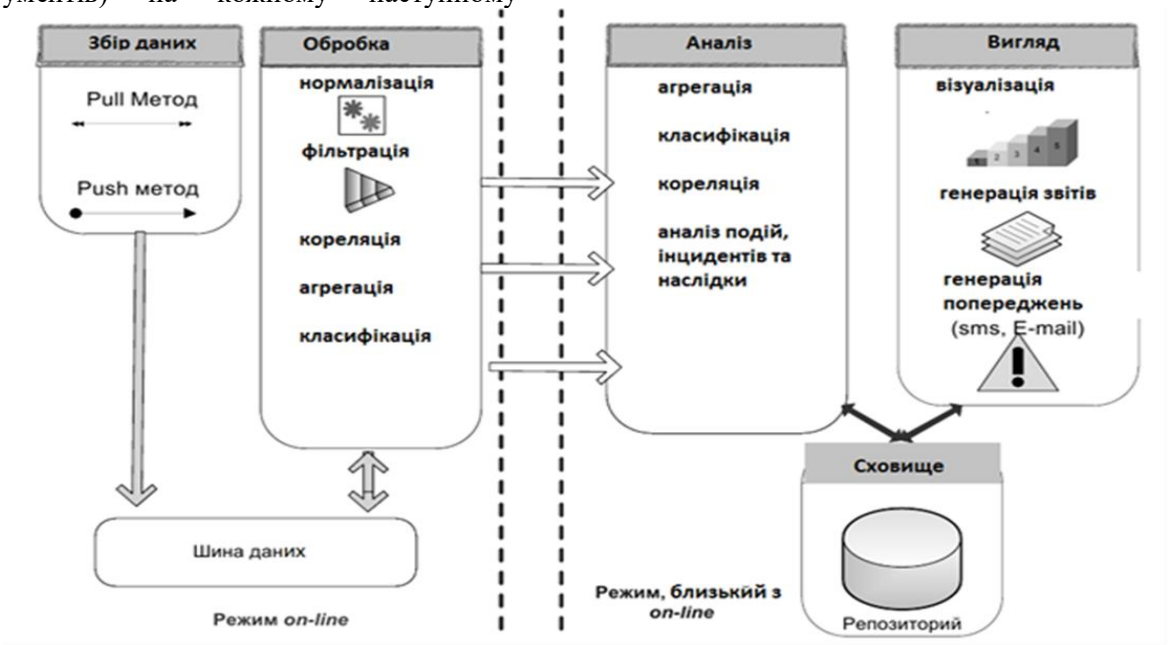


Рис. 3. Функціональна модель SIEM-системи (п'ять підсистем)

Як видно з рис. 3, в SIEM-системі можна виділити п'ять основних функціональних підсистем: збір даних, обробка, зберігання, аналіз, вигляд. До того ж перші дві функціонують у режимі online, інші – у близькому до нього. Дамо коротку характеристику цим підсистемам.

Підсистема збору даних. Для отримання інформації від джерел використовуються два основні методи: Push-(натисни) і Pull-(тягни). Суть методу Push полягає в тому, що джерело саме посилає дані записів своїх журналів подій в SIEM-систему. У методі Pull система сама здійснює процес отримання даних з журналів подій у SIEM-систему.

Підсистема обробки даних. Основні функції підсистеми полягають у зборі, видачі, накопиченні, збереженні та обробці великих

обсягів інформації. Збір інформації проводиться різного роду периферійними засобами, наприклад, через канали зв'язку за допомогою модемів, локальних та глобальних комп'ютерних мереж, різного роду датчиків тощо.

Підсистема аналізу даних. Призначена для організації моделювання даних, забезпечення процедур їх перетворення та поєднаного аналізу шляхом генералізації, агрегації, встановлення параметрів і обмежень за допомогою моделюючих функцій.

Підсистема зберігання даних – це сховище з програмно-апаратним рішенням з організації надійного зберігання інформаційних ресурсів та надання гарантованого доступу до неї споживачам. Ця підсистема може бути як частиною, так і основою підсистеми збору даних.

Підсистема вигляду. Візуалізація подій мережі призначена для консолідації і обробки інформації про роботу обладнання мережі. Перевага системи складається в формуванні візуальної картини стану роботи обладнання в режимі реального часу. Підсистема дає змогу:

реєстрації, редагування і перегляду подій, які надходять від різних об'єктів мережі;

формування, узгодження і обробки заявок на планові роботи в мережі;

централізованого зберігання переліку обладнання мережі;

доступу споживачів до головного і регіональних сховищ бази даних обладнання і подій у мережі;

візуалізації подій у мережі на електронних картах;

формування різноманітної статистики та звітності роботи обладнання;

настроювання і застосування ключових показників ефективності для моніторингу роботи обладнання мережі;

формування і зберігання звітів про події мережі, планових і аварійно-відбудовних роботах;

виводу інформації на екран монітору.

Пропонуються рекомендації щодо реалізації СПЗ управління подіями безпеки (SIEM) для функціонування єдиної інформаційної системи управління оборонними ресурсами DRMIS інформаційній інфраструктурі МО України:

1. Відповідальні особи за управління безпекою та управління ризиками мають визначити вимоги до програмно-технічного комплексу системи SIEM та форм звітності (визначення вимог має включати критерії для подальших етапів розгортання).

2. Проєкт реалізації СПЗ має включати рішення груп відповідальних за аудит, адміністрування, ідентифікацію, інформаційні технології, програмування.

3. Організація чи установа має надати опис топології розміщення мережі та системи, а також оцінені показники подій для подальшого вироблення рішення для конкретного варіанта розгортання системи.

4. Проєкт реалізації СПЗ має включати вимоги до поетапного розгортання та вдосконалення.

Типовим прикладом готового програмного продукту управління подіями безпеки є IBM TSIEM (Tivoli Security Information and Event Manager), який в області подання та зберігання подій використовує запатентовану методику W7 (Who, did What, When, Where, Where-from, Where to and on What). Відповідно, всі події трансформуються у єдиний формат, зрозумілий адміністраторам безпеки, аудиторам і управлінцям. Також, програмний продукт IBM TSIEM володіє розвиненими можливостями щодо формування звітів і моніторингу активності користувачів.

SIEM-система нового покоління [9] орієнтується на інфраструктуру сервісів, у якій обробка подій безпеки відрізняється інтелектуальністю, високою масштабованістю, багаторівністю і багатодоменністю. До того ж має бути реалізовано випереджаюче управління безпекою, а також надійний і стійкий збір даних про події.

Висновок. Отже, у статті було визначено роль і місце СПЗ управління подіями безпеки для функціонування єдиної інформаційної системи управління оборонними ресурсами DRMIS. Під час визначення програмної компоненти центру безпеки інформаційної інфраструктури та під час дослідження проблематики пошуку програмних рішень щодо створення SOC були надані рекомендації щодо реалізації СПЗ управління подіями безпеки з актуалізацією дослідження сучасних підходів за напрямом моніторингу та управління безпекою інформації. У результаті були досліджені рівні програмного компоненту системи захисту інформації в інформаційних системах, запропоноване технологічне рішення та шляхи побудови щодо впровадження системи захисту інформації в інформаційній інфраструктурі МО України.

Подальші дослідження слід присвятити аналізу програмно-технічної та організаційної складових SOC.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Information and Event Management (SIEM) Implementation / Miller, Harris, Harper та ін. New York: McGraw–Hill Companies, 2011. 465 с.
2. Kotenko I., Chechulin A. Common Framework for Attack Modeling and Security Evaluation in SIEM Systems // 2012 IEEE Intern. Conf. on Green Computing and Communications, Conf. on Internet of Things, and Conf. on Cyber, Physical and Social Computing, Besanson, France, Nov. 20-23, 2012 / Los Alamitos, California. IEEE Computer Society, 2012. P. 94–101.
3. Построение модели данных для системы моделирования сетевых атак на основе онтологического подхода/ И. В. Котенко, И. Б. Саенко, О. В. Полубелова, А. А. Чечулин. // Тр. СПИИРАН. 2013. № 26. С. 23–30.
4. Information and Event Management (SIEM) Implementation / Miller, Harris, Harper та ін. New York : McGraw–Hill Companies, 2011. 465 с.
5. Modeling modern network attacks and countermeasures using attack graphs / K. Miller, M. Chu, R. Lippmann та ін. // Annual Computer Security Applications Conference. 2009. С. 117–126.
6. Magic Quadrant for Security Information and Event Management / K. M. Kavanagh, T. Bussa // Gartner Reprint. 2018. URL: https://www.gartner.com/doc/reprints?id=1-4LC8PAW&ct=171130&st=sb (дата звернення: 19.02.2021).
7. Reviews for Security Information and Event Management (SIEM). 2018. URL: https://www.gartner.com/reviews/market/security-information-event-management/vendors (дата звернення: 19.02.2021).
8. Shenk J. ArcSight Logger Review. *A SANS Whitepaper*. 2009. URL: https://www.microfocus.com/en-us/products/siem-security-information-event-management/overview (дата звернення: 18.02.2021).
9. Тенденції розвитку спеціального програмного забезпечення технології SIEM / В. А. Федорієнко, О. С. Кульчицький та ін. // Збірник Наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. Київ, 2019. № 2 (66). С. 82–88.

Стаття надійшла до редакційної колегії 24.02.2021

Features of special software for ensuring secure events management of DRMIS system

Annotation

Carrying out criminal measures to interfere in the functioning of state information systems to block and leak information, lead to a revision and clarification of the basic principles and approaches to protecting the information infrastructure of the Ministry of Defense (MO) of Ukraine in cyber threats.

This article focuses on the study of the features of SDR information security management and event monitoring in the construction of the software component of the information protection system of the security center in a single information system for defense resources management DRMIS as part of the information infrastructure of the Ministry of Defense of Ukraine.

An event is a potential result of certain actions that, by influencing information or other components of an information system, may directly or indirectly cause data harm, as well as endanger the security of information resources of an object or subject of information activity.

The purpose of the article is to analyze the features of the security event management system of SIEM technology in the SOC to substantiate the recommendations for their implementation in the DRMIS system of the Ministry of Defense of Ukraine.

The first step in protecting the information infrastructure is the use of special software (SPZ) of the Information Security and Event Management (SIEM) system.

The second step is to consider this system as a software component of the Security Operation Center SOC, which is a fairly common solution for large organizations, businesses, government and defense agencies. The Security Center or SOC performs the functions of timely and rapid response to events in an attempt to affect the performance and integrity of the management system. Such steps are appropriate to ensure the functioning of the Unified Defense Resources Management Information System (DRMIS) of the Ministry of Defense of Ukraine.

Keywords: special SIEM software; Data Processing; cyberspace; informational security; information security events.

УДК 519.85 004.42 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/114-119

Бондарчук С. В. (0000-0003-0624-9782)
Галаган В. І., канд. військ. наук, доцент (0000-0001-9578-0895)
Рибидайло А. А., канд. техн. наук, ст. наук. співроб. (0000-0002-6156-469X)
Полішко С. В., канд. техн. наук, ст. наук. співроб. (0000-0002-2172-7611)

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

Пропозиції щодо класифікації тематичних груп термінів, які застосовуються в управлінні життєвим циклом інформаційних систем військового призначення

Резюме. У статті розглянуто термінологію та визначення щодо стандартів, які регламентують життєвий цикл інформаційних систем військового призначення. На основі проведеного аналізу надано пропозиції з визначення кількості та складу тематичних груп, які необхідно враховувати під час управління життєвим циклом інформаційних систем військового призначення, які розроблятимуться та впроваджуватимуться в діяльність Збройних Сил України.

Ключові слова: інформаційні системи військового призначення; модель життєвого циклу; класифікація тематичних груп; словник.

Постановка проблеми. Збройні Сили України на сьогодні знаходяться на етапі проведення оборонної реформи. Відповідно до положень розробленого та погодженого проєкту Стратегічного оборонного бюлетеня України [1], яким визначено перспективну модель Збройних Сил (ЗС) України зразка 2030 року за принципами та стандартами, прийнятими в державах – членах НАТО, ефективних, мобільних, оснащених сучасним озброєнням, військовою і спеціальною технікою сил оборони, здатних гарантовано забезпечити оборону держави та адекватно і гнучко реагувати на воєнні загрози національній безпеці України, раціонально використовувати при цьому наявний потенціал (спроможності) та ресурси держави.

Для досягнення поставлених завдань необхідною та обов'язковою умовою є автоматизація процесів управління ЗС України. Тому, одним із найбільш актуальних завдань під час оборонної реформи є створення та впровадження різноманітних інформаційних систем військового призначення.

Проблема розроблення та впровадження інформаційних систем військового призначення (далі – ІС ВП), окрім фінансових і політичних аспектів, має певні особливості, які стосуються функціонального призначення та умов їх експлуатації.

На теперішній час, у державі та ЗС України продовжуються спроби адаптації нормативної бази щодо створення інформаційних систем до вимог міжнародних стандартів ISO/IEC, якими користуються передові країни світу і передусім всі країни – члени НАТО.

Проведення процесів адаптації документації щодо створення, впровадження та супроводження ІС ВП часто призводить до складності або повної відсутності розуміння процесів, які проводяться під час даних етапів. Особливо це стосується класифікації термінів, що застосовуються в управлінні життєвим циклом ІС ВП.

Отже, приведення до єдиного розуміння термінології та визначень, які використовуються під часі створення, впровадження та супроводження ІС ВП ЗС України та країнами – членами НАТО є досить актуальним завданням.

Аналіз останніх досліджень і публікацій. Найбільш повно термінологія життєвого циклу інформаційних систем наведена у Національних стандартах України, які направлені на створення, впровадження та супроводження автоматизованих та інформаційних систем [2]. Указаний стандарт визначений як документ усталеної практики. Цей перелік національних стандартів України та словників для створення, впровадження та супроводження автоматизованих та інформаційних систем, а також інформація про умови доступу до них надається національним органом стандартизації – ДП "Українське агентство зі стандартизації" через Національний фонд нормативних документів [3]. Водночас, дані документи не мають розподілу термінології та визначень на

тематичні групи, що значно ускладнює роботу проєктних груп та розробників під час виконання процесів розроблення, впровадження та супроводження інформаційних систем.

У науково-дослідних установах ЗС України здійснюється перегляд та адаптація сучасних стандартів і доктринальних документів стосовно інформаційних технологій і впровадження їх у свою діяльність. Під час цього процесу доцільно дотримуватися чіткого та прозорого механізму моніторингу процесу опрацювання та впровадження стандартів НАТО із реалістичними та досяжними цілями на коротко- та середньострокову перспективу.

У розроблених і прийнятих до використання документах [4] здійснена спроба поєднання термінів у контексті життєвого циклу ІС ВП, але розподіл здійснено тільки на дві тематичні групи (основні та організаційні), що є зовсім недостатнім для ефективної роботи Замовника та Розробників інформаційних проєктів.

Зарубіжний досвід, зокрема вивчення стандартів країн – членів НАТО щодо інформаційних технологій [5–8] показує, що в цих документах визначаються тільки окремі військові терміни, які не мають логічного поєднання за тематичними групами або рубриками життєвого циклу інформаційних систем.

Метою статті є проведення детального аналізу стандартів, які регламентують життєвий цикл інформаційних систем та надання пропозицій з визначення кількості та складу тематичних груп, які необхідно враховувати під час управління життєвим циклом інформаційних систем військового призначення, які розроблятимуться та впроваджуватимуться в діяльність ЗС України.

Виклад основного матеріалу. Для повного та якісного визначення термінології та обґрунтування тематичних груп була розглянута та використана джерельна база керівних і доктринальних документів, загальні Національні стандарти України (ДСТУ), спеціальні Національні стандарти України (ДСТУ В-П) та іноземні видання, у яких не розглядаються тематичні групи [5–8].

Під *тематичною групою* в цій статті розуміється – певний набір термінів і визначень інформаційної сфери, які функціонально пов’язані з конкретними процесами життєвого циклу (розроблення, впровадження та супроводження) інформаційних систем.

За результатами дослідження та з урахуванням сучасного стану і перспектив розвитку ІС ВП, які використовуватимуться для потреб ЗС України [9], пропонується визначити класифікацію тематичних груп за категоріями процесів, які необхідно враховувати під час управління життєвим циклом ІС ВП:

1. Укладання угоди на придбання або розроблення.
2. Організаційне забезпечення проєкту.
3. Ведення проєкту.
4. Організація технічних процесів.
5. Реалізація програмних засобів.
6. Підтримання програмних засобів.
7. Менеджмент повторного застосування програмних засобів.
8. Заходи та процеси нижчого рівня.
9. Забезпечення технічного управління.

Цей розподіл на тематичні групи за категоріями процесів, які необхідно враховувати під час управління життєвим циклом ІС ВП був проведений за допомогою аналітичного програмного забезпечення.

Через значну кількістю керівних документів і термінів (визначень) [5–8, 10–12] для проведення їх обробки та аналізу було використано раніше апробовану сучасну систему бізнес-аналізу (*Business Discovery*) на базі програмного забезпечення ***QlikView***, яка дає змогу зменшити складність і вартість проведення аналізу вказаних документів.

Головною відмінною особливістю цієї аналітичної системи є широке використання асоціативного пошуку та обробка обчислень в оперативній пам’яті. Робота цієї аналітичної системи базується на асоціативних принципах побудови моделі, що використовує таблиці, які пов’язані за ключовими полями. Також, у процесі побудові моделі необхідно правильно побудувати первинну структуру даних, для чого необхідно враховувати основні вимоги, які висуває інструментарій: унікальність назв полів (у різних таблицях моделі може бути тільки одне поле з однаковою назвою); модель не може мати циклічних зв’язків. Зв’язки між таблицями моделі аналітична система будує за полями з однаковою назвою – ключовимb полям.

Побудову та роботу моделі можна розподілити на декілька етапів. На *початковому етапі*, проводиться аналіз змісту та тексту документів, які досліджуватимуться щодо процесів життєвого циклу ІС. У результаті визначаються терміни, поняття,

роз'яснення, які містяться у кожному документі та мають бути враховані під час формування та класифікації тематичних груп.

На *другому етапі*, кожний документ з текстової форми перетворюється у табличну. Для цього у табличному редакторі (наприклад: *Word, Excel*) готується попередня таблиця з назвами полів. У разі необхідності, залежно від змісту, у таблицю можуть додаватись додаткові поля без зміни структури та правил заповнення. Унаслідок таких дій отримуємо попередню таблицю готову до завантаження в аналітичну систему (наприклад, попередня таблиця перетворення документів ДСТУ ISO/IEC/IEEE 12207 та ДСТУ ISO/IEC/IEEE 15288 містить понад 1200 записів та 24 поля).

На *третьому етапі* проводиться завантаження попередньої таблиці, використовуючи вбудований інструментарій *Qlick View*. Для цього, дані з полів попередньої таблиці завантажуються в окремі внутрішні кінцеві таблиці, а система автоматично будує зв'язки між ними за визначеними раніше ключовими полями. Унаслідок проведених дій отримуємо ***асоціативну модель даних***, з декількох пов'язаних за ключовими полями внутрішніх кінцевих таблиць з даними. (наприклад, для наведеного вище прикладу модель містить шість внутрішніх кінцевих таблиць).

Результат роботи моделі. Після побудови моделі, відповідно до задуму, для наглядного представлення результатів дослідження здійснюється їх візуалізація, шляхом створення екранних форм.

Для прикладу, у табл. 1 наведено порівняння запропонованих тематичних груп (з категоріями процесів, що визначені документами [5–8, 10–12]), які необхідно враховувати під час управління життєвим циклом інформаційних систем військового призначення. Аналіз даних наведених у табл. 1 дає змогу визначення процентного співвідношення збігів запропонованих тематичних груп (рубрик), які необхідно враховувати під час управління життєвим циклом ІС ВП з аналогічною тематикою нормативних документів країн – членів НАТО.

Запропонована класифікація за трьома групами (1, 2, 4) співпадає повністю, що становить 33,3 % від загальної кількості груп. Шість груп (3, 5–9) співпадають лише частково, що складає 66,6 % від загальної кількості.

Таблиця 1

№	Термінологічний словник		Джерело ISO/IEC/IEEE, AAP	Примітки
	Тематична група (рубрика)	Категорії процесів		
1	Укладання угоди на придбання або розроблення	Процеси угоди (узгодження)	ISO/IEC/IEEE 15288 , ISO/IEC/IEEE 12207, AAP -48 NATO	Співпадає
2	Організаційне забезпечення проєкту	Процеси організаційного забезпечення проекту. Організаційні процеси, які сприяють реалізації проєктів	ISO/IEC/IEEE 15288 , ISO/IEC/IEEE 12207, AAP -48 NATO	Співпадає
3	Ведення проєкту	Проєктні процеси (Процеси проєкту)	ISO/IEC/IEEE 12207, AAP -48 NATO	Співпадає частково (відсутні в ISO/IEC/IEEE 15288)
4	Організація технічних процесів	Технічні процеси	ISO/IEC/IEEE 15288 , ISO/IEC/IEEE 12207, AAP -48 NATO	Співпадає
5	Реалізація програмних засобів	Процеси реалізації програмних засобів	ISO/IEC/IEEE 12207	Співпадає частково (відсутні в AAP -48, ISO/IEC/IEEE 15288)
6	Підтримання програмних засобів	Процеси підтримання програмних засобів	ISO/IEC/IEEE 12207	Співпадає частково (відсутні в AAP -48, ISO/IEC/IEEE 15288)
7	Повторне застосування програмних засобів	Процеси повторного застосування програмних засобів	ISO/IEC/IEEE 12207	Співпадає частково (відсутні в AAP -48, ISO/IEC/IEEE 15288)
8	Заходи та процеси нижчого рівня	Процеси нижчого рівня	ISO/IEC/IEEE 12207	Співпадає частково (відсутні в AAP -48, ISO/IEC/IEEE 15288)
9	Забезпечення технічного управління	Процеси технічного управління	ISO/IEC/IEEE 15288	Співпадає частково (відсутні в AAP -48, ISO/IEC/IEEE 12207)

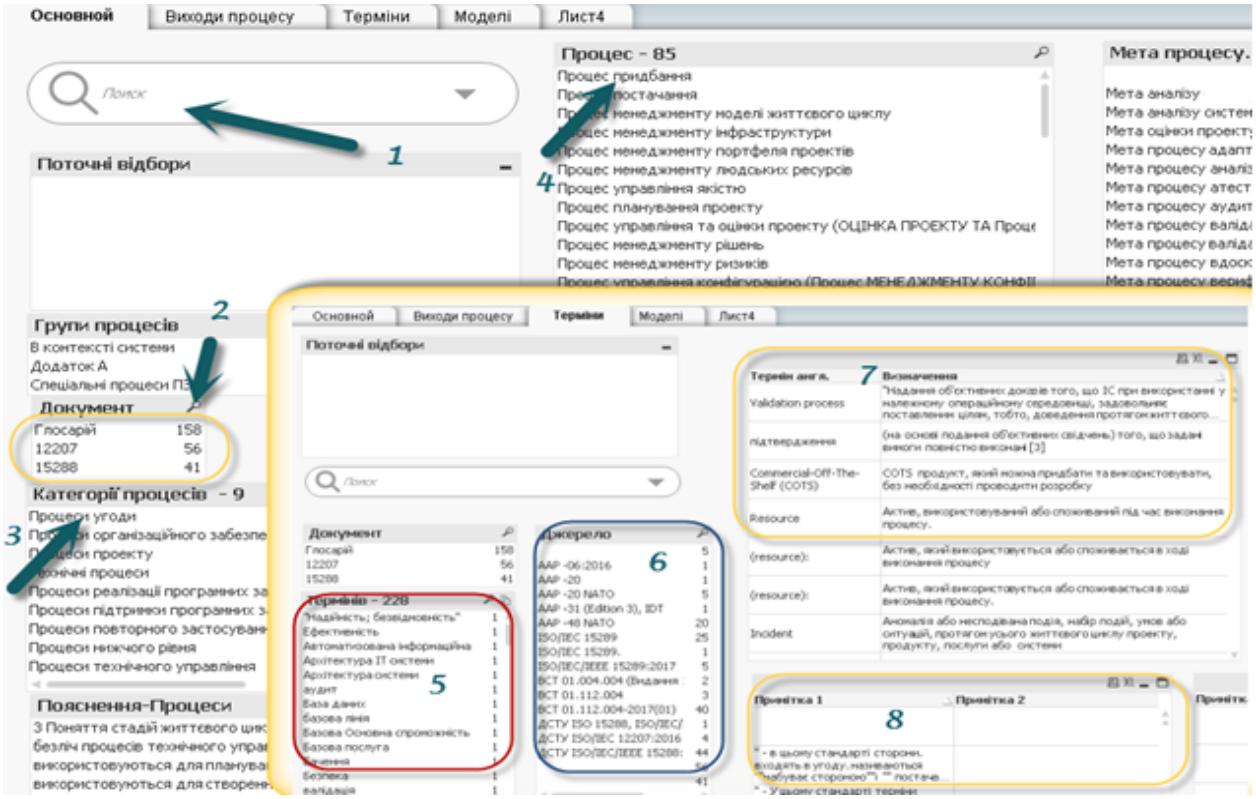


Рис. 1. Інтерфейс аналітичної системи щодо аналізу процесів, визначень та термінів

Для більш зручного проведення аналізу термінології було розроблено інтерфейс у вигляді аркуша з декількома закладками (рис. 1). На головному аркуші, для проведення дослідження, до поля пошуку (рис. 1, позначка 1) є можливість введення: терміну, визначення, коду чи будь-якої іншої інформації. Аналітична система проводить пошук за всіма наявними даними бази та виділяє: зеленим кольором прямо пов'язані документи, процеси, джерела; білим кольором частково пов'язані; сірим кольором не пов'язані.

Ще до початку проведення дослідження система аналізує наявну базу даних та показує кількість документів доступних для проведення аналізу, кількість термінів і визначень пов'язаних з пошуком, що виконується (рис. 1, позначка 2), загальну кількість категорій та процесів (рис. 1, позначки 3, 4). Знайдені за результатами пошуку терміни та визначення, відображення їх зв'язків з документами, джерелами, кількісні та якісні показники, через вбудовану систему відображення кольором виконуються та відображаються на закладці "Терміни" у вигляді списків і таблиць (рис. 1, позначки 5–8).

За допомогою створеного інструментарію були проаналізовані: документи, які необхідно враховувати під час управління життєвим циклом; виявлена класифікація тематичних за категоріями груп процесів; групи процесів за кожною встановленою категорією; процеси за кожною групою; кількість збігів з термінологією країн – членів НАТО.

Аналітична система має достатньо гнучкий та розвинутий інструментарій, який дає змогу змінювати інтерфейс під потреби дослідника, та додавати будь-яку кількість документів у вже існуючу базу і використовувати її як спільну базу знань.

До вказаної аналітичної моделі було завантажено близько трьох тисяч записів, серед яких було виявлено 9 категорій тематичних груп, 85 процесів та 228 термінів. З'ясовано, що ключовим визначенням стандартів стосовно життєвого циклу ІС ВП є процес (*process*), який позиціонується, як сукупність взаємопов'язаних або взаємодіючих видів діяльності, що супроводжується зміною властивостей елементів інформаційної системи.

Аналіз табл. 1 дає змогу дійти висновків, що запропонована класифікація тематичних груп співпадає (зокрема, частково) з класифікацією країн – членів НАТО на 85,7 %. Аналізуючи вказані джерела варто зазначити, що в них наведена лише частина існуючих тематичних груп і термінів щодо життєвого циклу ІС ВП.

Визначену класифікацію тематичних груп тематичних груп термінів, що застосовуються в управлінні життєвим циклом ІС ВП пропонується погодити із

зацікавленими структурними підрозділами ЗС України та використати під час написання Глосарія (військового стандарту) стосовно життєвого циклу ІС ВП.

Висновок. Визначена класифікація тематичних груп дасть змогу більш повного використання під час створення, впровадження та супроводження ІС ВП, ефективного проведення гармонізації структури термінологічного словника з урахуванням термінології країн – членів НАТО та міжнародних стандартів, для їх єдиного розуміння і поступового впровадження в діяльність ЗС України та освітній процес вищих військових навчальних закладів. Більш деталізований розгляд тематичних груп з їх характеристиками може бути темою окремого дослідження.

Надалі, перелік термінів за напрямом інформаційних технологій з урахуванням термінів країн – членів НАТО може бути використаний під час розроблення військового стандарту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про Стратегічний оборонний бюлетень України. URL: http://www.president. gov.ua/news/prezident-zatverdiv-strategichnij-oboronnij-byuleten-ukrayin-37309 (дата звернення: 15.08.2021).
2. Національні стандарти України для створення, впровадження та супроводження автоматизованих і інформаційних систем. URL: https://data.gov.ua/dataset/6a813896-efe9-4686-845f-534bff4be0b3 (дата звернення: 15.08.2021).
3. Національний фонд нормативних документів. URL: http://uas.org.ua/ua/natsionalniy-fond-normativnih-dokumentiv/struktura-natsionalnogo-fondu/ (дата звернення: 15.08.2021).
4. Перелік стандартів та керівних документів НАТО, вимоги яких впроваджено в національних нормативних документах. URL: https://www.mil.gov.ua/content/pdf/Standart_NATO_Dod.pdf. (дата звернення: 28.07.2021).
5. NATO – AAP-20 NATO PROGRAMME MANAGEMENT FRAMEWORK (NATO Life Cycle Model). URL: https://standards.globalspec.com/std/9970689/aap-20/ (дата звернення: 15.08.2021).
6. AAP-06. Edition 2020. NATO GLOSSARY OF TERMS AND. DEFINITIONS (ENGLISH AND FRENCH). GLOSSAIRE OTAN DE TERMES ET. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/Other_Pubs/aap6.pdf. (дата звернення: 15.08.2021).
7. NATO – AAP-48 NATO SYSTEM LIFE CYCLE STAGES AND PROCESSES. URL: https://tssodyp.ssb.gov.tr/genel/ReferansDokumanlar/AAP48%20NATO%20System%20Life%20Cycle%20Processes-Mart%202013.pdf. (дата звернення: 15.08.2021).
8. NATO – AAP-31(A) NATO GLOSSARY OF COMMUNICATION AND INFORMATION SYSTEMS TERMS AND DEFINITIONS. URL: https://isotranslations.com/resources/AAP-31-NATO%20GLOSSARY%20OF%20COMMUNICATION%20AND%20INFORMATION%20SYSTEM.pdf. (дата звернення: 15.08.2021).
9. Про затвердження Концепції інформатизації Міністерства оборони України : наказ Міністерства оборони України від 17.09.2014 р. № 650. URL: https://zakon.rada.gov.ua/rada/show/v0650322-14#Text/ (дата звернення: 15.08.2021).
10. ДСТУ ISO/IEC/IEEE 15288:2016 (ISO/IEC/IEEE 15288:2015, IDT) Інженерія систем і програмного забезпечення Процеси життєвого циклу систем. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=71827/ (дата звернення: 29.07.2021).
11. ДСТУ ISO/IEC/IEEE 12207:2018 (ISO/IEC/IEEE 12207:2017, IDT) Інженерія систем і програмного забезпечення. Процеси життєвого циклу програмного забезпечення. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=77957/ (дата звернення: 29.07.2021).
12. ДСТУ ISO/IEC/IEEE 24748-4:2018 (ISO/IEC/IEEE 24748-4:2016, IDT) Інженерія систем і програмних засобів. Керування життєвим циклом. Частина 4. Інженерне проектування систем. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=80148 (дата звернення: 15.08.2021).

Стаття надійшла до редакційної колегії 12.08.2021

Proposals for the classification of thematic groups of terms used in the management of the life cycle of military information systems

Annotation

Currently, the Armed Forces of Ukraine are at the stage of defense reform. Automation of the Armed Forces management processes is a necessary and obligatory condition for achieving the set goals. Therefore, one of the most urgent tasks in the course of defense reform is the creation and implementation of military information systems.

The problem of development and implementation of military information systems has certain features that relate to the functional purpose and conditions of their operation. Attempts by the Armed Forces of Ukraine to adapt the regulatory framework for the creation of information systems to the

requirements of international ISO / IEC standards used by NATO member states continue. The process of adapting documentation on the creation, implementation and maintenance of military information systems sometimes leads to difficulties in understanding the processes carried out during the intermediate stages. In particular, this applies to the classification of terms used in the management of the life cycle of military information systems.

The purpose of the article is to conduct a detailed analysis of the standards governing the life cycle of information systems and provide suggestions for determining the number and composition of thematic groups that need to be considered during its management.

The defined classification of thematic groups will allow for fuller use in the creation, implementation and maintenance of military information systems, and bringing the structure of the glossary to the terminology of NATO member countries and international standards, with a view to their common understanding and further implementation in the Armed Forces of Ukraine. process in higher military educational institutions.

Keywords: military information systems; life cycle model; classification of thematic groups; vocabulary.

УДК 395.424 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/120-127

Підгородецький М. М., канд. військ. наук[1] (0000-0003-4807-8635)
Куртсеітов Т. Л., д-р техн. наук, професор[1] (0000-0001-6478-6469)
Ясько В. А., канд. військ. наук, доцент[2] (0000-0002-4905-083X)
Ментус І. Е., канд. військ. наук, доцент[2] (0000-0003-2223-4775)

[1] – Національний університет оборони України імені Івана Черняховського, Київ;
[2] – Кам'янець-Подільський національний університет імені Івана Огієнка, Кам'янець-Подільський

Фізичне моделювання мін та інженерних боєприпасів, адекватних за показником теплової інерції

Резюме. Запропонований підхід щодо тестування та проведення експериментів із використанням фізичних моделей мін адекватних за показником теплової інерції дасть змогу розширити коло учасників, які зможуть брати участь у розробленні сучасних і вкрай необхідних засобів розвідки, пошуку, ідентифікації, знешкодження мін та вибухонебезпечних предметів.

Ключові слова: міна; модель міни; вибухонебезпечний предмет; показник теплової інерції; саморобні вибухові пристрої.

Постановка проблеми. Аналіз збройних протистоянь останніх десятиліть, які характеризуються широким застосуванням мін та вибухонебезпечних предметів (ВНП), у тому числі саморобних вибухових пристроїв (СВП), свідчить про значне зростання кількості втрат особового складу і військової техніки [1]. Щоденно по всьому світі внаслідок підриву на протипіхотних чи протитанкових мінах, або на вибухових пристроях, що діють аналогічним чином, я саме розтяжках, або внаслідок детонації вибухонебезпечних залишків війни (ВЗВ) гине та зазнає поранень щонайменше 10 осіб [2]. Як показує реальність сьогодення, жертвами мін стають некомбатанти, які підриваються на мінах, якими забруднена значна територія східних областей України. Так, за офіційною інформацією Управління Верховного комісара ООН з прав людини, упродовж усього періоду конфлікту на сході України з 14 квітня 2014 року по 30 квітня 2021 року загинуло та було поранено близько 10 000 осіб [3]. Оскільки терени окремих районів Донецької і Луганської областей є найбільш забрудненими мінами та боєприпасами в світі, то зменшення ризиків, які можуть виникати внаслідок підриву вибухонебезпечних предметів, до безпечного для життя і здоров'я населення рівня визначено однією із цілей протимінної діяльності в Україні.

Здійснюється ця діяльність на засадах державної підтримки, залучення національних та іноземних інвестицій і допомоги у сфері протимінної діяльності. Зазначене свідчить про зростання ролі виконання заходів розмінування, підвищення актуальності питань пошуку, виявлення, ідентифікації, знешкодження мін та ВНП як під час гуманітарного розмінування, так і під час ведення бойових дій.

Одним із найбільш складних проблемних питань сьогодення в галузі розмінування є забезпечення ефективного функціонування систем, засобів, комплексів пошуку, виявлення мін і ВНП (СВП).

Аналіз функціонування системи протимінної діяльності свідчить [4], що на етапі розроблення та адекватної практичної апробації зразків пошуку, виявлення, ідентифікації, знешкодження мін та вибухонебезпечних предметів виробники та розробники зустрічаються з проблемою використання натуральних мін. Оскільки розробники та виробники, не мають допуску, доступу та ліцензії на роботи із вибуховими речовинами та інженерними боєприпасами у зв'язку з правовими регуляторними обмеженнями щодо поводження із зазначеними речовинами та засобами [5–7], то вони відмовляються від подальшого дослідження та розроблень новітніх засобів.

Усе це свідчить про зниження конкурентності у сфері розроблення та створення новітніх засобів розвідки, пошуку мін та вибухонебезпечних предметів, що, відповідно, призводить до монополізації у сфері протимінної діяльності та зниження якості розроблених засобів.

На теперішній час фізичне моделювання мін та інженерних боєприпасів здійснюється лише з урахуванням таких показників, які характеризують геометричну подібність, вагу міни, матеріал корпусу, тип вибухової речовини. Принцип дії новітніх засобів розвідки, пошуку мін та вибухонебезпечних

предметів, які базуються на методі теплової індукції потребує урахування показників теплової інерції [8–11]. На сьогодні моделювання з урахуванням показника теплової інерції не проводиться. Тому фізичне моделювання мін та інженерних боєприпасів, адекватних за показником теплової інерції є актуальною науковою проблемою.

Аналіз останніх досліджень і публікацій. Проблематика створення та функціонування ефективної системи протимінної діяльності розкрита у працях іноземних та вітчизняних фахівців і вчених. Аналіз останніх досліджень і публікацій іноземних та вітчизняних фахівців і вчених [8–11] показав, що в них розглянуто проблематику створення та функціонування ефективної системи протимінної діяльності. У [8, 11] розглядаються напрями застосування безпілотної авіації для виконання завдань розмінування та дистанційного знищення ВНП. У матеріалах [9, 10] наведені результати теоретичних наукових досліджень, спрямованих на моделювання процесів та обґрунтування вимог до засобів пошуку та виявлення ВНП різними методами.

Проведений аналіз світових сучасних розробок та тенденцій у галузі розмінування показав, що найбільш перспективними та ефективними засобами розмінування є засоби із використанням новітніх технологій, таких як технологія автоматизованого виявлення мін із використанням багатоспектральної зйомки з безпілотних літальних апаратів, що узагальнена у так званому підході безконтактної дистанційної розвідки, виявлення та ідентифікація мін. Ще одним підходом є застосування інфрачервоної апаратури, яка реагує на різницю температур між міною та поверхнею місцевості. Зазначені технології, насамперед, націлені на збереженні життя та здоров'я людей під час проведення зазначених робіт.

Таким чином аналіз відомих доступних досліджень і публікацій дав змогу дійти висновку, що ці роботи спрямовані на дослідження та визначення фундаментальних засад функціонування зазначених систем тощо. Водночас, питання пов'язані з розвитком, розробленням та апробацією засобів розвідки, пошуку, виявлення, ідентифікації, знешкодження мін та ВНП із використанням фізичних моделей мін з урахуванням показників теплової інерції є новими не лише для України, але й для усього світу. Отже у відкритому друці така інформація майже не публікується.

Мета статті. Систематизувати світовий досвід, дослідити та теоретично обґрунтувати сучасні підходи до фізичного моделювання мін та інженерних боєприпасів, адекватних за показником теплової інерції.

Виклад основного матеріалу. Рівень вимог, які висуваються до якості зразків пошуку, ідентифікації, знешкодження мін і ВНП мають відповідати світовим і державним стандартам у сфері протимінної діяльності [7, 12]. Вирішення цього складного завдання практично неможливе без впровадження новітніх технологій та розробок.

Міна або інженерний боєприпас (ІБ) являє собою складну систему, яка характеризується фізичними, фізико-хімічними та конструктивними параметрами. Під моделлю міни слід розуміти деякий геоморфний об'єкт, більш простий в усіх відношеннях, окрім тих параметрів та ознак, вплив яких необхідно визначити та дослідити. Для того ж самого об'єкта моделювання можна обрати декілька моделей, які відрізняються одна від одної кількістю параметрів, які беруться до уваги. Модель, може відображати одночасно ознаки окремих частин об'єкта та його самого або ж тільки властивості об'єкта в цілому. Вибір моделі визначається вирішенням практичних завдань. За способами реалізації, моделі можуть бути знаковими та реальними. Знакові моделі являються математичним описом процесів. Реальні моделі якими являються фізичні об'єкти, поділяють на фізичні та математичні [13].

Фізичне моделювання мін та ІБ – це спосіб експериментального дослідження на моделях, що мають однакову фізичну природу з об'єктом моделювання (бойових мін), та являють собою деякий макет об'єкта, що вивчається. Для інженерів-конструкторів метод фізичного моделювання особливо привабливий, оскільки фізична природа моделі та об'єкта моделювання не змінюється і фізична модель відображає усі сторони процесу, який досліджується, що дає змогу уточнювати деякі деталі, які не мали відображення у вихідній знаковій моделі. Однак вказану модель можна реалізувати лише за наявності подібної моделі у об'єкта моделювання. До того ж під подібною слід розуміти модель, яка відрізняється лише змінами масштабу вхідних величин, тобто які можна охарактеризувати однаковими знаковими моделями в безрозмірній формі.

У процесі математичного опису процесу в зазначеній формі, параметри об'єднуються у

вигляді комплексів. Для подібних між собою процесів значення безрозмірних комплексів мають співпадати. Отже такі комплекси, або критерії подібності, визначають групу подібних об'єктів та число незалежних параметрів моделі (мір свободи) [13].

Критерії подібності дають змогу встановити аналогію між різними явищами, а можливість фізичного моделювання можна визначити за формулою

$$f = m - n \ , \qquad (1)$$

де f – число мір свободи;

m – кількість параметрів, критеріїв, які характеризують процес;

n – число критеріїв подібності, які слід підтримувати однаковими в процесі дослідження.

У разі якщо незалежні параметри відсутні $f < 0$, то немає свободи вибору параметрів моделі та об'єкт моделювання міна або ІБ немає собі подібного. У цьому разі фізичне моделювання неможливо здійснити. У разі, якщо результати протікання процесу практично не залежать від будь-якого критерію подібності, тоді можливе приблизне фізичне моделювання [13].

Теорія подібності є основою запропонованого фізичного моделювання, яка встановлює умови подібності моделі та оригіналу, дає змогу узагальнювати одиничні експерименти в безрозмірних критеріях і застосовувати знайдені залежності на подібні системи [13]. Фізичні моделі мають відтворювати увесь комплекс властивостей та явищ об'єкта [14]. Перевагами фізичного моделювання мін та ІБ перед іншими способами моделювання є наочність (фізична модель відтворює практично усі властивості оригіналу), можливе вивчення процесу без складання його математичного опису та можливість виробничого процесу в лабораторних умовах. Адекватність моделювання є однією з властивостей, яка показує ступінь відповідності моделі, тому реальному об'єкту для опису якого воно створюється і від якої залежить якість проведеного експерименту.

Основним принципом теорії подібності при фізичному моделюванні, передбачається не лише геометрична подібність моделі з об'єктом моделювання, але й подібність ваги, сил, матеріальних середовищ тощо [13–15]. Водночас фізична модель мін або ІБ має відповідати критеріям подібності основними з яких є: критерій гідродинамічної подібності (Критерій Рейнольдса); критерій теплової подібності (Критерій Нуссельта, Число Грасгофа, Критерій Пекле,), критерій теплопровідності (Фур'є, Біо), на основі яких визначають наскільки модель міни та ІБ подібна оригіналу [13–15].

Фізичне моделювання мін та ІБ починається з визначення відношення основних показників об'єкта моделювання, які характеризують геометричну подібність (ширину, висоту, діаметр, об'єм та інші), масу міни, матеріал корпусу, тип вибухової речовини тощо. Водночас для розроблення та тестування засобів пошуку, виявлення, ідентифікації, знешкодження мін та вибухонебезпечних предметів, що функціонують на різних фізичних принципах дії із використанням фізичних моделей мін, які створені з урахуванням лише зазначених характеристик мін, не достатньо (табл. 1) [16, 17].

Таблиця 1

Основні характеристики протитанкових мін

Характеристика	ТМ-62М	ТМ-62П3	ТМ-62Т	ТМ-62П2	ТМ-62П
Матеріал корпусу	метал	поліетилен	капронова тканина	пластмаса	пластмаса
Маса, кг	9,5-10	8,0-8,7	8,3-9,2	9,4-10	9,0-11.0
Маса вибухової речовини, кг (тротил)	7,0-7,5	6,5-7,2	7,0-7,9	6,5-7,0	7,6-8,0
Амонітом А-50	-	-	-	-	7,5
Амонітом А-80	-	-	-	-	6,6
Діаметр, мм	320	320	320	320	340

У фізичних моделях мін для імітації вибухових речовин використовуються різні інертні матеріали (дерево, гіпс, пісок, шлак, цементна суміш тощо), фізичні властивості яких не відповідали реальному об'єкту моделювання або ж їх відповідність не доводилась за відсутності необхідності, або ж потреби в цьому. А моделювання фізичних властивостей вибухових речовин у моделях мін завершувалась максимум моделюванням маси [16, 17], що зі свого боку унеможливлює їх використання для тестування новітніх засобів розвідки, пошуку мін та вибухонебезпечних предметів, які базуються на методі теплової індукції який потребує урахування показників теплової інерції [8–11].

Оскільки фізичне моделювання лише згідно із зазначеними параметрами не завжди

відповідає критерію теплової подібності Нуссельта, який характеризує інтенсивність конвективного теплообміну N_u та визначається за формулою [15]

$$N_u = kL/\lambda \ , \qquad (2)$$

де k – коефіцієнт тепловіддачі;

L – характеристичний розмір (об'єм);

λ – коефіцієнт теплопровідності.

Коефіцієнт тепловіддачі k характеризує інтенсивність тепловіддачі та дорівнює кількості теплоти, яка передана в одиницю часу через одиницю площі поверхні за температур 1К між поверхнею та середовищем-теплоносієм [15].

Густина потоку q тепла визначається за формулою

$$N_u = k \cdot S \cdot \Delta T \ , \qquad (3)$$

де S – площа поверхні теплообміну;

ΔT – різниця температур.

Сукупність властивостей матеріалу, пов'язаних із теплопровідністю і об'ємною теплоємністю в інженерному та науковому моделюванні теплопередачі називають тепловою інерцією. Показник теплової інерції I матеріалу визначається за формулою [15]

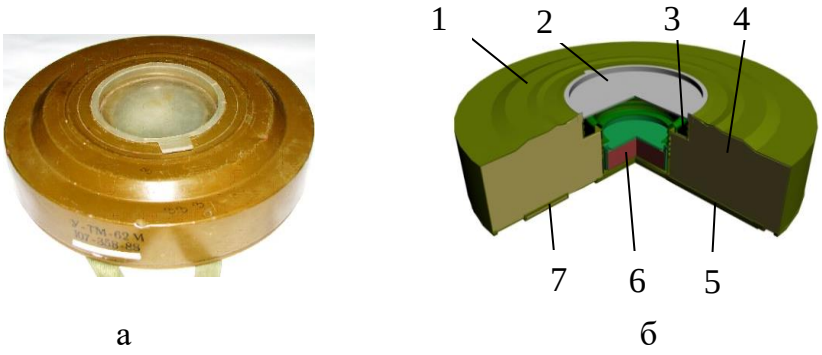
$$I = \sqrt{k \cdot \rho \cdot c} \ , \qquad (4)$$

де ρ – густина матеріалу;

c – питома теплоємність матеріалу.

Із стрімким розвитком новітніх технологій, які впроваджуються в процеси розвідки та пошуку мін на принципі багато- та гіперспектрального аналізу виникла необхідність визначення та перевірки нових показників у фізичних моделях мін та ІБ. Розрахунки та експерименти в стаціонарному стані й у різних середовищах можуть дати неточні результати з урахуванням того, що теплова інерція як міни, так і фізичної моделі міни є важливими. Особливо це стосується систем, які корелюються та чутливі до теплових показників об'єктів.

Існує декілька способів підтвердження адекватності фізичних моделей мін та ІБ. Як варіант для перевірки відповідності об'єкту моделювання та підтвердження адекватності фізичної моделі мін та ІБ у роботі запропоновано використовувати показники теплової інерції. Для виготовлення інженерних боєприпасів використовуються різні типи вибухових речовин. Відповідно їх фізичні характеристики різні. У відкритих джерелах відсутні відомості щодо теплофізичних характеристик ВР, окрім тротилу та аміачної селітри [16, 17], які вкрай важливі для проєктування та виготовлення фізичних моделей мін та ІБ (рис. 1).



а б

Рис. 1 **а** – вигляд фізичної моделі міни ТМ-62М в транспортному стані;
б – розріз міни ТМ-62М з пробкою: 1 – корпус; 2 – поліетиленова кришка; 3 – прокладка; 4 – заряд ВР; 5 – дно; 6 – ДД; 7 – провушина для закріплення ручки для перенесення.

Отже проведені у роботі розрахунки показників теплової інерції матеріалів (табл. 2) дають змогу надалі підбирати матеріали для замінника вибухових речовин, адекватного не лише за показником маси, а й за показником теплової інерції. Для прикладу, порівняно з тротилом, найкращими матеріалами для його фізичного моделювання будуть: піногіпс марки 846; пінобетон марки 916.

Водночас фізико-хімічні властивості зазначених матеріалів дають змогу варіювати із показником теплової інерції шляхом зміни пористості матеріалу.

Перевірка достовірності моделювання та оцінюванн ступеня відповідності моделі міни об'єкта моделювання (бойової міни або ІБ) у роботі проведено з використанням методів теорії подібності.

Таблиця 2

Визначенні значення показників теплової інерції основних матеріалів

Найменування матеріалу	**Густина, кг/м^3**	**Теплопровідність λ, Вт/(м^3·°С)**	**Питома теплоємність c, кДж/кг·°С**	**Теплова інерція матеріалу I, кДж/кг·°С**
Скловата	200	0,0372	0,67	2,232666567
Дерев'яні труски	200	0,07	2,7	6,14817046
Пінобетон марки 366	366	0,098	1,13	6,366383589
Цегла ізоляційна	500	0,1395	0,8	7,469939759
Піногіпс марки 641	641	0,142	0,88	8,949824579
Пінобетон марки 611	611	0,14	1,13	9,831591936
Піногіпс марки 740	740	0,169	0,88	10,49060532
Піногіпс марки 715	715	0,178	0,88	10,58289185
Дерево сосна	448	0,107	2,7	11,37660758
Цегла будівельна	800	0,23	0,8	12,13260071
Слюда	290	0,582	0,88	12,18714076
Піногіпс марки 850	850	0,199	0,88	12,20049179
Піногіпс марки 846	846	0,204	0,88	12,32371373
Тротил	**1500**	**0,43**	**0,328**	**14,54510227**
Пінобетон марки 916	916	0,217	1,13	14,9870731
Пінобетон марки 927	927	0,234	1,13	15,65622368
Резина	1200	0,163	1,38	16,42948569
Дерево дуб	800	0,207	1,75	17,02351315
Пісок сухий	1500	0,326	0,798	19,75403756
Земля суха	1500	0,1385	2,01	20,43471311
Гіпс	1650	0,291	0,88	20,55558318
Парафін	920	0,268	2,2	23,2901696
Портландцемент	1900	0,303	1,13	25,50570524
Шлакобетон	2150	0,43	0,88	28,5229732
Цукор пісок	1600	0,582	1,26	34,25364214
Крейда	2000	0,93	0,88	40,45738499
Глина вогнетривка	1845	1,04	1,09	45,73283284
Земля волога	1700	0,658	2,01	47,4171488
Асфальт	2110	0,698	2,09	55,48071917
Бетон	2300	1,28	1,13	57,67772534
Свинець	11400	34,9	0,129	226,5478757

Як відомо [14], рівнянням Фур'є описується задача теплопровідності для трьохвимірного тіла за відсутності в ньому джерел тепла.

$$\frac{\partial T}{\partial t} = \alpha\left(\frac{\partial^2 T}{\partial x^2} + \frac{\partial^2 T}{\partial y^2} + \frac{\partial^2 T}{\partial z^2}\right), \qquad (5)$$

де $T(\mathrm{x},\mathrm{y},\mathrm{z},\mathrm{t})$ – температура, t – час, *x, y, z* – просторові координати, $\alpha = \lambda/c\rho$.

Для визначення розв'язку конкретної задачі до рівняння Фур'є додаємо умови єдиності його розв'язку, які складаються з початкових та граничних умов. Початкова умова в задачі теплопровідності завжди має вигляд

$$T(\mathrm{x},\mathrm{y},\mathrm{z},0) = T_\Omega(x,y,z), (x,y,z) \in \Omega,$$

і означає, що в початковий момент задається значення температури в кожній точці області Ω, яку займає тіло (модель міни).

За відомими працями [14] у задачах з теплопровідністю граничні умови задаються, як правило, ***трьох типів***.

Перший – задається розподіл температури на поверхні тіла, як функція часу $\mathrm{T}(\mathrm{x},\mathrm{y},\mathrm{z},t)_{(\mathrm{x},\mathrm{y},\mathrm{z})\in S} = T_S(\mathrm{x},\mathrm{y},\mathrm{z},t), \quad t > 0$ умову такого типу досить рідко вдається реалізувати на практиці.

Другий – заданий тепловий потік в усіх точках поверхні тіла. Зважаючи на означення теплового потоку

$$(q = -\lambda \partial T/\partial \vec{n} = -\lambda\, \vec{n}\, grad\, T),$$

гранична умова може бути записаною у вигляді

$$\frac{\partial T}{\partial \vec{n}}\Big|_{(\mathrm{x},\mathrm{y},\mathrm{z})\in S} = -\frac{q_S(\mathrm{x},\mathrm{y},\mathrm{z},t)}{\lambda}, \qquad t > 0,$$

теж досить рідко зустрічається в конкретних фізичних задачах.

В інтересах дослідження та вирішення

задачі доцільно застосувати *третю* умову, оскільки відома температура зовнішнього по відношенню до тіла середовища T. Звернемося до закону Фур'є: тепловий потік між середовищем та тілом у деякій точці поверхні тіла пропорційний з коефіцієнтом пропорційності a, який називається коефіцієнтом теплообміну, різниці між температурою середовища та температурою поверхні моделі міни або ІБ в даній точці. На основі закону Фур'є гранична умова в цьому разі набуває вигляду

$$\left(\frac{\partial T}{\partial \vec{n}} + \frac{a}{\lambda}T\right)_{(\mathrm{x,y,z})\in S} = \frac{a}{\lambda}T_c(\mathrm{x,y,z},t), \qquad t > 0.$$

Зауважимо, що інколи задається змішана гранична умова, тобто на різних, доповнюючих одна одну частинах поверхні моделі міни задаються різні умови із зазначених вище.

За відомим підходом знаходження умов подібності в задачах теплопровідності, позначимо через $T_\mathrm{t}, T_l, \mathrm{x}_0, \mathrm{y}_0, \mathrm{z}_0, t_0$, відповідно характерні значення для розподілу температури в часі та в просторі, характерні значення довжин у трьох просторових вимірах та характерне значення часу. Тоді в безрозмірних змінних

$$T' = \frac{T}{T_\mathrm{t}}, T'' = \frac{T}{T_l}, t' = \frac{t}{t_\mathrm{t}},$$
$$x' = \frac{x}{x_0}, y' = \frac{y}{y_0}, z' = \frac{z}{z_0},$$

вираз Фур'є набуває вигляду

$$\frac{\partial T'}{\partial t'} = \frac{\alpha T_l t_0}{T_t}\left(\frac{1}{x_0^2}\frac{\partial^2 T''}{\partial x'^2} + \frac{1}{y_0^2}\frac{\partial^2 T''}{\partial y'^2} + \frac{1}{z_0^2}\frac{\partial^2 T''}{\partial z'^2}\right).$$

Для температури введено два характерних значення (T_t, T_l), а для геометричних розмірів – три ($\mathrm{x}_0, \mathrm{y}_0, \mathrm{z}_0$). Якщо для цих величин ввести по одному характерному значенню T_t та l, то зазначений вираз трансформується в

$$\frac{\partial T'}{\partial t'} = \frac{\alpha t_0}{l^2}\frac{T_l/T_0}{T_\mathrm{t}/T_0}\left(\frac{l^2}{x_0^2}\frac{\partial^2 T''}{\partial x'^2} + \frac{l^2}{y_0^2}\frac{\partial^2 T''}{\partial y'^2} + \frac{l^2}{z_0^2}\frac{\partial^2 T''}{\partial z'^2}\right).$$

Отже, єдиним степеневим комплексом, збереження свого значення яким залишає рівняння теплопровідності інваріантним, є

$$\frac{at_0}{l^2} \equiv Fo.$$

Визначений комплекс називається критерієм Фур'є [14].

Оскільки значення T_t, T_l, $\mathrm{x}_0, \mathrm{y}_0$, та z_0 задані параметрами натуральної міни та досліджуваного середовища, то відношення $\frac{T}{T_0}, \frac{T}{T_l}, \frac{x_0}{l}, \frac{y_0}{l}, \frac{z_0}{l}$ входять у розв'язок у вигляді параметричних критеріїв.

Початкова умова не додає критеріїв у вигляді степеневого комплексу і приводиться до безрозмірного вигляду. Єдине, що вона може додати – це характерне значення T, тобто параметричний критерій T_l/T_0. Аналогічний результат, але відносно параметричного критерію T_t/T_0, отримуємо привівши до безрозмірного вигляду граничні умови

$$\mathrm{T(x,y,z,}t)_{(\mathrm{x,y,z})\in S} = T_S(\mathrm{x,y,z},t),\ t > 0$$

або

$$\frac{\partial T}{\partial \vec{n}}\Big|_{(\mathrm{x,y,z})\in S} = -\frac{q_S(\mathrm{x,y,z},t)}{\lambda},\ t > 0.$$

Інша ситуація виникає з третьою умовою, яка в безрозмірному вигляді зводиться до виразу

$$\left[\left(\frac{\lambda}{al}\right) = \left(\frac{l}{x_0}\frac{\partial^2 T''}{\partial x'}\mathrm{n}_x + \frac{l}{y_0}\frac{\partial^2 T''}{\partial y'}\mathrm{n}_y + \frac{l}{z_0}\frac{\partial^2 T''}{\partial xz'}\mathrm{n}_z\right) + T''\right]_{(\mathrm{x,y,z})\in S} = \frac{T_t/T_0}{T_l/T_0}T_c(\mathrm{x,y},z,t).$$

Окрім параметричних критеріїв T_l/T_0, $T_t/T_0, x_0/l$, $\mathrm{y}_0/l, z_0/l$ зазначений вираз утримує комплексний критерій, відомий як Біо.

$$\frac{\lambda}{al} = Bi.$$

Отже, у дослідженні задача теплопровідності загалом характеризується двома критеріями подібності комплексного типу: Fo та Bi. Її загальний розязок може бути представлений у вигляді

$$\frac{T}{T_0} = f\left(\frac{x}{l}, \frac{y}{l}, \frac{z}{l}, \frac{t}{\mathrm{t}_0}, Fo, \mathrm{Bi}, P_1, P_2, \ldots\right),$$

що вказує на те, що температурні поля в геометрично подібних системах (міні та її фізичної моделі) будуть подібними, якщо для них критерії Фур'є та Біо зберігатимуть свої значення. Рівність параметричних критеріїв P_j для моделі міни та натури не є стуттєвою і пов'язує між собою лише характерні значення відповідних змінних [14, 15].

Так, згідно з [14], для подібності явищ достатньо вимагати лише незмінності критерію Біо. У подібних процесах однаковим значенням числа Фур'є відповідають подібні моменти часу.

Слід зазначити, що критерій Фур'є

встановлює певне співвідношення між швидкістю зміни умов зовнішнього середовища та швидкістю зміни розподілу температурного поля всередині фізичної моделі міни. Дійсно, характерне значення часу визначає темп зміни температури зовні моделі, в той час як комбінація параметрів відповідає за темп зміни внутрішньої температури. Отже, критерій Фур'є вказує на те, що в подібних явищах теплообміну темп зміни внутрішньої температури пропорційний швидкості зміни температури зовнішнього середовища.

Розглянувши критерій Біо, який об'єднує в собі один параметр, що характеризує геометричні розміри системи (моделі та бойової міни), та два фізичні параметри, що характеризують інтенсивність передачі тепла, між моделлю міни й середовищем та всередині моделі міни, являє собою міру відношення температурного перепаду в тілі до температурного тиску, який діє між моделлю міни та середовищем.

Оскільки просторові параметри моделі міни та натурного об'єкта (бойової міни) співпадають. Проведені в дослідженні розрахунки показників теплової інерції матеріалів (табл. 2) та порівняння їх показниками теплової інерції тротилу, що зі свого боку доводить відповідність моделі міни за критеріями подібності теплопровідності Фур'є та Біо, і вказує на адекватність проведеного моделювання.

Це означає, що всі процеси, які виникатимуть у моделі міни та в об'єкті моделювання за зазначених умов, подібні без будь-яких обмежень.

Висновки і перспективи подальших досліджень. Отже, в статті теоретично обґрунтовано шляхи визначення показника теплової інерції натурних (фізичних) моделей мін, розроблені практичні рекомендацій щодо натурного моделювання мін та вибухових речовин для забезпечення якості проведення експериментів.

Напрямами подальших досліджень слід вважати: розроблення сигнатур вибухових речовин та технічних вимог для створення фізичних моделей мін із урахуванням показника теплової інерції для забезпечення якості виготовлення, фізичних моделей мін та інженерних боєприпасів для проведення експериментів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Валецкий О. В. Минное оружие: вопросы минирования и разминирования. Москва : Крафт, 2009. 576 с.
2. Мосов С. П., Нероба В. Напрями застосування безпілотної авіації для виконання завдань розмінування: світовий досвід. *Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки*. Хмельницький, 2020. № 1 (79). С. 172–185. DOI: https://doi.org/10.32453/3.v79i1.105.
3. Втрати серед цивільних осіб в Україні, пов'язані з конфліктом. URL: https://ukraine.un.org/sites/default/files/2021-05/Conflict-related%20civilian%20casualties%20as%20of%2030%20April%202021%20%28rev%206%20May%202021%29%20UA.pdf. (дата звернення: 21.06.2021).
4. Протимінна діяльність в Україні потребує нових підходів – Мін ТОТ. URL: https://oldsite.mtot.gov.ua/ua/protyminna-diyalnist-v-ukrayini-potrebuye-novyh-pidhodiv (дата звернення: 23.06.2021).
5. Про протимінну діяльність в Україні : Закон України від 06.12.2018 р. № 2642-VIII. URL: https://zakon.rada.gov.ua/rada/show/2642-19#Text (дата звернення: 23.06.2021).
6. ДСТУ-П IMAS 07.30:2016 (IMAS 07.30:2016, IDT) Акредитація організацій та операцій із протимінної діяльності. URL: http://document.ua/akreditacija-organizacii-ta-operacii-iz-protiminnoyi-dijalnostd34578.html. (дата звернення: 23.06.2021).
7. ДСТУ-П IMAS 03.30:2016 (IMAS 03.30:2013, IDT) Керівництво з дослідження технологій, пов'язаних із протимінною діяльністю.
8. Бочаров О. А. Методы дистанционного обезвреживания взрывоопасных предметов. *Артиллерийское и стрелковое вооружение*. 2008. № 2. С. 34–37.
9. Коцюруба В. І. Моделювання процесу пошуку та виявлення вибухонебезпечних предметів радіолокаційним методом. *Сучасні інформаційні технології у сфері безпеки та оборони*. Київ, 2015. № 2 (23). С. 65–69.
10. Коцюруба В. І. Синтез структури пошукових пристроїв виявлення вибухонебезпечних предметів. *Збірник наукових праць ХНУПС*. Харків, 2016. № 4 (49). С. 97–99.
11. Безпілотна авіація у військовій справі: монографія / С. П. Мосов, М. В. Погорецький, С. М. Салій, О. В. Сєлюков, А. Л. Фещенко]. Київ : Інтерсервіс, 2019. 324 с.
12. ДСТУ-П IMAS 03.40:2016 (IMAS 03.40:2013, IDT) Випробування та оцінка обладнання, пов'язаного з протимінною діяльністю.
13. Левеншпиль О. Инженерное оформление химических процессов. Москва : Химия, 1969. 624 с.
14. Кепич Т. Ю. Основи теорії подібності та аналізу розмірностей та їх застосування в задачах механіки : навч. посібник / упорядники: Т. Ю. Кепич та О. Г. Куценко. Київ : КНУ імені Тараса Шевченка, 2004. 100 с.

15. Василенко С. М., Українець А. І , Олішевський В. В. Основи тепломасообміну : підручник. Київ : НУХТ, 2004. 250 с.
16. Про затвердження Керівництва з підривної (вибухової) справи у Міністерстві оборони України та Збройних Силах України : наказ МО України від 02.01.2013 р. № 1.
17. Про затвердження Керівництва з застосування інженерних боєприпасів у Міністерстві оборони України та Збройних Силах України : наказ МО України від 27.12.2010 р. № 700.

Стаття надійшла до редакційної колегії 02.07.2021

Physical modeling of mines and engineering ammunition, adequate in terms of thermal inertia

Annotation

Ensuring the implementation of state policy and the implementation of Ukraine's international obligations in the field of mine action involves taking measures to develop means of reconnaissance, search, identification, disposal of mines and explosives.

The products of many enterprises of the defense-industrial complex of Ukraine are means of search, identification, neutralization of mines and explosive objects. Domestic developers and manufacturers of these tools to maintain their position in a competitive market need to pay more attention to the development of their products, which are produced and developed in the shortest possible time. The level of quality, terms of development and acceptance for production directly depends on the term of practical approbation of samples.

At the same time, developers and manufacturers should use mines for adequate practical testing of samples of search, identification, disposal of mines and explosives, which is not always possible for developers and manufacturers who do not have access to work with explosives and engineering munitions in connection with legal regulatory restrictions on the handling of these substances and agents.

Therefore, testing and experimentation with samples of search and identification, is proposed to conduct using full-scale (physical) models of mines. In models of mines to replace explosives to use materials whose physical properties correspond as much as possible to natural. The adequacy of modeling is one of the properties that expresses the degree of conformity of the model to the real object for the description of which is created and on which the quality of the experiment depends.

The proposed approach testing and conducting experiments using physical models of mines will expand the range of participants who will be able to participate in the development of modern and much-needed means of reconnaissance, search, identification, disposal of mines and explosives.

Keywords: mine; mine model; explosive object; thermal inertia index; improvised explosive devices.

УДК 355.41:164(075) DOI: https://doi.org/10.33099/2304-2745/2021-2-72/128-134

Кривогуз Г. І., канд. військ. наук, доцент[1] (0000-0001-7009-7344)
Нагорнюк В. Ф., канд. військ. наук, доцент[1] (0000-0002-8850-5016)
Прима М. В.[2] (0000-0002-8363-1929)

[1] – Військова академія, Одеса;
[2] – Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Класифікація бойових документів логістичного забезпечення (по службах тилу) тактичної ланки: зміни і доповнення

Резюме. Розглянуто проблемні питання класифікації бойових документів логістичного забезпечення (по службах тилу) військової частини (підрозділу) і надано пропозиції щодо внесення змін і доповнень до відповідних нормативних документів. Запропоновано за ознакою функціонального призначення бойові документи логістичного забезпечення (по службах тилу) поділити на три класи (організаційно-розпорядчу, звітно-статистичну та первинно-облікову документацію). Визначено місце цих класів в основних процесах логістичного забезпечення.

Ключові слова: бойові документи; звітно-статистична документація; логістичне забезпечення; матеріально-технічні засоби; організаційно-розпорядча документація; первинно-облікова документація; служби тилу.

Постановка проблеми. Положення ДСТУ 2732:2004 [1] і Державного класифікатора управлінської документації (ДКУД) ДК 010-98 [2] не повністю враховані у класифікації бойових документів, зокрема логістичного забезпечення (по службах тилу) на тактичному рівні управління військами, які викладені у військових керівних деталізованих публікаціях (ВКДП) Збройних Сил (ЗС) України [4–11]. У ДКУД не згадуються уніфіковані форми документів (УФД) з управління військами, а в існуючій класифікації бойових документів логістичного забезпечення (по службах тилу) відсутні такі класи ДКУД: організаційно-розпорядча, первинно-облікова і звітно-статистична документація. Отже виникає необхідність внесення змін і доповнень стосовно вказаної класифікації у нормативні документи військової (у тому числі щодо логістичного забезпечення) і цивільної сфер управлінської діяльності.

Аналіз останніх досліджень і публікацій. У ДСТУ 2732:2004 [1] та його проєкті за 2017 рік подано перелік видів документів без зазначення ознак поділу документів на види. Відповідно до цього стандарту документи за формою фіксування інформації можуть бути текстовими, зображувальними, електронними. Водночас зображувальний документ залежно від поєднання способів відображення характеристик об’єкта матиме вигляд графічного, аудіовізуального документа, фотодокумента, кінодокумента, відеодокумента. У ВКДП [5, 8, 9, 11] класифікація бойових документів відрізняється від положень цього стандарту (наприклад, замість терміну “текстовий документ” використовується термін “текстуальний документ”, а графічні документи не віднесено до зображувальних документів). До того ж у цьому стандарті відсутні визначення видів бойових документів.

ДКУД [2] є номенклатурним переліком назв УФД з унікальними кодовими позначеннями і містить 15 класів, серед яких до класифікації бойових документів може бути застосовано організаційно-розпорядчу (код 02), первинно-облікову (код 03), звітно-статистичну (код 06), планову (код 07) і бухгалтерсько-облікову (код 18) документацію.

У новій редакції Класифікатора управлінської документації (КУД) [3] ключовими назвами УФД організаційно-розпорядчої документації є: статут, положення, договір, правила, інструкція, план, наказ, розпорядження, протокол. Переважна більшість перелічених назв УФД використовується в управлінській діяльності службових осіб служб тилу військових частин (підрозділів) на підставі нормативних документів [4–11] як у мирний час, так і в особливий період без зазначення ознаки їх класифікації.

Відповідно до Основних положень логістичного забезпечення ЗС України (далі – Основні положення) [4] документи, якими регламентуються основні положення щодо логістичного забезпечення ЗС України, складають систему керівних документів [4, 5, 9–11], побудовану у вигляді трирівневої

структури: перший (стратегічний), другий (оперативний) і третій (тактичний) рівень. Класифікація і назви бойових документів логістичного забезпечення (по службах тилу) військової частини (підрозділу), які будуть результатом застосування вказаної системи керівних документів, не визначені.

Керівні документи логістичного забезпечення ЗС України відповідно до Тимчасового порядку оформлення військових публікацій у ЗС України [5] є військовими публікаціями, які за способом розповсюдження поділяються на друковані та електронні. Зважаючи на тлумачення терміна "військові публікації", вони за способом позначення поділяються на дві групи [5]: керівні документи (спільні (міжвидові, міжвідомчі) публікації (СП) – доктрина, концепція тощо; військові керівні публікації (ВКП) – доктрина, концепція тощо; військові керівні деталізовані публікації (ВКДП) – настанови, керівництва, правила, положення, норми, порядки, інструкції тощо; бойові публікації (БП) – бойові статути, курси, переліки, каталоги тощо) і навчально-методичні матеріали (військові навчально-методичні публікації (ВП) – методики, підручники, посібники, рекомендації, інструкції, довідники, порадники, пам'ятки тощо; тренувальні навчально-методичні публікації (ТП) - збірники, програми тощо). Оскільки військові публікації встановлюють правила, загальні принципи чи характеристики різних видів діяльності або їх результатів, то відповідно до ДСТУ 2732:2004 [1] вони є нормативними документами, а бойові документи логістичного забезпечення (по службах тилу) є результатом застосування ВКДП, БП, ВП тощо, відповідно до яких первинно-облікові документи з логістичного забезпечення (по службах тилу) не віднесені до бойових документів.

Відповідно до проєкту Тимчасової настанови з логістичного забезпечення бойових дій військових частин (підрозділів) Сухопутних військ ЗС України (далі – Тимчасова настанова) [6] планування логістичного забезпечення бойових та інших дій на тактичному рівні проводиться за трьома етапами з розробленням документів з управління підрозділами військової частини (плануючих і виконавчих), звітно-інформаційних і довідкових документів. До того ж первинно-облікові документи з логістичного забезпечення (по службах тилу) не розглядаються як бойові документи.

Частини I і II Бойових статутів механізованих і танкових військ Сухопутних військ ЗС України (БС МТВ СВ ЗСУ) [7, 8] розкривають зміст управлінської діяльності посадових осіб військової частини (підрозділу) на тактичному рівні управління, у тому числі стосовно тилового, технічного та інших видів всебічного забезпечення бойових та інших дій. При цьому не використовуються такі назви УФД: "графік", "календарний план","директива". Бойові (оперативні) документи у Додатку 2 частини II БС МТВ СВ ЗС України [7] і Тимчасового порядку оформлення оперативних (бойових) документів (далі – Тимчасовий порядок) [9] поділяються на три групи (текстуальні, графічні, електронні) без зазначення ознаки їх класифікації. Такий поділ стосується і бойових документів логістичного забезпечення (по службах тилу) військової частини (підрозділу). Проте під час виконання службами тилу військової частини (підрозділу) завдань матеріального-технічного забезпечення бойових та інших дій застосовуються первинно-облікові документи, які не віднесені до бойових документів.

У Додатку 2 частини II БС МТВ СВ ЗС України [7] не наведено тлумачення терміну "електронний документ". Визначення цього терміну відповідно до ДСТУ 2732:2004 [1] відрізняється від визначення, наданого в Інструкції з діловодства та документування управлінської інформації в електронній формі в Міністерстві оборони України та Генеральному штабі ЗС України (далі – Інструкція з діловодства) [10]. Деякі з перелічених видів службових документів у цій Інструкції мають спільні з бойовими документами логістичного забезпечення ЗС України назви УФД. Інші ознаки класифікації службових документів, окрім способу фіксації та відтворення інформації, не зазначені.

Відповідно до частини II Настанови з оперативної роботи штабів [11] бойовими є документи, які регламентують порядок підготовки і ведення бою (бойових дій). Вони класифікуються за такими ознаками: за призначенням, за змістом, за формою. За призначенням бойові документи поділяються на: документи бойової готовності, документи бойового чергування, документи з управління військами. За змістом до документів з управління військами віднесені: планувальні, директивні, звітно-інформаційні, розрахунково-довідкові, особисті службових осіб. До того ж донесення по тилу є звітно-інформаційним документом. Особистими документами службових осіб є: робочі карти, кальки (оверлеї), довідки, формалізовані документи, документи кодованого зв'язку. За формою бойові документи можуть бути: текстуальні, графічні,

табличні, фотографічні, відео- та аудіоформату. Текстуальні бойові документи можуть бути відпрацьовані формалізовано або в довільній формі. У зазначеній класифікації відсутні електронні документи відповідно до Додатку 2 частини ІІ БС МТВ СВ ЗС України [7] і Тимчасового порядку [9] та не вказані первинно-облікові документи для оформлення основних процесів логістичного забезпечення (по службах тилу) бойових та інших дій відповідно до Інструкції з обліку військового майна у ЗС України [12] (далі – Інструкція з обліку) і Порядку списання військового майна у ЗС України [13] (далі – Порядок списання). До того ж первинно-облікові документи не вважаються бойовими.

Мета статті. Удосконалення класифікації бойових документів логістичного забезпечення (по службах тилу) тактичного рівня, визначення їх місця в основних процесах логістичного забезпечення бойових дій та надання пропозицій щодо внесення змін і доповнень до відповідних нормативних документів у цивільній і військовій сферах управлінської діяльності.

Виклад основного матеріалу. З огляду на аналіз положень ДСТУ 2732:2004 [1] та його проєкту за 2017 рік, у ВКДП [6–9, 11] пропонується внести відповідні зміни щодо визначення сутності графічних бойових документів як одного з видів зображувального елемента, замінити термін "текстуальний документ" на "текстовий документ", а також надати з урахуванням положень Інструкції з діловодства [10] тлумачення терміна "електронний документ".

У ДКУД [2] пропонується планову документацію (код 07) з урахуванням положень проєкту КУД [3] включити до складу організаційно-розпорядчої (код 02), а бухгалтерсько-облікову документацію (код 18) – до складу первинно-облікової документації (код 03).

Відповідно до ДКУД [2] у проєкті Тимчасової настанови [6] пропонується бойові документи з логістичного забезпечення бойових та інших дій військових частин (підрозділів) поділити на три класи: організаційно-розпорядчу (код 02), первинно-облікову (код 03), звітно-статистичну (код 06) документацію. Довідкові документи можуть бути віднесені до звітно-статистичної документації.

Зважаючи на назви УФД, які застосовуються в системі логістичного забезпечення ЗС України, перелік організаційно-розпорядчої документації проєкту КУД [3] бажано доповнити такими ключовими термінами: "графік", "доповідь", "пропозиції", "вказівки", "замисел", "рішення", "директива", "розпорядження", "попередні розпорядження", "робоча карта" тощо.

На підставі аналізу системи керівних документів, зазначеної в Основних положеннях [4], можуть бути виділені дві групи документів стосовно мирного часу, тобто, повсякденної життєдіяльності та особливого періоду стосовно застосування сил і засобів логістичного забезпечення. До *першої групи* можуть бути віднесені організаційно-розпорядчі, первинно-облікові та звітно-статистичні документи мирного часу [2, 4, 5, 10, 12, 13] і документи бойової підготовки, а до *другої групи* – документи бойової і мобілізаційної готовності, бойові (оперативні) документи [6–9, 11–13].

У Додатку 2 частини ІІ БС МТВ СВ ЗС України [8] і Тимчасовому порядку [9] основною ознакою поділу бойових документів пропонується вважати форму фіксування інформації. Відповідно до ДКУД [2] і проєкту КУД [3] за ознакою функціонального призначення бойові документи слід віднести до класів організаційно-розпорядчої, первинно-облікової і звітно-статистичної документації.

Заявки, звіти, донесення і довідки, зазначені в Інструкції з діловодства [10], можуть бути віднесені до класу звітно-статистичної документації (код 06), а облікові документи з питань логістичного забезпечення (по службах тилу) військових частин (підрозділів) – до класу первинно-облікової документації ДКУД (код 03).

Відповідно до ДСТУ 2732:2004 [1] та його проєкту за 2017 рік, а також ДКУД [2] і проєкту КУД [3] до частини ІІ Настанови з оперативної роботи штабів [11], окрім доповнення щодо терміну "електронний документ" та уточнення терміну "текстовий документ", пропонується документи з управління військами (у тому числі з управління логістичним забезпеченням (по службах тилу)) віднести до організаційно-розпорядчої (планувальні, директивні, робочі карти, кальки (оверлеї), формалізовані документи, документи кодованого зв'язку) і звітно-статистичної (звітно-інформаційні (у тому числі донесення з логістичного забезпечення), розрахунково-довідкові) документації.

Відповідно до ДКУД [2], проєкту Тимчасової настанови [6], Інструкції з обліку [12] і Порядку списання [13] на рис. 1 викладені

погляди на можливе місце в основних процесах системи логістичного забезпечення (по службах тилу) військової частини (підрозділу) трьох класів: організаційно-розпорядчої (ОРД), звітно-статистичної (ЗСД) і первинно-облікової документації (ПОД).

На підставі проєкту Тимчасової настанови [6] виділені такі основні процеси системи логістичного забезпечення (по службах тилу) військової частини (підрозділу): планування забезпечення озброєнням і військовою технікою (ОВТ), матеріально-технічними засобами (МтЗ), послугами (у тому числі визначення потреб та їх витребування); отримання; підвезення (подача); облік і зберігання; видавання; експлуатація (використання) і витрачання; технічне обслуговування, евакуація та відновлення (ремонт); списання та утилізація.

Зазначені процеси стосуються таких основних функціональних сфер логістичного забезпечення ЗС України [6]: забезпечення ОВТ, МтЗ та послугами; технічне обслуговування та відновлення (ремонт); переміщення та перевезення (транспортування). Функціональні сфери логістичного забезпечення ЗС України [6] щодо інфраструктурногозабезпечення, укладання контрактів і фінансування не розглядалися.

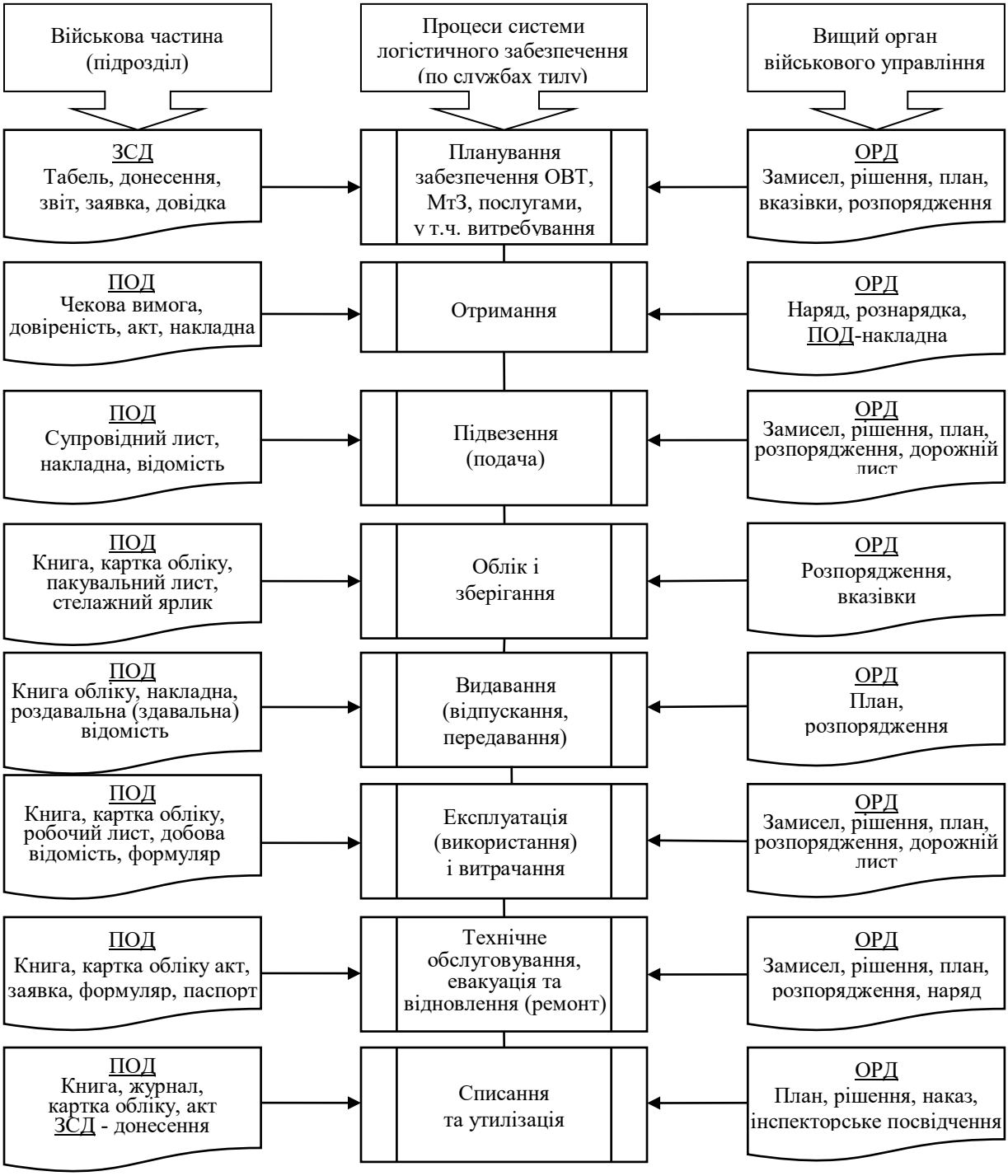


Рис. 1. Класифікація бойових документів за основними процесами системи логістичного забезпечення (по службах тилу) військової частини (підрозділу)

Відповідно до Інструкції з обліку [12] облікові документи залежно від їх призначення поділяються на первинні документи (накладні, вимоги, відомості, акти, атестати тощо), облікові регістри (книги, картки обліку військового майна, картки обліку військового майна особистого користування та інші носії (паперові, електронні) спеціального формату), документи допоміжного характеру (зведені та інші відомості, крім роздавальних (здавальних), листи, розкладки продуктів, стелажні ярлики тощо). У цій Інструкції доречно термін "облікові документи" замінити на термін "первинно-облікові документи" відповідно до ДКУД [2], а також внести доповнення щодо віднесення первинно-облікової документації (код 03) до бойових документів під час підготовки і ведення бойових та інших дій.

Таблиця 1

Пропозиції щодо класифікації первинно-облікових документів за основними процесами системи логістичного забезпечення (по службах тилу) військової частини (підрозділу)

Назва документа	Номер додатка згідно з	
	Інструкцією з обліку [12]	Порядком списання [13]
Первинні документи		
Довіреність	+	
Акт якісного (технічного) стану		1
Акт списання		3
Акт технічного стану військового майна	6	
Акт приймання-передачі військового майна	22	
Чекова вимога	34	
Накладна на видавання (здавання) військового майна у військовій частині	57	
Роздавальна (здавальна) відомість	58	
Акт зняття залишків	60	
Добова відомість наявності та руху продовольства	64	
Робочий лист агрегату	82	
Розкладка-накладна на видавання продуктів для приготування їжі	92	
Виробничий лист	94	
Акт виготовлення сумішей	101	
Акт списання природних втрат	+	
Інші	+	+
Облікові регістри		
Книга реєстрації облікових документів	1	
Книга обліку ремонту (обслуговування, обробки) ОВТ та іншого військового майна	15	
Картка обліку військового майна (некатегорійного)	21	
Картка обліку некомплектності	26	
Картка обліку військового майна (категорійного)	31	
Книга обліку наявності та руху військового майна (служба забезпечення)	46	
Книга обліку за номерами і закріплення ОВТ та іншого військового майна	47	
Книга обліку ОВТ та іншого військового майна за номерами і технічним станом	48	
Книга обліку роботи машин, витрати пального і масел	84	
Журнал обліку ведення бойових дій	+	
Інші	+	+
Документи допоміжного характеру		
Супровідний лист на перевезення військового майна	27	
Відомість складу і завантаженості автомобільної колони		
Стелажний (штабельний) ярлик	28	
Пакувальний лист на майно, яке спаковано у тару	37	
Інші	+	
Організаційно-розпорядчі документи		
Інспекторське посвідчення		2
Наряд на видавання (приймання) військового майна	4	
Рознарядка	5	
Наряд на ремонт (модернізацію, зберігання, дослідження технічного стану, виготовлення, обробку)	30	
Дорожній лист	82	
Інші	+	
Звітно-статистичні документи		
Донесення про наявність та рух військового майна	17	

Зважаючи на запропонованої класифікації бойових документів за основними процесами системи логістичного забезпечення (по службах тилу) військової частини (підрозділу), серед первинно-облікових документів відповідно до Інструкції з обліку [12] та Порядку списання [13] можуть бути додатково виділені організаційно-розпорядчі та звітно-статистичні документи (табл. 1).

Отже, до ДКУД [2] і проєкту КУД [3] пропонується внести доповнення назв УФД, які застосовуються в системі управління ЗС України (зокрема і в системі управління логістичним забезпеченням ЗС України) під час підготовки і ведення операцій (бойових дій), наприклад, замисел, директива, попереднє розпорядження, робоча карта. До ВКДП [6–9,1 1, 12] доречно внести відповідні зміни щодо визначення сутності графічних бойових документів і доповнення щодо сутності електронного документа та класифікації бойових документів з логістичного забезпечення бойових та інших дій військових частин (підрозділів) з кодуванням класів організаційно-розпорядчої (код 02), первинно-облікової (код 03) і звітно-статистичної (код 06) документації з урахуванням положень ДКУД [2] і проєкту КУД [3].

Висновки. Бойові документи логістичного забезпечення (по службах тилу) військової частини (підрозділу) можуть бути віднесені до трьох класів ДКУД: організаційно-розпорядча (замисел, рішення, план, розпорядження, наряд, рознарядка, дорожній лист, інспекторське посвідчення тощо), звітно-статистична (заявка, звіт, донесення, довідка тощо) і первинно-облікова (накладна, відомість, робочий лист, акт, картка обліку, книга обліку, журнал обліку ведення бойових дій тощо) документація особливого періоду. У ДКУД і ВКДП мають бути внесені відповідні зміни і доповнення щодо класифікації документів логістичного забезпечення (по службах тилу) військової частини (підрозділу) в особливий період, які конкретизовано у пропозиціях.

Перспективи подальших досліджень. Серед напрямів подальших досліджень можуть бути: використання штучного інтелекту під час планування та управління логістичним забезпеченням військових частин (підрозділів) видів ЗС України; введення єдиних електронних зразків первинно-облікових документів для автоматизованого документального оформлення процесів системи логістичного забезпечення (по службах тилу) військової частини, а також автоматизоване подання звітної документації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. ДСТУ 2732:2004. Діловодство й архівна справа. Терміни та визначення понять. [Чинний від 2005-07-01]. Вид. офіц. Київ : Держспоживстандарт України, 2005. IV. 26 с. URL: https://vn.court.gov.ua/userfiles/27_2732-2004(1).pdf (дата звернення: 10.07.2020).
2. Державний класифікатор України. Державний класифікатор управлінської документації ДК 010-98 [Чинний від 1999-06-01] : затв. наказом Держстандарту України від 31.12.1998 р. № 1024. URL: https://zakon.rada.gov.ua/rada/show/v1024217-98 (дата звернення: 10.07.2020).
3. Бойко В. Ф. Розроблення нової редакції Класифікатора управлінської інформації. *Архіви України*. 2016. С. 153–158. URL: http://nbuv.gov.ua/UJRN/ay_2016_5-6_13 (дата звернення: 10.07.2020).
4. Основні положення логістичного забезпечення Збройних Сил України : затв. наказом Міністерства оборони України від 11.10.2016 р. № 522.
5. ВКДП 1-00(03).01. Тимчасовий порядок оформлення військових публікацій у Збройних Силах України : затв. наказом Генерального штабу ЗС України від 26.12.2018 р. № 460.
6. Тимчасова настанова з логістичного забезпечення бойових дій військових частин (підрозділів) Сухопутних військ ЗС України. Проєкт. Одеса: НДЛ ВА, 2020. 308 с.
7. Бойовий статут механізованих і танкових військ Сухопутних військ Збройних Сил України. Частина І. Бригада. Київ : Командування СВ ЗСУ, 2016.
8. Бойовий статут механізованих і танкових військ Сухопутних військ Збройних Сил України. Частина ІІ. Батальйон, рота. Київ : Командування СВ ЗСУ, 2016.
9. Тимчасовий порядок оформлення оперативних (бойових) документів : затв. наказом Головнокомандувача Збройних Сил Українивід 11.09.2020 р. № 140.
10. Інструкція з діловодства та документування управлінської інформації в електронній формі в Міністерстві оборони України та Генеральному штабі Збройних Сил України : затв. наказом Міністерства оборони України від 26.07.2018 р. № 370. URL: http://www.mil.gov.ua/content/mou_orders/370_nm_2018_instruction.pdf. (дата звернення: 10.07.2020).
11. Настанова з оперативної роботи штабів, частина ІІ (військова частина). Київ : ГШ ЗС України, 2016. 78 с.
12. Інструкція з обліку військового майна у Збройних Силах України : затв. наказом Міністерства оборони України від 17.08.2017 р. № 440
13. Порядок списання військового майна у Збройних Силах України : затв. наказом Міністерства оборони України від 12.01.2015 № 17.

Стаття надійшла до редакційної колегії 14.07.2020

Classification of combat papers of logistic support (on services of rear) of the tactical level (changes and additions)

Annotation

Provisions of DSTU 2732: 2004 and the State Classification of Administrative Documentation (DKUD) DK 010-98 are not fully taken into account in the classification of combat documents of logistics (rear services) at the tactical level, which are set out in the military detailed guidelines (VKDP) of the Armed Forces of Ukraine).

The unified forms of documents (UFD) for the management of troops are not mentioned in the DKUD, and in the existing classification of combat documents of logistical support (for rear services) the following classes of DKUD are absent, namely:

Organizational and administrative;

Primary accounting and reporting and statistical documentation.

Therefore, there is a need to make changes and additions to this classification in the regulations of the military (including logistics) and civilian areas of management.

The purpose of the article is to improve the classification of combat documents of logistical support (rear services) of the tactical level, determine their place in the main processes of logistical support of combat operations and provide proposals for changes and additions to relevant regulations in civil and military spheres of management.

Based on the draft Interim Guidelines, the following main processes of the logistics system (for rear services) of the military unit (unit) are identified:

planning the provision of weapons and military equipment (weapons), logistics (MTZ), services (including identification of needs) and their requirements);

receiving;

transportation (supply);

accounting and storage; publication;

operation (use) and consumption;

maintenance, evacuation and restoration (repair);

write-off and disposal.

The DKUD and VKDP proposed appropriate changes and additions to the classification of logistics documents.

Keywords: combat documents; reporting and statistical documentation; logistics support; material and technical means; organizational and administrative documentation; primary accounting documentation; rear services.

УДК 355.5 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/135-138

Тіхонов Г. М., канд. військ. наук, ст. наук. співроб. (0000-0003-1941-744X)
Кірілкін Є. І., канд. військ. наук, доцент (0000-0003-1194-9580)
Шпанчук Г. В., канд. військ. наук, ст. наук. співроб. (0000-0001-5455-631X)
Баталюк В. І. (0000-0003-0041-3094)

Національний університет оборони України імені Івана Черняховського, Київ

Підходи до застосування грейдингу в системі управління персоналом Збройних Сил України

Резюме. На основі аналізу результатів досліджень, висвітлених у відкритих джерелах, обґрунтовані підходи до застосування грейдингу в системі управління персоналом Збройних Сил України.

Ключові слова: грейдинг; грейдинг посади; грейдинг працівника; грейдування посад; мотивація персоналу; оцінювання персоналу; система грейдів.

Постановка проблеми. В останні роки завданням кожної організаційної структури є успішне функціонування на ринку праці та отримання максимального прибутку від своєї діяльності. Великі комерційні структури, з метою підвищення ефективності їх роботи через матеріальне стимулювання, застосовують систему ефективного розрахунку зарплати співробітникам та активно впроваджують систему оцінювання посад – грейдинг.

Грейдинг (англ. *Grading*) – угруповання посад за певними підставами (визначення "ваги", класифікація) з метою побудови системи мотивації. Суть грейдингу – у зіставленні внутрішньої значущості посад для організації (внутрішня цінність) з цінністю цієї роботи на ринку (зовнішня цінність).

Аналіз посадових окладів військовослужбовців показує, що за навіть приблизно однаковому обсязі виконання функціональних обов'язків вони можуть відрізнятися між собою. Особливо бачиться ця різниця між посадовцями, які проходять військову службу у військах, органах військового управління, наукових установах та у ВНЗ. Ця різниця склалася ще з часів появи штабів, коли з'ясовувалося, що на посади призначалися найбільш наближені особи і яким встановлювався більш високий посадовий оклад. У Радянському Союзі ця градація залишилася.

На теперішній час серед військовослужбовців Збройних Сил України тривають подальші дискусії з питання зрівняння посадових окладів за військовими званнями.

Аналіз останніх досліджень і публікацій. Робота [1] присвячена актуальним питанням оцінювання персоналу та практичним аспектам застосування грейдингу під час формування заробітної плати, а також аналізу завдань управлінців щодо мотивації персоналу.

У роботі [2] зроблена спроба систематизації теоретичного і практичного досвіду застосування грейдування в системі оплати праці управлінського персоналу організацій.

У роботі [3] встановлено роль грейдингової системи оплати праці на підприємствах різних форм власності, а також здійснено її порівняння з іншими системами.

У роботі [4] наведені особливості мотивації персоналу в контексті оплати праці.

У роботі [5] викладені наукові основи роботи органів військового управління щодо організації кадрової роботи на основі широкого використання кадрового менеджменту кадровими органами усіх рівнів для ефективного використання кадрового потенціалу Збройних Сил України та забезпечення якісної укомплектованості військ (сил) особовим складом.

Водночас у наведених джерелах питання оцінювання персоналу у військових організаційних структурах залишається недостатньо вирішеним через наявні проблеми, пов'язані, як правило, із суб'єктивним підходом керівної особи та комісії, яка здійснює оцінювання, що не сприяє підвищенню мотивації до виконання службових обов'язків.

Метою статті є обґрунтування підходів до застосування грейдингу у системі управління персоналом Збройних Сил України.

Виклад основного матеріалу. Персонал є однією зі складових функціонування будь-якого суб'єкта управління. Зазвичай військові керівники акцентують увагу на навчально-бойових питаннях, проблемах виконання планів бойової підготовки та завдань військових

частин, не приділяючи достатньої уваги людському ресурсу, який має безперервний вплив на ефективність діяльності військової організаційної структури. Отже однією з головних функцій в управлінні персоналом є мотивація, яка сприяє залученню кожної особистості на тлі своїх досягнень внести найбільший вклад в успіх організації.

Термін "грейдинг" (від англ. *grade* – етап, ступінь, ранг) почав застосовуватися у колі HR-спеціалістів і прогресивних керівників західних компаній та нині став популярним в управлінні компаніями багатьох країн. Існує значна кількість поглядів на використання грейдингу. Один з головних – грейдинг це інструмент, який дає змогу навести порядок у системі оплати праці та дозволить організації сприяти:

досягненню цілей організації та реалізації її стратегії;

отриманню максимальної віддачі від інвестиції у персонал;

залученню та утриманню в організації найкращих спеціалістів.

Взагалі визначається, що грейдинг (система грейдів) – це процедура або система процедур щодо проведення оцінювання та ранжирування посад, унаслідок якої посади відповідно до їх цінності для організації розподіляються за грейдами.

Грейд – це група посад, що мають приблизно однакову цінність для організації. Кількість грейдів може варіюватися залежно від розміру організації. Кожному грейду відповідає свій оклад (або "вилка окладів"), який може періодично переглядатися, але система залишається незмінною.

Підходи до системи грейдів. Грейдинг розуміє оцінювання посадових позицій у практиці управління персоналом та використовується у двох основних значеннях:

1. Грейдинг посад або робіт – відбувається оцінювання посад та їх ранжирування незалежно від того, який працівник, яку з них обіймає. Грейд залежить від цінності та важливості цієї посади для організації.

2. Грейдинг робітників – оцінюються та розподіляються по грейдам працівники особисто. У сукупності враховується і цінність роботи, яку він виконує та цінність самого робітника, яка залежить від його ступеня кваліфікації, досвіду, майстерності та рівня розвитку його професійних компетенцій.

Визначається, що другий підхід виправданий в організаціях де функції, що виконують, завдання, обсяги самостійності та відповідальності й інші параметри залежать переважно не від посади, а від кваліфікації та спроможностей самого виконавця.

Порівняльний аналіз двох підходів наведено у табл. 1.

Таблиця 1

Порівняльний аналіз підходів до системи грейдів

Критерій	**Грейдинг посад (характерно для військових частин)**	**Грейдинг працівників (характерно для великих штабів, навчальних закладів)**
Що оцінюється	Цінність посади для організації	Цінність конкретного працівника для організації
Критерії оцінювання	Компенсаційні чинники, які мають відношення до самої посади: потрібний рівень кваліфікації; складність роботи; ступінь відповідальності; ступінь самостійності; вплив на виконання завдань і загальний результат виконання мети організаційної структури; аналітичне та інформаційне навантаження; умови виконання обов'язків тощо	Окремі компенсаційні чинники : ступінь відповідальності; вплив на кінцевий результат досягнення мети організаційної структури; критерії щодо оцінювання самого працівника та його кваліфікації; результативність роботи тощо
Організації для яких рекомендується даний підхід	Організації з фіксованими та (бажано) чітко визначеними функціями посад, де різні виконавці можуть обіймати аналогічні посади та виконувати аналогічні функції	Організації, де функції, що виконуються та завдання, залежать насамперед від самого виконавця. Зазвичай це організації в яких висуваються вимоги до рівня освіти та кваліфікації виконавців, їх творчих спроможностей
Результат	Збалансована мережа посадових окладів, побудована з урахуванням цінності посад для організації та їх можливій вартості на ринку праці	Розподіл персональних окладів виконавців за грейдами з урахуванням їх кваліфікації, професійного досвіду, компетенції та іноді за результатами виконання обов'язків

Підходи, наведені у табл. 1, мають орієнтовний характер. Проаналізувавши

табл. 1, можна констатувати, що грейдинг працівників більш широке поняття, ніж грейдинг посад.

Аналіз грейдингових систем (*HAY, Mercer, Towers* тощо) показує, що кожна з них має свій набір показників, за якими оцінюються посади, але ці показники частково перетинаються один з одним. Під час первинного грейдування рекомендується взяти будь-яку з існуючих систем за основу, хоча б для того, щоб потім порівняти рівень заробітної плати та рівень компенсацій з ринковими даними (які надаються в рамках будь-якої стандартної грейдингової структури) щодо визначення конкурентоспроможності цієї посади з аналогічними ринковими [6].

Застосування грейдування у системі мотивації дасть змогу отримати додаткові результати, а саме:

точне визначення паспорту посади (кваліфікація, необхідна для отримання посади, різноманітність та комплексність робіт);

рівень відповідальності особи;

самостійність і складність виконання завдань посади;

характер робіт, що визначають зміст службових обов'язків;

перегляд існуючих посадових обов'язків (наприклад, виявлення дублювання функцій);

адекватні та чітко прописані посадові інструкції;

отримання балансу між утриманням особового складу, виплачуючи їм конкурентоспроможну винагороду за працю, та збереженням ефективності своїх витрат на фонд оплати праці.

Також слід зазначити, що при всій своїй гнучкості, система грейдування не має зазнавати будь-яких змін, доповнень чи адаптації щонайменше півроку. Саме такий строк є достатнім для апробації, впровадження і виявлення слабких і сильних сторін подібних нововведень [7].

Сучасний порядок проходження служби у військових частинах показує, що існує декілька рівнів посад. Кожний військовослужбовець має проходити послідовно усі етапи. Призначення на вищу посаду відбувається на грунті проходження визначеного терміну та атестації. Перехід з рівня на рівень відбувається:

за рішенням керівника (наказом);

за результатами підвищення кваліфікації чи отримання вищого рівня освіти.

До того ж посадовий оклад військовослужбовця протягом достатньо тривалого часу може залишатися незмінним. По суті, в питаннях мотивації проходження служби необхідно запустити грейдову систему таким чином, щоб вона сприяла підвищенню виконання завдань військовою організаційною структурою за рахунок більшої мотивації особового складу на виконання завдань організації через особистий внесок персоналу.

Тому пропонується при призначенні на посаду військовослужбовцю визначати певний рівень грейду. Його перегляд проводити один раз на півроку та підвищувати у таких випадках:

за результатами атестування, збільшивши його тому, хто має найвищий рейтинг серед рівних за посадою військовослужбовців та включенням його в список на просування;

підвищення особистої кваліфікації внаслідок закінчення в даному періоді курсів за своєю спеціальністю;

участі у науковій роботі (особливо для науково-педагогічних працівників) шляхом написання наукових праць.

Визначення грейду через наказ, а не місячні премії дасть змогу більш об'єктивно оцінювати результати, створити систему змагання щодо ліпшого виконання посадових обов'язків.

Варіант покрокового введення грейдової системи наведений у табл. 2.

Необхідно зауважити, що існує деякий суб'єктивний фактор під час використання грейдингу. Цей метод дає змогу мотивувати особовий склад через підвищення особистого рівня забезпечення на якісне виконання завдань, що стоять перед військовою організаційною структурою. Застосування цього методу дасть змогу керівному складу, справедливо та водночас індивідуально, винагороджувати своїх підлеглих, враховуючи їх вміння, навички, виконання поставлених перед ними завдань, дотримання посадових обов'язків тощо. Грейдинг дає змогу організації мати прозору систему посадових окладів, яка буде зрозуміла усьому особовому складу. Адже відомо, що виконавець, відчуваючи причетність до організації та цілковиту поінформованість про внутрішні процеси, є більш відданим організації. Базуючись на цьому, доцільно надалі розглядати грейдинг саме як сучасну технологію системи мотивації у розрізі матеріальної складової.

Висновки. Отже, грейдування є сучасною технологією матеріальної мотивації персоналу. На сьогодні система грейдів є однією з найбільш прогресивних систем нарахування посадових окладів. Упроваджуючи та використовуючи систему грейдів, кожна військова організаційна структура має змогу не лише удосконалити систему мотивації, а й поліпшити систему управління персоналом заголом.

Таблиця 2

Варіант покрокового введення грейдової системи

Кроки	Заходи
1	Збір даних для оцінювання персоналу: положення про атестацію, особисті справи, досягнені результати, соціологічні анкети, інформація про курси підвищення кваліфікації, психологічні тести
2	Проведення співбесіди: можливості вирішення завдань та ситуацій у сфері виконання обов'язків та суміжних напрямів діяльності
3	Занесення індивідуальних результатів оцінювання персоналу до особистих справ для ведення звітності, визначення рейтингу та можливості виконання обов'язків
4	Прийняття рішення стосовно кожного претендента (просування службовими сходами, порядок підвищення кваліфікації, скорочення, переведення на іншу посаду тощо) щодо рівня грейду
5	Видання наказу з призначення грейдів (раз на півроку або на рік)

Перспективами подальшого дослідження та розвитку грейдування є розроблення й адаптація системи грейдів для більшості військових організаційних структур Збройних Сил України, які націлені на те, щоб відповідати вимогам стандартів НАТО з питань управління персоналом. Напрями подальшого дослідження полягають в обґрунтуванні механізму введення грейдингу у систему матеріального заохочення персоналу у Збройних Силах України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Яшкіна Н. В. Грейдинг як сучасний метод оцінювання ефективності праці персоналу. DOI: https://doi.org/10.32782/2524-0072/2018-17-61
2. Чуланова О. Л. Грейдинг как технология привлечения и удержания высококвалифицированных управленческих кадров. *Науковедение*. 2014. Вып. 5 (24). С. 1–14.
3. Кропивницький Р. С. Система грейдів як інноваційний підхід щодо державного управління науковими установами. Інвестиції: практика та досвід. № 13/2018. С. 118–124.
4. Швець В. Я., Іванова М. І., Саннікова С. Ф. Особливості мотивації персоналу в контексті оплати праці. Причорноморські економічні студії. 2017. № 13–1. С. 219–223.
5. Управління персоналом у Збройних Силах України : підручник / колектив авторів. Київ : НУОУ ім. Івана Черняховського, 2017. 404 с.
6. Савочкин Д. Формирование грейдинговой сетки компании. *Управление персоналом – Украина*. 2012. № 10 (229). С. 29–31.
7. Ковтун І. Є. Аналіз системи управління персоналом підприємства та розробка заходів щодо її удосконалення. *Молодий вчений*. 2016. № 6 (33). С. 46–50.

Стаття надійшла до редакційної колегії 01.09.2021

Approaches to the application of grading in the personnel management system of the Armed Forces of Ukraine

Annotation

In recent years, the task of each organizational structure is to function successfully in the labor market and get the maximum profit from its activities. Large commercial structures, in order to increase the efficiency of their work through material incentives, apply a system of effective calculation of salaries to employees and actively implement a system of job evaluation – grading.

Grading is a grouping of positions on certain grounds (definition of "weight", classification) in order to build a system of motivation. The essence of grading is in comparing the internal significance of positions for the organization (internal value) with the value of this work in the market (external value).

A grade is a group of positions that have about the same value for an organization.

Based on the analysis of the results of research covered in open sources, the approaches to the application of grading in the personnel management system of the Armed Forces of Ukraine are substantiated.

Personnel are one of the components of the functioning of any management entity. Therefore, one of the main functions in personnel management is motivation, which helps to attract each individual against the background of their achievements to make the greatest contribution to the success of the organization.

Approaches to the grading system. Grading understands the evaluation of job positions in the practice of personnel management and is used in two main meanings:

1. Grading of positions or works – there is an assessment of positions and their ranking, regardless of which employee holds each of them.

2. Grading of workers – workers are evaluated and distributed on grades personally.

The use of grading in the motivation system will allow to obtain additional results, namely:

precise definition of the position passport; the level of responsibility of the person; independence and complexity of the tasks; the nature of the work that determines the content of official duties; review of existing job responsibilities; adequate and clearly defined job descriptions; obtaining a balance between the retention of personnel, paying them competitive remuneration for work.

Keywords: grading; position grading; employee grading; grading of posts; motivation of staff, staff assessment; grade system.

УДК 34.06:007 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/139-145

Шопіна І. М., д-р юрид. наук[1] (0000-0003-3334-7548)
Котляренко О. П. канд. юрид. наук[2] (0000-0001-8776-2515)

[1] – Львівський державний університет внутрішніх справ, Львів;
[2] – Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Проблеми правового та організаційного забезпечення розвитку інформаційної культури військовослужбовців Збройних Сил України

Резюме. Розглянуто актуальні проблеми, пов'язані з розвитком інформаційної культури військовослужбовців у сучасних умовах, визначено правові та організаційні умови їх подолання.

Ключові слова: інформаційна культура; інформаційна безпека; військовослужбовці; Збройні Сили України; інформаційні війни; інформаційно-психологічні операції; інформаційні впливи.

Постановка проблеми. Важливість підвищення інформаційної культури військовослужбовців у сучасних умовах пояснюється зростанням значущості інформаційної складової збройних конфліктів, активним використанням різноманітними суб'єктами засобів інформаційного впливу для досягнення військових і невійськових цілей. У світовій практиці є приклади тотального зниження боєздатності урядових військових формувань за допомогою влучного застосування інформаційних засобів: так, в Афганістані у 2021 році завдяки руху "Талібан", у тому числі, активному використанню соціальних мереж та власних інформаційних ресурсів, залученню відомих блогерів для пропагандистської діяльності, вдалося практично без спротиву встановити контроль над більшістю території держави. Цьому передувала активна багатолітня підготовка: ще у 2012 році представник "Талібану" К. Ю. Ахмаді заявляв, що перемога у медіавійні означає перемогу більш ніж наполовину, і що найбільш важливим у війні є завоювання сердець та умів послідовників [1]. Примітно, що ця фраза належить до арсеналу структур цивільно-військового співробітництва (CIMIC), які вели активну діяльність в Афганістані, тобто можна констатувати, що таліби успішно засвоїли базові постулати інформаційно-психологічних операцій. Отже, свідомість та світогляд кожного військовослужбовця завжди можуть бути використані противником для досягнення власних цілей, що потребує більш детального розгляду проблем інформаційної культури як конструкту, що забезпечує стійкість до більшості деструктивних інформаційних впливів.

Аналіз останніх досліджень і публікацій. Проблеми інформаційної культури розглядалися у роботах [2, 4], у яких загалом феномен інформаційної культури розглядається як засіб протидії негативним інформаційним впливам та елемент інформаційної безпеки людини, суспільства, держави. У [3, 5, 6] досліджувались тенденції розвитку Збройних Сил України протягом останніх двох десятиліть, що свідчить про зростання ролі інформаційної культури в організації функціонування цього військового формування та міжнародних операціях із підтримання миру і безпеки. Водночас, попри вагомий внесок учених у дослідження, зокрема це стосується ролі інформаційної культури в організації функціонування військових формувань, потребує проведення ґрунтовних наукових досліджень визначення основних правових та організаційних проблем у сфері забезпечення належного рівня інформаційної культури військовослужбовців Збройних Сил України.

Мета статті – визначити основні правові та організаційні проблеми у сфері забезпечення належного рівня інформаційної культури військовослужбовців Збройних Сил України, а також створення правового підґрунтя, що охопить низку нормативних і інтерпретаційних актів, якими визначатимуться принципи, суб'єкти та форми підвищення рівня інформаційної культури рядового та командного складу на ціннісному, світоглядному та діяльнісному рівнях.

Виклад основного матеріалу. Питання важливості інформаційної складової професійної компетентності військовослужбовців обумовлені вимогами

низки нормативно-правових актів, серед яких:

Закон України "Про національну безпеку України", у ч. 4 ст. 3 якого визначено, що державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, кібербезпеки України тощо [7];

Закон України "Про основні засади забезпечення кібербезпеки України", у ч. 1 ст. 10 якого закріплено, що державно-приватна взаємодія у сфері кібербезпеки здійснюється у тому числі шляхом підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проєктів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту [8];

Закон України "Про оборону України", ч. 3 ст. 11 якого визначає, що Генеральний штаб Збройних Сил України бере участь в організації використання та контролю за повітряним, водним і інформаційним простором держави та здійснює його в особливий період [9];

Стратегія воєнної безпеки України, якою в якості одного із завдань визначено упровадження сучасних інформаційних та космічних технологій, автоматизація управлінських процесів і діяльності в силах оборони України з відповідним рівнем захищеності інформації, що обробляється [10];

Стратегія національної безпеки України, у п. 60 якої закріплено, що Україна зміцнить бойовий потенціал Збройних Сил України, інших органів сил оборони шляхом трансформації професійної культури на основі доктринальних підходів і принципів командування й контролю, підготовки, освіти НАТО; удосконалення та розвитку на основі сучасних технологій систем управління, телекомунікацій, розвідки, логістики [11];

Доктрина зі стратегічних комунікацій, затверджена Головнокомандувачем Збройних Сил України 12 жовтня 2020 року, згідно з п. 3.1.1 якої командири та фахівці зі стратегічних комунікацій для досягнення переваги в інформаційному середовищі мають здійснювати його аналіз з метою постійного підтримання повної обізнаності щодо кількісних і якісних характеристик як окремих елементів інформаційного середовища, так і їх сукупності та взаємодії задля своєчасного виявлення змін у цьому стані для вживання відповідних заходів з коригування діяльності підрозділів та установ Збройних Сил України в інформаційному просторі [12].

Положення наведених, а також інших правових актів у досліджуваній сфері свідчать, що інформаційна культура військовослужбовців у сучасних умовах є невід'ємним елементом комплексу їх професійно важливих знань, вмінь та навичок.

У наукових дослідженнях з інформаційного права феномен інформаційної культури розглядають на трьох рівнях. Загальнодержавний рівень інформаційної культури обумовлює наявність відповідного підґрунтя для функціонування держави за допомогою досконалого правового регулювання, висвітлення діяльності органів державної влади та місцевого самоврядування за допомогою інформаційних технологій, які дають змогу максимально збільшити коло реципієнтів інформаційних повідомлень, розвиток інформаційної свідомості державних службовців та інших представників державного апарату, збільшення частки електронних послуг у загальній системі адміністративних послуг. За допомогою розвитку загальнодержавного рівня інформаційної культури стає можливим здійснення ефективного громадського контролю за діяльністю держави: оприлюднення рішень державних інституцій, звітування про свою діяльність, доступ до публічної інформації роблять можливим аналіз ступеня ефективності їх роботи та нівелювання корупційних ризиків у їх функціонуванні.

Інформаційна культура на рівні окремих соціальних інститутів являє собою більш складне та різноспрямоване явище. Під час його вивчення доцільно керуватися здобутками соціологічної науки, яка відносить до соціальних інститутів економічні, політичні, культурно-виховні, релігійні, родинні та інші. Зі свого боку, в кожній із названих груп можливо виокремити свої підгрупи. Так, серед економічних інститутів можна виділити корпоративні структури великих суб'єктів господарювання, в кожній з яких існують свої критерії та стандарти інформаційної культури.

На особистісному рівні інформаційна культура може бути описана на ціннісно-

мотиваційному рівні, який є визначальним для всіх інших складових, когнітивному рівні, який включає у тому числі наявність інформаційних знань, вмінь і навичок, а також на емоційно-вольовому рівні, який обумовлює емоційне відношення до застосування та розвитку вказаних знань, вмінь та навичок, а також прийняття рішень щодо їх застосування в певних ситуаціях. Розгляд інформаційної культури у сукупності її елементів можливий не лише відповідно до описаних вище рівнів, до яких належать загальнодержавний, рівень окремих соціальних інститутів і особистісний. Залежно від обраних критеріїв можливо виокремити ще галузеві елементи інформаційної культури, яка знаходить свій прояв у конституційно-правових, адміністративно-правових, цивільно-правових та інших видах правовідносин; векторні елементи, до яких належать технологічна та гуманітарна сфери тощо [13]. У цілому погоджуючись з представленим розподілом, необхідно додати, що вимоги до розвитку інформаційної культури у представників різних соціальних інститутів можуть мати значні відмінності: якщо для деяких професійних груп вони виступають як бажані, то для окремих категорій, зокрема й для військовослужбовців, відповідні знання, вміння та навички є критично необхідними, оскільки їх нерозвиненість не лише знижує ефективність виконання поставлених завдань, а й утворює численні ризики та небезпеки, як корпоративного, так і загальнодержавного характеру [5].

На жаль, нерозривна єдність правової та інформаційної культури та їх вирішальне значення для оцінювання загального рівня культури особистості військовослужбовця ще не повною мірою відображена на рівні військово-управлінських рішень [5].

Так, у наказі Генерального штабу Збройних Сил України від 04.01.2017 № 4 “Про затвердження Інструкції з організації інформаційно-пропагандистського забезпечення у Збройних Силах України” вказане інформаційно-пропагандистське забезпечення розуміється як цілеспрямована діяльність органів військового управління, командувачів, командирів (начальників), посадових осіб структурних підрозділів морально-психологічного забезпечення щодо інформаційного впливу на свідомість особового складу з метою зміцнення його морально-психологічного стану, формування і поширення ідейних переконань, національних цінностей, стійкої мотивації та готовності до збройного захисту державного суверенітету, територіальної цілісності України, адекватного розуміння військовослужбовцями воєнно-політичної та суспільно-політичної обстановки, завдань, покладених на війська (сили), умов та особливостей їх виконання [14]. Заслуговує на увагу використання у вказаному правовому акті характерного для радянської педагогіки терміну “вплив на свідомість”, який відображає так званий “суб’єкт-об’єктний підхід”, за якого учень, вихованець, студент, військовослужбовець сприймався як пасивний об’єкт інформаційно-виховних впливів, який зобов’язаний вмістити всі ті ідеологічні доктрини, особливості світогляду, погляди та переконання, що нав’язувалися йому з метою забезпечити бездумне виконання ним будь-яких наказів. Неефективність суб’єкт-об’єктного підходу, використання якого позбавляє особистість ініціативи, креативності та негативно впливає на вольові якості, виховуючи уникання відповідальності як рису характеру, давно визнано у світовій та українській педагогіці, віковій та професійній психології. У дослідженнях з цього приводу констатується, що “об’єкт” виконує лише інертну, безініціативну функцію; він виявляється у відносинах, зумовлених потребами і можливостями суб’єкта [15]; відчуває вплив, який виявляється у пасивній, пригніченій позиції [16], і за таких умов неможливий гармонійний розвиток і саморозвиток особистості [17].

Додамо, що суб’єкт-об’єктний підхід заперечує цінність особистості військовослужбовця, що не може не впливати негативно як на методи військового управління в цілому, так і на адаптацію військовослужбовців до умов військової служби. Знецінення особистості, як доведено численними дослідженнями у галузі психології, сприяє протестній та суїцидальній поведінці внаслідок фрустрованих потреб [18] та нудного, заорганізованого дозвілля, його невідповідності інтересам і особистим потребам військовослужбовців [19]; порушенню дисциплінарних вимог, вчиненню інших правопорушень, проявам боулінгу [20], знижує мотивацію професійної діяльності [21] тощо.

Отже, активна, креативна і відповідальна поведінка

військовослужбовця за умови відповідності військово-управлінських відносин поставленим перед силами оборони цілям слугує запорукою його успішної адаптації до умов військової служби. Безумовно, гуманістичний характер сучасної військової педагогіки усвідомлюється нині не на всіх рівнях військового управління. Однак розвиток інформаційних технологій обумовлює невпинне зниження ефективності суб'єкт-об'єктних впливів. Якщо у середині минулого століття дефіцит джерел інформації обумовлював певну монополію суб'єктів інформаційних впливів на свідомість військовослужбовця, то нині спостерігається агресивна конкуренція адресантів (тих, хто продукує інформаційні повідомлення) за увагу реципієнтів (тих, хто такі повідомлення сприймає). За таких умов наочність, динамічність подання інформації, використання спеціальних приймів та методів непрямого впливу (ефектів ореола, тиску референтної групи, пересичення тощо) обумовлюють перевагу засобів масової інформації та соціальних мереж над застарілими методами прямого переконання та примусу. Отже, учасниками процесів формування особистості військовослужбовців є сьогодні велика кількість суб'єктів, які визначають спрямованість та наповненість різноманітних інформаційних ресурсів – мас-медіа, соціальних мереж, каналів інтернет-меседжерів, ігрових чатів, розважальних інтернет-ресурсів тощо. До того ж унаслідок використання багатьма з них методів соціальної інженерії, величезним обсягам матеріальних ресурсів, які дають змогу залучати для створення інформаційного контенту кращих фахівців, яких можна знайти на ринку праці, ефективність діяльності означених засобів формування свідомості реципієнтів, у тому числі й військовослужбовців, є достатньо високою [5]. Якщо ж врахувати, що частина таких каналів передачі інформаційних повідомлень прямо чи опосередковано контролюється противником, можна переконатися, що завдання формування високого рівня інформаційної культури військовослужбовців виступає сьогодні завданням першочергового значення.

Значення інформаційної культури військовослужбовця за умов невідповідності широко розповсюджених у силах оборони методів переконання та примусу особового складу особливостям інформаційного суспільства обумовлена комплексним характером досліджуваного виду культури і його зв'язку з світоглядним рівнем розвитку особистості. На жаль, термін "культура" стосовно виховання нового типу військовослужбовця ще сприймається дуже вузько, в аспекті перегляду кінострічок патріотичної спрямованості і участі у гуртках художньої самодіяльності. Так, наприклад, основними шляхами реалізації культурологічної роботи вважаються: проведення культурно-мистецьких заходів, які спрямовані на формування та підтримання стійкого морально-психологічного стану, зняття негативних емоційних наслідків, відновлення моральних, психічних та фізичних сил, мобілізації особового складу військ (сил) на успішне виконання завдань за призначенням, а основними формами культурологічної роботи визначені концерт; вистава; перегляд кіно- і відеофільмів та телевізійних передач; обговорення творів літератури та мистецтва; заходи відпочинку; огляд-конкурс; виставка; зустріч з видатними особистостями; екскурсія; вшанування кращих військовослужбовців [14]. Жодним чином не заперечуючи цінності емоційно-естетичних аспектів культури для формування особистості військовослужбовця, зауважимо однак, що в умовах збройного конфлікту більш важливими уявляються розвиток тих якостей, знань, вмінь та навичок, які сприяють підвищенню рівня критичності у сприйнятті інформаційних повідомлень. Зокрема, це вміння класифікувати інформаційні джерела за ступенем достовірності відомостей та даних, розуміти прямий та прихований зміст та спрямованість інформаційних впливів, виокремлювати власні та навіяні вербальними та невербальними способами емоції, які використовуються для полегшення наступних психологічних впливів, у тому числі тих, що є елементом інформаційно-психологічних операцій противника. Нехтування інформаційно-культурним аспектом формування особистості військовослужбовців призводитиме, на нашу думку, до того, що цей процес безперешкодно, завдяки інформаційним технологіям, будуть здійснювати інші суб'єкти, у тому числі противник [5].

Одним із засобів формування інформаційної культури на етапі підготовки

кадрів в інтересах Збройних Силах України у вищих військових навчальних закладах є формування академічної доброчесності. Особливостями сучасного етапу розвитку правового забезпечення вищої освіти є активне закріплення етичних вимог щодо академічної доброчесності викладачів, науковців та здобувачів освіти в кодексах академічної доброчесності, ухвалених зборами трудових колективів або вченими радами університетів. У вказаних документах знайшли своє відображення правила і норми академічної доброчесності учасників освітнього процесу, особливості політики закладів вищої освіти у вказаній сфері, процедури розгляду питань про академічну недоброчесність та правовий статус органів, які такі процедури здійснюють [22]. Активне впровадження вимог академічної доброчесності у навчальний процес вищих військових навчальних закладів дає змогу одночасно наочно продемонструвати курсантам та слухачам можливості визначення початкового джерела відомостей та даних, закономірності поширення інформації на певних спеціалізованих ресурсах мережі Інтернет, сприяє формуванню у них критичного ставлення до неперевірених інформаційних повідомлень та зменшує вірогідність копіювання ними у письмовому чи усному вигляді неперевірених повідомлень невстановлених осіб, серед яких в умовах збройного конфлікту можуть бути і представники противника.

Серед засобів розвитку інформаційної культури військовослужбовців необхідно назвати ініціативу “AM&PM” (“Against manipulation and propaganda messages” – “проти маніпуляцій і пропаганди”), започатковану курсантами Військового інституту Київського національного університету імені Тараса Шевченка. Основна ціль команди “AM&PM” – навчити військових бути медіаграмотними, розпізнавати фейки, поширювати тільки достовірну інформацію. У межах проєкту створюються авторські матеріали, проводяться навчальні тренінги, зустрічі з експертами, та досліджуються загрозливі наративи та фейки проти України. На початку проєкту аналітична група команди “AM&PM” провела дослідження серед діючих військовослужбовців та експертів у сфері медіа. Це допомогло краще зрозуміти потреби та уподобання цільової аудиторії. Також з’ясували, які ресурси та канали обирають українські військові для отримання інформації. Результати дослідження показали – важливим елементом боротьби з інформаційними атаками Росії є підвищення рівня медіаграмотності та розвитку критичного мислення щодо інформації у ЗМІ [23]. “AM&PM” має власний сайт http://am-pm.org.ua/ та веде сторінку у соціальній мережі фейсбук, а також має свої площадки на інших інтернет-платформах.

Діяльність “AM&PM” є одним із прикладів активної участі здобувачів військової освіти у формуванні власної інформаційної культури, що відповідає сутності суб’єкт-суб’єктного підходу до формування особистості військовослужбовців і дає змогу максимально ефективно використовувати власний потенціал системи військової освіти для її вдосконалення. Можна прогнозувати, що подальший розвиток інформаційного суспільства буде постійно знижувати і без того недостатньо високу ефективність вертикальних інформаційно-пропагандистських і виховних впливів з одночасним збільшенням ваги горизонтальних ініціатив та проєктів [5]. Отже, перед науковцями та практиками нині постає амбітне завдання узгодження таких ініціатив з особливостями ієрархічно-дисциплінарних відносин у Збройних Силах України.

Висновки. Основними правовими умовами підвищення рівня інформаційної культури військовослужбовців Збройних Сил України є створення несуперечливого правового підґрунтя, яке включало б як програмні документи (Стратегію розвитку інформаційної культури військовослужбовців Збройних Сил України), так і низку нормативних і інтерпретаційних актів, у яких було б визначено мету, принципи, суб’єкти та форми підвищення рівня інформаційної культури рядового та командного складу на ціннісному, світоглядному та діяльнісному рівнях. На організаційному рівні особливу важливість має керованість процесом її формування та зміцнення, що вимагає: визначення ключових індикаторів наявного рівня інформаційної культури як на індивідуальному, так і на організаційному рівні, систематичного проведення моніторингу з метою визначення динаміки таких індикаторів.

Напрями подальших досліджень. Надалі на основі отриманих результатів

доцільно визначити шляхи правового закріплення комплексу заходів щодо розвитку інформаційної культури у Збройних Силах України на рівні довгострокової програми, до виконання якої доцільно залучити, окрім внутрішньовідомчих, ресурси громадянського суспільства, що забезпечить більш об'єктивну оцінку отриманих результатів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Interview: Taliban Spokesman Qari Yousef Ahmadi. Asharq Al-Awsat. 2012. Apr 15. URL: https://eng-archive.aawsat.com/theaawsat/interviews/interview-taliban-spokesman-qari-yousef-ahmadi (дата звернення: 23.08.2021).
2. Беляков К. І., Онопрієнко С. Г., Шопіна І. М. Інформаційна культура: правовий вимір : монографія. Київ, КВІЦ, 2018. 168 с.
3. Шопіна І. М., Коропатнік І. М. Роль інформаційної культури в підвищенні ефективності функціонування Збройних Сил України. *Наука і правоохорона.* 2017. № 2. С.47–54.
4. Khomiakov D., Khrystynchenko N., Shopina I., Zhukov S., Shpenov D. Cybersecurity: Legal and Organizational Support in Leading Countries, NATO and EU Standards**.** *Journal of Security & Sustainability Issues.* 2020/3/1. Volume 9, Issue 3. P. 977–992.
5. Шопіна І. М., Коропатнік І. М. Проблеми підвищення інформаційної культури військовослужбовців в умовах збройного конфлікту. Війни інформаційної епохи: міждисциплінарний дискурс : монографія /за ред. В. А. Кротюка. Харків: ХУПС, 2021. 558 с.
6. Гущин О. О. Інформаційна культура учасників міжнародних операцій з підтримання миру та безпеки. *Наука і правоохорона*. 2017. № 2. С. 114–118.
7. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 22.08.2021).
8. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 22.08.2021).
9. Про оборону України : Закон України від 06.12.1991 р. № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text (дата звернення: 22.08.2021).
10. Стратегія воєнної безпеки України: затверджено Указом Президента України від 25.03.2021 р. № 121/2021. URL: https://zakon.rada.gov.ua/ laws/show/121/2021#Text (дата звернення: 22.08.2021).
11. Стратегія національної безпеки України: затверджена Указом Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#n5 (дата звернення: 22.08.2021).
12. Доктрина зі стратегічних комунікацій: затверджена Головнокомандувачем Збройних Сил України 12 жовтня 2020 року. http://stratcom.nuou.org.ua (дата звернення: 22.08.2021)
13. Онопрієнко С. Г. Класифікація елементів інформаційної культури. *Форум права.* 2016. № 5. С. 135-138. URL: http://nbuv.gov.ua/UJRN/FP_index.htm_2016_5_24 (дата звернення: 21.0.2021).
14. Про затвердження Інструкції з організації інформаційно-пропагандистського забезпечення у Збройних Силах України: наказ Генерального штабу Збройних Сил України від 04.01.2017 № 4. URL: https://dovidnykmpz.info/ipz/nakaz-heneral-noho-shtabu-zbro-nykh-sy-4/ (дата звернення: 20.08.2021).
15. Войтко В. Психологический словарь. Киев : Высшая школа, 1982. 108 с.
16. Леонтьев А. Педагогическое общение. Москва, 1979. URL: http://www.twirpx.com/file/1206617 (дата звернення: 19.08.2021).
17. Слюсаренко Н., Кульбацька М. Суб'єкт-суб'єктний підхід до організації педагогічного процесу. *Людинознавчі студії. Педагогіка*. 2015. № 1 (33). С. 196.
18. Поляков І. О., Щербак С. М. Основні причини та приводи здійснення потенційними суїцидентами фатального кроку. *Проблеми екстремальної та кризової психології*. 2014. Вип. 15. С. 208–214.
19. Корольчук В. В. Профілактика суїциду серед військовослужбовців. 2016. URL: http://elar.naiau.kiev.ua/bitstream/123456789/6285/1/zbir_pcuxolog2_p019-023.pdf (дата звернення: 19.05.2021).
20. Король А. Причини та наслідки явища булінгу. *Відновне правосуддя в Україні*. 2009. № 1–2 (13). С. 84–93.
21. Попов В. М., Астапенкова В. М. Психологічні особливості вивченої безпорадності працівників ДСНСУ. *Проблеми екстремальної та кризової психології.* 2014. Вип. 15. С.214–221.
22. Шопіна І. Ґенеза правового забезпечення академічної доброчесності. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки.* 2020. Вип. 1. С. 36–39.
23. Команда нашого інституту називається "AM&PM" – "Against manipulation and propaganda messages" – "проти маніпуляцій й пропаганди". URL: http://am-pm.org.ua/about (дата звернення: 29.05.2021).

Стаття надійшла до редакційної колегії 01.09.2021

Problems of legal and organizational support for the development of information culture of servicemen of the Armed Forces of Ukraine

Annotation

The importance of improving the information culture of servicemen in modern conditions is explained by the growing importance of the information component of armed conflicts, the active use of various subjects of information influence to achieve military and non-military goals. In world practice, there are examples of a total reduction in the combat effectiveness of government military formations through the accurate use of information media. Thus, the consciousness and worldview of each soldier can always be used by the enemy to achieve their goals. In turn, this requires a more detailed consideration of the problems of information culture as a construct that provides resistance to most destructive information influences.

The purpose of the article is to identify the main legal and organizational problems in the field of ensuring the appropriate level of information culture of servicemen. This will also be facilitated by the creation of a legal basis that will cover a number of regulations and interpretative acts, which will determine the principles, subjects and forms of raising the level of information culture of servicemen.

The main legal conditions for raising the level of information culture of servicemen of the Armed Forces of Ukraine are the creation of a consistent legal basis. The legal basis will include both program documents and a number of normative and interpretative acts, which would define the purpose, principles, subjects and forms of raising the level of information culture of the rank and file at the value and worldview levels. At the organizational level, process control, formation and strengthening are of particular importance, which requires: identification of key indicators of the current level of information culture at both individual and organizational level, systematic monitoring to determine the dynamics of such indicators.

Keywords: information culture; informational security; military; Armed Forces of Ukraine; information wars; information and psychological operations; information influences.

ВІДОМОСТІ ПРО АВТОРІВ

АНДРІЯНОВА Н. М. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського кандидат політичних наук;

БАТАЛЮК В. І. – доцент кафедри КШІ застосування військ (сил) НУО України імені Івана Черняховського;

БЕЛЯЧЕНКО В. В. – науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

БОБРОВ С. В. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат технічних наук, доцент;

БОГДАНОВИЧ В. Ю. – провідний науковий співробітник ЦНДІ Збройних Сил України, доктор технічних наук, професор;

БОНДАРЧУК С. В. – науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

БОЧАРНІКОВ В. П. – головний науковий співробітник НДУ ЦВСД НУО України імені Івана Черняховського, доктор технічних наук, професор;

БРАТКО А. В. – докторант Національної академії Державної прикордонної служби України імені Богдана Хмельницького;

БУТЕНКО М. П. – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

ВОРОВИЧ Б. О. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат військових наук, доцент;

ГАЛАГАН В. І. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат військових наук, доцент;

ГОЛОПАТЮК Л. С. – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат військових наук;

ДЕРГИЛЬОВА О. В. – старший науковий співробітник НОВ ЦВСД НУО України імені Івана Черняховського, кандидат технічних наук, старший науковий співробітник;

ЗАГОРКА О. М. – головний науковий співробітник ЦВСД НУО України імені Івана Черняховського, доктор військових наук, професор;

ЗАГОРКА І. О. – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

ЗАКАЛАД М. А. – начальник НДВ ЦВСД НУО України імені Івана Черняховського;

ЗАХАРЧУК Д. О. – доцент кафедри національної безпеки та управління Національної академії Державної прикордонної служби України імені Богдана Хмельницького;

ЗУБКОВ В. П. – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

ІЛЬЯШОВ О. А. – провідний науковий співробітник науково-дослідного управління військової частини А1906, доктор військових наук, професор;

КІРІЛКІН Є. І. – професор кафедри КШІ застосування військ (сил) НУО України імені Івана Черняховського, кандидат технічних наук, доцент;

КОВАЛЕНКО Г. А. – офіцер Стратегічного командування НАТО з трансформації;

КОТЛЯРЕНКО О. П. – начальник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат юридичних наук;

КОМАРОВ В. С. – начальник науково-дослідного управління військової частини А1906, доктор військових наук, професор;

КРИВОГУЗ Г. І. – доцент кафедри організації тилового (логістичного) забезпечення Військової академії, Одеса, кандидат військових наук, доцент;

КУЛЬЧИЦЬКИЙ О. С. – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

КУРСТЕЙТОВ Т. Л. – начальник кафедри Інституту оперативного забезпечення та логістики доктор технічих наук, професор;

ЛЕВЧУК О. В. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат економічних наук, доцент;

МУДРАК Ю. М. – начальник НДВ ЦВСД НУО України імені Івана Черняховського;

НАГОРНЮК В. Ф. – викладач кафедри організації тилового (логістичного)

забезпечення Військової академії, Одеса, кандидат військових наук, доцент;

МЕНТУС І. Е. – доцент кафедри Кам'янець-Подільського НУ імені Івана Огієнка, кандидат військових наук, доцент;

ОЛЕКСІЮК В. В. – начальник науково-дослідного відділу науково-дослідного управління військової частини А1906, кандидат військових наук;

ПАВЛІКОВСЬКИЙ А. К. – начальник ЦВСД НУО України імені Івана Черняховського, кандидат військових наук, доцент;

ПІДГОРОДЕЦЬКИЙ М. М. – заступник начальника кафедри Інституту оперативного забезпечення та логістики кандидат військових наук;

ПОЛІШКО С. В. – начальник НДЛ НДВ ЦВСД НУО України імені Івана Черняховського, кандидат технічних наук, старший науковий співробітник;

ПОЛЯЄВ А. І. – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

ПОПЕЛЬСЬКИЙ М. І. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

ПРИМА А. М. – начальник НДВ ЦВСД НУО України імені Івана Черняховського, доктор філософії;

ПРИМА М. В. – науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

РОЗУМНИЙ О. Д. – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

РИБИДАЙЛО А. А. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат технічних наук, старший науковий співробітник;

САГАНЮК Ф. В. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат юридичних наук, доцент;

СВЄШНІКОВ С. В. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат технічних наук, старший науковий співробітник;

СНІЦАРЕНКО П. М. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, доктор технічних наук, старший науковий співробітник;

САРИЧЕВ Ю. А. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат технічних наук, старший науковий співробітник;

ТІХОНОВ Г. М. – начальник кафедри КШІ застосування військ (сил), НУО України імені Івана Черняховського кандидат військових наук, старший науковий співробітник;

ТКАЧЕНКО В. А. – начальник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат військових наук;

ТОРІЧНИЙ В. О. – доцент кафедри прикордонної служби Національної академії Державної прикордонної служби України імені Богдана Хмельницького;

УТЮШЕВ М. К. – науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

ФЕДОРІЄНКО В. А. – старший науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського;

ФУЧКО А. Й. – начальник НДВ ЦВСД НУО України імені Івана Черняховського;

ШАПТАЛЕНКО М. І. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат технічних наук, доцент;

ШОПІНА І. М. – професор кафедри адміністративно-правових дисциплін, Львівського державного університету внутрішніх справ, доктор юридичних наук, професор;

ШПАНЧУК Г. В. – начальник НДЛ кафедри КШІ застосування військ (сил) НУО України імені Івана Черняховського, кандидат військових наук, старший науковий співробітник;

ШПУРА М. І. – провідний науковий співробітник НДВ ЦВСД НУО України імені Івана Черняховського, кандидат військових наук, старший науковий співробітник;

ЯСЬКО В. А. – старший викладач кафедри Кам'янець-Подільського НУ імені Івана Огієнка, кандидат військових наук, доцент.

ВИМОГИ ДО СТАТЕЙ

Відповідно до Постанови ВАК України № 7-05/1 від 15 січня 2003 року наукові статті мають містити такі елементи:

постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

аналіз останніх досліджень і публікацій, у яких започатковано розв'язання даної проблеми і на які спирається автор, виділення нерозв'язаних раніше частин загальної проблеми, яким присвячується стаття;

формулювання **мети статті** (постановка завдання);

виклад **основного матеріалу** дослідження з повним обґрунтуванням отриманих наукових результатів;

висновки і перспективи подальших досліджень розвитку в цьому напрямі;

анотація до статті та ключові слова – розміщуються після назви статті.

У статті слід дотримуватись загальноприйнятої термінології. Усі скорочення та нові терміни мають бути розкриті автором.

Назва, список авторів, назва установи, анотація (не більше 40 слів), ключові слова (7 слів) готуються на трьох мовах: українській, російській та англійській.

Обсяг статті разом із таблицями, рисунками та списком літератури не більше 10 сторінок А4.

Текст статті набирається в редакторі **Microsoft Word** шрифтом **Times New Roman 14. Вирівнювання по ширині. Інтервал між рядками тексту – 1,0.**

Формат сторінки – А4. Поля: ліве – 27 мм; верхнє і нижнє – 20 мм; праве – 20 мм.

Не використовуйте для форматування тексту пропуски, табуляцію тощо. Не встановлюйте ручне перенесення слів, не використовуйте 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 Microsoft Equations курсивом (крім особливих випадків) без обрамлення і заливки. Забороняється використовувати для набору формул графічні об'єкти, кадри і таблиці.

Вирівнювання по центру, нумерація – у дужках, праворуч. Нумерувати потрібно тільки ті формули, на які є посилання у тексті.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ складається у порядку посилання в тексті та подається наприкінці статті згідно з ДСТУ ГОСТ 7.1:2015. – ***кегль 12***

У редакцію надається друкований 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., д-р техн. наук, професор[1]; – ***Times New Roman кегль – кегль 14 пт***
Іванов В. А.[2]
Бунин В. В., д-р техн. наук, профессор[1];
Иванов В. О.[2]
V. Bunin, Phd[1];
V. Ivanov[2]

[1] – Департамент воєнної політики та стратегічного планування Міністерства оборони України, Київ;
[2] – Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ
[1] – Департамент военной политики и стратегического планирования Министерства обороны Украины, Киев;
[2] – Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, 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 named after Ivan Cherniakhovskyi, Kyiv

Матрична модель OLAP-систем (*кегль 14 пт напівжирний*)
Матричная модель OLAP-систем
Matrix model of OLAP-systems

Резюме (2-3 речення). Розглянуто особливості матричних моделей … ***(кегль 12 пт)***
Анотація (1800 знаків).
Ключові слова: модель, OLAP-система, інформаційні технології.

Аннотация (1800 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 ; 2 *- 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 імені Івана Черняховського

№ 2(72), 2021

Відповідальні за випуск:
Відповідальний за випуск: Рибидайло А. А.
Технічний редактор: Руденська Г. В.
Комп'ютерне верстання: Рибидайло А. А.
Коректори: Андріянова Н. М., Уварова Т. В., Терещенко С. А.
Підтримка вебсайту збірника: Кірпічніков Ю. А., Петрушен М. В.

Підписано до друку 20.09.2021. Формат 60х84 1/8.
Папір офсетний. Обл.- вид.арк.8,55. Друк. арк.18,75
Зам. 337. Наклад 100 прим.

Видання Національного університету оборони України імені Івана Черняховського
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 р.

Надруковано у друкарні Національного університету оборони України імені Івана Черняховського
03049, м. Київ, Повітрофлотський пр-т, 28