ISSN 2304-2699

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

№ 3(86), 2025

УДК 355:623 (08)

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

Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України.
2025. № 3(86).

Створений у 1997 році, *внесений до* ***Переліку наукових фахових видань України в галузі технічних та військових наук*** (категорія "Б", наказ МОН України від 02.07.2020 № 886):
F3 – Комп'ютерні науки;
K5 – Військове управління (за видами збройних сил)

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

***Програмні цілі журналу*:** інформування науково-дослідних організацій, закладів вищої освіти Міністерства оборони України, інших міністерств і відомств, потенційних замовників науково-технічної продукції Центру воєнно-стратегічних досліджень Національного університету оборони України та публікація результатів здобувачів наукового ступеня (журнал внесено до Реєстру суб'єктів у сфері медіа рішенням Національної ради України з питань телебачення і радіомовлення від 31.10.2023 № 1214 та присвоєно ідентифікатор медіа R30-01600).

Рекомендовано до друку рішенням Вченої ради Національного університету оборони України (протокол № 15 від 29.12.2025)

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

C O N T E N T

З М І С Т

УДК 351.86: 340.137(477) https://doi.org/10.33099/2304-2745/2025-3-86/6-16

Машталір В. В., доктор історичних наук, професор (0000-0002-8132-217X)
Іващенко А. М., кандидат технічних наук, доцент (0000-0002-8131-5463)
Уварова Т. В., кандидат технічних наук, старший дослідник (0000-0003-2388-4059)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Від всеохоплюючої до комплексної оборони: пошук моделі для України

Резюме. У статті досліджуються моделі національної оборони від закінчення Другої світової війни до війни РФ проти України. Розглянуто поступовий розвиток моделей національної оборони з урахуванням безпекового середовища, що склалося з лютого 2022 р. та практичні аспекти імплементації цих моделей. Пропонуються рекомендації, які необхідно враховувати в поточному воєнно-політичному та науковому дискурсі щодо майбутньої моделі оборони України.

Ключові слова: національна оборона; модель оборони; перехідна модель оборони; стратегічна оборона; всеохоплююча оборона (Total Defence); цивільно-військова інтеграція (Civil-Military Integration, CMI); воєнно-цивільне об'єднання (Military-Civil Fusion, MCF); комплексна оборона (Comprehensive Defence); інтегрована оборона (Integrated Defence System).

Постановка проблеми. Порівняно з війнами XIX–XX століть, війни XXI століття актуалізували зворотний логістичний та інноваційний потік: цивільний сектор став важливим джерелом спроможностей, ресурсів і інновацій на полі бою. Причиною цього стала зміна характеру сучасної війни [1]: ведення бойових дій у багатодоменному просторі, швидке впровадження нових технологій, зростання показників стратегічної глибини оборони, бойових втрат озброєння, ресурсної бази та складності логістики. Україна не може дозволити собі класичну, високовартісну модель стратегічної оборони, де повний цикл стратегічного планування – від стратегії до озброєння і ресурсів, – триває роками. Натомість асиметричний підхід спонукає інтегрувати наявні цивільні спроможності, ресурси і технології в нові бойові конфігурації, які не мають прямих аналогів у силах оборони інших, навіть високорозвинутих країнах. Це створює умови для розбудови унікальної моделі національної оборони України, такої, що ґрунтується не на наявних воєнних спроможностях і ресурсах, а на інноваціях і широкому застосуванні цивільних ресурсів та технологій у бойовій логіці. У стратегічному вимірі це означає перехід від моделі всеохоплюючої оборони до моделі адаптованої комплексної оборони, розширеної до умов реальної поточної безпекової ситуації. Така модель потребує як розвитку воєнно-теоретичних засад, так і розроблення концепції сучасної системи національної оборони.

Аналіз останніх досліджень і публікацій. Дослідженню проблем побудови моделі національної оборони присвячені численні праці як вітчизняних, так і зарубіжних науковців [2–12].

У монографії [2] наведено результати системного аналізу сучасних концепцій стримування в контексті забезпечення національної оборони. Крім класичного стримування, в роботі розглядаються інші типи стримування, засновані на запереченні, делегітимізації, збільшенні витрат, дезінформації, а також інтегроване, кумулятивне, кібернетичне, терористичне, гібридне, комплексне, міждоменне, адаптоване та розширене стримування. Автори пропонують низку нових концепцій стримування та розширену бібліографію. Як проблемне питання досліджують достатність моделі оборони, яка заснована на стримуванні, для забезпечення національної безпеки, враховуючи сучасні виклики та загрози.

Монографія відомого науковими працями з вивчення холодної війни та двадцятирічним досвідом викладання університетського навчального курсу з формування національної (великої) стратегії професора Єльського університету Джона Льюїса Геддіса [3] присвячена мистецтву державного управління, методам балансування високих цілей з наявними спроможностями, адаптивності та врахуванню досвіду перемог і невдач. Автор проводить аналіз теорії і практики національної безпеки і оборони від давнього світу до Другої світової війни.

Монографія [4] призначена для розробників сучасних воєнних стратегій. У роботі досліджено мінливу і регулярну складову характеру війни, визначено основні тренди потенційних воєнних конфліктів найближчого десятиліття, напрями вдосконалення стратегій і доктрин оборони та ведення війни, трансформації і адаптації моделі оборони та збройних сил.

Дослідник Національної академії оборони Латвії у статті [5] надає огляд розвитку сучасних концепцій національної оборони країн Європи. Обґрунтовує необхідність переходу європейських країн на концепцію комплексної оборони, визначає дві нові фундаментальні складові комплексної оборони: національний опір та національна стійкість, пропонує доповнити діючий перелік (каталог) оборонних спроможностей спроможностями суспільства чинити опір і його стійкістю.

У статті [6] автори констатують швидкий розвиток оборонних спроможностей протягом останніх тридцяти років. Зазначають, що розвиток сучасної теорії національної оборони, її структурованої концепції і моделі відстає. Однак, незважаючи на цей дисбаланс, країни світу постійно витрачають значні ресурси на розвиток оборони. Автори також обґрунтовують основні наукові підходи до розроблення концепції національної оборони і оборонного потенціалу. Показують, що взаємодія між технологіями і соціальними компонентами оборони є особливо слабкою, а відповідні теорії та методи із суміжних галузей не враховуються. Доказують важливість урахування у подальшому розвитку концепції і моделі оборони не тільки положень воєнної науки, а й інших галузей знань. Обґрунтовують потенційний кластер міждисциплінарних досліджень, необхідний під час розроблення концепції і моделі оборони.

У статті [7] розглядається модель комплексної оборони Латвії, заснованої на загальносуспільному підході до протистояння гібридним загрозам.

У роботі [8] автор досліджує модель комплексної оборони Фінляндії. Зазначає, що країна має тривалий досвід поєднання військових і невійськових аспектів оборони. Під час холодної війни цей досвід був покладений у концепцію "тотальної оборони" – мобілізації всього суспільства для досягнення воєнних цілей.

Дослідник з університету оборони Литви у статті [10] визначає три базові складові тотальної оборони: зміцнення національного воєнного потенціалу, розвиток інфраструктури для розміщення військ союзників та участь суспільства в національній обороні. Підкреслює, що незважаючи на значне збільшення витрат на оборону, участь суспільства у національній обороні залишається обмеженою, оскільки стратегія національного спротиву незатверджена, а участь громадян, неурядових організацій та приватного сектору в національній обороні залишається формальною.

Китайські дослідники з Тайпею у статті [11] проводять аналіз практики цивільно-військової інтеграції Китаю та її перехід до військово-цивільного об'єднання. Автори розкривають сутність нової концепції, наводять чинники, які спонукали Китай її впровадити та як це було реалізовано практично, визначають напрями подальшого розвитку китайської моделі оборони. Також стверджують, що політичні цілі Китаю щодо воєнної трансформації та самодостатні оборонно-промислової бази стали основними чинниками переходу від концепції військово-цивільної інтеграції до концепції цивільно-військового об'єднання.

У праці [12] досліджено роль і місце енергетичного комплексу в моделі комплексної національної оборони та особливості взаємодії між воєнними і цивільними секторами оборони. Енергетична безпека є важливим містком між національною стійкістю та комплексною національною обороною. Конфігурація енергетичної системи має забезпечувати її спроможності підтримувати оборонні зусилля. Методика дослідження включає два етапи: розроблення показників оцінювання енергетичної безпеки під час розроблення моделі комплексної національної оборони та якісне оцінювання впливу на енергетичну безпеку різних сценаріїв розвитку енергетики. Дослідження визначає, що цивільна інфраструктура рідко конфігурується або розвивається з акцентом на оборону, однак існують позитивні системні ефекти для оборони під час збільшення диверсифікації енергетичної системи, особливо в умовах обмеження зовнішнього постачання та вірогідних масштабних руйнувань у разі збройної агресії. Однак такі зміни в енергетичній системі мають бути враховані під час вибору моделі оборони, стратегії

ведення війни, впровадженні нових тактичних прийомів і технологій.

Однак у розглянутих наукових працях не враховано низку нових трендів і змін у підходах до організації сучасної системи національної оборони, які були практично перевірені та підтверджені під час протидії широкомасштабній російської агресії проти України.

Метою статті є дослідження сучасних моделей національної оборони та розроблення рекомендацій щодо визначення ефективної моделі національної оборони України з урахуванням поточного безпекового середовища.

Обмеження та припущення. Дослідження зосереджено на порівняльному аналізі моделей і рішень, прийнятих у сфері оборони різних країн світу. У процесі дослідження використовуються загальнодоступні документи, які визначають політику, стратегії та концепції і моделі оборони в умовах протидії переважаючому противнику. Цифри та тенденції, пов'язані з обґрунтуванням моделі оборони, взяті з відкритих офіційних джерел. Аналітичні звіти зарубіжних дослідних центрів з питань безпеки і оборони підтверджують достовірність отриманих результатів та посилюють аргументацію.

Хоча відношення провідних країн світу до виконання Будапештського меморандуму, недієздатність сучасної системи нерозповсюдження ядерної зброї, зміна політики США з питань міжнародної безпеки, призвели до зростання кількості держав (Німеччина, Польща, країни Балтії, Південна Корея, Японія, Тайвань, Австралія, М'янма, Бразилія, Іран), які розглядають можливість виготовлення, придбання або розміщення на власній території ядерної зброї, робити висновки щодо потенційного впливу ядерної зброї на вибір майбутньої моделі оборони України уявляється передчасним. З огляду на це, для цілей цієї статті згадану тему було навмисно уникнуто.

Виклад основного матеріалу.

1. Моделі національної оборони

Модель воєнно-стратегічної оборони

Воєнно-стратегічна оборона – один з класичних концептів стратегії національної безпеки або воєнної стратегії. Метою стратегічної оборони є запобігання, опір чи відбиття широкомасштабної агресії, яка здійснюється у наземному, морському, повітряному та кібердоменах шляхом вторгнення або нападу, або як атаки у ході кібервійни. Воєнно-стратегічна оборона може включати нанесення превентивних ударів. У воєнному контексті стратегічної обороною вважається війна, яка може тривати від кількох днів до кількох поколінь, або окремі воєнні кампанії під час війни, що включають низку операцій, розділених у часі та просторі, і з певною спільною досяжною метою, для яких виділена певна частина наявних збройних сил. Як кампанія, стратегічна оборона може складатися з кількох битв, деякі з них можуть бути наступальними за природою, або можуть виникнути внаслідок відходу на нові позиції, оточення, або облоги сторони, яка захищається, спрямовані на забезпечення стратегічної ініціативи [13].

Як правило, модель стратегічної оборони включає політичне та воєнне керівництво, організації сектору безпеки і оборони [14]. Значна кількість держав світу у мирний час метою своєї воєнної політики визначає організацію і забезпечення стратегічної оборони.

Модель тотальної (всеохоплюючої) оборони

Історично тотальна, або всеохоплююча, оборона (total defence) передбачає участь цивільного населення у війні, яку веде держава. Основою концепції тотальної оборони є те, що у разі загрози або початку війни держава здійснює швидку та результативну мобілізацію необхідної кількості людей, здатних і підготовлених до ведення бойових дій. Концепція тотальної оборони передбачає економію ресурсів завдяки усуненню необхідності утримувати багаточисельні регулярні збройні сили. Тому тотальна оборона вважається ефективним рішенням для малих і середніх держав і сприймається як модель, яка забезпечує самодостатність у сфері оборони. У процесі реалізації такої моделі враховуються характеристики потенційного театру бойових дій, який сприяє обороні. Найскладнішими елементами тотальної оборони зазвичай є протиповітряна, територіальна та цивільна оборона [15].

Сучасна концепція тотальної оборони базується на досвіді холодної війни. Наявні концептуальні та організаційні документи різних країн підкреслюють складність загроз і визначають необхідні дії щодо реагування на них, як основні передумови тотальної оборони.

Модель комплексної оборони (Comprehensive Defence)

Одночасно зі змінами у характері сучасних війн, стратегії ведення війни та тактики бойових дій, моделі національної оборони також динамічно змінюються. Ці зміни обумовлюють перехід до наступного рівня – комплексної національної оборони. Комплексне розуміння оборони означає, що суспільство (цивільний сектор) організовано та підготовлено для захисту держави від усіх форм нападу, як військового, так і невійськового характеру.

Незалежно від характеру загроз, комплексна модель національної оборони включає як стратегічну (традиційну) воєнну оборону, тотальну (всеохоплюючу) оборону, так і нові системні аспекти національної оборони: стримування, національну стійкість, національний спротив, територіальну оборону, міжнародне співробітництво і партнерство, спроможності цивільного сектору, психологічний захист, внутрішню безпеку та спільне використання ресурсів. Комплексна оборона охоплює захист від військових і невійськових загроз та включає як воєнні, так і невоєнні дії у всій множині доменів протиборства.

Характерною рисою моделі комплексної оборони є скоординована участь державних установ, приватного сектору, громадських організацій та окремих громадян у підготовці до оборони та її проведенні.

На практиці здійснити перехід від моделі тотальної до моделі комплексної оборони дуже складно. Тому в окремих, особливо потужних з воєнної точки зору країнах з амбітними політичними цілями впроваджуються проміжні перехідні моделі. До них можна віднести модель національної оборони США на основі цивільно-військової інтеграції (Civil-Military Integration, CMI) та модель національної оборони Китаю на основі військово-цивільного об'єднання (Military-Civil Fusion, MCF). Інші держави, як правило, розробляють і впроваджують окремі елементи моделі комплексної оборони.

Перехід від моделі тотальної оборони до моделі комплексної оборони визначається еволюцію сучасної війни і дає змогу досягти оптимального балансу у використанні воєнних і цивільних ресурсів для забезпечення національної оборони, національного відродження і технологічного прогресу.

Крім розглянутих моделей, у науковій літературі за тематикою та низці офіційних документів використовується термін "інтегрована оборона" (Integrated Defence System, IDS). У межах цього дослідження під системою інтегрованої оборони будемо розуміти організаційну, інформаційну або технічну підсистему, яка забезпечує спільне (інтегроване) функціонування окремих складових системи національної оборони. Системи інтегрованої оборони можуть бути складовими будь-якої моделі оборони – від стратегічної до комплексної. Прикладом сучасної системи інтегрованої оборони може бути модульна система Palantir Edge AI – набір універсальних алгоритмів, які налаштовуються під окремі завдання з різними наборами даних. Використовується як система ситуативної обізнаності (типу української розробки Delta), яка дає змогу автоматично обробляти різні джерела та наносити інформацію на карту, проводити OSINT-дослідження на основі алгоритмів штучного інтелекту.

Порівняння сучасних моделей національної оборони наведено в Табл. 1.

2. Приклади впровадження моделей національної оборони

2.1. Модель тотальної (всеохоплюючої) оборони

Тотальна оборона покладена в основу воєнної стратегії країн Північної Європи. Так, національне законодавство Швеції до тотальної оборони відносить усі види діяльності, необхідні для підготовки країни до війни. У цьому підході оборона включає два взаємодоповнюючі види діяльності: безпосередньо воєнну та цивільну (цивільна оборона). Модель тотальної оборони Данії передбачає використання всіх ресурсів для підтримки організованого, функціонального суспільства та захисту людей і національного майна. Протидія складному характеру сучасних загроз потребує спільних рішень і тісної координації між відповідальними міжнародними і національними органами влади [16] Термін "тотальна оборона" також використовується в основоположних документах оборонної політики Литви, у яких наголошується, що оборона Литви є тотальною та безумовною. Тотальна оборона означає, що не лише національні збройні сили та сили союзників НАТО захищають Литву, а також передбачає, що всі національні ресурси мобілізовані для національної оборони, і що кожен громадянин Литви та нація в цілому чинитимуть опір усіма дозволеними міжнародним правом способами. Тотальна оборона Литви включає традиційну оборону воєнними засобами та участь невійськових

установ і суспільства в цивільному русі опору [17].

Розуміння національної оборони Естонії призводить до інтеграції національної воєнної оборони, діяльності всіх урядових міністерств, участі суспільства в національній обороні та захисту населення в межах комплексного підходу до національної оборони [18]. Такий підхід до національної оборони передбачає використання спільних зусиль збройних сил, установ та суспільства всієї країни для забезпечення безпеки Естонії у разі загрози воєнної агресії.

Модель тотальної оборони також впроваджена в неєвропейських країнах. Сінгапур прийняв концепцію тотальної оборони через прогнозовані зміни в характері збройних конфліктів, обмежені державні ресурси, характер суспільства та розміри держави. Можливості тотальної оборони охоплюють не лише збройні сили Сінгапуру, а й цивільне населення. Кожен сектор суспільства мобілізований та відіграє певну роль у забезпеченні безпеки і оборони Сінгапуру від усіх форм нападу, як військового, так і невійськового. Сінгапурська концепція тотальної оборони розрізняє шість сфер діяльності, включаючи воєнну оборону, цивільну оборону, економічну оборону, соціальну оборону, а також цифрову та психологічну оборону [19].

Таблиця 1

Порівняльна характеристика сучасних моделей національної оборони

Основні та *проміжні* **моделі оборони**	**Тип системи управління**	**Ресурси**	**Домени**	**Сильні сторони**	**Слабкі сторони**	**Впровадження**
Воєнно-стратегічна	Військове командування	Військові	Наземний Повітряний Морський	Високий рівень готовності	Висока вартість, обмежена стійкість	Європейські країни – члени НАТО
Всеохоплююча (Total Defence)	Військове командування	Військові Цивільні (по мобілізації)	Наземний Повітряний Морський Інформаційний Кібер	Зниження вартості, підвищення стійкості	Збільшення часу на приведення у вищі ступені готовності	Європейські країни, які не були членами НАТО
Цивільно-військова інтеграція (Civil-Military Integration)	Військове (стратегічний рівень) Інтегроване	Військові Цивільні	Наземний Повітряний Морський Інформаційний Кібер Космічний	Зниження вартості, підвищення стійкості та готовності	Складність управління і планування	США
Воєнно-цивільне об'єднання (Military-Civil Fusion)	Військове (стратегічний рівень) Об'єднане Цивільне	Військові Цивільні Приватні	Наземний Повітряний Морський Інформаційний Кібер Космічний Економічний Наукових досліджень	Висока стійкість, об'єднання ресурсів	Складність управління і планування	Китай
Комплексна (Comprehensive Defence)	Комбіноване мережецентричне	Військові Цивільні Територіальних громад Приватні	Усі	Доступ і управління всіма національними ресурсами	Висока складність системи управління і планування	На етапі впровадження США, Китай, Великобританія та інші

2.2. Моделі комплексної оборони (Comprehensive Defence)

На теперішній час жодна з країн світу не впровадила модель комплексної оборони в повному обсязі. Однак окремі країни, які мають геополітичні амбіції та потужні збройні сили, активно впроваджують проміжні моделі національної оборони, а саме: модель оборони на основі цивільно-військової інтеграції та модель оборони на основі військово-цивільного об'єднання.

2.2.1 Модель оборони на основі цивільно-військової інтеграції

Трансформація національної оборони США від стратегічної до комплексної моделі розпочалася в 1990-х роках із запровадження Концепції цивільно-військової інтеграції [20]. Мета концепції – об'єднання оборонної та комерційної технологічно-промислової баз та створення єдиної національної технологічно-промислової бази, яка передбачає спільне використання технологій, процесів та ресурсів

військового і цивільного секторів для забезпечення національної безпеки та економічної конкурентоспроможності. Проведена трансформація забезпечила зростання спроможностей комерційної промислової бази до рівня, який перевищував спроможності оборонно-промислової бази. У разі широкомасштабної війни і бойових дій високої інтенсивності спроможностей тільки оборонно-промислової бази було явно недостатньо.

По суті, цивільно-військова інтеграція – це багатогранна концепція, яка базується на сильних сторонах як військового, так і цивільного секторів для досягнення цілей національної оборони та забезпечення зростання економіки. Для успішного впровадження цієї концепції необхідно ретельне врахування правових, регуляторних, етичних та операційних проблем.

За останні 30 років США здійснили значну роботу в цьому напрямі та суттєво розширили кількість питань цивільно-військової інтеграції. Було проведено понад 6 000 різних конференцій, навчань і проєктів щодо теоретичного та практичного розвитку питань цивільно-військової інтеграції. Їх опис та аналіз виходять далеко за межі цієї статті. Як приклад, розглянемо один з останніх проєктів цивільно-військової інтеграції, особливо актуальних для України.

З 2022 р. Об'єднане управління боротьби з малими безпілотними літальними системами армії США (JCO) та аналітичний центр RAND Corporation провели шість воєнних ігор щодо вивчення питань захисту населених пунктів, об'єктів критичної інфраструктури та воєнних баз від застосування ударних дронів. Метою ігор був пошук креативних рішень підвищення ефективності збройних сил і національної гвардії у реагуванні на масовані атаки дронами. У навчаннях також досліджувалося як об'єднані військові служби та державні установи можуть максимізувати обмін даними та ситуаційну обізнаність, а також як результативно використовувати технології боротьби з дронами, такі як глушіння сигналів GPS та обмеження у роботі мобільного зв'язку та Інтернету.

У звіті RAND Corporation [21] зазначається, що ключовий висновок проведених навчань полягає в тому, що захист населених пунктів, об'єктів інфраструктури та внутрішніх воєнних баз не може бути виключно завданням військових. Крім того, на навчаннях підтверджені такі висновки:

результативність ідеї створення "груп для боротьби з дронами", які складаються з мобільних систем боротьби з безпілотниками та навченого персоналу, розгортаються за допомогою цивільних (державних і комерційних) ресурсів за потреби;

підвищення ефективності груп досягається їх підсиленням засобами глушіння, мікрохвильовою та лазерною зброєю, а також кінетичною зброєю, такою як кулемети;

у перспективі групи мають стати елементом системи багаторівневого захисту населених пунктів та об'єктів інфраструктури;

актуальність створення системи інтеграції, забезпечення та синхронізації заходів і дій державних, місцевих, територіальних органів влади та громад для протидії дронам у містах, на воєнних базах або поблизу них, однак це, зі свого боку, потребує вирішення низки юрисдикційних і комунікаційних питань;

визначена провідна роль Національної гвардії у захисті населених пунктів, об'єктів інфраструктури і воєнних баз від ударів дронами;

особливо цінними були б групи цивільної підтримки Національної гвардії, які доступні цілодобово, можуть бути розгорнуті протягом 90 хвилин і "мають достатні бюджети, які можуть компенсувати витрати на оснащення та навчання для операцій проти безпілотників".

2.2.2. Модель оборони на основі військово-цивільного об'єднання

Протягом десятиліть Китай готує своє суспільство до війни. За допомогою патріотичного виховання, ідеологічної дисципліни та механізмів соціального контролю Пекін виховав населення, привчене підтримувати державу у війні. З іншого боку, спроможності китайських збройних сил залежать від загальнонаціональної підтримки для швидкого розгортання і тривалого забезпечення. Китайські військові визнають, що сучасні конфлікти все більше стирають межу між військовими і цивільними, а взаємозв'язок між цивільною і військовою сферами стає особливо важливим. Стратегія Тайваню була протилежною: деполітизація, демілітаризація та сподівання на стримування через союзництво з іншими державами. Ця розбіжність може стати для Тайваню катастрофічною [22].

Ще за часів Мао Китай почав дублювати і впроваджувати окремі елементи американської моделі національної оборони

на основі цивільно-військової інтеграції. Перехід до моделі на основі військово-цивільного об'єднання (моделі MCF) підкреслює еволюцію стратегічних пріоритетів Китаю. Попередня "Ініціатива про воєнну модернізацію" (цивільно-військова інтеграція) була зосереджена на використанні оборонних підприємств для цивільних потреб. Модель MCF чітко визначила зворотне: використання комерційних технологічних досягнень для досягнення воєнних цілей.

У 2014 р. Сі Цзіньпін закладає модель MCF в основу національної стратегії безпеки [23]. У 2017 р. було поставлено нове завдання "сформувати поглиблену модель військово-цивільної об'єднання, побудувати інтегровану воєнно-цивільну стратегічну систему національної оборони та розвинути її спроможності", керуючись стратегічним мисленням та сприяючи поглибленому впровадженню стратегії MCF [24]. До моделі MCF включаються такі сфери, як будівництво, наука, освіта, виробництво зброї, соціалізація військової підтримки та мобілізація для національної оборони [25]. Сі закликає "розробити інтегровані національні стратегії та інтегровані стратегічні спроможності" [24]. Таким чином, "інтеграція національної оборони та воєнного будівництва в національну систему економічного та соціального розвитку" стала фундаментом китайської стратегії національної безпеки [26].

У 2021–2025 рр. у межах виконання завдань 14-го п'ятирічного циклу стратегічного планування детально визначаються процедури об'єднання військового і цивільного секторів для досягнення самодостатності та глибокого поєднання цивільних і військових ресурсів, як ключового компонента національної стратегії Китаю. У модель MCF включаються нові сфери: дослідження океану, аерокосмічна, кіберпростору, біології, нової енергетики, штучного інтелекту та квантової науки і технологій, упроваджується спільне використання ресурсів військових і цивільних науково-дослідних установ [27]. Як результат, оборонно-промислова база Китаю різко зростає. У звіті SIPRI щодо провідних компаній-виробників озброєння у світі зазначається, що три з десяти найкращих та шість з п'ятнадцяти найкращих – китайські [28]. Зростання та реформування оборонно-промислової бази є прямим результатом зусиль щодо впровадження моделі MCF протягом майже трьох десятиліть.

Модель MCF вважається ключовою концепцією для досягнення стратегічних цілей Китаю, швидкої модернізації збройних сил, реалізації "китайської мрії", досягнення самодостатності у виробництві оборонної продукції та утвердження китайської воєнної могутності на світовій арені [29].

2.2.3. Модель комплексної оборони Латвії

Латвія визначає свій підхід до оборони як комплексний [30] Модель комплексної оборони Латвії визначає такі складові: військовий потенціал, державно-приватне співробітництво, державну освіту, цивільну оборону, стратегічні комунікації, економічну стійкість, психологічну стійкість.

2.2.4. Модель колективної оборони НАТО

Лідери НАТО у Декларації Вашингтонського саміту 2024 р. [31] зобов'язались інтегрувати цивільне і оборонне планування, підвищити стійкість критично важливої інфраструктури та ланцюгів постачання.

3. Воєнно-цивільне об'єднання для протидії широкомасштабній агресії: український досвід

Стратегія воєнної безпеки України 2021 р. [32] вводить термін "всеохоплююча оборона України", як комплекс заходів, основний зміст яких полягає у:

превентивних діях і стійкому опорі агресору на суші, на морі та в повітряному просторі України, протидії в кіберпросторі та нав'язуванні своєї волі в інформаційному просторі;

використанні для відсічі агресії всього потенціалу держави та суспільства (воєнного, політичного, економічного, міжнародно-правового (дипломатичного), духовного, культурного тощо);

застосуванні всіх форм і способів збройної боротьби з агресором, зокрема асиметричних та інших дій для оборони України, з дотриманням принципів і норм міжнародного права.

Завчасно підготовлена та всебічно забезпечена всеохоплююча оборона України будується на засадах стримування, стійкості та взаємодії.

Широкомасштабна агресії росії проти України внесла суттєві зміни на погляди щодо оборони. У повному обсязі вплив російсько-української війни на об'єднання воєнних і цивільних спроможностей можливо повністю оцінити тільки після закінчення війни. Проте вже проглядається низка реалій, які

визначатимуть майбутню модель оборони України, організацію воєнно-промислового комплексу, структуру оборонних видатків, напрями подальшого розвитку Сил оборони України, розподіл відповідальності щодо завдань національної оборони між воєнним і цивільним секторами, структуру та чисельність Збройних Сил України й інше.

На сьогодні вже можливо визначити декілька напрямів успішного об'єднання воєнних і цивільних спроможностей. До них відносяться: виготовлення і модернізація безпілотних і безекіпажних бойових систем, розвідка, логістика.

Уряд України дозволив фінансувати цивільні компанії та постачати безпілотники безпосередньо в бригади Сил оборони. Це дало змогу підрозділам безпілотних систем спільно з розробниками тестувати нові вироби безпосередньо на полі бою. Станом на початок 2025 р. в Україні налічувалось понад 400 компаній, більшість із яких приватні, які виробляють різні безпілотники для Сил оборони. Об'єднання цивільних і військових спроможностей за цим напрямом дало змогу сформувати стійку, територіально розподілену мережу виробників безпілотних систем.

Провідні держави світу тривалий час були монополістами в галузі розвідки, використовуючи складні методи збору та аналізу. Бар'єри для входу були високими та потребували значних ресурсів на побудову супутникових мереж, розгортання мереж агентурної розвідки та впровадження спеціалізованих аналітичних спроможностей. На теперішній час державна монополія зникла, спроможності розвідки по відкритих джерелах (OSINT), які раніше потребували величезних державних інвестицій, доступні цивільному сектору і недержавним суб'єктам. Суб'єкти з меншими ресурсами можуть застосовувати складні розвідувальні спроможності без відповідної інституційної інфраструктури. Незалежні аналітики всі частіше демонструють спроможності, які конкурують з державними розвідувальними і аналітичними структурами. Воєнно-цивільне об'єднання у розвідці ґрунтується на трьох взаємопов'язаних трендах: технологічна доступність, методологічна прозорість і доступність аналітичних інструментів. Разом ці фактори перетворили спроможності, які колись потребували мільярдних державних інвестицій, на доступні опції для будь-якого мотивованого учасника OSINT-спільноти з доступом до Інтернету та певними аналітичними і технічними навичками.

Комерційні супутники Maxar, Planet та BlackSky надають знімки із субметровою роздільною здатністю і потребують мінімальних комерційних підписок для щоденного доступу. Колишня виключна перевага держав з космічними програмами нівельована, роздільна здатність та покриття комерційних супутників постійно покращується. Прозорість методології є не менш важливою. Методи, які колись ретельно охоронялися в розвідувальних службах, тепер відкрито викладаються на онлайн-курсах, навчальних посібниках на YouTube та у спеціалізованих Інтернет-спільнотах. Група DeepState, яка розробила власні методології з відкритим кодом для відстеження переміщення військ на полі бою, конкурує зі спроможностями державного сектору.

Дослідження RAND та Конгресу США показують, що невеликі групи OSINT можуть генерувати до 70–90 % аналітичної закритої інформації, працюючи приблизно за 2 % від вартості такої інформації від воєнної розвідки. Це співвідношення "витрати-результативність" досягає найбільшого значення за такими напрямами, як аналіз моделей оборони, прогнозування розвитку війни, документування воєнних злочинів, відстеження ухилення від санкцій. Ці функції є центральними в сучасних війнах.

Успіх Bellingcat як недержавної розвідувальної організації являє собою зміну парадигми проведення складного аналізу моделі оборони поза традиційними аналітичними структурами. Методологія Bellingcat демонструє, як мережеві підходи можуть замінити традиційні методи стратегічного аналізу. Замість формування комплексних власних спроможностей, Bellingcat використовує глобальну мережу учасників зі спеціалізованими навичками в таких галузях, як аналіз супутникових знімків, ідентифікація озброєння, візуалізація даних та регіональна воєнно-політична обстановка. Мережева модель, де спроможності формуються завдяки горизонтальним зв'язкам, а не централізації, створює організаційну стійкість та аналітичну глибину, що перевищує те, чого могли б досягти традиційні державні аналітичні структури.

Для побудови результативної моделі оборони мережева структура створює безпрецедентні стратегічні спроможності. Отримана внаслідок упровадження мережевої структури асиметрія фундаментально впливає на модель оборони, зменшує інформаційні переваги супротивника.

Актуальність забезпечення адекватної логістики ставить питання, як доставляти критично важливі вантажі в район активних бойових дій. Забезпечення Сил оборони спроможностями і потенціалом для швидкого транспортування боєприпасів, палива і постачання до міста призначення має вирішальне значення для організації протидії агресору. Оскільки попередні документи стратегічного планування не зосереджуються на транспортних можливостях (хоча і є окремі згадки), проблема існує. Сили оборони стикаються з обмеженнями у швидкому перекиданні вантажів і особового складу по території країни на постійній основі в зоні інтенсивних бойових дій. Для заповнення дефіциту широко використовуються цивільні транспортні засоби. Водночас, їх застосування в прифронтових районах ускладнено через юридично-правові та безпекові причини.

4. Проблемні питання впровадження нової моделі національної оборони

Воєнно-політичне керівництво та громадські діячі України все частіше звертаються до наративу, що надійну національну безпеку і оборону можуть забезпечити тільки Збройні Сили України та український народ. Разом з тим, економічні обмеження внаслідок тривалої війни, значні витрати на відновлення країни, виробництво та придбання озброєння і військової техніки, соціальну підтримку ветеранів та інвалідів російсько-української війни навряд чи забезпечать можливість утримання поточної чисельності Збройних Сил України. За таких умов особливу актуальним є обґрунтування та впровадження результативної моделі оборони України. З об'єктивних причин жодна з розглянутих вище моделей національної оборони не може бути застосована в Україні. Постає проблема теоретичного обґрунтування нових засад і складових сучасної моделі оборони України. До нової моделі оборони доцільно включити такі елементи, як стримування, національна стійкість, національний спротив, територіальна оборона, міжнародне співробітництво (постійні та тимчасові альянси з питань безпеки і оборони, двостороннє співробітництво), цивільна оборона включно з протидроновим захистом, інформаційна та кібербезпека, органи управління активним резервом та організації призову, управління державними і приватними ресурсами в особливий період, підготовка і безпека критичної та цивільної інфраструктури. В основу нової моделі оборони пропонується включити цивільно-військове об'єднання. Необхідно врахувати історичний досвід українського народу: організацію життя і ведення війни Запорізької Січі (др. пол. XVI – кінець XVIII ст.), військових поселень півдня України (1817–1857 рр.). Окремі елементи досвіду СРСР з управління воєнними і цивільними секторами з одного центру, підготовці цивільної інфраструктури і населення до війни, з урахуванням змін у характері війни, також можуть стати корисними.

Низка великих українських міст (Харків, Суми, Запоріжжя, Херсон) знаходяться в ближній зоні до тимчасово окупованих територій. Організувати їх повноцінне функціонування можливо буде тільки на основі постійного об'єднання цивільних і військових спроможностей на постійні основі. Україна не зможе підтримувати чисельні збройні сили, однак наявність значного, чисельністю 1–2 млн осіб оперативного високопідготовленого і оснащеного резерву стане суттєвим аргументом стримування агресора.

Необхідно переглянути процеси стратегічного і оборонного планування. Американська система PPBSE, яка покладена в основу системи стратегічного і оборонного планування в Україні, безумовно, відіграла свою роль. Однак це розробка 60-х років минулого століття, яка була замовлена і реалізована після того, як США програли війну у В'єтнамі. Сучасні війни мають вже зовсім інший характер.

На жаль, планування на основі спроможностей унаслідок своєї складності та орієнтації певним чином на експедиційні сили, не знайшло практичного розповсюдження. У разі необхідності врахування під час планування оборони цивільних спроможностей і ресурсів ця система стане ще складніше і її результативність буде знижена. У процесі розроблення сучасної моделі оборони потрібен пошук інших, більш об'єктивних і зрозумілих показників.

Висновки. Отже, розроблення сучасної результативної моделі національної оборони України є міждисциплінарною, комплексною проблемою. Як попередній варіант, можлива комбінація окремих елементів з апробованих моделей оборони інших країн. Однак зрештою Україна змушена буде пройти власний шлях через спроби та помилки під час розроблення моделі та становлення сучасної оборони. Але перед цим необхідно знайти відповіді на

проблемні питання, поставленні авторами вище, та врахувати наведені рекомендації.

У подальшому передбачається на основі методів стратегічного аналізу та оцінювання політичної, воєнної, економічної, соціальної, інформаційної та інфраструктурної складових, безпекового середовища та часу (метод PMESII-PT) надати порівняльні оцінки результативності моделей національної оборони.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Іващенко А. М., Уварова Т. В. Адаптація воєнної стратегії: приклади російсько-української війни // Теоретико-прикладні аспекти російсько-української війни: всеохоплююча оборона, розвиток та посилення спроможностей : монографія / колектив авторів ; за заг.ред. М. В. Коваля. Київ : НУОУ, 2025. С. 36–44.
2. Ouellet E., D'Agata M., Stewart K. Deterrence in the 21st Century: Statecraft in the Information Age (Beyond Boundaries). Alberta, Calgary : University of Calgary Press, 2024. 400 p.
3. John Lewis Gaddis J. L. On Grand Strategy. London : Pengion Press, 2018. 384 p.
4. Ryan M. War Transformed: The Future of Twenty-First-Century Great Power Competition and Conflict Hardcover. Annapolis, Maryland : Naval Institute Press, 2022. 312 p.
5. Berzina I. From 'total' to 'comprehensive' national defence: the development of the concept in Europe // Journal on Baltic Security. 2020. Vol. 6, No. 2. P. 1–9.
6. Liwang H., Andersson K. E., Bang M., Malmio I., Tarnholm T. How can systemic perspectives on defence capability development be strengthened? // Defence Studies. 2023. Vol. 23, No. 3. P. 399–420.
7. Berzins J. Latvia: From Total Defense to Comprehensive Defense // Prism: a Journal of the Center for Complex Operations. 2023. Vol. 10, No. 2. P. 38–53.
8. Райтасало Ю. Фінський захист. Ліворуч від вибуху // Призма: журнал Центру складних операцій. 2023. Т. 10, Вип. 2. С. 78–91.
9. Koval M., Ivashchenko A., Telelym V. Hybrid warfare: strategies and countermeasures // Theoretical and applied aspects of the rssian-ukrainian war: hybrid aggression and national resilience : monograph / M. Koval and others. Kharkiv: Technology Center PC, 2023. P. 4–19. ISBN 978-617-7319.
10. Rogulis D. From rhetoric to reality: Lithuania's total defence response to russian threats // Baltic Journal of Law & Politics. 2023. Vol. 16, No. 2. P. 176–193.
11. Bindu G., Jash A. China's Shift from CMI to MCF: Military Modernization and the Defense Industry at the Core Taipei // Issues and Studies. 2024. Vol. 60, No. 3. P. 1–30.
12. Liwång H. Future National Energy Systems, Energy Security and Comprehensive National Defence. *Energies*. 2023. Vol. 16, 6627. DOI: https://doi.org/10.3390/en16186627.
13. Dupuy T. N. Understanding War: History of Theory of Combat. Barnsley, South Yorkshire, England : Leo Cooper/Pen & Sword Books Ltd., 1992. 312 p. ISBN 10: 0850522935 / ISBN 13: 9780850522938.
14. Про національну безпеку України : Закон України від 21.06.2018 № 2469-VIII : станом на 21.08.2025.
15. Marczuk K. P. Obrona totalna // Leksykon bezpieczeństwa wewnętrznego / W. Fehler, J. Piątek, R. Podgórzańska (eds). Szczecin, 2017. P. 340–341.
16. Lindgren F., Odlund A. Total Defence at the Crossroads : Offprint from Strategic Outlook 7. November 2017. URL: https://sldinfo.com/wp-content/uploads/2018/12/http___webbrapp.ptn_.foi_.se_pdf_cb1cc21f-26c9-4738-a70f-9c81b92c0744.pdf (дата звернення: 25.08.2025).
17. The Military Strategy of the Republic of Lithuania : Approved by the Order No. V-252 of the Minister of National Defence of the Republic of Lithuania, 17 March 2016. URL: http://mepoforum.sk/wp-content/uploads/2018/04/Military-Strategy-Lithuania-20l6.pdf (дата звернення: 25.08.2025).
18. Basic National Defence Documents. The Republic of Estonia, Ministry of Defense. URL: https://www.kaitseministeerium.ee/en/objectives-activities/basic-national-defence-documents (дата звернення: 25.08.2025).
19. What Is Total Defence?. A Singapore Government Agency, 2021. URL: https://www.mindef.gov.sg/oms/imindef/mindef_websites/topics/totaldefence/about.html (дата звернення: 26.08.2025).
20. U.S. Congress. Assessing the Potential for Civil-Military Integration: Technologies, Processes, and Practices. OTA-ISS-611. Washington, D.C.:U.S. Government Printing Office, September 1994.
21. Peck M. These wargames explored drone attacks on US military bases. *Defense News*. Jul 25, 2025. URL: https://www.defensenews.com/unmanned/2025/07/25/these-wargames-explored-drone-attacks-on-us-military-bases/ (дата звернення: 26.00.2025).
22. Burtsev D., Golod V. Taiwan's Civil Society Is Not Ready for War. Ukraine's civil society was well-prepared, psychologically and practically, for Russia's invasion. Taiwan's is not. *The Diplomat*. August 04, 2025. URL: https://thediplomat.com/2025/08/taiwans-civil-society-is-not-ready-for-war/ (дата звернення: 26.08.2025).
23. Xi J. (2017, November 3). Full text of Xi Jinping's report at 19th CPC National Congress. Xinhuanet. URL: http://www.xinhuanet.com/english/special/2017-11/03/c_136725942.htm (дата звернення: 27.08.2025).
24. Kaichuang xinshidai junmin ronghe shendu fazhan xinjumian [Ff €] #7 FRE RAR SRE 46 J&# Æ a, Create a new situation in the new era of in-depth development of militarycivilian integration]. (2018). Xinhuawang [#7 3 49, Xinhuanet]. URL: http://www.xinhuanet.com/politics/2018-07/16/c_1123133733.htm (дата звернення: 27.08.2025).

25. Wang L. [E 381. (2017, November 21). Tuidong junmin ronghe shendu fazhan (shenru xuexi guanche Xi Jinping xinshidai Zhongguo tese shehuizhuyi sixiang) [38 $y € KARAR BEER GRAF ERBEN PERE FELEO), Indepth study and implementation of Xi Jinping Thought on socialism with Chinese characteristics for a new era and promote the in-depth development of military-civilian integration]. Renmin Ribao [AR B#k, Peoples Daily]. URL: http:/www.taiwan.cn/lilunpindao/lists/201711/12017 1121 11869550.htm (дата звернення: 27.08.2025).
26. People's Government of Fujian Province. (2021, August 9). Outline of the 14th Five-Year Plan (2021–2025) for national economic and social development and Vision 2035 of the Peoples Republic of China. URL: https://www.fujian.gov.cn/ english/news/ 202108/1202108095665713.htm (дата звернення: 28.08.2025).
27. Pollpeter K., Allen K. W. (Eds.). (2012, June 14). The PLA as organization v2.0. China Aerospace Studies Institute. URL: https://apps.dtic.mil/sti/ citations/AD1082742 (дата звернення: 28.08.2025).
28. SIPRI Yearbook 2024 Armament, Disarmament and International Security. Stockholm : Oxford Press, 2024. 768 p.
29. How China Fights in Large-Scale Combat Operations. U.S. Army's Training and Doctrine Command (TRADOC), 2025 URL: https://www.army.mil/article/285395/ how_china_ fights_in_large_scale_combat_operations (дата звернення: 28.08.2025).
30. Comprehensive National Defence in Latvia, Ministry of Defense, 2019. URL: https://www.mod.gov.lv/sites/mod/files/document/ Comprehensive%20National%20Defence%20in% (дата звернення: 28.08.2025).
31. Декларація Вашингтонського саміту видана главами держав і урядів, які взяли участь у засіданні Північноатлантичної ради у Вашингтоні, округ Колумбія, 10 липня 2024 р. URL: nato.int/cps/uk/natohq/official_texts_ 22768.htm (дата звернення: 28.08.2025).
32. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року "Про Стратегію воєнної безпеки України" : Указ Президента України від 25.03.2021 № 121/2021.

Стаття надійшла до редакції 10.09.2025

From Total to Comprehensive Defence: Searching for a Model for Ukraine

Annotation

Ukraine cannot afford a classic, costly model of strategic defence, where the full cycle of strategic planning – from strategy to armaments and resources – takes years. This creates conditions for the development of a unique model of national defence for Ukraine, one that is based not on existing military capabilities and resources, but on innovation and the widespread use of civilian resources and technologies in combat logic.

The article examines models of national defence from the end of World War II to the Russian Federation's war against Ukraine. It considers the gradual development of national defence models, taking into account the security environment that has existed since February 2022, and the practical aspects of implementing these models.

The study focuses on a comparative analysis of models and decisions adopted in the field of defence in different countries around the world. The study uses publicly available documents that define policies, strategies, concepts, and models of defence in the context of countering a superior enemy. The figures and trends related to the justification of the defence model are taken from open official sources. Analytical reports from foreign research centers on security and defence issues confirm the reliability of the results obtained and reinforce the argumentation.

The development of a modern and effective model of national defence for Ukraine is an interdisciplinary and complex problem. As a preliminary option, it is possible to combine individual elements from proven defence models of other countries. However, in the end, Ukraine will have to go its own way through trial and error in developing a model and establishing a modern defence. But before that, it is necessary to find answers to the problematic questions posed by the authors above and take into account the recommendations provided.

Keywords: national defence; defence model; transitional defence model; Strategic Defence; Total Defence; Civil-Military Integration (CMI); Military-Civil Fusion (MCF); Comprehensive Defence; Integrated Defence System.

УДК 623.365 093 531 53 14 https://doi.org/10.33099/2304-2745/2025-3-86/17-23

Нижник Я. В. (0009-0000-2431-3309)
Журахов О. В. (0000-0003-4547-1546)
Захарченко Д. С. (0000-0003-3009-5648)

Центр протимінної діяльності Державної спеціальної служби транспорту, Чернігів

Обґрунтування вибору безпілотного роботизованого комплексу розмінування шляхом визначення рівня технічної досконалості

Резюме. Розглянуто мету національної стратегії протимінної діяльності, а саме звільнення територій від ризиків, пов'язаних із наявністю вибухонебезпечних предметів. Одним з підходів для досягнення мети є використання безпілотних роботизованих комплексів для технічного обстеження та очищення територій, забруднених вибухонебезпечними предметами. В умовах відсутності державного стандарту та загальних вимог (кількісних показників) для безпілотного роботизованого комплексу виникає питання оцінювання рівня їх технічної досконалості. Запропоновано методику та проведено оцінку рівня технічної досконалості зразків безпілотних роботизованих комплексів.

Ключові слова: безпілотний роботизований комплекс; технічна досконаліть; протимінна діяльність; розмінування.

Постановка проблеми. Для досягнення стратегічної мети національної стратегії протимінної діяльності [1], а саме звільнення територій від ризиків, пов'язаних із наявністю вибухонебезпечних предметів (далі – ВНП), для їх безпечного та продуктивного використання передбачено, зокрема, створення сприятливого середовища для впровадження інновацій у сфері протимінної діяльності, а також розвиток національного виробництва засобів для розмінування та їхнього технічного обслуговування в Україні. Ці аспекти підкреслюють складність глобальної проблеми розмінування та нагальну потребу в інноваційних підходах до її розв'язання.

Одним із таких підходів є застосування безпілотних роботизованих комплексів (далі – БРК) для технічного обстеження та очищення територій, забруднених ВНП. Використання різних конфігурацій навісного обладнання та датчиків у складі БРК дає змогу значно прискорити процес розмінування. Продуктивність наземних машин для розмінування, зазвичай, становить від 3000 м² до 15000 м² на добу [2], тоді як ручне розмінування одним сапером обмежується не більше ніж 10 м² за той самий період.

Забезпечення безпеки персоналу є ключовим аспектом проведення робіт з розмінування. Важливою перевагою використання БРК є можливість дистанційного керування, що мінімізує ризики для фахівців з розмінування, переміщуючи їх на безпечну відстань від зони ураження [3].

Нині існує гостра потреба у створенні методики для визначення технічної досконалості БРК для найбільш ефективного виконання поставлених завдань підрозділами з розмінування в завчасно визначених умовах.

Аналіз останніх досліджень та публікацій. *Технічна досконаліть БРК* – це сукупність його властивостей і характеристик, які визначають, наскільки ефективно, надійно та безпечно він виконує свої функції. Це міра того, наскільки БРК відповідає сучасним інженерним стандартам і вимогам експлуатації.

Наразі існує значна кількість робіт, присвячених оцінюванню рівня технічної досконалості зразків озброєння та військової техніки.

У роботі [4] розглянуто питання щодо вибору рівня технічної досконалості і характеристик перспективних однотипних зразків озброєння та військової техніки на прикладі зразків броньованих ремонтно-евакуаційних машин (далі – БРЕМ). Побудовані залежності:

коефіцієнта рівня технічної досконалості від суми балів існуючого зразка БРЕМ, яка дає змогу оцінити загальну суму балів для перспективного зразка вищого рівня технічної досконалості;

кількості балів від параметра показника існуючого БРЕМ, яка дає змогу вибрати параметри та технічні характеристики перспективного технічно досконалого зразка.

Запропоновано алгоритм вибору рівня технічної досконалості і характеристик перспективного зразка озброєння та військової техніки (далі – ОВТ),

впровадження якого дсть змогу визначити напрями розроблення нових та модернізації існуючих зразків ОВТ з метою підвищення рівня їхньої технічної досконалості.

У роботі [5] розглянуто методику комплексної порівняльної оцінки тактико-технічних показників однотипних зразків озброєння та військової техніки шляхом введення нового узагальненого показника з використанням методів кваліметрії, порівняльного аналізу та експертної оцінки.

У роботі [6] проведено оцінку рівня технічної досконалості вітчизняних легких броньованих автомобілів із найкращими однотипними закордонними зразками. Наведено порівняльний аналіз за оцінкою рівня технічної досконалості однотипних зразків озброєння та військової техніки.

У патенті [7] наведено спосіб оцінки рівня технічної досконалості однотипних зразків озброєння і військової техніки, який полягає у визначенні комплексного показника. За комплексний показник було вибрано суму добутків балів технічних і тактико-технічних характеристик, отриманих за пропорційною шкалою оцінок, на коефіцієнт вагомості технічних і тактико-технічних характеристик однотипних зразків озброєння і військової техніки.

На сьогодні відсутня методика визначення рівня технічної досконалості для обґрунтування вибору безпілотного роботизованого комплексу розмінування. Ураховуючи досить велику номенклатуру БРК українського та іноземного виробництва запропонована методика надасть можливість комплексно порівняти технічні характеристики зразків для виконання поставлених завдань у заданих умовах використання.

Метою статті є висвітлення методики визначення рівня технічної досконалості БРК та її застосування для найбільш розповсюджених зразків БРК легкого та середнього класів. Ця методика дає змогу вдосконалити інформаційне забезпечення підрозділів розмінування в частині застосування інноваційних технологій пошуку, виявлення, ідентифікації та знищення (знешкодження) ВНП шляхом розроблення науково обґрунтованих рекомендацій щодо впровадження сучасних технологій роботизації у сферу гуманітарного та оперативного розмінування.

Виклад основного матеріалу. В умовах відсутності державного стандарту та загальних вимог (кількісних показників) для БРК виникає питання оцінки рівня їх технічної досконалості.

Ураховуючи досить велику номенклатуру БРК іноземного виробництва, оцінка рівня технічної досконалості вітчизняних зразків може проводитись методом експертних оцінок, порівняльного аналізу, прогресуючого еталону, визначення технічної досконалості тощо.

За рахунок покращення технічних характеристик зразка можна підвищити рівень його технічної досконалості.

Для вибору рівня технічної досконалості та показників технічних характеристик перспективного зразка пропонується такий алгоритм:

а) вибрати показники технічних характеристик, які визначають обрис і вимоги та забезпечують найбільш ефективне застосування зразка;

б) перевести значення одиниць вимірювання показників у бали за допомогою пропорційної шкали оцінок;

в) визначити загальну суму балів, коефіцієнт рівня технічної досконалості існуючого зразка.

У перспективі цей підхід забезпечить можливість обрати технічні характеристики, які дадуть змогу покращити техніко-економічну спроможність зразка для виконання поставлених завдань.

Серед загальних вимог до проведення випробувань та визначення необхідного переліку технічних характеристик зразка, для подальшого визначення рівня та перспектив покращення технічної досконалості зразка слід відмітити такі:

а) оцінка обґрунтованості призначення необхідної точності та достовірності визначення характеристик зразків;

б) оцінка обґрунтованості та достатності вибору складу контрольованих при випробуваннях параметрів для визначення характеристик зразків;

в) перевірка відповідності заданої точності вимірювань для визначення характеристик зразків;

г) оцінка методик (методів) вимірювань на можливість забезпечення необхідної точності вимірювань характеристик зразків;

ґ) оцінка обґрунтованості вибору та створення засобів і систем вимірювань та контролю для випробувань;

д) оцінка відповідності забезпечуваної методиками випробувань достовірності контролю характеристик зразків заданим вимогам;

е) оцінка методик визначення фактичної точності результатів випробувань зразків з урахуванням сумарної похибки вимірювань, передавання та обробки вимірювальної інформації;

є) оцінка відповідності фактичної точності результатів вимірювань і обробки вимірювальної інформації заданим вимогам;

ж) контроль виконання вимог державних стандартів та інших нормативних документів за формами представлення результатів вимірювань;

з) контроль включення в програму випробувань вимог з підготовки і реалізації заходів з метрологічного забезпечення випробувань;

и) контроль виконання заданих у тактико-технічному завданні вимог з метрологічного забезпечення випробувань;

і) контроль виконання вимог нормативних документів щодо метрологічного забезпечення випробувань.

Як показав проведений аналіз, загальний методичний підхід щодо досліджень з визначення відповідності зразків вимогам нормативних документів має включати такі етапи:

Перший етап – оцінка технічного стану зразка: визначення необхідності проведення повноцінних випробувань. Етап включає роботи з контрольного огляду, який передбачений експлуатаційно-технічною документацією. При цьому визначаються умови експлуатації, робочі процедури, характерні дефекти та несправності, можливість їх усунення. Можуть підтвердити результати попередніх випробувань.

Другий етап – лабораторні випробування, які проводяться в контрольованих умовах з метою усунення негативних впливів зовнішніх факторів;

Третій етап – аналіз результатів досліджень, відпрацювання звітної документації та проєктів директивних документів.

Причинами виникнення невідповідності вимірювань можуть бути: недосконаліть методів вимірювання, технічних засобів, зміна умов проведення досліджень. Зміна умов проведення досліджень може впливати на фізичну величину, технічні засоби і самого випробувача.

Кожна з наведених причин виникнення невідповідності вимірювань зумовлена багатьма чинниками, під впливом яких формується загальна невідповідність. Їх можна об'єднати у дві великі групи:

1. Чинники, що з'являються нерегулярно і зникають несподівано або проявляються з непередбачуваною інтенсивністю. До них належать: перекоси елементів приладів за їх напрямними, нерегулярні зміни моментів в опорах, зміна зовнішніх умов та умов навколишнього середовища, послаблення уваги спостерігача тощо. Складова сумарної невідповідності, яка виникає під впливом цих чинників, – випадкова невідповідність вимірювань.

2. Постійні чинники або такі, що закономірно змінюються у процесі вимірювання фізичної величини. До них належать методичні похибки, зміщення стрілки приладу та недосконаліть елементів (пружних) засобів вимірювання. Складові сумарної невідповідності, що виникають під дією чинників другої групи, – систематична невідповідність вимірювань [8].

Використовуючи метод оцінки рівня технічної досконалості, методика якого запропонована у [7, 9], проведено вибір показників технічних характеристик машин для розмінування, які визначають обрис і вимоги, забезпечують найбільш ефективне її застосування і є вихідними для визначення комплексного показника рівня технічної досконалості. Для забезпечення наочності та систематизованої обробки дані заносяться до Табл. 1.

Для переведення значення параметрів технічних характеристик різних одиниць вимірювання в бали використовують пропорційну шкалу оцінок. Кількість балів $O_{бал}$ розраховується за формулою [7]

$$O_{бал} = \left(\frac{X_{оцін} - X_{мін}}{X_{макс} - X_{мін}} \right) \cdot 100, \quad (1)$$

де $X_{оцін}$, $X_{макс}$, $X_{мін}$ – оцінене, максимальне та мінімальне значення характеристик у групі [5].

З Табл. 1 витікає, наприклад, що $X_{мін}$ для характеристики "робоча глибина обробки залежно від місцевості" складає 15 см (тип машини "Змій") та $X_{макс}$ – 32 см (тип машини "MV-4"). Аналогічно визначаються кількісні значення показників $X_{мін}$ та $X_{макс}$ для інших характеристик групи.

Результати переведення значень параметрів технічних характеристик в бали за формулою (1) наведені у Табл. 2.

Таблиця 1

Значення технічних характеристик показників технічної досконалості безпілотних роботизованих комплексів [10]

№ з/п	Тип машини	Робоча глибина обробки в залежності від місцевості, см	Продуктивність, м²/год. Легкий грунт / середня рослинність	Продуктивність, м²/год. Середній грунт / середня рослинність	Продуктивність, м²/год. Важкий грунт / густа рослинність	Очищення / Ширина обробки, см	Максимальна операційна швидкість руху, км/год	Максимальна дальність керування, м
		1	2	3	4	5	6	7
Легкі машини								
1	MV-4 (ціпи)	До 32	2184	1896	944	173	1,26	1500
2	Twin 75V2	До 18	1350	1165	583	135	3	200
3	Змій	До 15	1028	947	809	135	0,75	1000
Середні машини								
1	GCS-200	До 25	2000	1270	920	200	2,3	1000
2	MV-10 Bison	До 40	4000	2460	1875	245	3	1500
3	Bozena 5	До 50	4900	2400	1050	265	4	5000
4	Armtrac 400	До 35	5000	2350	1915	290	3	800
5	MP.5100	До 30	4200	2040	1580	250	1,5	650

Таблиця 2

Оцінка показників технічної досконалості однотипних машин

№ з/п	Тип машини	Номер показника							Сума балів $\sum$	$K_{ТД}$
		1	2	3	4	5	6	7		
Легкі машини										
1	MV-4 (ціпи)	100	100	100	100	100	22,7	100	622,7	0,89
2	Twin 75V2	17,6	27,9	23	0	0	100	0	168,5	0,24
3	Змій	0	0	0	62,6	0	0	61,5	124,1	0,18
Середні машини										
1	GCS-200	0,0	0,0	0,0	0,0	0,0	32,0	8,0	40,0	0,06
2	MV-10 Bison	60,0	66,7	100,0	96,0	50,0	60,0	19,5	452,2	0,65
3	Bozena 5	100,0	96,7	95,0	13,1	72,2	100,0	100,0	576,9	0,82
4	Armtrac 400	40,0	100,0	90,8	100,0	100,0	60,0	3,4	494,2	0,71
5	MP.5100	20,0	73,3	64,7	66,3	55,6	0,0	0,0	279,9	0,40

Слід зазначити, що перетворення (1) дало змогу привести показники, які наведені у Табл. 1 до єдиної шкали, тобто максимальне кількісне значення показника кожної характеристики $a_{макс}$ дорівнює 100 балам.

Кількісне значення відносної характеристики якості зразка – коефіцієнт рівня технічної досконалості *j*-го зразка $K_{ТД_j}$ – наведено в останньому стовпчику Табл. 2. $K_{ТД_j}$ визначається за формулою

$$K_{ТД_j} = \frac{\sum_{i=1}^{I} a_i}{a_{макс} \cdot I}, \quad (2)$$

де a_i – кількісне значення показника *i*-ї характеристики у балах;

I – кількість показників, які досліджуються (у нашому випадку $I = 7$);

$a_{макс} = 100$ – максимальна кількість балів, яку може набрати показник.

Для прикладу наведемо розрахунки $K_{ТД}$ за формулою (2) для:

легкої машини MV-4: $K_{ТД_1} = \frac{6 \cdot 100 + 22,7}{100 \cdot 7} = 0,89$;

Twin 75V2: $K_{ТД_2} = \frac{17,6 + 27,9 + 23 + 100}{100 \cdot 7} = 0,24$.

Оскільки шкала оцінок пропорційна, то її можна розбити на рівні за балами. У відповідності з балами визначено коефіцієнт градації і рівень технічної досконалості однотипних зразків машин для розмінування (Табл. 3) [5].

Таблиця 3

Градація порівняльного рівня технічної досконалості безпілотних роботизованих комплексів для розмінування

Значення коефіцієнта	Сума балів	Рівень технічної досконалості	Тип машини
0,8-0,99	560-700	Високий	MV-4 Bozena 5
0,70-0,79	490-560	Відмінний	Armtrac 400
0,50-0,69	350-490	Добрий	MV-10 Bison
0,31-0,49	210-350	Середній	MP.5100
0,16-0,30	105-210	Задовільний	Змій Twin 75V2
≤ 0,15	< 105	Незадовільний	GCS-200

Як видно з Табл. 3, незадовільний рівень досконалості за оцінюваними показниками має БРК для розмінування GCS-200, відмінний рівень – Armtrac 400, високий рівень – MV-4 та Bozena 5.

Для проведення цього аналізу були застосовані не всі показники, які характеризують ефективність роботи машини, тому перелік як показників, так і зразків машин може бути розширений для більш детального визначення рівня технічної досконалості.

Для проведення графічного аналізу показників технічної досконалості були використані стовпчасті гістограми (рис. 1).

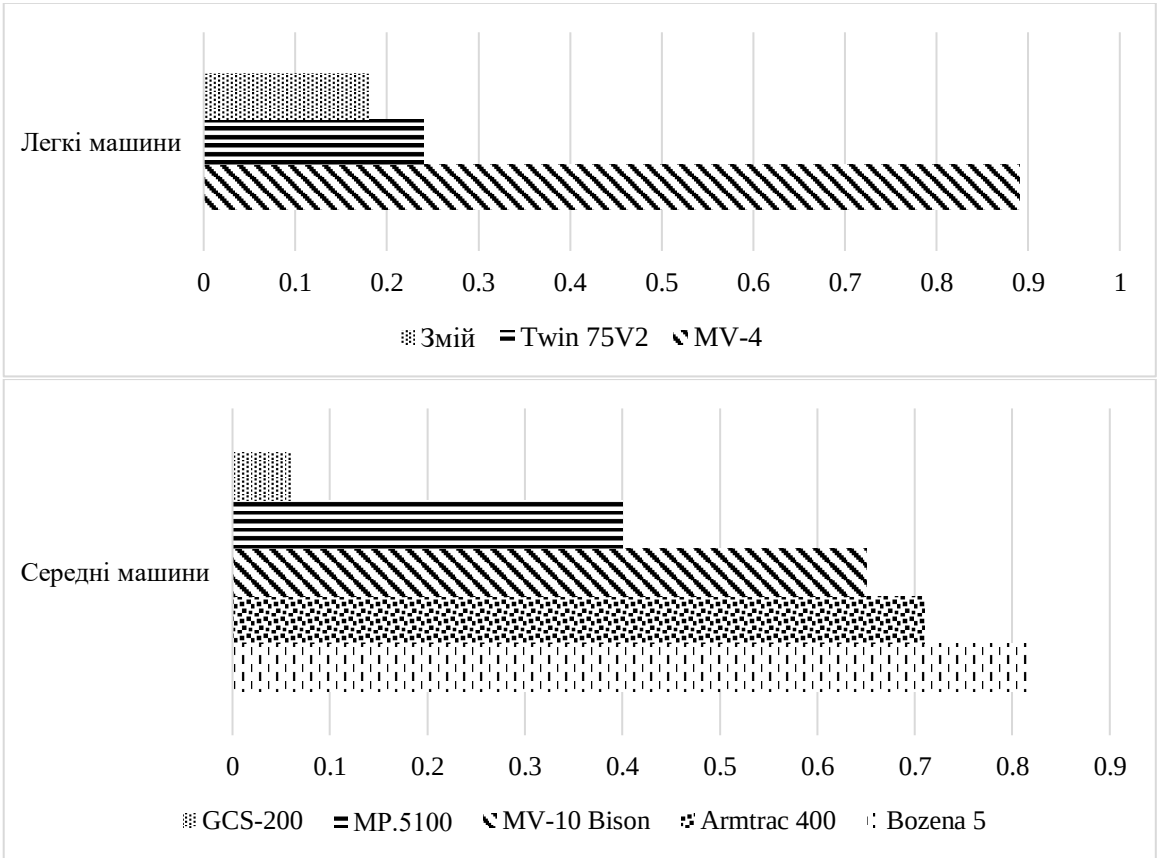

Рис. 1. Гістограми показників досконалості безпілотних роботизованих комплексів

Описану методику також можна використовувати для розрахунку як для безпілотних літальних апаратів, так і для підводних роботизованих комплексів, змінюючи відповідні тактико-технічні характеристики, що аналізуються.

За результатами аналізу можуть бути надані практичні рекомендації щодо параметрів технічних характеристик перспективного (модернізованого) технічно досконалого зразка машини для розмінування, що дасть змогу визначити напрями розроблення нових і модернізації існуючих зразків з метою підвищення рівня їхньої технічної досконалості .

Висновки. Враховуючи доцільність та необхідність дослідження і відбору найбільш пристосованих зразків безпілотних роботизованих комплексів для розмінування, запропонована та описана методика

визначення показника технічної досконалості вказаних комплексів. Запропонований набір параметрів, найбільш актуальних при використанні безпілотних роботизованих комплексів. Запропонована за застосована градація порівняльного рівня технічної досконалості для безпілотних роботизованих комплексів. Визначені технічно найдосконаліші представники легкого та середнього класів безпілотних роботизованих комплексів для розмінування за сукупністю розглянутих параметрів. За результатами визначення рівня технічної досконалості складена порівняльна графічна гістограма.

Напрями подальших досліджень. Запропонована методика оцінки рівня технічної досконалості безпілотних роботизованих комплексів має перспективи до подальших досліджень. Одним з таких напрямів є введення додаткових параметрів та характеристик комплексів, що аналізуються, при розширенні вимог до умов використання даних комплексів, а також цілей, які перед ними ставляться. Також цю методику можна розширювати у напрямі дослідження рівня технічної досконалості для машин і механізмів, призначених для виконання інших завдань оборонного та гуманітарного призначення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Уряд схвалив Національну стратегію протимінної діяльності та Операційний план її реалізації на перші 3 роки. URL: https://www.kmu.gov.ua/news/uriad-skhvalyv-natsionalnu-stratehiiu-protyminnoi-diialnosti-ta-operatsiinyi-plan-ii-realizatsii-na-pershi-3-roky (дата звернення: 24.03.2025).
2. A Handbook of Mechanical Demining. GICHD, Geneva, July 2010. URL: https://www.gichd.org (дата звернення: 24.03.2025).
3. Удосконалення методичного апарату експериментальних досліджень обладнання та засобів захисту у сфері протимінної діяльності, шифр “Основа” : звіт про НДР (ост.) / Центр протимінної діяльності ; наук. керівн. І. М. Лаппо ; відп. викон. О. В. Журахов. Чернігів, 2023. 242 с.
4. Русіло П. О., Костюк В. В., Варванець Ю. В., Калінін О. М., Шевцов М. М. Вибір рівня технічної досконалості і технічних характеристик перспективного зразка озброєння та військової техніки (на прикладі зразків броньованих ремонтно-евакуаційних машин) // Військово-технічний збірник. 2017. Вип. 16. С. 48–53.
5. Нор П. І., Борохвостов І. В. Методика комплексної порівняльної оцінки зразків озброєння та військової техніки // Озброєння та військова техніка. 2016. Вип. 3 (11). С. 14–19.
6. Будяну Р. Г. Обґрунтування тактико-технічних вимог для розроблення перспективних зразків і подальшої модернізації вітчизняних “легких” броньованих автомобілів // Науковий вісник НЛТУ України. 2015. Вип. 25.3 С. 156–165.
7. Спосіб оцінювання рівня технічної досконалості однотипних зразків озброєння та військової техніки : патент на корисну модель 88195 Україна : МПК G01N 27/27 (2006.01). № 201308548; заявл. 08.07.2013; опубл. 11.03.2014, Бюл. № 5. 5 с.
8. Метрологія, стандартизація та управління якістю / Л. П. Клименко та ін. Миколаїв : ЧДУ ім. Петра Могили, 2011. 207 с.
9. Машина інженерної розвідки та розмінування : патент на корисну модель 84430 Україна : МПК (2011.01) F41H 11/12. № 201303522; заявл. 22.03.2013; опубл. 25.10.2013, Бюл. № 20. 8 с.
10. K. Koppetsch. Mechanical Demining Equipment Catalogue 2010, GICHD, Geneva, January 2010. URL: https://www.gichd.org/ (дата звернення: 24.03.2025).

Стаття надійшла до редакції 02.09.2025

Justification for the selection of an unmanned robotic demining complex by determining the level of technical perfection

Annotation

To achieve the strategic goal of the national mine action strategy, namely to free territories from the risks associated with the presence of explosive objects (EO), their safe and productive use, it is envisaged, in particular, to create a favorable environment for the introduction of innovations in the field of mine action, as well as the development of national production of demining equipment and its technical maintenance in Ukraine. One such approach is the use of unmanned robotic complexes (URCs) for technical inspection and clearance of areas contaminated with EO.

The purpose of the article is to highlight the methodology for determining the level of technical perfection of URCs and its application to the most common models of light and medium class URCs.

A set of parameters most relevant to the use of URCs is proposed. A gradation of comparative technical perfection levels for URCs is proposed and applied. The most technically advanced representatives of the light and medium classes of URCs for mine clearance are identified based on a set

of parameters considered. A comparative graphical histogram is compiled based on the results of determining the level of technical perfection.

This methodology makes it possible to improve the information support of demining units in terms of the application of innovative technologies for searching, detecting, identifying, and destroying (neutralizing) explosive remnants of war by developing scientifically based recommendations for the introduction of modern robotization technologies in the field of humanitarian and operational demining.

Keywords: unmanned robotic complex; technical perfection; mine countermeasures; demining.

УДК 355.04: 004.056 https://doi.org/10.33099/2304-2745/2025-3-86/24-32

Саричев Ю. О., кандидат технічних наук, старший науковий співробітник (0000-0003-1380-4959)
Мазуренко І. М., доктор філософії (0000-0003-2233-7563)
Зубков В. П. (0009-0008-5755-2339)
Піщанський Ю. А. (0000-0003-4392-3318)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Загальні передумови досягнення інформаційної переваги під час зародження воєнного конфлікту

Резюме. Обґрунтовано загальні передумови досягнення інформаційної переваги під час зародження воєнного конфлікту. Доведено, що врахування таких передумов дає змогу сформувати вимоги щодо формування системи заходів протидії інформаційним загрозам та нейтралізації негативного інформаційного впливу, зокрема на етапі зародження (виникнення) воєнного конфлікту.

Ключові слова: воєнний конфлікт; інформаційний простір; інформаційна перевага; інформаційна безпека; інформаційна загроза; інформаційний вплив.

Постановка проблеми. Повномасштабна збройна агресія РФ проти України поставила перед дослідниками воєнної сфери багато складних питань, серед яких важливим є дослідження умов зародження та розвитку воєнного конфлікту, які призвели до такої агресії. Зазвичай, воєнні конфлікти виникають внаслідок зростання протиріч між суспільними інтересами держав, які відбуваються в економічній, соціальній, інформаційній та воєнно-політичній сферах. Такі протиріччя мають прояв через фактори соціального значення у цих сферах, що і виражають передумови такого конфлікту. Їх виявлення та врахування мають важливе значення для аналізу та подальшої генерації рекомендацій стосовно прийняття рішень щодо подальших дій на всіх етапах ескалації конфлікту: зародження (виникнення), розвиток і припинення.

Загалом, сучасний воєнний конфлікт носить “гібридний” характер з чітко вираженою інформаційною складовою, починаючи з етапу його зародження. При цьому *під зародженням воєнного конфлікту* слід розуміти процес, що передує прямому застосуванню збройної сили та характеризується напруженням між суб’єктами конфлікту, наростанням протиріч, загостренням відносин та, зрештою, переходом до воєнних дій [1]. Розвиток такого явища, зокрема за досвідом подій, що відбуваються в сучасній Україні, показує, що процеси в інформаційній сфері інтенсивно супроводжували зародження (виникнення) воєнного конфлікту. Вже на цьому етапі питання досягнення інформаційної переваги над супротивною стороною є актуальним, передусім для зниження напруження між суб’єктами з подальшим зменшенням протиріч, вирішенням проблемних питань мирним шляхом та недопущенням воєнних дій. Отже це питання потребує окремої уваги та розгляду.

Аналіз останніх досліджень і публікацій. Протягом останніх десятиліть в Україні маємо певну кількість публікацій, дотичних до питання досягнення інформаційної переваги над противником. Серед вітчизняних вчених і фахівців цій темі приділено певну увагу в роботах [2–8], де висвітлюються важливі для досягнення інформаційної переваги питання, як-то:

захист інформаційного простору України;

особливості забезпечення інформаційної безпеки держави у контексті протидії інформаційним війнам;

еволюція форм і способів сучасної інформаційної боротьби під час підготовки до збройного конфлікту.

Аналіз показав, що ці публікації не враховують особливостей інформаційних процесів на етапі зародження воєнних конфліктів, що свідчить про обмеженість таких досліджень і є недоліком. Ці роботи:

присвячені вивченню окремих складових проблем для умов мирного часу і не враховують специфіку часових показників переходу до надзвичайного і воєнного стану;

не мають термінологічної єдності уживання базових категорій в описі інформаційних процесів, характерних під час зародження воєнних конфліктів, що ускладнює їх розуміння;

використовують різнорідні підходи під

час розгляду інформаційних процесів на етапі зародження воєнного конфлікту;

не систематизують ознаки процесу зародження воєнного конфлікту, що не дає змоги чітко визначити поточний стан воєнно-політичних, соціально-економічних та інших відносин між суб'єктами конфлікту тощо.

Проте ознаки процесу зародження воєнного конфлікту виявляються за усіма сферами його протікання: воєнної (воєнно-технічної), політичної, дипломатичної, економічної, соціальної тощо. Законодавство України [9] визначає початковий період зародження воєнного конфлікту як латентну (неактивну) фазу збройного конфлікту – ситуацію, за якої відбувається виникнення суперечностей з приводу визначеного об'єкта (політики, економіки, території тощо), зростання недовіри і напруженості, висування односпрямованих або взаємних претензій, мінімізація контактів, прагнення довести правомірність своїх домагань, звинувачення супротивника в небажанні вирішувати спірні питання "справедливими" методами, замикання на своїх власних стереотипах, упередженість і неприязнь у сфері двосторонніх відносин, виникнення поодиноких збройних інцидентів та збройних провокацій, зокрема на державному кордоні.

Латентна фаза характеризується відсутністю або малою інтенсивністю застосування зброї та може проявлятися з певною періодичністю після активних фаз (загострень) у довготривалих, заморожених конфліктах.

За ознаки зародження воєнного конфлікту може бути прийнято такі стадії:

напруження – це стадія, коли між суб'єктами конфлікту виникають протиріччя та розбіжності, які можуть бути економічного, соціального, політичного, або навіть культурного характеру;

посилення напруження – протиріччя загострюються, відносини між суб'єктами конфлікту погіршуються, можуть відбуватися провокації та демонстрація воєнної сили;

максимальне (пікове) напруження – напруження використовується як інструмент впливу на протиборчу сторону конфлікту, можуть проводитися демонстрації воєнної сили, заявлятися вимоги та погрози;

підготовка до воєнних дій – суб'єкти конфлікту починають готуватись до збройного протистояння: відбувається мобілізація ресурсів, проводяться бойові злагодження підрозділів та військових частин, накопичується військова техніка та озброєння.

Ключові фактори, що сприяють зародженню воєнного конфлікту:

політичні та територіальні протиріччя – конфлікт може виникати внаслідок суперечностей у політичних системах, територіальних претензіях, або ж у питаннях влади;

економічні інтереси – конфлікт може бути спровокований боротьбою за ресурси, контроль над ринками, або ж економічні розбіжності;

соціальні та культурні розбіжності – національні, релігійні, расові, або ж інші соціальні та культурні відмінності можуть призвести до загострення конфлікту;

нездатність до переговорів та компромісів – відсутність ефективного діалогу та готовності до компромісів може призвести до ескалації конфлікту.

Огляд зазначених сфер і факторів вказує на те, що інформаційні процеси є рушійною силою кожного з них. Саме тому такі ознаки найбільш характерно проявляються в інформаційній сфері, проте дослідники не приділяють достатньої уваги цим питанням зародження воєнного конфлікту.

Зазначене свідчить про недосконалість інформаційної складової теорії воєнних конфліктів. Неврахування особливостей сучасних інформаційних процесів унеможливлює повною мірою втілювати в життя практичні дії для досягнення інформаційної переваги над противником, зокрема, що вкрай важливо, на етапі зародження воєнного конфлікту.

Усе це спричиняє актуальну науково-практичну проблему удосконалення складової теоретичних основ воєнних конфліктів, зокрема яка стосується інформаційної сфери. Ця проблема може бути вирішена шляхом розв'язання низки питань щодо досягнення інформаційної переваги, в тому числі через врахування сукупності суттєвих факторів інформаційного характеру, насамперед на етапі зародження сучасного воєнного конфлікту. Тому одним з напрямів досліджень слід вважати аналіз загальних передумов досягнення інформаційної переваги над противником на цьому етапі в інтересах вирішення проблемних питань мирним шляхом та недопущення воєнних дій.

Зважаючи на зазначене, **метою статті** є визначення передумов досягнення інформаційної переваги над противником в ході зародження воєнного конфлікту шляхом

врахування основних факторів інформаційної сфери (наявність релевантної інформації (даних) про суперника, своєчасність та достовірність її отримання, захищеність тощо).

Виклад основного матеріалу. Оскільки існуючі в публікаціях дефініції не враховують особливостей зародження воєнного конфлікту, доцільно сформулювати базові визначення. На основі стандарту [10], пропонується тлумачення понять:

інформаційна перевага – перевага над протидіючою стороною в оперативності та якості інформаційного забезпечення процесів державного (військового) управління на свою користь;

інформаційне забезпечення – сукупність заходів органів державного управління усіх рівнів, дій військ (сил) та інших суб'єктів інформаційної діяльності з метою створення (формування) і використання в інформаційному просторі необхідних інформаційних ресурсів для реалізації процесів державного управління.

Ця перевага може бути також використана для досягнення таких цілей, як вплив на громадську думку, воєнний, політичний, дипломатичний або економічний вплив на противника.

Загалом, у сучасному світі чинник інформаційної переваги стає все більш важливим для різних сфер життєдіяльності держави, а саме забезпечує [11]:

у політичній сфері – дієвий контроль над суспільним інформаційним простором, що дає змогу впливати на громадську думку та вибори;

у воєнній сфері – перевагу шляхом здатності оперативно та якісно здійснювати інформаційне забезпечення процесів військового управління з урахуванням інформаційних спроможностей (можливостей) противника;

в економічній сфері – швидкий доступ до інформації та її аналіз, що дає компаніям конкурентну перевагу;

в інформаційній сфері (захисті інформаційних інтересів держави) – інформаційну безпеку держави, що є важливою складовою її національної безпеки.

Відповідно, наростання протиріч за кожною з цих сфер може бути виявлене через певну сукупність ознак процесу зародження воєнного конфлікту. Для ґрунтовного аналізу ситуації, що склалася в інформаційній сфері України, розглянемо основні аспекти, які супроводжують процес зародження (виникнення) воєнного конфлікту, що є важливим і для теорії, і для практики пошуку шляхів досягнення інформаційної переваги над противником.

Серед таких аспектів доцільно виділити [11]:

моніторинг (пошук) – збір даних про противника, його можливості, плани та слабкі місця;

аналіз даних – їх перетворення на корисні знання (інформацію), які можна використовувати для прийняття рішень;

часові показники – перемога у війні часто залежить від здатності збирати дані та отримувати і використовувати поточну інформацію швидше та ефективніше, ніж противник;

захист інформації – запобігання витоку власної інформації та захист критично важливих об'єктів (систем) інформаційної інфраструктури від руйнування;

кібердії (дії в кіберпросторі) – кіберрозвідка для визначення слабких місць системи (інфраструктури) противника з метою порушення її сталої роботи у випадку початку конфлікту;

інформаційно-психологічні операції – здійснення заходів пропаганди та дезінформації для впливу на противника шляхом поширення певної інформації щодо його дискредитації.

Перелічені аспекти значною мірою є складовими забезпечення інформаційної безпеки держави та суттєво впливають на її рівень. Тому інформаційна перевага у протистоянні неможлива без досягнення сталого рівня інформаційної безпеки будь-якої держави [12], зокрема це актуально і для України. Стаття 17 Конституції України [13] наголошує, що це є найважливішою функцією держави, справою всього Українського народу. Виконання цієї функції потребує від усіх інститутів держави концентрації зусиль, щоб за потреби мати досягнення інформаційної переваги над противником. Вкрай важливим є вирішення питання інформаційної безпеки держави заздалегідь (превентивно), ще до зародження воєнного конфлікту, спрямованого проти України.

Інформаційна безпека, як важлива функція будь-якої держави, покликана гарантувати сприятливі умови для життя і продуктивної діяльності громадян, державних інститутів, захищати життєво важливі інтереси людини, суспільства й держави в її інформаційному просторі від зовнішніх і внутрішніх інформаційних загроз. Така

захищеність забезпечується відповідним комплексом заходів органів державного управління щодо зменшення або усунення ймовірних загроз інформаційній безпеці (інформаційних загроз).

Наразі керівництво держави приділяє значну увагу питанням досягнення інформаційної переваги над противником. Так, створені основні структурні елементи (органи управління, виконавчі органи, об'єкти впливу, органи моніторингу) системи забезпечення інформаційної безпеки України, розроблена та набрана чинності низка законодавчих актів України, які стосуються інформаційної сфери [14–23] (закони України, укази Президента України, постанови Кабінету Міністрів України тощо). Ці заходи слід розглядати через призму загального питання досягнення інформаційної переваги.

Водночас, аналіз подій в інформаційній сфері України за цей період свідчить, що окремі складові існуючої системи забезпечення інформаційної безпеки функціонують небездоганно, з різних причин не весь перелік заходів на рівні держави був спланований та виконаний, мали місце непорозуміння, неузгодженість та не координованість дій різних суб'єктів сил оборони України, що негативно впливає на стан досягнення інформаційної переваги.

Детальний аналіз [12] існуючого в законодавстві України [14] визначення інформаційної безпеки показує на певну його недосконаліть, хоча воно може бути взяте за основу власного модифікованого визначення в редакції:

інформаційна безпека України – складова частина національної безпеки України, стан захищеності, за якого запобігається нанесення шкоди життєво важливим інтересам людини, суспільства і держави через:

неповноту, невчасність та невірогідність інформації, що використовується, а також відсутність інформації за її потреби;

негативний інформаційний вплив;

нерегульоване або злочинне застосування інформаційних технологій;

несанкціоноване розповсюдження, використання й порушення цілісності інформації та інших ІР з обмеженим доступом;

недосконаліть комунікативної політики держави;

недостатній рівень медіакультури суспільства.

Таке визначення враховує усі фактори інформаційної сфери, що відображають передумови досягнення інформаційної переваги Україною над противником, зокрема в ході зародження воєнного конфлікту.

Посеред основних суттєвих факторів можна вказати на недостатній рівень розвитку теоретичних основ забезпечення інформаційної безпеки держави, який є в Україні, що впливає на досконаліть функціонування існуючої системи забезпечення інформаційної безпеки держави, а це особливо важливо під час зародження воєнного конфлікту. Це не дає змоги якісно, однозначно і зрозуміло для усіх суб'єктів системи планувати практичну діяльність. Наслідком цього практична діяльність дезорієнтується, що призводить до довільного розуміння власних дій, а відповідно і планування та виконання заходів, тобто конкретної діяльності. Особливо негативні наслідки настають у випадку формування та реалізації комплексу заходів державної інформаційної політики, яка концентровано визначається нормами національного законодавства.

Більшість фахівців інформаційної сфери стверджують, що майбутнє збройного протиборства та можливість досягнення інформаційної переваги все більше зміщується у бік інформатизації всіх процесів державного та військового управління, надання інформаційним ресурсам будь-якого (тактичного, оперативного та стратегічного) рівня першочергового значення. Існуючий стан інформаційного простору України в сучасних умовах інформаційного протиборства викликає певну стурбованість із-за його чутливості та уразливості від значної кількості потенційних і реальних інформаційних загроз. При цьому *під інформаційною загрозою державі* слід розуміти наміри, дії або явища, які шляхом інформаційного впливу на соціальні об'єкти, інформаційну інфраструктуру та інформаційні ресурси можуть ускладнити (унеможливити) реалізацію національних інтересів держави (функцій її структурних органів) [11].

Аналіз таких загроз показує, що, насамперед, потрібно враховувати умови і чинники, які діють на процес їх виникнення та розвиток. Виходячи з розмаїття і мінливості дій таких факторів, необхідно мати на увазі різнорідність інформаційних ресурсів держави та здатність до їх захисту, складу її інформаційної інфраструктури, коло можливих змін стану інформаційних загроз, можливість реалізації того або іншого виду загрози тощо. Характеристики інформаційного впливу

віддзеркалюють всі основні аспекти функціонування інформаційних загроз. Якщо узагальнити ці інформаційні процеси, то можна визначити динаміку розвитку інформаційного впливу:

чинник інформаційної загрози (виклик) →
прояв інформаційної загрози →
→ реалізація загрози (інформаційний вплив)
→ результати впливу.

Причому чинники інформаційної загрози не завжди можна одразу виявити та ідентифікувати, вони, як правило, приховані, їх прояв можна оцінити лише за результатами такого впливу. Реалізація таких загроз може викликати:

підрив обороноздатності країни шляхом порушення функціонування об'єктів інформаційних систем органів державного і військового управління, що забезпечують національну безпеку, і як наслідок, позбавлення можливості своєчасної організації оборони держави і досягнення інформаційної переваги над противником;

дезорганізацію роботи систем та засобів інфраструктури критично важливих галузей (фінансового сектора, енергозабезпечення, водопостачання, транспорту і т.п.), що призводить до хаосу в економіці, масовим безладам, зниження промислового, економічного й оборонного потенціалу;

несанкціонований доступ до державних, військових і комерційних конфіденційних даних;

психологічну дію на персонал органів державного і військового управління, деморалізацію населення за рахунок розповсюдження інформації провокаційного або підривного характеру;

примушення до небажаної альтернативи рішення, а в подальшому і до недоцільного варіанта дій шляхом дезінформації.

За результатами такого огляду можна дійти висновку, що найбільш вірогідними чинниками (джерелами зовнішніх загроз) для власного інформаційного простору є сили і засоби недружніх іноземних держав, а також терористичні й злочинні угруповання, агресивні промислово-фінансові групи, хакери. Крім того, не слід виключати можливість виникнення внутрішніх загроз і зі сторони співробітників власних установ та підрозділів.

Отже більш детально зупинимося на групі факторів державного рівня, зокрема пов'язаних з існуванням загроз інформаційного характеру під час процесу зародження (виникнення) воєнного конфлікту та необхідністю їх нейтралізації. Серед таких загроз найбільш небезпечними є:

зовнішні загрози:

усі види розвідувальної діяльності ззовні, спрямованої на доступ до інформаційних ресурсів держави у воєнній сфері;

інформаційно-технічні впливи на інформаційну інфраструктуру суб'єктів сил оборони України та інформаційні ресурси у воєнній сфері з метою порушення їх дієздатності, виведення із ладу або знищення;

інформаційно-психологічні впливи на керівний (особовий) склад суб'єктів сил оборони України, як у мирний час, так і під час зародження воєнного конфлікту;

міжнародна інформаційна діяльність іноземних політичних, економічних і воєнних структур, яка спрямована проти національних інтересів держави у воєнній сфері, приниження її міжнародного іміджу;

наявність на озброєнні армій іноземних держав високоточної зброї, зокрема, самонавідної на радіовипромінювання, як засобу вогневого ураження елементів інформаційної інфраструктури суб'єктів сил оборони України;

внутрішні загрози:

недосконалість нормативно-правової бази держави у сфері національної безпеки, у тому числі законодавча невизначеність щодо повного переліку суб'єктів сил оборони України, розподілу їх функцій, завдань і механізмів взаємодії при підготовці та веденні воєнних дій;

відсутність єдиної (інтегрованої) інформаційної інфраструктури суб'єктів сил оборони України, відомчий характер політики та заходів щодо забезпечення інформаційної безпеки;

нездатність сил оборони України в межах його інформаційної інфраструктури реалізувати весь перелік основних інформаційних процесів, необхідних для забезпечення достатності (повноти) інформаційного простору держави в умовах сучасного воєнного конфлікту;

обмежені спроможності держави упродовж конкретної кризової ситуації підтримувати сталість створеної інформаційної інфраструктури її сил оборони України шляхом всебічного ресурсного забезпечення (матеріально-технічного, фінансового, кадрового, медичного), а також здійснити захист цієї інфраструктури від фізичного знищення засобами вогневого ураження противника;

відсутність розуміння необхідності впровадження концепції "управління противником" у воєнному конфлікті як ідеологічної бази військового будівництва та підготовки сил оборони України до захисту від зовнішньої агресії в умовах сучасної війни та війн майбутнього, що перешкоджає організації основних інформаційних процесів та їх взаємозв'язку для формування єдиного інформаційного простору держави у воєнній сфері;

недосконаліть комплексної системи захисту інформаційних ресурсів, доступних для елементів інформаційної інфраструктури сил оборони України;

зловмисні та невмотивовані (випадкові) шкідливі дії персоналу (особового складу) інформаційної інфраструктури сил оборони України;

нерозвиненість наукових основ підготовки та проведення інформаційних операцій елементами інформаційної інфраструктури сил оборони України в умовах воєнного конфлікту;

слабкість державницької ідеології, освітянської, виховної та адміністративної практики, спрямованих на зміцнення патріотичної свідомості громадян, а також забезпечення психологічної стійкості персоналу (особового складу) структур суб'єктів сил оборони України у воєнному конфлікті;

неналежний рівень професійної підготовки персоналу (особового складу) інформаційної інфраструктури сил оборони України, особливо у ланці керівних органів;

недостатність міжнародної інформаційної діяльності держави щодо формування її позитивного іміджу у воєнній сфері, а також проведення заходів контрпропаганди у міжнародному інформаційному просторі.

Реалізація описаних загроз, в тому числі під час зародження воєнного конфлікту, може здійснюватися різними способами втручання в наявні інформаційні ресурси та роботу систем та засобів інформаційної інфраструктури. Серед них на сьогодні можна виділити:

навмисне фізичне пошкодження або руйнування апаратних засобів, модифікація повідомлень та даних, перевантаження мереж обміну інформацією, маршрутизаторів або серверів інформаційно-керуючих систем;

внесення змін до функціонування системи (порушення логіки роботи, помилкова відмова в доступі або квитанції);

втручання зсередини (перегляд і розкрадання трафіку та даних);

перехоплення інформації, що передається, дослідження запитів до бази даних і їх криптографічний аналіз.

Нейтралізація зазначених загроз може бути здійснена шляхом реалізації виваженої державної інформаційної політики, спрямованої на проведення в життя комплексу заходів щодо створення та розвитку єдиного інформаційного простору України, зокрема у воєнній сфері (силах оборони), та його всебічного захисту від *негативного інформаційного впливу*, що потребує визначення відповідних концептуальних засад забезпечення інформаційної безпеки України у воєнній сфері.

Загалом, *під інформаційним впливом* слід розуміти організоване цілеспрямоване втручання у свідомість (підсвідомість) чи фізичний стан цільової аудиторії та/або в процес функціонування технічних об'єктів інформаційної інфраструктури шляхом застосування інформаційних засобів і технологій [8, 10]. Основною метою здійснення деструктивного інформаційного впливу на об'єкти інформаційної інфраструктури, зокрема воєнної сфери, є досягнення переваги в умовах інформаційного протиборства шляхом дестабілізації або виведення з ладу системи військового управління противника, а також деморалізації особового складу його військ (сил). При цьому засобами інформаційного впливу є засоби масової інформації, лінгвістичні, програмні, технічні та інші спеціальні засоби, які призначені для реалізації інформаційного впливу.

Інформаційний вплив поділяється на інформаційно-технічний та інформаційно-психологічний.

Інформаційно-технічний вплив – цілеспрямоване втручання в процес функціонування технічних об'єктів інформаційної інфраструктури та фізичний стан людини шляхом застосування засобів і технологій радіоелектронного впливу та кібернетичної зброї [10]. Його результатом може бути дестабілізація інформаційної діяльності об'єкта впливу внаслідок пошкодження, викривлення, руйнування, блокування інформаційних ресурсів або виведення об'єкта з ладу шляхом:

використання комп'ютерних "вірусів" (комп'ютерних програм для деструктивної зміни програмного забезпечення ПЕОМ та комп'ютерних мереж);

застосування “комп’ютерних бомб“ (спеціальних комп’ютерних закладних програм руйнівного характеру);

поширення фальшивої інформації в комп’ютерних мережах;

обмеження або заборони доступу до інформаційних ресурсів законним користувачам комп’ютерних мереж;

програмного ураження інформаційно-телекомунікаційних систем з боку вітчизняних комп’ютерних злочинців або хакерів противника;

ненавмисного порушення встановленого порядку роботи з інформаційними ресурсами персоналом (особовим складом) інформаційної інфраструктури;

радіоелектронного придушення радіотехнічних засобів (зв’язку, спостереження, навігації, радіо, телебачення);

зміни фізичного або психічного стану людини.

Деструктивний інформаційно-технічний вплив, зокрема, може бути спрямований на такі об’єкти в інформаційній інфраструктурі воєнної сфери, як: інформаційно-телекомунікаційні мережі (комп’ютерні мережі та засоби зв’язку, електронні засоби масової інформації; електронні архіви (сховища) та банки даних і знань довготривалого зберігання; засоби автоматизації систем управління військами та зброєю; радіоелектронні засоби і системи (навігації, спостереження, армійські радіостанції, телебачення тощо); інформація, що циркулює на об’єктах інформаційної інфраструктури в реальному часі; людина (соціальні групи) безпосередньо.

Інформаційно-психологічний вплив – цілеспрямоване інформаційне втручання у свідомість (підсвідомість) цільової аудиторії з метою корекції її поведінки та (або) світогляду, зміни морально-психологічного стану [10].

Засобами інформаційно-психологічного впливу є засоби масової інформації, спеціальна друкована продукція, публічна голосова агітація, агентурна діяльність, спеціальні інформаційні технології тощо. Його результатом може бути внесення негативних змін у свідомість та морально-психологічний стан особового складу військових формувань, керівництва та населення держави-противника, що також впливає на досягнення над ним інформаційної переваги.

Для визначення рівня деструктивного інформаційного впливу на цільові об’єкти на рівні держави необхідно мати систему оцінювання такого впливу з певною сукупністю показників, а для визначення його значимості – відповідні критерії. Відмітимо, що одним із підходів для отримання якісних оцінок деструктивного інформаційного впливу на наявні інформаційні ресурси та елементи інформаційної інфраструктури може бути застосування методів експертного оцінювання, які враховують досвід фахівців інформаційної сфери, в тому числі під час зародження воєнного конфлікту. На основі цього підходу запропоновано реалізувати базові методичні елементи для такого оцінювання, які описані, зокрема, в роботах [24, 25].

Таким чином, наведений аналіз умов і чинників та їх деталізація дають змогу сформулювати передумови досягнення інформаційної переваги над противником в ході зародження воєнного конфлікту. Зазначене досягається шляхом забезпечення інформаційної безпеки держави – координованого комплексного процесу недопущення збитковості в інформаційному просторі держави як реалізація запобіжних заходів проти нанесення шкоди у різних галузях життєдіяльності із-за актуальних загроз її інформаційній безпеці (намірів, що передбачають вчинення деструктивних дій в інформаційному просторі; вчинення деструктивних дій в інформаційному просторі; власної бездіяльності в інформаційному просторі; непереборних явищ (процесів) в інформаційному просторі).

Серед таких заходів слід виділити наступні, що формують кібернетичний контур управління [26] щодо досягнення інформаційної переваги:

моніторинг та збір даних про противника;

кіберрозвідка для визначення слабких місць системи (інфраструктури) противника з метою порушення її сталої роботи у випадку початку конфлікту;

аналіз даних та їх перетворення на інформацію;

використання отриманої інформації для прогнозування можливих дій ймовірного противника;

захист інформації для запобігання її витоку;

недопущення ураження критично важливих об’єктів власної інформаційної інфраструктури;

здійснення заходів пропаганди та дезінформації для впливу на противника шляхом поширення певної інформації щодо його дискредитації.

Висновки. Досягнення інформаційної переваги дає змогу під час зародження воєнного конфлікту знизити напруження між суб'єктами воєнного конфлікту з подальшим зменшенням протиріч, вирішенням проблемних питань мирним шляхом та недопущенням воєнних дій. Головною передумовою інформаційної переваги є досягнення сталого рівня інформаційної безпеки держави, який гарантує необхідний стан захищеності інформаційного простору держави в умовах впливу внутрішніх та зовнішніх інформаційних загроз.

Подальші дослідження слід зосередити на розробці пропозицій щодо формування та реалізації виваженої державної інформаційної політики, спрямованої на досягнення необхідного рівня інформаційної безпеки держави в інтересах інформаційної переваги, зокрема шляхом впровадження комплексу заходів для створення та розвитку єдиного інформаційного простору України та його всебічного захисту від негативного інформаційного впливу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Магда Є. В. Гібридна агресія Росії: уроки для Європи Київ : Каламар, 2017. 268с.
2. Богуш В. М., Юдін О. К. Основи інформаційної безпеки держави: вступ до спеціальності. Харків : Консум, 2004. 439 с.
3. Юдін О. К., Богуш В. М. Інформаційна безпека держави: навч. посібник. Харків : Консум, 2005. 576 с.
4. Горбулін В. П., Биченок М. М. Проблеми захисту інформаційного простору України : монографія. Київ : Інтертехнологія, 2009. 136 с.
5. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання : монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. Київ : Інтертехнологія, 2009. 164 с.
6. Інформаційна безпека держави у контексті протидії інформаційним війнам : навч. посіб. / за ред. В. Б. Толубка. Київ : НАОУ. 2004. 315 с.
7. Руснак І. С., Телелим В. М. Розвиток форм і способів інформаційної боротьби на сучасному етапі // Наука і оборона. 2000. № 2. С.18–23.
8. Левченко О. В. Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та застосування : монографія. Житомир : ПП "Євро-Волинь", 2021. 172 с.
9. Про затвердження Порядку розроблення Плану оборони України : Постанова Кабінету Міністрів України від 22.07.2020 № 636. URL: http://zakon.rada.gov.ua/laws/show/636-2020-%D0%BF/conv#Text (дата звернення: 24.05.2025).
10. Військовий стандарт. Інформаційна безпека держави у воєнній сфері. Терміни та визначення: ВСТ 01.004.004 – 2014 (01). [Чинний від 2014 – 02 – 27]. Київ 2014. 22 с.
11. Горбулін В. П. Світова гібридна війна: український фронт : монографія / за заг. ред. В.П. Горбуліна. Київ : НІСД, 2017. 496 с.
12. Інформаційна безпека України у воєнній сфері: засадничі елементи становлення теоретичних основ її забезпечення: монографія / В. В. Грицюк, І. В. Єфіменко, В. П. Зубков, В. В. Машталір, С. А. Микусь, А. К. Павліковський, Ю. А. Піщанський, Ю. О. Саричев, П. М. Сніцаренко, В. А. Ткаченко ; за заг. ред. П.М. Сніцаренка, 2-е вид., допов. Київ : НУОУ, 2025. 300 с.
13. Конституція України. Прийнята ВР України 28.06.1996 р.
14. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 09.01.2007 № 537-V. URL: http://zakon3.rada.gov.ua (дата звернення: 24.05.2025).
15. Про інформацію : Закон України від 13.01.2011 № 2938-VI. URL: http://zakon3.rada.gov.ua (дата звернення: 25.05.2025).
16. Закон України "Про телекомунікації" від 18.11.2003 р. № 1280-IV // Законодавство України URL: http://zakon2.rada.gov.ua (дата звернення: 25.05.2025).
17. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: http://zakon2.rada.gov.ua (дата звернення: 25.05.2025).
18. Стратегія національної безпеки України: Указ Президента України від 26.05.2015 р. № 287/2015 URL: http://zakon5.rada.gov.ua (дата звернення: 26.05.2025).
19. Про рішення РНБО України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента України від 28.12.2021 № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 26.05.2025).
20. Стратегія кібербезпеки України : Указ Президента України від 15.03.2016 № 96/2016. URL: http://president.gov.ua (дата звернення: 26.05.2025).
21. Про невідкладні заходи з кібероборони держави : Указ Президента України від 26.07.2021 № 446/2021. URL: http://president.gov.ua (дата звернення: 27.05.2025).
22. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану : Указ Президента України від 19.03.2022 № 152/2022. URL: http://president.gov.ua (дата звернення: 27.05.2025).
23. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінету Міністрів України від 15.05.2013 № 386-р. URL: http://zakon.rada.gov.ua (дата звернення: 27.05.2025).
24. Методичний підхід до виявлення та оцінювання негативного інформаційно-психологічного впливу на особовий склад військ (сил) / П. М. Сніцаренко, Ю. О. Саричев,

Ю. І. Міхєєв, М. В. Праута // Наука і оборона. № 3-4. 2017. С. 18–25.
25. Комплексна система протидії негативному інформаційно-психологічному впливу на особовий склад Збройних Сил України / П. М. Сніцаренко, Ю. О. Саричев, В. А. Ткаченко, Л. В. Хоменко // Наука і оборона. № 2. 2018. С. 40–45.
26. Винер Н. Кибернетика или управление и связь в животном и машине. Москва : Сов.радио, 1968. 328 с.

Стаття надійшла до редакції 25.07.2025

General preconditions for achieving information superiority during the onset of military conflict

Annotation

The onset of military conflict should be understood as the process preceding the direct use of armed force and characterized by tension between the parties to the conflict, growing contradictions, escalating relations, and, ultimately, the transition to military action. The development of this phenomenon, particularly based on the experience of events taking place in modern Ukraine, shows that processes in the information sphere intensively accompanied the emergence (onset) of military conflict. Already at this stage, the issue of achieving information superiority over the opposing side is relevant, primarily to reduce tensions between the parties, followed by a reduction in contradictions, the peaceful resolution of problematic issues, and the prevention of military action.

The purpose of this article is to identify the preconditions for achieving information superiority over the enemy during the emergence of a military conflict by taking into account the main factors in the information sphere: the availability of relevant information (data) about the opponent, the timeliness and reliability of its acquisition, security, etc.

The analysis of conditions and factors and their detailing allow us to formulate the preconditions for achieving information superiority over the enemy during the onset of a military conflict. This is achieved by ensuring the information security of the state – a coordinated comprehensive process of preventing losses in the information space of the state as the implementation of preventive measures against damage in various areas of life due to current threats to its information security. The main precondition for information superiority is the achievement of a stable level of state information security, which guarantees the necessary state of protection of the state's information space in the face of internal and external information threats.

Keywords: military conflict; information space; information superiority; information security; information threat; information influence.

УДК 621.396.946 https://doi.org/10.33099/2304-2745/2025-3-86/33-37

Гордієнко С. Б., кандидат технічних наук, доцент[1] (0000-0001-2345-6789)
Ворович Б. О., кандидат військових наук, доцент[2] (0000-0002-4083-3707)
Прийма Я. О.[2] (0000-0001-7783-2698)

[1] – Кафедра технологій захисту кіберпростору Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії СБ України Київ;
[1] – Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Питання системного підходу щодо забезпечення безпеки інформації об’єктів інформаційної інфраструктури

Резюме. У статті розглянуті аспекти системного підходу щодо створення та впровадження системи безпеки інформації стосовно об’єктів інформаційної інфраструктури.

Ключові слова: системний підхід; управління безпекою інформації; об’єкт інформаційної інфраструктури; реалізація рішення.

Постановка проблеми. За умов складних загальносуспільних відносин, воєнного стану та постійних деструктивних посилів з боку держави агресора – Російської Федерації (РФ) застосування системного підходу до наукових та організаційних спрямувань щодо забезпечення та підтримання ефективних заходів безпекового характеру інформаційної та технологічної складової функціонування об’єктів інфраструктури є найбільш актуальним з точки зору їх розробки та подальшого використання.

Оскільки управлінська діяльність тісно пов’язана із системним підходом, то саме необхідність виконання управлінських завдань змушує широко застосовувати системні ідеї, переводячи їх на рівень технологічних схем керування. Тому потреби управління виступають найважливішою рушійною силою застосування системного підходу. При цьому, розширення сфери використання в управлінських процесах інформаційних систем та їх ускладнення спричиняє загострення проблеми безпеки інформації (загалом інформаційних ресурсів) у таких системах та викликає потребу її забезпечення шляхом побудови (впровадження) підсистем безпеки інформації та управління ними на принципі системного підходу.

Аналіз останніх досліджень і публікацій. З часів інтенсивного розвитку інформаційних відносин в Україні та до сьогодні, за умов воєнного стану, питання безпеки інформації досліджувалися та розвивалися, зокрема, провідними вітчизняними науковцями переважно під кутом забезпечення інформаційної безпеки. На особливу увагу в цій сфері заслуговують праці [1–5]. Характер їх досліджень в галузі інформаційної безпеки спрямований на досягнення ефективних методів та підходів щодо забезпечення вимог політики безпеки, системи управління інформаційною безпекою (СУІБ) на об’єктах інформаційної інфраструктури. Також значна увага спрямовувалася на розроблення питань застосування сучасних безпекових технологій та окремих методик комплексної системи безпеки та управління нею за умов активної інформаційної агресії з боку РФ з деструктивним впливом на стійкість функціонування процесів життєзабезпечення нашої країни. Проте у наведених джерелах недостатньо уваги приділено питанням застосування системного підходу щодо розробки технологій забезпечення безпеки інформації, створення перспективних засобів управління безпекою інформації.

Між тим, аналіз показує, що міжнародними стандартами серії ISO/IEC2700, які імплементовані в Україні як державні стандарти [6–8], де ключовим є словосполучення “*information security*”, що може перекладатися як “*інформаційна безпека*” або “*безпека інформаці*” (що не є еквівалентними [9, 10]), у повному обсязі на основі системного підходу забезпечується викладення методологічних засад створення та застосування технологій якраз *безпеки інформації*, що передбачає сукупність процедур її всебічного захисту. Але питання порядку (шляхів) практичного впровадження таких технологій на об’єктах інформаційної діяльності значною мірою ще залишається сьогодні поза увагою наукового обґрунтування.

Метою статті є обґрунтування застосування системного підходу щодо

створення та забезпечення ефективного процесу функціонування системи безпеки інформації на об'єктах інформаційної інфраструктури на основі положень ДСТУ серії ISO/IEC 2700.

Виклад основного матеріалу. Забезпечення безпеки інформації на об'єктах інформаційної інфраструктури полягає в організації та реалізації відповідного процесу управління, що включає планування, виконання (побудову), контроль і технічне обслуговування всієї інфраструктури безпеки та дотримання вимог політики безпеки. Тобто, це необхідна сфера впливу на шляху побудови захищеного простору обігу інформації. Це передбачає обов'язковий етап діагностичного обстеження інформаційної інфраструктури (системи) з оцінкою її вразливостей і загроз, на основі чого проводиться проєктування підсистеми безпеки інформації, впровадження, супровід та обслуговування, а в подальшому управління нею. Системне вирішення комплексу цих питань передбачено, зокрема, національним стандартом ДСТУ ISO/IEC 27001:2023 [6], яким регламентується створення та використання *системи управління безпекою інформації* як частини загальної системи управління підприємством (організацією), що ґрунтується на врахуванні бізнес-ризиків та інших ризиків антикризового менеджменту і призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення *політик безпеки інформації*. Іншими словами, система управління безпекою інформації складається з політик, процедур, інструкцій, практик і технологій, які дають змогу захищати конфіденційну інформацію від загроз та ризиків. Отже, реалізація загроз і ризиків для інформації може суттєво вплинути на такі її властивості як конфіденційність цілісність та доступність.

Конфіденційна інформація – це інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

Цілісність інформації – це внутрішня єдність, пов'язаність усіх частин інформаційного продукту в єдине ціле. В інформаційній системі – стан даних та програм, що забезпечує: стійку роботу системи. Для інформаційної системи можна розглядати такі поняття як цілісність даних, цілісність інформації, цілісність бази даних, цілісність інформаційної системи, захист від несанкціонованої модифікації даних і таке інше. Інформація має залишатися недоторканою та не піддаватися змінам без дозволу.

Доступність інформації – це властивість інформації бути захищеною від несанкціонованого блокування, що гарантує можливість її використання уповноваженими користувачами, коли це необхідно.

Послаблення або нівелювання реалізації загроз і викликів може бути досягнено шляхом застосування певних заходів.

Аутентифікація та авторизація – перевірка ідентичності користувачів та надання їм відповідних прав доступу до інформації. Аутентифікация – підтвердження ідентичності користувача. Авторизация – підтвердження системою безпеки, що користувачу надано дозвіл до визначених дій.

Управління ризиками – це оцінка потенційних загроз для інформації та впровадження заходів для їх запобігання або зменшення впливу.

Шифрування – захист інформації шляхом перетворення її в нечитабельний формат, який може бути розкодований тільки з використанням відповідного ключа.

Аудит та моніторинг – систематичний контроль за подіями та діяльністю для виявлення несправностей системи або потенційних загроз інформації.

Усвідомлення та навчання – забезпечення освіченості персоналу та навчання його правилам дотримання безпеки інформації.

Беручи до уваги зазначене, організація підсистеми (системи) управління безпекою інформації відповідно до стандарту [6] потребує також дотримання низки вимог та потреб, зокрема:

врахування *контексту організації (Context of the organization)* – розуміння організаційного контексту, потреб і очікувань "зацікавлених сторін" та визначення сфери застосування системи управління безпекою інформації;

лідерства (Leadership) – вище керівництво має продемонструвати лідерство та відданість СУІБ, визначити політику та призначити ролі, обов'язки та повноваження щодо безпеки інформації;

планування (Planning) – описує процес виявлення, аналізу та планування усунення інформаційних ризиків, уточнення цілей інформаційної безпеки та управління змінами

системи управління безпекою інформації;

підтримки (Support) – мають бути виділені відповідні, компетентні ресурси, підвищена обізнаність, підготовлена та контрольована документація;

операційності (Operation) – більш детальніше оцінювання та усунення інформаційних ризиків, керування змінами та документування речей (частково для того, щоб їх могли перевірити аудитори сертифікації);

оцінки ефективності (Performance evaluation) – моніторинг, вимірювання, аналіз та оцінка/аудит/перегляд засобів контролю, процесів і системи управління безпекою інформації, систематично вдосконалюючи речі, де це необхідно;

удосконалення (Improvement) – звернутись до висновків аудитів та оглядів (наприклад, невідповідності та коригувальні дії), систематично удосконалюючи систему управління безпекою інформації.

Зазначене засвідчує системність підходу у цьому стандарті до управління і забезпечення безпеки інформації в процесі практичної діяльності будь-якого суб'єкта.

Постановку задачі та прийняття рішення щодо застосування системи управління безпекою інформації організації (установи) на основі системного підходу у кожному конкретному випадку необхідно розглядати відповідно до *принципів системного аналізу* [11], таких як:

процес прийняття рішень починається з аналізу та визначення важливих проблем і чіткого формулювання конкретної мети системи;

при розгляді проблеми в цілому слід виявити всі наслідки і взаємозв'язки кожного окремого рішення;

визначити і дослідити всі можливі альтернативи шляхів рішення проблеми і досягнення мети;

цілі окремих підсистем повинні бути узгоджені з метою всієї системи;

в процесі аналізу доцільно перейти від абстрактного до конкретного;

необхідно виявити зв'язки між елементами системи, дослідити їх взаємодію.

Застосування елементів системного аналізу не замінює сутності політики безпеки інформації об'єктів інформаційної діяльності, а істотним чином доповнює розгляд її особливостей. Зокрема, деталізується вплив ризиків щодо системи безпеки, які змінюються, сприяючи появі нових вразливостей та нових загроз безпеці [11, 12], що становить основу реалізації політики безпеки об'єктів та потребує розширення аналізу, як-то:

явищ безпекового характеру, технологічних процесів та господарсько-фінансової діяльності організації (установи) в цілому;

окремих сторін управлінської діяльності та стратегічного планування розвитку організації (установи);

також діяльності окремих специфічних підрозділів матеріального, фінансового, безпекового та іншого забезпечення.

До того ж, враховуються показники, які обґрунтовані даними обліку, звітності та плану. Але для повного і глибокого вивчення проблеми необхідно не тільки використовувати дані, отримані в результаті вивчення технічних, економічних, фінансових, безпекових та інших сторін діяльності організації (установи), а також психологічний клімат і соціальні явища, які виявлені при здійсненні загального ризик-менеджменту.

Таким чином, системний аналіз дає змогу дослідити питання безпеки інформації організації (установи) більш глибоко і всебічно, ніж при спрощеному аналізі ризиків безпекового характеру, оскільки він передбачає використання як жорстких кількісних методів, так і логічних суджень, досвіду та інтуїції.

Переходячи безпосередньо до побудови системи безпеки з позиції системного аналізу, необхідно передбачити виконання таких завдань:

1. Визначення меж оптимізації системи – управління безпекою інформації може бути здійснено лише в межах безпосереднього впливу та дії зовнішніх та внутрішніх факторів системи, що підлягає оптимізації. Межі системи відносно критеріїв безпеки інформації визначаються охопленням методами і засобами забезпечення політики безпеки конкретного об'єкта інформаційної діяльності;

2. Визначення головного показника (критерію) ефективності, за яким можна оцінити характеристики рішення, що відшукується – доцільно застосовувати найбільш прийнятний і зрозумілий для керівництва показник, яким може бути безпековий, фінансовий, репутаційний або матеріальний критерій, також рівень прогнозованих затрат щодо створення ефективної системи управління безпекою інформації.

3. Вибір внутрішньосистемних незалежних змінних, які мають адекватно описувати функціонування системи управління безпекою інформації – мають адекватно описувати та характеризувати ефективність функціонування системи за напрямом управління безпекою інформації, мають бути дієвими складовими зв'язків (відносин) між елементами системи. Визначення цих незалежних змінних конкретно може бути характерним проявом та ознакою тільки індивідуального підходу до функціонування системи або її окремого елементу.

4. Побудова моделі, що має описувати взаємозв'язки між змінними та відображати вплив незалежних змінних на рівень показника ефективност – на етапі побудови і дослідження конкретних моделей безпеки інформації, які характерні для застосування на конкретних об'єктах (в організаціях), реалізуються такі три базові функції:

оцінювання цілей і засобів їх досягнення;

вибір оптимального варіанта рішення;

впровадження рішення і оцінювання його ризиків та наслідків.

При цьому доцільно зазначити і питання про відповідність (адекватність) моделей реальності. У реальних системах цілком можливе логічне обґрунтування моделей елементів (складових) системи управління безпекою інформації. Ці моделі саме і необхідно будувати мінімально-достатніми, тобто простими настільки, наскільки це можливо без втрати сутності та ефективності процесів управління в такій системі.

Зважаючи на викладене, процес прийняття рішення на основі системного підходу щодо створення та забезпечення ефективного функціонування системи безпеки інформації інформаційної інфраструктури організації (установи) як невід'ємної складової її загальної системи управління, можна подати послідовність виконання відповідного набору фаз (етапів) дій як наведено в Табл. 1.

Таблиця 1

Зміст основних етапів прийняття та реалізації рішень щодо забезпечення безпеки інформації організації (установи) на основі системного підходу

№	Фаза прийняття рішення	Зміст фази прийняття рішення
1	Збір інформації про можливі проблеми забезпечення безпеки інформації	Спостереження за внутрішнім та зовнішнім середовищем діяльності організації (установи)
2	З'ясування та визначення причин виникнення проблем щодо порушення політики безпеки	Опис проблемної ситуації Формулювання проблеми, оцінювання її важливості та з'ясування причин виникнення проблеми
3	Формулювання цілей вирішення проблеми щодо забезпечення безпеки інформації	Визначення контексту інформаційної складової діяльності організації. Формулювання критеріїв вирішення проблеми, щодо політики безпеки
4	Діагностичне обстеження з оцінкою вразливостей (ризиків) інформаційної системи і загроз	Детальний опис об'єкта захисту. Визначення розмаху варіації факторів пливу (ризиків). Визначення обмежень
5	Розроблення відповідних кроків забезпечення політики безпеки інформації в організації (установі)	Формулювання актуальних задач, пошук ідей розв'язання кожної задачі. Визначення та знаходження можливих варіантів (моделей) рішення безпекової проблеми. Узагальнення результатів розв'язання по окремих рішеннях. Прогнозування наслідків прийняття раціональних рішень по забезпеченню системи безпеки
6	Вибір кращого варіанта вирішення проблеми	Прогнозування наслідків прийняття раціональних рішень по забезпеченню системи безпеки
7	Коригування та узгодження рішення	Аналіз рішення з виконавцями (операторами безпеки інформації). Узгодження рішення з функціонально взаємодіючими службами. Затвердження рішення
8	Реалізація рішення	Підготовка робочого плану реалізації. Реалізація. Внесення змін у робочий план під час реалізації рішення. Оцінювання ефективності реалізації прийнятого рішення

Висновки. Показано можливість отримання рішення щодо побудови системи безпеки інформації інформаційної інфраструктури організації (установи) на основі системного підходу, закладеного в положеннях державного стандарту ДСТУ ISO/IEC 27001: 2023, а також з використанням елементів системного аналізу. Запропоновано загальну схему (послідовність) дій в інтересах ухвалення рішення керівництвом щодо

побудови системи безпеки інформації інформаційної інфраструктури як невід'ємної складової загальної системи управління організації (установи).

Подальші дослідження доцільно зосередити на розвитку системи управління безпекою інформації, що буде пов'язано з інтеграцією в цілісну форму системного підходу до управління організацією в цілому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Технічний захист інформації./ В. О. Богуш, В. Бровко, О. Кобус. Київ : Ліра-К, 2022. 508 с.
2. Домарєв В. В. Управління інформаційною безпекою в банківських установах (Теорія і практика впровадження стандартів серії ISO 27k). Донецьк : Велстар, 2012. 146с.
3. Системний аналіз та прийняття рішень в інформаційній безпеці : підручник / С. В. Толюпа та ін. Київ :ДУТ, 2015. 345 с.
4. Інформаційна безпека держави : підручник : в 2 т. / В. М. Петрик та ін. ; за заг. ред. В. В. Остроухова. Київ : Кн. палата України, 2016. Т. 1. 387 с. Т. 2. 328 с.
5. Інформаційна безпека : підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей та ін. ; під ред. В. В. Остроухова. Київ : Ліра-К, 2021. 412 с.
6. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
7. ДСТУ ISO/IEC 27005:2023. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2011, IDT).
8. ДСТУ ISO/IEC 27006:2023. Інформаційні технології. Методи захисту. Вимоги до організацій, які надають послуги з аудиту і сертифікації систем управління інформаційною безпекою (ISO/IEC 27006:2011, IDT).
9. Архипов О., Архипова Є. Особливості розуміння понять "інформаційна безпека" та "безпека інформації". Матеріали XI міжнародної науково-практичної конференції / ІПРІ НАН України. Київ, 2014. С. 18–30.
10. Інформаційна безпека України у воєнній сфері: засадничі елементи становлення теоретичних основ її забезпечення : монографія / кол. Авторів ; за заг. ред. П. М. Сніцаренка. Київ : НУОУ, 2025. 300 с.
11. Теорія систем і системний аналіз : конспект лекцій /укладач С. В. Соколов. Суми : Сумський державний університет, 2020. 171 с.
12. Гордієнко С. Б. Актуальні питання управління IT-ризиками на об'єктах критичної інформаційної інфраструктури // Телекомунікаційні та інформаційні технології. 2022. №1 (74). С. 29–35.

УДК 351.746.1 https://doi.org/10.33099/2304-2745/2025-3-86/38-43

Михайленко О. В., кандидат військових наук, доцент (0000-0002-6385-536X)
Грінченко В. В., доктор філософії (0000-0002-2158-4389)

Національна академія Державної прикордонної служби України імені Богдана Хмельницького, Хмельницький

Аналіз підходів до побудови охорони державного кордону на ділянці підрозділу

Резюме. Розглянуто підходи до побудови охорони державного кордону як ключового елемента організації оперативно-службової діяльності на ділянці підрозділу охорони державного кордону. Обґрунтовано доцільність розмежування ділянки відповідальності по рубежам та смугам місцевості. Порівняно переваги та недоліки лінійної й об'єктової побудови охорони державного кордону.

Ключові слова: охорона державного кордону; побудова охорони державного кордону; лінійна побудова; об'єктова побудова; підрозділ; рубіж; смуга місцевості.

Постановка проблеми. Законодавство України визначає основні функції Державної прикордонної служби України (далі – ДПСУ), виконання яких забезпечує недоторканість державного кордону та охорони суверенних прав України в її прилеглій зоні та виключній (морській) економічній зоні [1], зокрема:

охорона державного кордону України на суші, морі, річках, озерах та інших водоймах з метою недопущення незаконної зміни проходження його лінії, забезпечення дотримання режиму державного кордону та прикордонного режиму;

охорона суверенних прав України в її виключній (морській) економічній зоні та контроль за реалізацією прав і виконанням зобов'язань у цій зоні інших держав, українських та іноземних юридичних і фізичних осіб, міжнародних організацій;

участь у боротьбі з організованою злочинністю та протидія незаконній міграції на державному кордоні України та в межах контрольованих прикордонних районів.

Якість виконання покладених на підрозділи ДПСУ завдань із забезпечення недоторканості державного кордону, крім інших факторів, залежить насамперед й від ефективної побудови охорони державного кордону.

Визначення доцільної побудови охорони державного кордону здійснюється під час другого етапу підготовки до оперативно-службової діяльності в наступному календарному році [2]. Також, перебудова охорони державного кордону може бути здійснена у разі суттєвої зміни обстановки і попередній варіант не буде задовольняти результати виконання завдання. Під час визначення доцільності побудови охорони державного кордону, як правило, здійснюється аналіз завдання, оцінка обстановки, розроблення варіантів дій, аналіз варіантів дій, порівняння та вибір остаточного варіанта дій.

На теперішній час, порядок побудови нормативно не конкретизований і не достатньо деталізований, застосовується різна термінологія, тому й в органах охорони державного кордону відсутні єдині підходи до здійснення цього процесу. Це, в свою чергу, викликає необхідність наукового обґрунтування вибору найбільш доцільного варіанта побудови охорони державного кордону на ділянці підрозділу.

Аналіз останніх досліджень і публікацій. Питання процесу побудови охорони державного кордону, в тому числі, на різних ділянках, в різних фізико-географічних умовах та умовах обстановки досліджувала низка вітчизняних учених. Зокрема, наукові дослідження з питань визначення найбільш раціональної побудови охорони державного кордону із застосуванням різних методів та методик проводили А.В. Братко [3, 4], О.В. Михайленко, Ю.А. Паламарчук [5], С.В. Бурбела [6], О.С. Андрощук, В.В. Грінченко [7], О.С. Більовський [8] та інші. Однак дані роботи здебільшого були присвячені підвищенню якості оперативно-службової діяльності підрозділів за рахунок визначення найбільш обґрунтованого варіанта застосування сил та засобів підрозділу. Окремо розглядались системи, як складові побудови, але в той же час це питання не достатньо вивчено як цілісний кінцевий процес.

Мета статті – визначення основних підходів щодо побудови охорони державного кордону із врахуванням потенційних загроз, які впливають на її ефективність та вимог Адміністрації Державної прикордонної

служби України із застосуванням запропонованої термінології.

Викладення основного матеріалу. Враховуючи особливості здійснення оперативно-службової діяльності на різних ділянках кордону викликані збройною агресією з боку РФ в статті досліджено порядок побудови охорони державного кордону з країнами Євросоюзу та Республікою Молдова.

Керівні документи Адміністрації ДПСУ визначають, що побудова охорони державного кордону – це доцільне розташування наявних та доданих сил і засобів по напрямках, районах, пунктах пропуску через державний кордон, ділянках відповідальності, районах та секторах [9]. В інших джерелах визначено, що побудова охорони державного кордону полягає в розташуванні сил та засобів, що забезпечує своєчасне виявлення і затримання правопорушників в межах ділянки відповідальності прикордонного підрозділу, прикордонного загону.

Але в обох випадках вона характеризується своєю глибиною, щонайменше до зовнішньої межі контрольованого прикордонного району та зосередженню основних зусиль на найважливіших напрямках і в потрібний час, що забезпечить своєчасне виявлення і затримання правопорушників у межах ділянки відповідальності.

Побудова охорони державного кордону має відповідати отриманому завданню, задуму дій і забезпечувати комплексне та ефективне застосування сил та засобів для активного виявлення і припинення правопорушень, протидію яким законодавством віднесено до компетенції ДПСУ.

Побудова охорони державного кордону на ділянці підрозділу охорони державного кордону повинна забезпечувати: збирання (добування), аналіз та реалізацію даних обстановки; проведення режимних і контрольних заходів; дієвий інженерно-технічний контроль; наявність чергових сил, засобів та резервів.

Проаналізувавши розпорядчі документи начальників органів охорони державного кордону встановлено відсутність єдиного підходу щодо визначення побудови на ділянках відповідальності. Здебільшого вона здійснюється за рубежами:

перший рубіж – у смузі місцевості від державного кордону до лінії прикордонних інженерних споруд;

другий рубіж – у смузі місцевості від лінії прикордонних інженерних споруд до тилової межі прикордонної смуги;

третій рубіж – у смузі місцевості від тилової межі прикордонної смуги на глибину ділянки відповідальності (тилової межі контрольованого прикордонного району).

Інші органи охорони будують охорону за ділянками місцевості:

перша ділянка – від державного кордону на глибину прикордонної смуги;

друга ділянка – від тилової межі контрольованого прикордонного району на глибину контрольованого прикордонного району;

третя ділянка – від тилової межі контрольованого прикордонного району на глибину адміністративної області.

Також, розглядаються варіанти об’єктової побудови охорони державного кордону.

Слід зауважити, що для визначення найбільш оптимального варіанта побудови охорони державного кордону слід визначитись з поняттями, які застосовуються вище, а саме: рубіж, смуга, ділянка [10].

Рубіж – це лінія, межа, що відділяє кого-, що-небудь від когось, чогось. У військовій справі “рубіж” може означати умовну лінію або площину в просторі, з якої відраховується початок або кінець певного етапу військових дій.

Смуга – видовжена, обмежена чим-небудь частина якоїсь поверхні, простору, що виділяється на загальному фоні своїм виглядом, кольором та інше. *Смуга місцевості* – це ділянка території, яка визначається для певних цілей, наприклад, для встановлення прикордонного режиму або для інших адміністративних потреб. Вона може мати різні ширину та призначення в залежності від конкретного законодавства або ситуації. Смуга місцевості обмежується конкретними лініями (боковими та глибинними межами), які визначають розміри, відповідальність і межі дій на місцевості.

Ділянка – окрема частина земельної площі, використовувана з якоюсь метою, виділена за якою-небудь ознакою, зокрема, частина земельної площі з установленими межами для використання під забудову, сільське господарство або з іншою метою. Це поняття також застосовується до інших сфер, означаючи окрему частину тіла, ділянку фронту, наукову галузь чи відрізок чогось, що має протяжність. Ділянка фронту визначається

як частина лінії фронту, де діє певне військове з'єднання.

У цьому тлумаченні термін "*ділянка відповідальності*" доцільно застосовувати як частина місцевості, яка розташована в межах контрольованого прикордонного району, на якій підрозділ ДПСУ виконує визначені законодавством функції. Така ділянка обмежується по фронту державним кордоном, по тилу – тиловою межею контрольованого прикордонного району, праворуч, ліворуч – стиками та розмежувальними лініями. І саме в межах ділянки відповідальності підрозділу створюється побудова охорони державного кордону.

Отже застосування зазначеної термінології потребує вірного тлумачення при визначені ділянки відповідальності підрозділу та об'єктів побудови охорони державного кордону. Враховуючи вищевикладене пропонується термін "побудова охорони державного кордону" визначити, як розташування за єдиним замислом наявних і доданих сил та засобів, технічних засобів охорони державного кордону, інженерних споруд та загороджень в межах ділянки відповідальності підрозділу в певний період часу.

Також, пропонується для побудови охорони державного кордону визначати рубежі, а нарощення ресурсів підрозділу здійснювати в смугах місцевості, які обмежені зазначеними рубежами і відповідно стиками та розмежувальними лініями між сусідніми підрозділами.

Як приклад, для здійснення побудови на класичній ділянці державного кордону визначити:

перший рубіж – державний кордон;

другий рубіж – лінія прикордонних інженерних споруд;

третій рубіж – тилова межа прикордонної смуги;

четвертий рубіж – тилова межа контрольованого прикордонного району (тилова межа ділянки відповідальності підрозділу);

нарощення сил і засобів розподіляти по трьом смугам місцевості:

перша – між першим та другим рубежем;

друга та третя – відповідно між другим і третім, третім і четвертим.

Причому, слід зауважити, що рубежі не обов'язково визначаються відповідно до наведеного прикладу, а залежатимуть від конкретної обстановки та особливостей фізико-географічних умов місцевості, і можуть проходити по околицям населених пунктів, основних магістралей та доріг, вздовж державного кордону, по характерним орієнтирам на місцевості тощо. Також, і кількість їх відповідно може бути більшою або меншою.

Враховуючи наведений приклад пропонується – *у межах першої смуги* місцевості в основу покласти заходи контролю та дотримання режиму державного кордону, які реалізовувати шляхом організації служби основних видів прикордонних нарядів "Прикордонний патруль", "Пост спостереження", "Секрет" та облаштування ділянки комплексом різного роду інженерних споруд, загороджень, сигналізаційних та контролюючих засобів, які дають змогу виявляти та фіксувати протиправну діяльність, а також уповільнюють або унеможливлюють переміщення правопорушників. А також ведення технічного (оптичного, оптико-електронного, радіолокаційного, сейсмічного тощо) цілодобового спостереження за державним кордоном та суміжною стороною на глибину технічних можливостей засобів спостереження прикордонними нарядами "Оператор комплексу спеціальних технічних засобів".

У межах другої смуги місцевості – в основу покласти заходи контролю та дотримання прикордонного режиму, які здійснювати шляхом організації служби прикордонних нарядів з охорони державного кордону із завданням виявлення та затримання правопорушників, або інформування прикордонних нарядів в першій смузі про напрямок їх руху; контролю підходів до лінії прикордонних інженерних споруд, виявлення спроб її подолання прикордонними нарядами та ведення технічного спостереження; комплексного застосуванням безпілотних авіаційних систем.

До складу прикордонних нарядів активно залучати представників взаємодіючих правоохоронних органів та місцевого населення.

У межах третьої смуги місцевості – в основу покласти службу прикордонних нарядів спільно з представниками правоохоронних органів шляхом виставлення прикордонних нарядів "Контрольний пост" та "Пост спостереження"; роботу в населених пунктах інспекторського складу підрозділів моніторингу обстановки із завданням збору даних обстановки, перевірки місць перебування потенційних правопорушників,

контролю за дотриманням правил прикордонного режиму; роботу оперативно-розшукових підрозділів з виявлення та припинення діяльності організованих злочинних угрупувань; проведення профілактичних заходів для попередження вчинення правопорушень.

Пропонується основну щільність прикордонних нарядів, інженерних споруд та загороджень, технічних засобів мати в межах першої та другої смуги місцевості, а основні зусилля з охорони державного кордону зосереджувати на напрямку (районі), де можливі найбільш активні прояви протиправної діяльності, тобто на напрямку зосередження основних зусиль.

Для найбільш ефективної побудови охорони державного кордону необхідно врахувати висновки з результатів проведення тактичних розрахунків, які мають передбачати:

тактику дій правопорушників – характер та напрями протиправної діяльності, хитрощі, що ними застосовуються, пособницьку базу, час вчинення правопорушень тощо;

можливості своїх сил і засобів – їх наявність і стан, щільність охорони державного кордону, умови маневру, потрібний час прикордонним нарядам, черговим силам та резерву для перекриття загрозливих напрямків;

характер місцевості, стан доріг, обладнання ділянки інженерними загородженнями, контрольними та технічними засобами, віддаленість загороджень, сигналізаційних засобів від кордону; пору року, час доби, погодні умови тощо.

Застосування такого варіанта лінійної побудови охорони державного кордону дасть змогу контролювати всю ділянку відповідальності, спростить організацію та управління оперативно-службовою діяльністю підрозділу, забезпечить постійну присутність прикордонних нарядів в межах прикордонної смуги та контрольованого прикордонного району, що забезпечить профілактичний ефект (видима присутність сил стримує потенційних правопорушників). Але виникне необхідність у застосуванні значної кількості сил та засобів, зменшиться маневреність у розподілі сил між ділянками, не буде досягнута достатня ефективність на протяжних або малонаселених ділянках (особливо в гірській та лісистій місцевості).

Уникнути зазначених недоліків надасть можливість застосування *об'єктової побудови охорони державного кордону*, яка передбачає зосередження основних зусиль підрозділу на охороні окремих важливих об'єктів, напрямків або ділянок, що мають підвищене оперативне чи тактичне значення. Об'єктова побудова здійснюється з урахуванням конкретних об'єктів контролю (пунктів пропуску, населених пунктів, транспортних вузлів, переправ, природних перешкод, інженерних споруд тощо), основним принципом якої є селективність охорони – посилення контролю там, де ймовірність порушення чи загроза безпеці найбільша.

Об'єктова побудова охорона державного кордону буде найбільш доцільна:

при недостатній кількості необхідних сил і засобів, достатньо великій ділянці відповідальності підрозділу та особливостей протиправної діяльності;

у змішаних або населених районах, де багато транспортних комунікацій;

під час посиленої охорони державного кордону, а також проведення прикордонних операцій чи спеціальних заходів.

Застосування такого підходу дасть змогу забезпечити більш ефективне використання наявних сил та засобів, зосередити увагу на найбільш уразливих або важливих об'єктах, підвищити маневреність і гнучкість реагування на зміни обстановки. Основними елементами об'єктової побудови будуть: безпосередньо сам об'єкт охорони, прикордонні наряди, системи спостереження та технічного контролю, чергові сили та резерви, наявність взаємодії з іншими правоохоронними органами та військовими формуваннями.

Разом з тим, слід урахувати, що такий підхід матиме і свої недоліки:

недостатня увага для охорони суміжних ділянок, що створює ризик використання "проміжків" правопорушниками;

необхідність високого рівня оперативної взаємодії та координації;

підвищена вимога до аналітичної діяльності та системи збору даних обстановки.

Висновки. Побудова охорони державного кордону – це динамічна, адаптивна складова організації оперативно-службової діяльності, яка базується на пріоритетності, аналітичному управлінні та взаємодії сил. Вона забезпечує баланс між контролем і мобільністю**,** що особливо актуально в умовах сучасних загроз безпеці України. Тому, на вибір варіанта побудови охорони державного кордону впливатиме достатньо велика кількість факторів і безумовно обрати той, чи інший спосіб, який

задовільнить усі потреби досить складно, завжди будуть певні переваги та недоліки. Застосування лінійної побудови охорони державного кордону буде найбільш доцільним при достатньому рівні укомплектованості і виконанні завдань на місцевості, яка не обмежує маневреність сил та засобів підрозділу. Об'єктова побудова навпаки, буде ефективна при дефіциті особового складу, технічних засобів, і виконанні завдань у важкодоступних районах. У сучасних умовах достатньо важко обмежитись якимось певним варіантом, оскільки на вибір впливає велика кількість чинників, тому доцільно буде застосування комплексного підходу для забезпечення ефективної охорони державного кордону.

Подальші дослідження можуть бути спрямовані на розроблення методики визначення варіанта побудови охорони державного кордону з урахуванням характеристики ділянки відповідальності підрозділу. Поданий матеріал може бути використано під час розроблення проєкту Методичних рекомендацій з організації оперативно-службової діяльності підрозділами охорони державного кордону.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про Державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV. URL: https://zakon.rada.gov.ua/laws/show/661-15#Text (дата звернення: 15.09.2025).
2. Порядок роботи органів управління Державної прикордонної служби України з підготовки до оперативно-службової діяльності в наступному календарному році або іншому періоді : затв. наказом Міністерства внутрішніх справ України від 26.04.2018 № 350.
3. Братко А. В. Методика організації роботи органів управління Державної прикордонної служби України щодо планування оперативно-службової діяльності // Social development and Security. 2023. Vol. 13, No. 1. P. 29–37. DOI: https://doi.org/10.33445/sds.2023.13.1.4.
4. Братко А. В. Науково-методичний апарат планування оперативно-службової діяльності Державної прикордонної служби України // Збірник наукових праць Національної академії Державної прикордонної України. Серія : військові та технічні науки. 2022. № 4 (89). С. 5–25. DOI: https://doi.org/ 10.32453/3.v89i4.1314.
5. Михайленко О. В., Паламарчук Ю. С. Методика роботи начальника прикордонної застави щодо управління оперативно-службовою діяльністю в умовах правового режиму воєнного стану // Збірник наукових праць Національної академії Державної прикордонної України. Серія : Військові та технічні науки. 2025. № 1 (98). С. 46–56. DOI: https://doi.org/10.32453/3.v98i1.1771.
6. Бурбела С. В.Модель побудови охорони державного кордону на річковій ділянці // Social development and Security. Vol. 12, No. 1. 2022. DOI: https://10.33445/sds.2022.12.1.3.
7. Грінченко В. В., Андрощук О. С. Розробка аналітичного методу аналізу ефективності охорони державного кордону із застосуванням ймовірнісно-статистичного підходу // Системи обробки інформації. 2021. № 1 (164). С. 6–11. DOI: https://doi.org/10.30748/soi.2021.164.01.
8. Братко А. В., Більовський О. С. Методика планування оперативно-службової діяльності Державної прикордонної служби України // Національні інтереси України. 2025. № 1 (6). С. 171–180. DOI: https://doi.org/10.52058/3041-1793-2025-1(6)-171-180.
9. Інструкція з організації оперативно-службової діяльності відділу прикордонної служби Державної прикордонної служби України. Частина І : затв. наказом Адміністрації Державної прикордонної служби України від 29.12.2009 № 1040 (зі змінами).
10. Словник UA – портал української мови та культури. URL: https://slovnyk.ua/index.php?swrd (дата звернення 15.09.2025).

Стаття надійшла до редакції 17.10.2025

Analysis of approaches to state border protection in the unit's area of responsibility

Annotation

The article examines the theoretical and practical aspects of organizing the protection of the state border as a key element in the structure of operational and service activities within the area of responsibility of a border protection unit. The paper analyzes regulatory and administrative acts, scientific approaches, and practical experience of border protection authorities regarding the definition of the structure and content of border security organization. The study establishes that there is currently no unified methodological approach to the organization of state border protection, which complicates the formation of an effective system for managing the forces and means of the unit.

The main factors influencing the effectiveness of the protection system are identified. The expediency of implementing a linear structure along designated lines and terrain zones is substantiated, which ensures an optimal distribution of forces and resources, the creation of a flexible response system, and the rational deployment of technical surveillance means, engineering structures, and barriers. A

comparative analysis of linear and object-based models of border protection is carried out, with their advantages, disadvantages, and conditions of effective application determined. In particular, the linear model provides continuous monitoring and timely detection of violations but requires significant human and material resources. The object-based model, in turn, allows for the concentration of efforts on the most critical directions, ensuring operational responsiveness and efficient resource utilization, though it provides insufficient control over secondary directions.

It is emphasized that the choice of border protection model should be based on the principles of flexibility, adaptability, and comprehensiveness, taking into account the prevailing operational situation. The study highlights the need to improve the scientific and methodological framework for determining the organization of state border protection, which will enhance the effectiveness of operational and service activities of border protection units.

Keywords: state border protection; organization of border security; linear model; object-based model; border unit; line; terrain zone.

УДК 355.02:330.16(477) https://doi.org/10.33099/2304-2745/2025-3-86/44-50

Гаврилюк І. Ю., кандидат військових наук, старший дослідник
(0000-0002-3514-0738)

Центральний науково-дослідний інститут Збройних Сил України, Київ

Рекомендації щодо підвищення рівня воєнно-економічної безпеки України

Резюме. Стаття присвячена формуванню рекомендацій щодо підвищення рівня воєнно-економічної безпеки України в умовах сучасних воєнних конфліктів. Проаналізовано сучасні виклики, пов'язані з гібридними загрозами, економічним тиском і руйнуванням інфраструктури, а також наведено систему показників оцінювання економічної стійкості.

Ключові слова: воєнно-економічна безпека; сучасні воєнні конфлікти; економічна стійкість; оборонно-промисловий комплекс; оборонне планування.

Постановка проблеми. Важливе місце в забезпеченні національної безпеки України займають економічні виклики, пов'язані із збройною агресією Російської Федерації (РФ) та тимчасовою окупацією частини території України. Руйнування економіки є цілеспрямованою дією противника та одним з методів гібридної війни, оскільки зруйнована економіка продукує незадоволеність владою, трудову міграцію, соціальну напругу в суспільстві та підриває довіру до державних інституцій [1]. При цьому широко використовуються економічні інструменти впливу, до яких належать санкції щодо українських товарів і послуг та тиск на інші держави з метою прийняття рішень, що суперечать основним національним і економічним інтересам України [2–3].

Наукові дослідження підкреслюють, що сучасні війни виходять за межі традиційних бойових дій. Економічний тиск, кібератаки, енергетичний шантаж та інформаційні операції стали ефективними інструментами впливу на національну безпеку держав [4–5]. Аналіз показує, що економічна стійкість і обороноздатність взаємопов'язані, а їх забезпечення потребує комплексного підходу, який поєднує правові, фінансові, технологічні та соціальні механізми управління [6].

Дослідження Національного інституту стратегічних досліджень демонструють, що стан економіки України стабілізувався у 2023 році, попри значні збитки від війни. Економічне зростання становить 5,3%, однак реальний ВВП – лише 75% від довоєнного рівня, а відновлення повного потенціалу може зайняти 6–7 років, що потребує значних інвестицій та довгострокової міжнародної підтримки [1–5].

Для забезпечення воєнно-економічної безпеки критично важливо визначати ключові показники стану економіки, що впливають на обороноздатність та економічну стійкість держави в умовах сучасних воєнних конфліктів. До таких показників належать ефективність витрат на оборону, мобілізаційні та логістичні спроможності, рівень розвитку критичної інфраструктури та фінансова стабільність [7–8]. Відповідно до наукових підходів, інтеграція ризик-орієнтованого аналізу з прогнозуванням кризових сценаріїв дає змогу обґрунтувати рекомендації щодо підвищення адаптивності економіки та оптимізувати розподіл ресурсів для потреб оборони [3].

Таким чином, актуальним є розроблення рекомендацій, які дають змогу підвищити рівень воєнно-економічної безпеки України в умовах збройної агресії РФ проти України.

Аналіз останніх досліджень і публікацій. Отримані результати дослідження засвідчують, що воєнно-економічна безпека України в умовах сучасних воєнних конфліктів формується під впливом комплексу взаємопов'язаних факторів – фінансових, ресурсних, виробничих, інституційних та управлінських. Відповідно до положень Закону України "Про національну безпеку України", економічна стійкість держави визначається як одна з ключових складових системи національної безпеки [10]. У процесі аналізу встановлено, що порушення збалансованості між оборонними потребами та економічними можливостями держави призводить до зростання ризиків дестабілізації всієї безпекової системи. Результати узгоджуються з положеннями Стратегії воєнної безпеки України, де наголошується на необхідності інтеграції економічного потенціалу у систему оборонного планування [11]. Таким чином, воєнно-економічна безпека розглядається як

динамічний процес адаптації економіки до умов воєнного протистояння.

На основі узагальнення наукових підходів доведено, що ключову роль для обґрунтування заходів щодо підвищення рівня воєнно-економічної безпеки відіграє обґрунтована система показників її оцінювання. Як свідчать результати досліджень, висвітлених у працях [4, 8] ефективна система індикаторів має відображати реальний стан оборонного виробництва, рівень фінансового забезпечення сектору безпеки, мобілізаційні можливості держави та спроможності логістичних систем. У процесі дослідження встановлено, що використання фрагментарних показників не дає змоги отримати повну картину стану воєнно-економічної безпеки. Натомість комплексний підхід забезпечує більш точне прогнозування кризових сценаріїв та можливих втрат оборонного потенціалу. Це підтверджує необхідність переходу до системного оцінювання воєнно-економічних загроз.

Результати аналізу сучасних воєнних конфліктів підтверджують зростання ролі ефективності оборонних видатків як одного з головних чинників воєнно-економічної безпеки. За даними дослідження [7] нераціональне використання фінансових ресурсів у секторі оборони суттєво знижує загальний рівень стійкості економіки в умовах гібридної війни.

Дослідження також свідчать, що навіть за умови зростання обсягів фінансування оборонної сфери відсутність прозорих механізмів управління витратами призводить до зниження їх ефективності. Водночас сучасна концепція управління економікою воєнного стану передбачає глибоку інтеграцію фінансового контролю, планування та стратегічного прогнозування [6]. Це потребує перегляду підходів до бюджетного забезпечення сектору безпеки й оборони.

Вагомим результатом дослідження є обґрунтування необхідності застосування ризик-орієнтованого підходу до формування рекомендацій щодо зміцнення воєнно-економічної безпеки. Як зазначено у [3] ефективна система воєнної безпеки повинна базуватися на постійному оцінюванні й прогнозуванні ризиків реалізації кризових сценаріїв. Аналогічні висновки зроблено у роботі [1], де доведено необхідність урахування не лише воєнних, а й економічних, логістичних та технологічних загроз. У результаті встановлено, що саме інтеграція ризик-орієнтованого підходу в систему оборонного планування дає змогу підвищити адаптивність економіки до затяжних воєнних конфліктів. Це створює основу для розроблення практично орієнтованих рекомендацій щодо зміцнення обороноздатності держави.

Мета статті – обґрунтування рекомендацій щодо підвищення рівня воєнно-економічної безпеки України з урахуванням змін у характері сучасних воєнних конфліктів.

Виклад основного матеріалу. Узагальнення результатів аналізу нормативно-правових засад, науково-методологічних підходів та сучасних ризиків воєнно-економічної безпеки дало змогу перейти від теоретичного осмислення проблеми до формування практично орієнтованих рекомендацій. Встановлено, що ефективне забезпечення воєнно-економічної безпеки держави в умовах трансформації характеру сучасних воєнних конфліктів потребує чіткої систематизації управлінських рішень за рівнями пріоритетності, з урахуванням їх впливу на стійкість економіки, оборонний потенціал та адаптивність інституцій. Саме це зумовило необхідність структурованого подання рекомендацій у вигляді ієрархічної моделі.

З огляду на це, у Табл. 1 подано систематизований перелік рекомендацій щодо підвищення рівня воєнно-економічної безпеки держави з урахуванням змін у характері сучасних воєнних конфліктів, розподілений за трьома рівнями пріоритетності із зазначенням їх орієнтовної частки впливу та очікуваних результатів реалізації.

До **пріоритету 1 (найвищого)**, що охоплює близько 50% загального впливу, віднесено стратегічну розбудову оборонно-промислового комплексу, забезпечення кібербезпеки критичної інфраструктури, протидію гібридним загрозам, формування резильєнтних ланцюгів постачання та зміцнення енергетичної стійкості. Саме ці напрями визначають базову здатність держави до автономного забезпечення фронту, зниження залежності від імпорту озброєнь, запобігання дестабілізації економіки та мінімізації вразливості до енергетичного й інформаційного тиску.

Пріоритет 2 (високий), частка якого становить орієнтовно 38%, спрямований на інституційне, фінансове та кадрове забезпечення воєнно-економічної безпеки. Йдеться про зміцнення фінансової безпеки та санкційної стійкості, удосконалення правового

регулювання воєнно-економічної мобілізації, розвиток людського капіталу для потреб оборони та децентралізацію виробництва і логістики. Реалізація цього блоку рекомендацій забезпечує безперервність фінансування сектору безпеки, прискорене переключення економіки на військові потреби та зниження вразливості до локальних уражень виробничої й транспортної інфраструктури.

Таблиця 1

Рекомендації щодо підвищення рівня воєнно-економічної безпеки держави з урахуванням змін у характері сучасних воєнних конфліктів

Пріоритет	Рекомендація	Вплив
Пріоритет 1 (Найвищий): Частка: ~50%	Стратегічна розбудова оборонно-промислового комплексу	Збільшить автономність у забезпеченні фронту, зменшить залежність від імпорту озброєнь
	Цілісна кібербезпека критичної інфраструктури та оборони	Зменшить ризик паралічу енергосистем, логістики та виробництва
	Комплексна протидія гібридним загрозам та інформаційним операціям	Зменшення політичної та соціальної дестабілізації, збереження довіри до інституцій
	Резилієнтні ланцюги постачання для критичних товарів	Стабілізація виробництва оборонної та цивільної продукції під час блокад
	Енергетична стійкість	Зменшує можливість енергетичного шантажу, підвищує стійкість логістики
Пріоритет 2 (Високий): Частка: ~38%	Фінансова безпека та санкційна стійкість	Забезпечує безперервність державного фінансування оборони
	Правове та регуляторне забезпечення воєнно-економічної мобілізації	Швидке переключення економіки на військові потреби
	Розвиток людського капіталу для оборони та критичних секторів	Забезпечує довгострокову спроможність виробляти, обслуговувати та модернізувати техніку
	Децентралізація виробництва та логістики	Знижує ефект від локальних ударів по виробництву/логістиці
Пріоритет 3 (Середній): Частка: ~12%	Стимулювання державно-приватного партнерства у фінансуванні оборонних ліній, інфраструктури та інновацій	Прискорює інвестиції в критичні потужності, розширює економічну базу для стійкості
	Контроль експорту/імпорту технологій	Перешкоджає потраплянню ключових технологій до супротивника
	Інституційна готовність до відновлення	Сприяє швидшому поверненню до економічної активності після атак/руйнувань

Пріоритет 3 (середній), частка якого складає близько 12%, охоплює інструменти довгострокового підсилення воєнно-економічної стійкості. До нього віднесено стимулювання державно-приватного партнерства у фінансуванні оборонних потужностей та інновацій, контроль експорту й імпорту критичних технологій, а також формування інституційної готовності до післявоєнного відновлення. Цей блок рекомендацій створює передумови для розширення інвестиційної бази оборонної економіки, унеможливлення витоку стратегічних технологій до противника та прискореного відновлення економічної активності після руйнувань.

Запропонована на рис. 1 сукупність загальних рекомендацій відображає інтегрований підхід до управління процесами забезпечення воєнно-економічної безпеки держави в умовах сучасних воєнних конфліктів. Її ключовою особливістю є поєднання стратегічних, інституційних та управлінських механізмів у єдину модель, орієнтовану на досягнення синергетичного ефекту. Координація заходів між органами державної влади, міжнародними партнерами та приватним сектором дає змогу мінімізувати дублювання функцій, підвищити ефективність використання ресурсів і забезпечити узгодженість дій у межах національної системи безпеки. Такий підхід відповідає сучасним уявленням про мережеву організацію оборонно-економічних процесів та необхідність багаторівневої взаємодії суб'єктів безпеки.

Важливою складовою запропонованої сукупності рекомендацій є залучення міжнародної підтримки як чинника фінансової, технологічної та інституційної стійкості держави. Розширення співпраці з міжнародними донорами та партнерами створює додаткові можливості для фінансування пріоритетних напрямів розвитку оборонно-промислового комплексу, модернізації критичної інфраструктури та впровадження сучасних технологічних рішень. У контексті тривалого воєнного протистояння міжнародна підтримка набуває не лише фінансового, а й стратегічного значення,

оскільки сприяє інтеграції України у глобальні безпекові та виробничі ланцюги, посилюючи її економічну та оборонну спроможність.

Окрему увагу в структурі загальних рекомендацій, представлених на рис. 1, приділено моніторингу прогресу реалізації заходів як інструмента адаптивного управління воєнно-економічною безпекою. Запровадження системи регулярного оцінювання ефективності дає змогу своєчасно виявляти відхилення від запланованих показників, коригувати стратегічні пріоритети та оперативно реагувати на зміну умов воєнно-економічного середовища. Такий механізм забезпечує гнучкість управлінських рішень, знижує рівень стратегічних ризиків і підвищує спроможність держави до стійкого функціонування в умовах високої невизначеності.

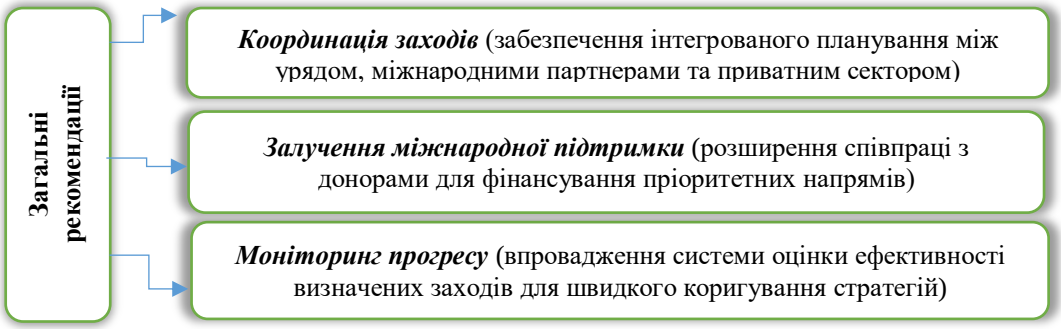

Рис. 1. Узагальнені рекомендації щодо забезпечення воєнно-економічної безпеки України в умовах сучасних воєнних конфліктів

Водночас загальні рекомендації щодо забезпечення воєнно-економічної безпеки (див. рис. 1) потребують конкретизації на рівні функціонування економічної інфраструктури як критичної основи обороноздатності держави. Саме стійкість інфраструктурних систем визначає здатність економіки витримувати тривалі воєнні навантаження, забезпечувати безперервність виробництва, енергопостачання, логістики та управління ресурсами. У зв'язку з цим наступним етапом дослідження є формування прикладних рекомендацій, спрямованих на підвищення стійкості економічної інфраструктури до сучасних воєнних загроз, що потребує поєднання інструментів моніторингу, прогнозування та адаптивного управління вже на операційному рівні.

В умовах зростання інтенсивності сучасних воєнних загроз особливої актуальності набуває проблема забезпечення стійкості економічної інфраструктури як системоутворювального елемента воєнно-економічної безпеки держави. Саме критична інфраструктура – енергетика, транспорт, зв'язок, промисловість, фінансовий сектор – визначає здатність економіки до безперервного функціонування в умовах бойових дій, ракетних атак, кібервпливів та логістичних обмежень. Тому формування спеціалізованих рекомендацій щодо підвищення її стійкості потребує застосування комплексного, проактивного та адаптивного підходів до управління, що зумовлює необхідність побудови відповідної структурно-логічної моделі.

Подана на рис. 2 структурно-логічна модель рекомендацій щодо підвищення стійкості економічної інфраструктури до сучасних воєнних загроз відображає поетапний і взаємопов'язаний характер управлінських рішень у сфері безпеки.

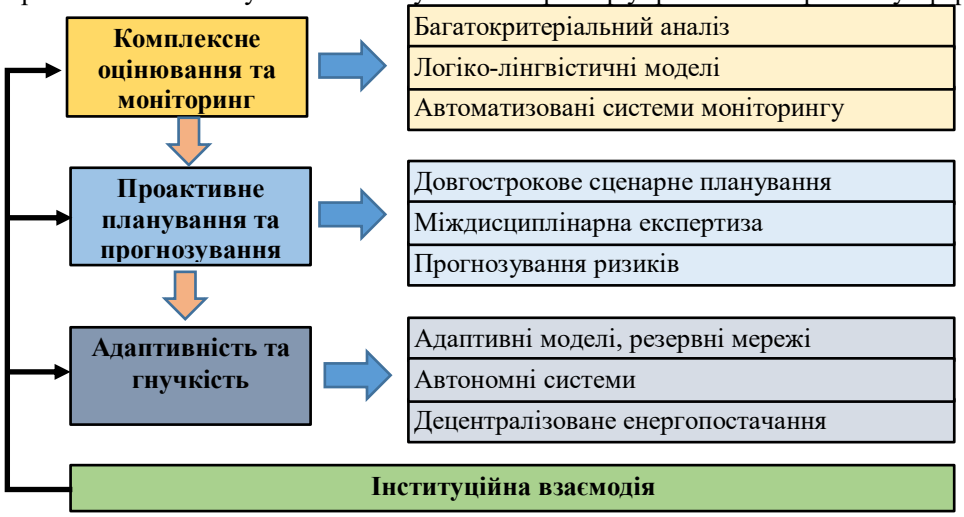

Рис. 2. Рекомендації щодо підвищення стійкості економічної інфраструктури до сучасних воєнних загроз

Базовим елементом цієї системи визначено комплексне оцінювання та моніторинг, що формує інформаційну основу для всіх наступних управлінських дій. Використання багатокритеріального аналізу, логіко-лінгвістичних моделей та автоматизованих систем моніторингу дає змогу забезпечити об'єктивність оцінювання стану інфраструктури, своєчасне виявлення уразливостей та прогнозування критичних відхилень у функціонуванні економічних об'єктів.

Наступним логічним рівнем, відображеним на рис. 2, є проактивне планування та прогнозування, що базується на результатах комплексного моніторингу. Довгострокове сценарне планування у поєднанні з міждисциплінарною експертизою створює основу для формування випереджальних управлінських рішень в умовах високої невизначеності. Прогнозування ризиків стійкості економічної інфраструктури (обмеження фінансування, застарілі технологічні процеси, необхідність захисту об'єктів критичної інфраструктури тощо) у цьому контексті дає змогу не лише реагувати на вже реалізовані загрози, а й завчасно формувати механізми їх мінімізації, що є критично важливим для забезпечення безперервності функціонування економічної інфраструктури в умовах воєнного протистояння.

Завершальним функціональним блоком моделі виступає адаптивність та гнучкість інфраструктурних систем, що передбачає впровадження адаптивних моделей управління, створення резервних мереж, розвиток автономних систем та децентралізованого енергопостачання. Саме цей рівень забезпечує практичну реалізацію стійкості економічної інфраструктури до фізичних, кібернетичних і техногенних впливів. Децентралізація критичних ресурсів зменшує вразливість до локальних уражень, а автономні системи підвищують здатність об'єктів до самостійного функціонування в умовах порушення централізованих каналів постачання.

Інтегрувальним елементом усієї представленої системи, як показано на рис. 2, є інституційна взаємодія, що поєднує органи державної влади, місцеве самоврядування, бізнес-структури та сектор безпеки і оборони. Саме узгодженість дій між цими суб'єктами забезпечує ефективність реалізації заходів моніторингу, планування та адаптації. Інституційна координація дає змогу мінімізувати фрагментарність управлінських рішень, підвищити швидкість реагування на загрози та сформувати єдину систему управління стійкістю економічної інфраструктури в умовах сучасних воєнних викликів.

Визначення необхідної величини державного бюджету для забезпечення обороноздатності держави є критичною складовою системи воєнно-економічної безпеки. Ефективне фінансування сил оборони дає змогу підтримувати високий рівень оперативної готовності та технологічного розвитку військового потенціалу, що є необхідним у контексті сучасних воєнних конфліктів та гібридних загроз [4, 7]. Наукові дослідження підкреслюють важливість комплексного підходу до формування оборонного бюджету, що враховує як економічні можливості держави, так і стратегічні потреби сектору безпеки і оборони [3]. Такий підхід передбачає інтеграцію методів оцінювання ризиків, прогнозування кризових сценаріїв та аналізу ефективності оборонних витрат, що сприяє забезпеченню сталості воєнно-економічного потенціалу держави.

Особливої уваги потребує розроблення методологічних засад, що визначають оптимальні пропорції розподілу бюджетних коштів між оперативною діяльністю, модернізацією озброєння та соціальною підтримкою особового складу [8, 9]. Досвід України та інших країн, що зазнають впливу сучасних воєнних загроз, демонструє, що стратегічне планування оборонного фінансування повинно бути гнучким і адаптивним, з можливістю оперативного коригування у відповідь на зміни зовнішньополітичної та безпекової ситуації [6, 12, 13]. У цьому контексті нормативно-правові документи, такі як Закон України "Про національну безпеку" та "Стратегія воєнної безпеки", відіграють ключову роль у визначенні мінімальних стандартів фінансування оборонного сектору та гарантують відповідність бюджетних рішень національним інтересам [10, 11].

Висновки. У статті запропоновано рекомендації щодо підвищення рівня воєнно-економічної безпеки України в умовах трансформації сучасних воєнних конфліктів. З огляду на це, надано систематизований перелік рекомендацій, розподілений за трьома рівнями пріоритетності із зазначенням їх орієнтовної частки впливу та очікуваних результатів реалізації. Визначено, що доля найвищого пріоритету рекомендацій охоплює близько 50% загального впливу на стратегічні

напрямки воєнно-економічної безпеки. Також визначено важливість процесу моніторингу реалізації заходів у стратегічних напрямках, як інструмента адаптивного управління воєнно-економічною безпекою.

В умовах зростання інтенсивності сучасних воєнних загроз запропоновано спеціалізовані рекомендації щодо забезпечення стійкості економічної інфраструктури як сукупності комплексного, проактивного та адаптивного підходів до управлінських рішень у сфері безпеки.

Подальші дослідження доцільно зосередити на моделюванні економічної стійкості держави з урахуванням глобальних загроз, інтеграції цифрових технологій для прогнозування воєнно-економічних ризиків та розробленні адаптивних стратегій управління ресурсами в умовах тривалих конфліктів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Семененко О., Абрамова М., Воронченко І., Добровольський Ю., Коротя В., Совгіря Т. Рекомендації щодо вибору та обґрунтування шляхів підвищення рівня воєнно-економічної безпеки України під час дії воєнного стану в умовах російсько-української війни (24.02.22–30.09.22 рр.) // Social Development and Security. 2022. Vol. 12, No. 5. P. 41–54. DOI: 10.33445/sds.2022.12.5.5.
2. Богданович В. Ю., Свида І. Ю., Скулиш Є. Д. Теоретико-методологічні основи забезпечення національної безпеки України : монографія : у 7 т. Київ : Науково-видавничий відділ НА СБ України, 2012. Т. 4. : Воєнна безпека держави і шляхи її забезпечення. 464 с.
3. Богданович В., Муженко В., Луцький О. Концепція забезпечення воєнної безпеки України на основі оцінювання та прогнозування ризиків реалізації кризових сценаріїв // Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки. 2023. № 4(93). P. 4–19.
4. Семененко О. М. Методологічні основи воєнно-економічного супроводження програм розвитку Збройних Сил України : дис. … д-ра військ. наук / ЦНДІ ЗС України. Київ, 2018.
5. Гаврилюк І., Клят Ю., Водчиць О. та ін. Щодо оцінювання воєнно-економічної безпеки України в умовах сучасних воєнних конфліктів // Social Development and Security. 2025. Vol. 15, No. 1. P. 19–25.
6. Соколи І. І., Близнюк О. В., Гребеникова Н. А., Хачатурянц Я. В., Краснюк А. В. Концептуальні основи управління економікою воєнного стану // Український журнал прикладної економіки та техніки. 2024. Vol. 9, No. 4. P. 395–402. DOI: 10.36887/2415-8453-2024-4-60.
7. Петренко І. Ефективність витрат на оборону в умовах гібридної війни: аналіз українського досвіду // Науковий вісник Міністерства оборони України. 2021. No. 60.
8. Семененко О. М., Бойко Р. В., Водчиць О. Г., Добровольський Ю. Б., Бердочник Д. В., Ярошенок А. В. Основні методологічні аспекти воєнно-економічного забезпечення обороноздатності держави: теорія та практика // Системи обробки інформації. 2017. № 3 (51). С. 165–175.
9. Методологія комплексного використання військових і невійськових сил та засобів сектора безпеки і оборони для протидії сучасним загрозам воєнній безпеці України : 2-ге вид., розш. та доповн. / В. Ю. Богданович та ін. Київ : НУОУ, 2021.
10. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII // Відомості Верховної Ради України. 2018. No. 31. Ст. 241.
11. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року “Про Стратегію воєнної безпеки України” : Указ Президента України від 25.03.2021 № 121/2021. URL: http://www.president.gov.ua/documents/1212021-37661 (дата звернення: 10.09.2025).
12. Семененко О. М., Бойко Р. В., Водчиць О. Г., Масловський В. В. Основні методологічні аспекти воєнно-економічного обґрунтування перспективних напрямів розвитку Збройних Сил України // Збірник наукових праць ХНУПС. 2018. № 1 (55). P. 37–45.
13. Семененко О. М., Водчиць О. Г., Кондратенко О. І., Іванов В. Л. Петренко С. В. Сучасні особливості формування оборонного та воєнно-економічного потенціалів України // Збірник наукових праць Військової академії (м. Одеса). 2020. Ч. ІІ, № 2 (14). P. 148–155.

Стаття надійшла до редакції 11.12.2025

Recommendations for increasing the level of military-economic security of Ukraine

Annotation

Economic challenges arising from the armed aggression of the Russian Federation (RF) and the temporary occupation of parts of Ukraine’s territory play a critical role in ensuring Ukraine's national security. Economic instruments of influence are being widely deployed, including sanctions against Ukrainian goods and services, as well as pressure on other states to adopt decisions that contravene Ukraine's fundamental national and economic interests.

To ensure military-economic security, it is vital to identify key economic indicators that impact the state's defense capability and resilience in modern armed conflicts. These indicators include the

efficiency of defense expenditures, mobilization and logistical capacities, the development level of critical infrastructure, and financial stability. According to scientific approaches, integrating risk-oriented analysis with crisis scenario forecasting enhances economic adaptability and optimizes resource allocation for defense needs.

The purpose of the article is to substantiate recommendations for improving the level of Ukraine's The article proposes specific recommendations for enhancing Ukraine's military-economic security amid the transformation of modern warfare. It is substantiated that determining the required volume of the state budget for the defense forces is not merely a technical calculation but a strategic tool for building national resilience. Effective financing must ensure a balance between the immediate needs of operational activities and long-term investments in arms modernization and critical infrastructure development. In this context, the budget serves not only as a financial resource but as a mechanism for managing defense potential and a factor in increasing the state's adaptability to changes in modern armed conflicts.

Keywords: military-economic security; modern military conflicts; economic stability; defense-industrial complex; defense planning.

УДК 658.012.32 https://doi.org/10.33099/2304-2745/2025-3-86/51-59

Артамощенко В. С., доктор військових наук, доцент (0000-0002-7734-4210)
Загорка О. М., доктор військових наук, професор (0000-0003-1131-0904)
Гудима О. П., кандидат технічних наук, старший науковий співробітник (0000-0002-3494-8583)
Поліщук С. В. кандидат військових наук, доцент (0000-0001-9050-6918)

Національний університет оборони України, Київ

Застосування нечіткого підходу до визначення складу організаційної структури

Резюме. Викладено методичні положення, на підставі яких розроблено методику визначення складу організаційної структури в умовах дій невизначених факторів, що впливають на створення і застосування (функціонування) організації. Методика ґрунтується на порівнянні варіантів організаційної структури з використанням методу таксономії, вихідними даними для якого є центр ваг нечітких чисел, що відповідають лінгвістичним змінним, які надаються експертами показникам, що характеризують функціонування організації.

Ключові слова: склад організаційної структури; групування завдань; планування експерименту; лінгвістичні змінні; центр ваги нечітких чисел; метод таксономії.

Постановка проблеми. Під час створення або удосконалення будь-якої організації, зокрема військової, виникає потреба у визначенні складу її структури для виконання завдань за призначенням відповідно до місії організації. Організаційна структура має забезпечувати потрібну ефективність виконання завдань організації при раціональних витратах на її створення і застосування, що характеризує її збалансованість.

Визначення складу організаційної структури здійснюється з урахуванням як різноманітних завдань, так і невизначеності факторів внутрішнього і зовнішнього середовища, що впливають на їх виконання.

Узагалі, визначення складу організаційної структури можна розглядати як задачу структурного синтезу, для розв’язання якої можна використовувати принципи системного аналізу, зокрема варіантний метод. Це потребує застосування методів багатовимірного порівняльного аналізу в умовах невизначеності факторів, що впливають на виконання завдань організації. При цьому слід вважати, що задача не може бути представлена у формалізованому вигляді у зв’язку з неможливістю отримання однозначних математичних виразів показників (критеріїв) для визначення найкращого варіанта складу організаційної структури.

Аналіз останніх досліджень і публікацій. Методологічні положення синтезу організаційних структур підприємств, які гуртуються на застосуванні методу таксономії [1] для порівняльного оцінювання рівня розвитку їх варіантів, наведено у праці [2]. Проте у праці не враховується вплив невизначеності факторів на створення і застосування організації. Також фрагментарно викладені підходи до формування можливих варіантів складу організаційної структури.

У праці [3] для формування варіантів організаційної структури запропоновано використовувати планування експерименту [4]. Невизначеність факторів, що впливають на створення і застосування організації у праці також не враховується. Слід також зазначити, що методичні підходи до групування завдань організації, що наведені у працях [2, 3] потребують найбільшого розкриття, що може позитивно вплинути на обґрунтованість визначення складу організаційної структури.

Варіанти організаційної структури під час визначення її складу розглядаються як альтернативи.

Для ранжирування альтернатив в умовах невизначеності у праці [5] під час прийняття рішень запропоновано використовувати вихідні дані у вигляді функцій належності нечітких чисел трикутного виду, лінгвістичні терми яких визначаються експертами. Проте методи ранжирування, що наведено у статті, не дають змоги обґрунтовано визначити найкращу альтернативу за принципами збалансованості через використанням узагальнених показників під час прийняття рішень.

Отже, потребують удосконалення питання, що стосуються групування завдань організації та врахування невизначеності дій факторів під час багатовимірного

порівняльного аналізу можливих варіантів складу організаційної структури. Це обумовлює доцільність проведення дослідження, присвяченого розвитку методичних положень визначення складу організаційних структур.

Мета статті – удосконалення методичних положень визначення складу організаційних структур на підставі врахування невизначеності факторів, що впливають на їх створення і застосування.

Виклад основного матеріалу. У теорії організації розглядається багато типів організаційних структур. Найбільш загальною вважається дивізіональна структура [2, 3], яку доцільно прийняти за основу під час удосконалення методичних положень визначення складу організаційних структур як цивільного, так і військового призначення.

Дивізіональна організаційна структура (рис. 1) має паралельні гілки, що містять свої підрозділи – виконавці завдань зі своїм керівництвом. Основні завдання організації виконуються підрозділами, які підпорядковані органам функціонального управління, а завдання забезпечення і обслуговування – органу загального керівництва організації [3].

Рис. 1. Дивізіональна організаційна структура

Основу організаційної структури визначають типи і кількість підрозділів, потрібних для виконання завдань організації.

Відповідно до місії (мети діяльності) організація повинна вирішувати m функцій $A_j\left(j=\overline{1,m}\right)$, для виконання яких визначається n завдань $B_i\left(i=\overline{1,n}\right)$. Однією з центральних задач синтезу організаційної структури є задача групування завдань [2] з метою визначення потрібних типів підрозділів – виконавців.

Сутність групування полягає у визначенні сукупності взаємопов'язаних завдань, що можуть виконуватися сумісно, за установленими принципами (ознаками) відповідно до функцій організації.

Під час оцінювання взаємозв'язку виконання завдань можуть враховуватися ознаки, які характеризують:

мету і результати виконання завдань;

протікання процесу виконання завдань, зокрема за часом;

професію фахівців для виконання завдань;

оснащеність підрозділів потрібним обладнанням, засобами;

райони (зони) місцевості застосування підрозділів тощо.

Ступінь взаємозв'язку i-го та ν-го завдання кількісно визначається експертами з урахуванням F ознак (f=$\overline{1,F}$), за формулою

$$a_{i\nu}=\sum_{\mathrm{f}=1}^{\mathrm{F}} \mathrm{w_f}\, a_{i\nu f}, \qquad (1)$$

де $\mathrm{w_f}$ – коефіцієнт значущості f-ї ознаки;

$a_{i\nu \mathrm{f}}$ – ступінь взаємозв'язку i-го та ν-го завдання за f-ю ознакою.

Далі складається матриця коефіцієнтів $[a_{i\nu}]_n$, яка є основою для формалізації задачі групування завдань.

Відповідно до методу розбивання елементів кінцевої множини на групи, що наведено у праці [1], з матриці $[a_{i\nu}]_n$ визначається критичний ступінь взаємозв'язку завдань за формулою

$$\rho=\overline{a}+\xi\sigma\ , \qquad (2),$$

де $\overline{a}=\frac{2}{n(n-1)}\sum_{i=1}^{n-1}\sum_{\nu=i+1}^{n} a_{i\nu}$,

$$\sigma=\left[\frac{2}{n(n-1)}\sum_{i=1}^{n-1}\sum_{\nu=i+1}^{n}(a_{i\nu}-\overline{a})^2\right]^{1/2};$$

ξ – коефіцієнт (дійсне невід'ємне число, визначається експертом).

Порядок групування завдань полягає у такому:

для кожного завдання $B_i\left(i=\overline{1,n}\right)$ з матриці $[a_{i\nu}]_n$, визначаються завдання B_μ, для яких виконується умова:

$$B_\mu=\left\{B_\mu \epsilon n: a_{i\nu}\geq\rho\right\}, i=\nu=\overline{1,n} \qquad (3);$$

підраховується кількість завдань b_i, для яких виконується вимога (3);

визначається перша група завдань, для якої b_i=maxb_i;

з матриці $[a_{i\nu}]_n$ виключаються завдання, які належать визначеній групі.

Таким же чином визначається наступна група завдань. Процедура продовжується до повного вичерпання завдань.

Кількість груп $K\left(k=\overline{1,K}\right)$ і кількість завдань у кожній k-й групі b_k залежить від коефіцієнта ξ. Частіше приймається ξ=1 [1, 3]. Кількість груп може збільшуватися як при збільшенні, так і при зменшенні коефіцієнта ξ. У першому випадку це пояснюється зменшенням кількості завдань у складі перших груп, у другому випадку – їх збільшенням, що викликає зниження можливостей формування наступних груп.

Під час визначення складу організаційної структури доцільно розглядати декілька варіантів групування завдань, які відрізняються коефіцієнтами ξ. За показник для порівняння варіантів групування завдань можна використати сумарну величину ступенів взаємозв'язку завдань A, яка визначається за формулою [2]

$$A=\sum_{k=1}^{K}A_k=\sum_{k}^{K}\sum_{i,v\epsilon b_k}a_{iv}, \qquad (4)$$

де A_k – сумарна величина ступенів взаємозв'язку k-ї групи завдань.

Кращим вважається варіант групування завдань, для якого показник A максимальний.

Відповідно до загальних принципів системного аналізу для визначення складу організаційної структури, як і у праці [3], використовується варіантний метод. Варіанти організаційної структури відрізняються кількістю підрозділів – виконавців, типи яких визначені шляхом групування завдань.

Для формування варіантів організаційної структури пропонується використати планування багатофакторного експерименту [4, 5]. За фактори (параметри) приймаються типи підрозділів – виконавців завдань. Звичайно використовуються три рівні варіювання параметрів: нульовий (початковий), мінімальний, максимальний. Рівні варіювання параметрів (кількості підрозділів – виконавців) призначаються, виходячи з досвіду створення подібних організаційних структур та потрібної кількості підрозділів за типами для виконання завдань, що визначається експертами. Ураховується також припустима кількість фахівців у підрозділах для виконання завдань. Таким чином складається матриця планування.

Вважається, що в матриці планування мають бути вичерпані всі можливі сполучення кількісних рівнів підрозділів – виконавців завдань. Кількість варіантів складу організаційної структури залежить від кількості типів підрозділів – виконавців завдань і кількості рівнів їх варіювання. Під час формування варіантів організаційної структури доцільно використовувати вже готові плани експериментів [7].

Функціонування організаційної структури, як правило, оцінюється сукупністю багатьох показників. Тому для визначення кращого варіанта організаційної структури потрібно використовувати методи багатовимірного порівняльного аналізу. Одним з таких методів, який отримав широке застосування під час розв'язання подібних задач, є метод таксономії [1]. Метод дає змогу врахувати під час порівняння альтернативних варіантів велику кількість різнорідних ознак (параметрів), які різним чином впливають на стан або функціонування об'єкта чи процесу дослідження.

Виконання завдань організацією здійснюється в умовах невизначеності дій факторів зовнішнього і внутрішнього середовища, вплив яких на функціонування організаційної структури породжує неоднозначність оцінювання показників, що є одним з видів невизначеності [8]. Одним з таких факторів є змінювання прогнозованих умов функціонування організаційної структури за період її створення. Можна вважати, що невизначеність притаманна вихідним даним, які використовуються під час розв'язання задачі визначення складу організаційної структури.

Традиційно під час розв'язання задач в умовах невизначеності застосовуються імовірнісно-статистичні методи [8]. Проте отримання законів розподілу чисельних значень показників, що характеризують функціонування організаційної структури, під час її створення не завжди можливе. Такі показники вважаються стохастично невизначеними.

Це обумовлює доцільність застосування під час визначення складу організаційної структури нечіткого множинного підходу, під час використанні якого оцінювання показників здійснюється експертами.

Пропоновано значення показників розглядати, як терми таких лінгвістичних змінних: дуже низький (ДН), низький (Н), середній (С), високий (В), дуже високий (ДВ).

Для представлення лінгвістичних змінних (фазифікації) використовуються трикутні терми, які описуються триплетами.

Коли дві сторони трикутників рівні, вказаним лінгвістичним змінним відповідають нечіткі числа (триплети): ДН (0; 0; 0,25); Н (0; 0,25; 0,50); С (0,25; 0,50; 0,75); В (0,50; 0,75; 1,00); ДВ (0,75; 1,00; 1,00).

Слід зазначити, що інтервали нечітких чисел, які відповідають лінгвістичним змінним, можуть відрізнятися за розміром, а триплети відповідати трикутникам, сторони яких розрізняються.

Кожний l-й показник $\left(l = \overline{1,L}\right)$ r-го варіанта організаційної структури $\left(r = \overline{1,R}\right)$ оцінюється експертами з використанням наведених вище лінгвістичних змінних. Нечіткі числа (триплети), що надаються кожним q-м експертом $\left(q = \overline{1,Q}\right)$ l-му показнику r-го варіанта організаційної структури, можна записати у такому вигляді:

$$\widetilde{\chi_{rl}^{q}} = \left(\chi_{rl_1}^{q}, \chi_{rl_2}^{q}\chi_{rl_3}^{q}\right), \quad (5)$$

де $\chi_{rl_1}^{q}, \chi_{rl_2}^{q}\chi_{rl_3}^{q}$ – мінімальне, найбільш імовірне, максимальне нечітке число лінгвістичної змінної, що надається l-му показнику r-го варіанта організаційної структури q-м експертом.

Зважені середні нечіткі числа визначаються за формулами:

$$\chi_{rl_1} = \sum_{q=1}^{Q} w_q\, \chi_{rl_1}^{q} \qquad \chi_{rl_2} = \sum_{q=1}^{Q} w_q\, \chi_{rl_2}^{q} \qquad \chi_{rl_3} = \sum_{q=1}^{Q} w_q\, \chi_{rl_3}^{q}, \quad (6)$$

де w_q – коефіцієнт значущості q-го експерта.

Таким чином за результатами експертного оцінювання визначається функція належності $\mu(\chi_{rl})$ трикутного виду l-го показника для r-го варіанта організаційної структури з нечіткими числами $\chi_{rl_1}, \chi_{rl_2}, \chi_{rl_3}$.

Для визначення кращого варіанта організаційної структури з використанням методу таксономії необхідно нечіткі числа [6] перетворити в чіткі – здійснити дефазифікацію. Для цього пропонується розраховувати центри ваг нечіткого числа [9] відповідних функцій належності $\mu(\chi_{rl})$.

Залежність для визначення центра ваги нечіткого числа функції належності трикутного виду має вигляд [5].

$$C_{rl} = \frac{(x_{rl_3} - x_{rl_1}) + (x_{rl_2} - x_{rl_1})}{3} + x_{rl_1}. \quad (7)$$

Коли терми лінгвістичних змінних описуються трикутниками з двома рівними сторонами, нечіткі числа, що визначаються за формулами (6), відповідають умові $\chi_{rl_3} - \chi_{rl_2} = \chi_{rl_2} - \chi_{rl_1}$. У цьому випадку центр ваги нечіткого числа визначається медіаною отриманого трикутника, тобто $C_{rl} = \chi_{rl_2}$.

Під час визначення складу організаційної структури експертами розглядаються показники, які характеризують ефективність (результативність) застосування організації за призначенням, а також витрати на її створення та функціонування. Звичайно розглядається тріада характеристик [3]: ефективність, час виконання завдань, витрати (вартість). Як варіант до таких показників належать:

ефективність функціонування (застосування) організації;

ефективність виконання завдань підрозділами визначеного типу;

час виконання завдань;

вартість створення організації;

вартість створення підрозділів визначеного типу – виконавців завдань;

вартість витрат на виконання завдань.

Наведена сукупність показників дає змогу з використанням методу таксономії визначити збалансований склад організаційної структури.

За результатами експертного оцінювання лінгвістичних змінних кожного l-го показника r-го варіанта організаційної структури для використання методу таксономії за формулою (7) розраховується центр ваги нечіткого C_{rl}. Для оцінювання показників можуть залучатися математичні моделі і аналітичні методики. Таким чином, складається матриця центрів ваг $[C_{rl}]RL$ для порівняння варіантів організаційної структури з використанням методу таксономії.

Відповідно до процедури застосування методу таксономії [1] здійснюється стандартизація центрів ваг нечітких чисел за формулою

$$C *_{rl} = \frac{C_{rl} - \overline{C_l}}{\sigma_l}, \quad (8)$$

де $\overline{C_l} = \frac{1}{R}\sum_{r=1}^{R} C_{rl}$; $\sigma_l = \left[\frac{1}{R}\sum_{r=1}^{R}(C_{rl} - \overline{C_l})^2\right]^{1/2}$.

Під час використання методу таксономії для порівняння альтернатив часто враховується важливість (значущість) показників, що сприяє отриманню збалансованого результату. Для оцінювання важливості показників доцільно використовувати експертний метод ранжирування [10].

Відповідно до цього методу експерт має розставити показники у порядку їх значущості і приписати кожному показнику числа натурального ряду. Показнику, що має найбільший вплив на створення організаційної структури, надається перший ранг, показнику, який є найменш впливовим – останній ранг.

Метод ґрунтується на використанні гіпотези про лінійну залежність між коефіцієнтом S_{lq}, що визначає відносну значущість l-го показника, і рангом P_{lq}, що

надається показнику q-м експертом. Коефіцієнт S_{lq} визначається за формулою

$$S_{lq} = 1 - \frac{P_{lq}-1}{L}. \quad (9)$$

Далі коефіцієнти S_{lq} масштабуються за формулою

$$b_{lq} = \frac{S_{lq}}{\sum_{l=1}^{L} S_{lq}}, \sum_{l=1}^{L} b_{lq} = 1. \quad (10)$$

Коли компетентність експертів однакова, коефіцієнт важливості l-го показника визначається як $b_l = \frac{1}{Q}\sum_{q=1}^{Q} b_{lq}$.

Коли компетентність q-го експерта оцінюється коефіцієнтом φ_q,

$\sum_{q=1}^{Q} \varphi_q = 1$, то $b_l = \sum_{q=1}^{Q} \varphi_q b_{lq}$. (11)

Вірогідність отриманих коефіцієнтів важливості показників оцінюється з використанням коефіцієнта конкордації

$$W = \frac{12D}{Q^2(L^3-L)}, \quad (12)$$

де $D = \sum_{l=1}^{L}(\sum_{q=1}^{Q} S_{lq} - \frac{1}{Q}\sum_{l=1}^{L}\sum_{q=1}^{Q} S_{lq})^2$. (13)

Вірогідність отриманих результатів вважається достатньою, коли $W \geq 0{,}7$.

У нашому випадку метод таксономії ґрунтується на використанні відстаней у багатомірному просторі між центрами ваг $C*_{rl}$, що характеризують показники варіантів організаційної структури, і еталонного варіанта $C*_{0l}$. Для визначення еталонного варіанта організаційної структури показники розподіляють на стимулятори і дестимулятори. Показники, збільшення яких спричиняє зростання ефекту застосування організації, відносять до стимуляторів, на відміну від дестимуляторів, зростання яких спричиняє зменшення такого ефекту. Відповідно до наведеної вище сукупності показників до стимуляторів належать показники, що характеризують ефективність, до дестимуляторів – час виконання завдань і вартість.

Еталонному варіанту організаційної структури відповідають значення центрів ваг

$$C*_{01}, C*_{02}, \dots, C*_{0l}, \dots, C*_{0L}, \quad (14)$$

де $C*_{0l} = maxC*_{rl}$, коли $l \in$ Ф;

$C*_{0l} = minC*_{rl}$, коли $l \in$ Ч;

Ф, Ч – стимулятори і дестимулятори відповідно.

Відстані визначаються за правилами аналітичної геометрії. Частіше для визначення відстаней використовується залежність [1]

$$Z_{r0} = \left[\sum_{l=1}^{L} b_l{}^2 (C*_{rl} - C*_{0l})^2\right]^{1/2}. \quad (15)$$

Ступінь переваги r-го варіанта організаційної структури визначається за формулою

$$\delta_r = 1 - \frac{Z_{r0}}{Z_0}, \quad (16)$$

де $Z_0 = \overline{Z_0} + 2\sigma_0$; $\overline{Z_0} = \frac{1}{R}\sum_{r=1}^{R} Z_{r0}$;

$\sigma_0 = \left[\frac{1}{R}\sum_{r=1}^{R}(Z_{r0} - \overline{Z_0})^2\right]^{1/2}$.

Кращому варіанту складу організаційної структури відповідає варіант, для якого показник $\delta_r = \max_r \delta_r$.

Обраний варіант складу організаційної структури перевіряється на відповідність вимогам за встановленим критеріям, зокрема щодо ефективності функціонування (застосування) організації. Коли вимоги не виконуються, можливе удосконалення групування завдань та планування експериментів, що обумовлює повторення розрахунків.

Структурна схема методики визначення складу організаційної структури показана на рис. 2.

Методикою визначається склад підрозділів – виконавців завдань організації. Склад органів загального керівництва і функціонального управління може визначатися на підставі врахування існуючих нормативів та досвіду створення подібних організацій.

При цьому враховуються функції A_j, які плануються вирішувати відповідно до мети діяльності організації.

Наведені методичні положення є подальшим розвитком праці [3], у якій під час визначення складу організаційної структури використовуються однозначні кількісні оцінки показників. Особливістю розроблених методичних положень є врахування невизначеності шляхом надання експертами показникам, що характеризують варіанти складу організаційної структури, лінгвістичних змінних для використання методу таксономії. Застосування такого підходу доцільно на етапі проєктування, коли кількісне оцінювання показників, що характеризують створення і функціонування (застосування) організаційної структури, скрутне, а у деяких випадках і зовсім неможливе.

Застосування методики визначення складу організаційної структури показано на ілюстративному прикладі. Розглядається 10 завдань, які повинна виконувати організація. Потрібна ефективність функціонування організації має бути не нижче 0,8.

Ступені взаємозв'язку завдань, що визначені експертами, наведені у Табл. 1.

Рис. 2. Структурна схема методики визначення складу організаційної структури

Таблиця 1

Ступені взаємозв'язку завдань

Номери завдань	1	2	3	4	5	6	7	8	9	10
1		0,75	0,28	0,32	0,40	0,31	0,79	0,82	0,64	0,42
2			0,34	0,51	0,65	0,41	0,30	0,70	0,82	0,50
3				0,83	0,78	0,30	0,25	0,68	0,15	0,35
4					0,56	0,78	0,20	0,35	0,42	0,81
5						0,62	0,31	0,84	0,71	0,62
6							0,16	0,50	0,83	0,74
7								0,14	0,10	0,15
8									0,63	0,18
9										0,20
10										

За результатами розрахунків середній ступінь взаємозв'язку завдань $\bar{a} = 0{,}49$, середнє квадратичне відхилення $\sigma = 0{,}25$. Звідки для коефіцієнта ξ=1 критичний ступінь взаємозв'язку завдань ρ=0.74.

Відповідно до порядку групування, що викладено вище, з матриці (див. табл. 1) визначено три групи завдань: (1, 2, 7, 8); (3, 4, 5); (6, 9, 10). Тому організаційна структура для виконання завдань повинна мати три типи підрозділів. Ураховуючи варіювання кількістю підрозділів на трьох рівнях, план експерименту містить 10 варіантів організаційної структури [7].

Початковими рівнями (0) під час складання плану експерименту визначено: для підрозділів першого типу – 4 підрозділи; для підрозділів другого і третього типу – 3 підрозділи. Мінімальний (–1) і максимальний (+1) рівні варіювання для підрозділів першого

типу складають 2 і 6 підрозділів, для другого і третього типу – 2 і 4 підрозділи відповідно. План обчислювального експерименту наведено у Табл. 2.

Таблиця 2

План обчислювального експерименту

Номер варіанта організаційної структури	Позначення рівня варіювання та кількість підрозділів – виконавців завдань		
	першого типу	другого типу	третього типу
1	(-1) / 2	(+1) / 4	(-1) / 2
2	(-1) / 2	(+1) / 4	(+1) / 4
3	(-1) / 2	(0) / 3	(0) / 3
4	(+1) / 6	(-1) / 2	(0) / 3
5	(-1) / 2	(-1) / 2	(-1) / 2
6	(0) / 4	(0) / 3	(+1) / 4
7	(-1) / 2	(-1) / 2	(+1) / 4
8	(+1) / 6	(0) / 3	(-1) / 2
9	(+1) / 6	(+1) / 4	(+1) / 4
10	(0) / 4	(+1) / 4	(0) / 3

Для визначення складу організаційної структури використовуються показники:

E_r – ефективність функціонування (застосування) r-го варіанта організаційної структури;

E_{rk} – ефективність виконання завдань підрозділами k-го типу r-го варіанта організаційної структури;

B_r – вартість створення r-го варіанта організаційної структури;

B_{rk} – вартість створення підрозділів k-го типу r-го варіанта організаційної структури.

Лінгвістичні змінні, що надані експертами показникам, наведені у Табл. 3.

Таблиця 3

Лінгвістичні змінні, що надані експертом показникам оцінювання організаційної структури

Варіант організаційної структури	Показники оцінювання організаційної структури							
	E_r	E_{r1}	E_{r2}	E_{r3}	B_r	B_{r1}	B_{r2}	B_{r3}
1	С	ДН	ДВ	Н	С	ДН	ДВ	ДН
2	В	Н	В	В	В	Н	В	В
3	С	ДН	С	С	С	Н	С	С
4	В	ДВ	ДН	С	В	ДВ	ДН	С
5	ДН	Н	Н	ДН	ДН	Н	Н	Н
6	В	С	С	ДВ	В	С	С	ДВ
7	С	ДН	Н	В	С	ДН	Н	В
8	В	ДВ	С	Н	В	ДВ	С	Н
9	ДВ	ДВ	В	В	ДВ	В	В	В
10	В	С	ДВ	С	В	С	ДВ	С

Таким же чином надаються показникам лінгвістичні змінні іншими експертами. Результати розрахунків центрів ваг C_{rl} нечітких чисел функцій належності, що відповідають показникам $(l = \overline{1, L})$, які характеризують створення і функціонування (застосування) організаційної структури, наведено у Табл. 4.

Таблиця 4

Центри ваг нечітких чисел функцій належності показників

Варіанти організаційної структури	Центри ваг нечітких чисел, C_{rl}							
	$C_{r1}(E_r)$	$C_{r2}(E_{r1})$	$C_{r3}(E_{r2})$	$C_{r4}(E_{r3})$	$C_{r5}(B_r)$	$C_{r6}(B_{r1})$	$C_{r7}(B_{r2})$	$C_{r8}(B_{r3})$
1	0,58	0,08	0,83	0,08	0,41	0,17	0,91	0,17
2	0,66	0,17	0,66	0,66	0,66	0,33	0,83	0,66
3	0,41	0,17	0,41	0,41	0,58	0,33	0,41	0,58
4	0,83	0,83	0,17	0,33	0,66	0,91	0,08	0,33
5	0,08	0,33	0,33	0,17	0,08	0,17	0,17	0,17
6	0,66	0,50	0,58	0,91	0,83	0,50	0,50	0,83
7	0,33	0,08	0,17	0,66	0,41	0,17	0,33	0,66
8	0,83	0,91	0,41	0,08	0,66	0,83	0,58	0,33
9	0,83	0,83	0,75	0,83	0,91	0,83	0,83	0,66
10	0,75	0,41	0,83	0,41	0,75	0,41	0,91	0,58
Коефіцієнти важливості b_l	0,19	0,18	0,17	0,16	0,09	0,08	0,06	0,07

У Табл. 4 також наведені коефіцієнти важливості показників b_l $(l = \overline{1, L})$, що визначені з використанням методу ранжирування.

Стимуляторами є показники E_r, E_{r1}, E_{r2}, E_{r3}, дестимуляторами – B_r, B_{r1}, B_{r2}, B_{r3}.

Стандартизовані значення центрів ваг $C *_{rl}$ наведені у Табл. 5.

Таблиця 5

Стандартизовані значення центрів ваг

Варіант організаційної структури	Стандартизовані центри ваг, $C*_{rl}$								Відстань Z_{r0}
	$C*_{r1}$	$C*_{r2}$	$C*_{r3}$	$C*_{r4}$	$C*_{r5}$	$C*_{r6}$	$C*_{r7}$	$C*_{r8}$	
1	-0,08	-1,17	1,33	-1,32	-0,86	-1,04	1,24	-1,50	0,656
2	0,25	-0,87	0,62	0,75	0,33	-0,46	0,96	0,73	0,602
3	-0,79	-0,87	-0,42	-0,14	-0,05	-0,46	-0,48	0,36	0,738
4	0,96	1,33	-1,41	-0,43	0,33	1,61	-1,62	-0,77	0,662
5	-2,17	-0,33	-0,75	-1,00	-2,43	-1,04	-1,31	-1,50	0,882
6	0,25	0,23	0,29	1,64	1,14	0,14	-0,17	1,50	0,524
7	-1,12	-1,17	-1,41	0,75	-0,86	-1,04	-0,76	0,73	0,817
8	0,96	1,60	-0,42	-1,32	0,33	1,32	0,10	-0,77	0,651
9	0,96	1,33	1,00	1,36	1,52	1,32	0,96	0,73	0,467
10	0,62	-0,07	1,33	-0,14	0,76	-0,18	1,24	0,36	0,556

Еталонному варіанту організаційної структури відповідають такі значення центрів ваг:

$C*_{01}$=0.96; $C*_{02}$=1.60; $C*_{03}$=1.55; $C*_{04}$=1.64;

$C*_{05}$=-2.43; $C*_{06}$=-1.04; $C*_{07}$=-1.62; $C*_{08}$=-1.50.

Відстані Z_{r0} між центрами ваг $C*_{rl}$, що характеризують показники варіантів організаційної структури і еталонного варіанта $C*_{0l}$, які розраховані за формулою (15), також наведені у Табл. 5.

Результати розрахунків ступенів переваги варіантів складу організаційної структури δ_r наведено на рис. 3.

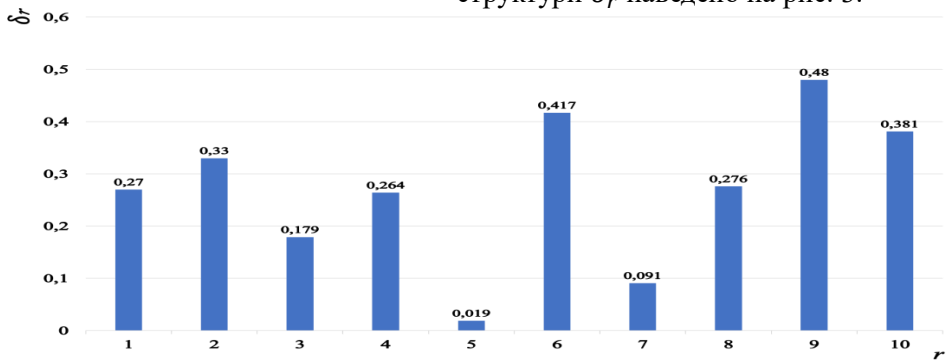

Рис. 3. Ступені переваги варіантів складу організаційної структури

Найбільшу перевагу має дев'ятий варіант організаційної структури у складі шістьох підрозділів для виконання завдань (1, 2, 7, 8), чотирьох підрозділів для виконання завдань (3, 4, 5) та чотирьох підрозділів для виконання завдань (6, 9, 10). Слід зазначити, що дев'ятому варіанту відповідала максимальна кількість підрозділів – виконавців кожного типу (див. Табл. 2).

Центр ваги нечіткого числа можна вважати як середнє значення відповідного показника. Тому ефективність застосування дев'ятого варіанта складу організаційної структури дорівнює 0.83 (див. Табл. 4), що відповідає заданому критерію. При цьому ефективність виконання завдань підрозділами становить 0.75–0.91.

Найближчим за ступенем переваги є шостий варіант складу організаційної структури. Проте цей варіант не відповідає заданому критерію ефективності застосування організації.

Враховуючи кількість підрозділів дев'ятого варіанта, що вважається кращим (раціональним), у складі організаційної структури доцільно мати чотири функціональних органи управління.

На прикладі докладно показано застосування розробленої методики для визначення складу організаційної структури в умовах дій невизначених факторів, що впливають на виконання завдань організації. Результати, що отримуються з використанням методики, дають змогу обґрунтовано аналізувати можливі варіанти складу організаційної структури і вибирати з них кращий з врахуванням збалансованості за ефективністю виконання завдань, часом їх виконання і вартістю.

Висновки. Розроблено методику визначення складу організаційної структури в умовах невизначеності, яка ґрунтується на використанні:

групування завдань організації для визначення потрібних типів підрозділів – виконавців;

планування експерименту для формування варіантів складу організаційної структури;

нечіткого підходу для визначення лінгвістичних змінних при оцінюванні

експертами показників, що характеризують створення і застосування організації;

методу таксономії для вибору кращого варіанта організаційної структури.

Застосування нечіткого підходу дає змогу визначити склад організаційної структури в умовах неможливості отримання кількісних значень показників, що характеризують створення і застосування (функціонування) організації.

Особливістю методики є застосування у якості вихідних даних під час використання методу таксономії центрів ваг нечітких чисел, що відповідають трикутним функціям належності показників.

Застосування методики показано на ілюстративному прикладі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Плюта В. Сравнительный многомерный анализ в экономических исследованиях: методы таксономии и факторного анализа / пер. с польск. В. В. Иванова ; научн. ред. В. М. Жуковской. Москва : Статистика, 1980. 151 с.
2. Городнов В. П., Фык О. В. Математическое моделирование, оценка эффективности и синтез организационных структур предприятий. Київ : МЭУ, 2005. 192 с.
3. Загорка О. М., Поліщук С. В., Загорка І. О., Фреган Н. М. Методичні положення обґрунтування складу організаційних структур // Сучасні інформаційні технології у сфері безпеки та оборони. 2024. № 1 (49). С. 5–15.
4. Барабащук В. И., Креденцер Б. П., Мирошниченко В. И. Планирование эксперимента в технике / под ред. Б. П. Креденцера. Київ : Техніка, 1984. 200 с.
5. Balezentis A., Balezentis T., Brauers W. K. MULTIMOORA-FG: A Multi-Objective Decision Making Method for Linguistic Reasoning With an Application to Personnel Selection // Informatics, Lith. Acad. Sci. 2012. 23. P. 173–190.
6. Ашмарин И. П., Васильев Н. Н., Амбросов В. А. Планирование экспериментов. Москва : Изд-во Моск. ун-та, 1974. 76 с.
7. Таблицы планов эксперимента для факторных и полиномиальных моделей : справочное изд. / В. З. Бродский и др. Москва : Металлургия, 1982. 350 с.
8. Герасимов Б. М., Локазюк В. М., Пономарьова О. Г., Поморова О. В. Інтелектуальні системи підтримки прийняття рішень : навч. посіб. Київ : Вид-во Європ. ун-ту, 2007. 335 с.
9. Свешников С. В., Бочарников В. П. Основы нечеткой технологии и примеры решения аналитических задач в государстве и бизнесе. Москва : ДМК Пресс, 2014. 408 с.
10. Денисов А. А., Колесников Д. Н. Теория больших систем управления : учеб. пособ. для вузов. Ленінград : Энергоиздат, Ленингр. отд-ние, 1982. 288 с.

Стаття надійшла до редакції 24.11.2025

Applying a fuzzy approach to determining the composition of the organizational structure

Annotation

When creating or improving any organization, particularly a military one, there is a need to determine its structural composition to fulfill designated tasks in accordance with the organization's mission. Determining the composition of an organizational structure can be viewed as a structural synthesis problem, which can be addressed using systemic analysis principles, specifically the variant method. This requires the application of multidimensional comparative analysis techniques under conditions of uncertainty regarding factors that influence the fulfillment of organizational tasks.

The purpose of the article is to improve the methodological provisions for determining the composition of organizational structures by accounting for the uncertainty of factors affecting their creation and application.

A methodology for determining the composition of an organizational structure under conditions of uncertainty has been developed, based on the following:

grouping organizational tasks to identify the required types of executing units;

design of experiments to formulate variants of the organizational structure's composition;

a fuzzy approach to define linguistic variables for expert evaluation of indicators characterizing the creation and application of the organization;

the taxonomy method for selecting the optimal variant of the organizational structure.

The application of a fuzzy approach allows for determining the organizational structure's composition when it is impossible to obtain quantitative values for indicators characterizing the creation and functioning of the organization. A specific feature of this methodology is the use of the centers of gravity of fuzzy numbers, corresponding to triangular membership functions of the indicators, as input data for the taxonomy method. The practical application of the proposed methodology is demonstrated through an illustrative example.

Keywords: organizational structure composition; task grouping; experimental design; linguistic variables; center of gravity of fuzzy numbers; taxonomy method.

УДК 355.716 https://doi.org/10.33099/2304-2745/2025-3-86/60-65

Солонніков В. Г., доктор технічних наук, професор[1] (0000-0002-7653-416X)
Гандзюк А. П., кандидат технічних наук, старший науковий співробітник[2] (0009-0003-5413-7862)
Прима А. М., доктор філософії[3] (0000-0002-0776-6864)
Горбачова Я. С., доктор філософії[4] (0000-0002-1652-2941)

[1] – Інститут стратегічних комунікацій Національного університету оборони України;
[2,4] – Інститут логістики та підтримки військ (сил) Національного університету оборони України;
[3] – Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Системний підхід до воєнно-інженерної підготовки території країни в умовах воєнного стану

Резюме. На підставі досвіду бойових дій РФ проти України обґрунтовано підходи до воєнно-інженерної підтримки та підготовки території країни, як театру бойових дій, на основі методу системного аналізу. Розроблено та запропоновано алгоритм організації заходів з воєнно-інженерної підготовки територій і інфраструктурних об’єктів.

Ключові слова: інженерна підтримка; підготовка території, оперативно-стратегічні вимоги; оперативні напрямки; театр бойових дій; логістичне та технічне забезпечення; безпілотний літальний апарат.

Постановка проблеми. Основними заходами воєнно-інженерної підготовки території до оборони завжди були: будівництво фортець на шляхах можливого просування ворожих армій, підготовка позицій, скритих засідок і відсічних позицій своїх військ, підготовка та утримання шляхів пересування і маневру підрозділів резерву, заготівля матеріалів для облаштування невибухових загороджень на ймовірних напрямках руху підрозділів противника.

Прикладом підготовки місцевості у воєнно-інженерному відношенні є існуюча система побудованих різноманітних земляних перешкод та кам’яних фортець на території: сучасної Словаччини в XIII–XIV століттях, а також такі фортифікаційні укріплення, як лінія Мажино (Франція), лінія Зігфрида (Німеччина), лінія Маннергейма (Фінляндія), лінія Метаксаса (Греція) укріплені райони за західному кордоні СРСР.

Надзвичайна важливість зазначених історичних воєнно-інженерних заходів характерна і для сучасного періоду, тільки на більш складному інженерно-технічному рівні їх виконання.

Проведений аналіз досвіду воєнно-інженерної підготовки території до оборони та результати науково-практичної конференцій у Командуванні Сил підтримки та Командуванні Сил логістики Збройних Сил України (далі – ЗС України) щодо підготовки і ведення бойових дій проти агресії РФ підтверджує необхідність обґрунтування і розробки системи організаційно-технічних заходів воєнно-інженерної підготовки і утримання території проведення воєнних операцій, що плануються [1, 2].

Аналіз останніх досліджень і публікацій. На сьогодні існує низка нормативно-правових документів, наукових досліджень і публікацій, зміст яких пов’язаний з проблемними питаннями з підготовки території держави як майбутнього театру бойових дій.

Так, з 2016 року визначені основні напрями діяльності усіх органів влади з підготовки території держави до ведення бойових дій, а також приведений причинно-наслідковий аналіз невиконаних у цьому відношенні організаційних, економічних і технічних заходів з облаштування території і інфраструктурних об’єктів до умов бойових дій [1].

На основі матеріалів з досвіду ведення бойових дій [2–4] вивчалися та аналізувалися особливості боїв, зіткнень та обґрунтовувалися пропозиції з плануванню оборони та розміщенню позицій протиракетних комплексів протиповітряної оборони (ППО) з метою підвищення їх ефективності та прикриття населених пунктів.

У публікації [5] обґрунтовані пропозиції воєнно-інженерної підтримки місцевості об’єднаних територіальних громад у період до та після воєнного стану в країні.

У роботі [6] особливий акцент приділено завчасному плануванню і виконанню усіх завдань і заходів з інженерної підтримки військ (сил), висвітлено проблеми

логістичного і технічного забезпечення у зв'язку зі значним розосередженням військ на території оперативно-стратегічних напрямків та застосування противником високоефективних засобів аеророзвідки і вогневого ураження.

Проте у зазначених публікаціях не розглянуті питання взаємодії між родами військ, структурними підрозділами територіальної оборони та відповідними органами управління щодо організації воєнно-інженерної підготовки території країни за оперативними напрямками в умовах сучасного ведення бойових дій.

Мета статті полягає в обґрунтуванні на основі системного підходу рекомендацій щодо підготовки і утримання території країни у воєнно-інженерному відношенні.

Виклад основного матеріалу. *Підготовка території держави до оборони* – це комплекс організаційних, технічних, інженерних та інших заходів, що здійснюються державними установами і ЗС України з метою підготовки місцевості та об'єктів інфраструктури, які забезпечують сприятливі умови для стратегічного розгортання підрозділів ЗС України і інших складових сил оборони до відбиття військової агресії [1]. Це означає завчасне визначення, планування і забезпечення конкретних заходів з підготовки території країни до оборони в загальнодержавному масштабі, тобто із залученням не тільки підрозділів ЗС України, а й відповідних територіальних установ і підприємств. При цьому усі заходи підготовки території країни до повномасштабної оборони мають плануватись і виконуватись після узгодження їх з Генеральним штабом ЗС України з урахуванням природніх і інфраструктурних особливостей та економічної спроможності на визначених оперативно-стратегічних напрямках.

До основних організаційних заходів із підготовки території країни відносяться:

створення центрального органу державного управління щодо підготовки території країни до оборони з представництвами (установами) в областях (районах);

включення в бюджети країни і областей статті фінансового забезпечення запланованих заходів з підготовки території країни;

розроблення формалізованих документів з планування і виконання заходів з підготовки території областей і країни в цілому до оборони;

визначення державних установ (підприємств) з утримання підготовлених об'єктів, споруд, ділянок облаштованої території у воєнно-інженерному відношенні;

надання контролюючих функцій законодавчо визначеним органам за станом підготовленої території, споруд, об'єктів тощо.

Організаційні заходи передбачають створення системи управління і контролю за виконанням заходів підготовки та утримання території країни.

Отже, технічні заходи за своїм призначенням і змістом мають забезпечити виконання усіх робіт з підготовки території країни і об'єктів інфраструктури, відповідно до розробленого і затвердженого плану та вимог щодо їх ефективності та живучості.

Основою виконання технічних заходів є спроможності спланованого економічного ресурсу, а саме:

заготівля необхідних матеріальних ресурсів (сортаменти лісоматеріалу, металу, будівельних матеріалів тощо);

визначення різноманітної техніки і технічних засобів, залежно від виду запланованих заходів та робіт;

логістичне забезпечення виконання запланованих заходів і робіт;

визначення цивільних суб'єктів технічного забезпечення і їх взаємодія з виконавцями запланованих заходів та робіт;

заходи з утримання головних транспортних комунікацій.

Станом на сьогодні ЗС України відповідають за комплекс заходів з підготовки місцевості, транспортних комунікацій та об'єктів інфраструктури в межах оперативно-стратегічного напряму ведення бойових дій, що суттєво ускладнює планування і реалізацію всіх видів забезпечення підрозділів військ та відповідності необхідному рівню їх боєздатності.

Щодо трудовитрат і матеріально-технічного забезпечення навантаження зазначеного комплексу заходів є непосильним на сьогодні для ЗС України. Тому, доречно розглянути варіанти делегування певних заходів суб'єктам об'єднаних територіальних громад, а контроль і технічний супровід їх виконання залишити за визначеними підрозділами територіальної оборони з підготовленими фахівцями, що мають бойовий досвід.

Вивчаючи досвід підготовки території країни до бойових дій і висновки з ведення бойових дій на території України, необхідно

об’єктивно оцінювати поточну ситуацію і спроможності економіки держави щодо оперативного облаштування території країни в воєнно-інженерному відношенні.

Системний підхід (рис. 1) є одним із загальнонаукових методологічних напрямів дослідження складних систем і процесів, який базується на принципі цілісності (емерджентності) досліджуваного об’єкта. Цей принцип виходить з того, що ціле має такі якості, яких немає у його частин. Щоб максимально виявити і використати ці якості, системний підхід потребує неперервної інтеграції уявлень про систему з різних точок зору на кожному етапі її досліджень.

Рис. 1. Основні принципи системного підходу як методологічного напряму проведення дослідження складних систем і процесів

Ураховуючи основні вимоги системного підходу а також існуючий стан економіки і особливості поточного воєнного стану, облаштування території країни у воєнно-інженерному відношенню доречно розглянути в два етапи.

1-й етап. Зміст 1-го етапу полягає у проведенні інженерної розвідки місцевості території, дотичної до оперативної лінії бойового зіткнення з противником, з метою отримання інформації про стан природніх та інфраструктурних ресурсів, використання яких важливе для виконання завдань інженерної підтримки військ 2-го ешелону оборони і стратегічного резерву ЗС України. Отримані дані інженерної розвідки передаються в штаби оперативних командувань для подальшого планування оборонних операцій. На цьому етапі особливе значення має наявність інформації про наступні об’єкти і ділянки території місцевості:

стан існуючих доріг, автомагістралей, шляхів за критерієм використання їх для пересування військ з озброєнням та військовою технікою (ОВТ);

стан мостів та шляхопроводів;

наявність природніх перешкод на ймовірних напрямах руху (військових шляхах);

оцінка маскувальних властивостей місцевості на ймовірних ділянках розташування військ в умовах польового табору;

наявність об’єктів інфраструктури поблизу районів можливого розташування військ та їх застосування;

виконання заходів з підвищення прохідності існуючих доріг і шляхів руху військ;

оцінка наявності та можливості використання природніх та місцевих ресурсів для облаштування позицій військ, ділянок місцевості під облаштування аеродромів, польових таборів військ;

визначення місць облаштування хибних споруд та макетів ОВТ, позицій комплексів ППО тощо;

визначення місць розташування об’єктів інфраструктури (складів, підприємств тощо) придатних для виконання завдань логістичного і технічного забезпечення.

2-й етап. На цьому етапі відпрацьовується робоча карта заходів з інженерної підтримки місцевості, оперативних напрямів, ґрунтуючись на сучасній інформації про стан їх території [7–8]. На основі затвердженої робочої карти оформлюються плани виконання інженерних заходів з підготовки території, до яких мають залучатися місцеві органи і підприємства територіальних громад, підрозділи територіальної оборони. У подальшому здійснюється формування спеціальних підрозділів з підтримання у належному стані виконаних заходів інженерної підтримки місцевості, об’єктів, споруд.

Комплексна оцінка заходів, що досліджуються, потребує:

аналізу бойових дій військ противника;

визначення спектру внутрішніх і зовнішніх факторів, які мають прямий вплив на результати оцінювання ефективності заходів;

достатності кваліфікованих і досвідчених експертів;

чіткої організації в проведенні досліджень і прийняття відповідних рішень.

Алгоритм організації розглянутої в цій статті проблематики наведено на рис. 2.

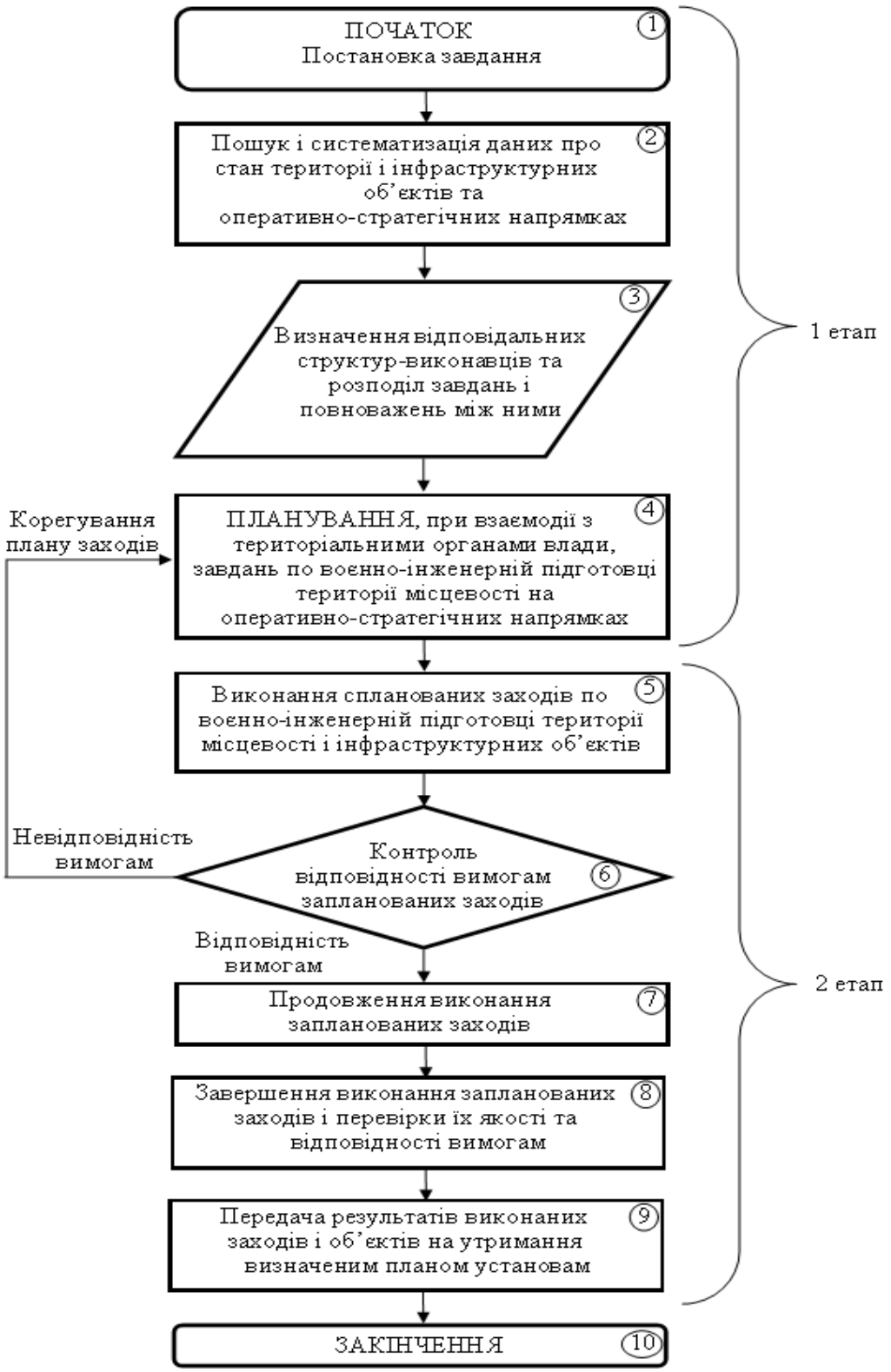

Рис. 2. Алгоритм організації заходів з воєнно-інженерної підготовки територій і інфраструктурних об'єктів

Основні складові плану заходів (робота, тривалість, економічний ефект) краще оформляти, з точки зору прозорості, у формі діаграми Ганта (Табл. 1) [9].

Наведена діаграма Ганта упорядковує планування заходів і поетапний контроль їх виконання, а також контроль за витратами ресурсів. На етапі завершальних робіт здійснюється аналіз усіх витрат (матеріальних і фінансових) та причин невідповідності термінів виконання заходів, які заплановані, з метою удосконалення планування. Такий підхід забезпечує відповідальність виконавців щодо виконання заходів з облаштування території у воєнно-інженерному відношенні у визначені терміни.

Таблиця 1

Основні складові плану заходів

№ з/п	Назва заходу	Дата / Термін / Вартість											
		1.01	10.01	31.01	1.02	10.02	28.02	1.03	10.03	31.03	1.04	10.04	30.04
1 1.1 . . 1.n	Заходи з планування	Д(Ц)	Д(Ц)		Д(Ц)								
2 2.1 . . 2.n	Виконання заходів					Д(Ц)	Д(Ц)		Термін (вартість)				
3 3.1 . . 3.n	Контрольні заходи					Д(Ц)		Д(Ц)		Д(Ц)			
4 4.1 . . 4.n	Завершальні заходи												Д(Ц)

Примітка: 1. Термін – в людино-годинах робочих днів (Д).
2. Вартість – у визначених умовних одиницях (Ц).

Оцінка ефективності запропонованого авторами підходу до воєнно-інженерної підготовки місцевості країни на основних оперативних напрямках можлива шляхом розрахунку ступеню досягнення системою підготовки місцевості поставленої перед нею мети. Ефективність може бути подана отриманим в процесі функціонування системи ефектом, який нормований до витрат ресурсів на визначеному інтервалі часу [10].

Велику увагу в сучасних умовах ведення бойових дій необхідно приділяти засобам і способам активного і пасивного (хибного) маскування на місцевості, де планується розгортання бойових позицій військ, шляхом імітації руху і маневру підрозділів військ. Теоретично ефективність таких засобів і способів оцінюється згідно існуючих методик [8]. Для отримання реальних результатів щодо ефективності маскувальних дій необхідно розробити технічні умови до перспективних маскувальних засобів і технічні вимоги до способів, але це є предметом майбутніх дослідно-конструкторських робіт.

Висновки. Характер сучасних бойових дій та економічні спроможності щодо їх забезпечення потребують оперативного виконання завдань логістичного забезпечення і воєнно-інженерної підтримки військ (сил).

Заплановані заходів з воєнно-інженерної підготовки територій до оборони потребують комплексної їх оцінки

Для вирішення проблемних питань щодо підготовки і утримання місцевості і об’єктів інфраструктури у воєнно-інженерному відношенні запропонований системний підхід, суть якого відображена алгоритмом на рис. 2.

Таким чином запропонований підхід до воєнно-інженерної підготовки території країни сприятиме якісному плануванню оборонної операції в сучасних умовах ведення бойових дій та ресурсного обмеження.

Подальші дослідження планується зосередити на оцінці ефективності запропонованого підходу до воєнно-інженерної підготовки території країни на основних оперативних напрямках.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Глобальна та національна безпека : підручник / авт. колектив ; за заг. ред. Г. П. Ситника. Київ : НАДУ, 2016. 784 с.
2. Сиротенко А. М., Щипанський П. В., Павліковський А. К., Лобко М. М. Актуальні проблеми планування оборони України: комплексний підхід // Наука і оборона. 2020. №1. С. 3–12.
3. Олещук М. М., Коваль В. В., Щипанський П. В., Загорка О. М., Поліщук С. В. Особливості організації оборони населених пунктів від ударів

балістичних ракет оперативно-тактичного і тактичного призначення // Наука і оборона. 2024. №1. С. 31–38.
4. Собко С. С., Пунда Ю. В., Музиченко Д. П. Територіальна оборона в перспективній моделі оборони України // Наука і оборона. 2023. № 2. С. 20–27.
5. Гандзюк А. П., Петренко М. М., Клонцак М. Я. Актуальні питання військово-інженерної підготовки місцевості та об’єктів об’єднаних територіальних громад України // Наука і оборона. 2020. № 4. С. 24–26.
6. Тягай С. В. Особливості виконання основних завдань інженерного забезпечення в антитерористичній операції. URL: http://www.irbis-nbuv.gov.ua (дата звернення: 02.04.2025).
7. Воєнно-історичний опис сил підтримки Збройних Сил України (липень-вересень 2024 р.). Київ : НУОУ, 2024. 52 с.
8. Обґрунтування вимог до облаштування та розташування польових таборів для розміщення особового складу військових частин Сухопутних військ Збройних Сил України : звіт про НДР (ост.). Київ, 2024. 317 с. Р/№ 0225U000933д.
9. Сітьовий графік, його елементи і параметри. URL: https://ua.kursoviks.com.ua (дата звернення: 02.04.2025).
10. Застосування сучасних інформаційних технологій у науковій діяльності : підручник / С. А. Микусь, В. Г. Солонніков та ін. Київ : НУОУ, 2021. 340 с.

Стаття надійшла до редакції 09.05.2025

A systematic approach to military engineering preparation of the country's territory under martial law

Annotation

Historically, the core measures of military engineering preparation of a territory for defense have included: the construction of fortresses along potential routes of enemy advancement; the preparation of positions, concealed ambushes, and switch positions for friendly forces; the preparation and maintenance of routes for movement and maneuver of reserve units; and the stockpiling of materials for the installation of non-explosive obstacles along probable directions of enemy movement.

The analysis of the experience in military engineering preparation of territory and the findings of scientific-practical conferences held at the Support Forces Command and the Logistics Forces Command of the Armed Forces of Ukraine (hereinafter – AF of Ukraine) regarding the preparation and conduct of combat operations against the aggression of the RF, confirm the necessity to substantiate and develop a system of organizational and technical measures for the military engineering preparation and maintenance of territories for planned military operations.

The purpose of the article is to substantiate recommendations for the preparation and maintenance of the national territory from a military engineering perspective, based on a systems approach.

Considering the fundamental requirements of a systems approach, as well as the current state of the economy and the specifics of the ongoing martial law, it is appropriate to consider the engineering organization of the national territory in two stages:

Stage 1 involves conducting engineering reconnaissance of the terrain adjacent to the operational line of contact with the enemy. The goal is to obtain information on the status of natural and infrastructure resources, the use of which is vital for the engineering support tasks of the second-echelon defense forces and the strategic reserve of the AF of Ukraine.

Stage 2 focuses on developing a working map of engineering support measures for the terrain and operational directions, based on up-to-date information regarding the state of these territories.

Keywords: engineering support; territory preparation; operational-strategic requirements; operational directions; theater of operations; logistical and technical support; unmanned aerial vehicle.

УДК 358.2:623.127(477) https://doi.org/10.33099/2304-2745/2025-3-86/66-71

Хоптій О. В. (0009-0001-9462-5559)
Підгородецький М. М., кандидат військових наук (0000-0003-4807-8635)

Інститут логістики та підтримки військ (сил) Національного університету оборони України, Київ

Аналіз застосування засобів подолання інженерних загороджень противника в операції (бою)

Резюме. Забезпечення успішного виконання завдання подолання інженерних загороджень під час ведення бойових дій угрупованням військ у сучасних умовах відбиття широкомасштабної збройної агресії РФ стає все більш актуальним. Проведено аналіз факторів, що впливають на виконання заходів подолання інженерних загороджень.

Визначені недоліки існуючих засобів інженерного озброєння, здійснено порівняння новітніх і вітчизняних зразків, які, насамперед, впливають на подолання інженерних загороджень. Визначені вимоги до перспективних зразків техніки для пророоблення проходів.

Ключові слова: інженерна підтримка; операції (бойові дії); інженерні загородження; розмінування; засоби інженерного озброєння; група розгородження, мінно-вибухові загородження.

Постановка проблеми. За досвідом відсічі збройної агресії РФ проти України, проведення Операції об’єднаних сил на території Донецької і Луганської областей та антитерористичної операції [1] бойові дії угрупованнями військ все більш потребують інженерної підтримки. Згідно з [2, 3] під час наступальних операціях інженерна підтримка мобільності військ (сил) включає: інженерну розвідку противника та місцевості, інженерну підтримку подолання водних перешкод або суходолів, виконання інженерних заходів щодо підготовки та утримання шляхів пересування військ (сил).

Аналіз звільнення Київщини, Харківщини, Херсонщини та досвіду виконання завдань Курської наступальної операції [4, 5], свідчить про те, що пророоблення проходів у інженерних загородженнях противника відіграє ключову роль. Отже вирішення питань щодо удосконалення цього процесу та аналіз факторів, які впливають на подолання інженерних загороджень, набувають більшої актуальності.

Аналіз останніх досліджень та публікацій. Проблемам удосконалення виконання завдань і заходів інженерної підтримки військ (сил) присвячена велика кількість робіт [6–8]. Аналіз ключових факторів, що впливають на ефективність інженерної підтримки наступальних операцій, рекомендації щодо оцінювання, підвищення ефективності подолання інженерних загороджень та перспектив подальшого розвитку цього завдання досліджено у своїх роботах такі вчені як: Ю.О. Фтемов, Ф.А. Демідчик, Д.А. Окіпняк та інші.

Проте вченими не повною мірою було досліджене питання інженерної підтримки мобільності своїх військ (сил) із застосуванням роботизованих комплексів та безпілотних літальних апаратів. Тому питання пов’язані з виконанням заходів інженерної підтримки мобільності своїх військ (сил) в операціях ОУВ були розкриті не повністю.

Метою статті є проведення порівняльного аналізу характеристик існуючих засобів, що впливають на виконання заходів (процесів) інженерної підтримки подолання інженерних загороджень противника в наступальних операціях (бойових діях) та визначення вимог до перспективних зразків.

Виклад основного матеріалу. Виконання завдань інженерної підтримки здійснюється під постійним впливом різних факторів [10, 11].

Проведений аналіз щодо організації і проведення інженерної підтримки мобільності своїх військ (сил), зокрема пророоблення проходів в інженерних загородженнях показав, що можливості угруповань військ (сил) щодо виконання завдань подолання мінно-вибухових загороджень у збройному конфлікті знаходяться під впливом цілої низки різнорідних зовнішніх та внутрішніх факторів.

До *зовнішніх факторів* відносяться: склад; бойові, маневрові та вогневі можливості; ймовірний характер і просторовий розмах дій противника; тип і щільність застосування мінно-вибухових загороджень (МВЗ) та вибухонебезпечних предметів (ВНП) іншого типу; характеристики приховуючого середовища; склад, характер дій угруповань наших військ (сил), місце та

роль його в операції (бойових діях); їх укомплектованість особовим складом; фізико-географічні та погодні умови операційного району.

Внутрішні фактори включають: укомплектованість особовим складом підрозділів розмінування; рівень навченості особового складу; морально-психологічний стан особового складу; організація виконання завдань подолання мінно-вибухових загороджень (зокрема їх оперативність); всебічне забезпечення процесу подолання мінно-вибухових загороджень при інженерній підтримці угруповання військ (сил); наявність та стан засобів інженерного озброєння.

Слід зазначити, що зовнішні фактори визначають вплив зовнішнього середовища та можуть бути як корисними (сприяти успішному виконанню обсягів завдань інженерної підтримки, так і шкідливими (протидіяти успіху), а внутрішні фактори, які визначаються особистими ознаками угруповання військ (сил) належать до керованих та відображають вплив на хід та результат виконання завдань інженерної підтримки.

На сьогодні можливості наявного складу засобів подолання мінно-вибухових загороджень в цілому дають змогу виконувати завдання за призначенням, однак їх стан характеризується поступовим моральним та фізичним старінням, що, зі свого боку, знижує ефективність їх застосування. Фізичне старіння викликане тривалим перебуванням в експлуатації та на зберіганні засобів розмінування, як складових засобів інженерного озброєння. Лише 5% від загальної чисельності засобів інженерного озброєння припадає на нові та модернізовані зразки. Решта зразків знаходяться в експлуатації понад 15 років та потребують ремонту і відновлення боєздатності.

Стандартами НАТО не передбачається можливість виконання завдання щодо прокладення проходів в загородженнях противника інженерними підрозділами самостійно, без надійного пригнічення противника на ділянці де проходи прокладаються військами, які наступають [12–14]. Особливо це застереження стосується організації подолання інженерних загороджень перед переднім краєм оборони противника.

Для визначення пріоритетності виконання заходів інженерної підтримки мобільності наших військ, здійснено декомпозицію на процеси із подальшим визначенням доцільності роботизації засобів (комплексів) їх реалізації (Табл. 1).

Таблиця 1

Потреба у роботизації процесів інженерної підтримки наступу (бойових дій) угруповання військ

№	Процеси	Способи	Вид бою	Потреба
1	Тралення мін	Механічний	Наступ	Потрібно
2	Прокладення проходів	Вибуховий, механічний, вручну	Наступ	Потрібно
3	Суцільне розмінування	Вибуховий, механічний, вручну	Наступ, оборона	Частково
4	Знищення (знешкодження) мін	Механічний, вибуховий	Наступ, оборона	Частково
5	Маркування	Вручну, механічний	Наступ, оборона	Не потрібно

Аналіз процесів, наведених у Табл. 1, показав, що основну увагу з питань роботизації потребують способи реалізації процесів тралення мін, прокладення проходів у мінно-вибухових загородженнях. Вказані засоби та способи можуть частково замінити ручне або пілотоване механічне розмінування.

Враховуючи результати аналізу технічного рівня засобів розмінування, досвіду воєнних конфліктів сучасності [15], можна зазначити, що основні зусилля розвитку засобів розмінування доцільно зосередити на проведенні модернізації існуючих засобів (комплексів) розмінування та розробці нових дистанційно-керованих безпілотних систем розмінування, які відповідають сучасним вимогам.

Для подолання проходів у масових загородженнях і руйнуваннях у частинах і з'єднаннях створюються групи розгородження або загін розгородження [16].

До складу груп розгородження з танковим мостоукладачем, машиною розгородження (інженерним танком) входять 1-2 танки (БТР) з тралами (БМР), установкою розмінування. Група створюється на період виконання завдання і діє самостійно в інтересах підрозділів першого ешелону.

Загін розгородження має у складі декілька груп розгородження з централізованим керуванням. При цьому передбачається виділення груп зі складу загону розгородження на більш складні

напрями та повернення після того, як буде вичерпана необхідність у їх діях.

Приклад складу груп розгородження

Варіант 1: ісвід, БМР – 1 од., УР-77 – 1 од., ІМР – 1 од.; МТУ-20 (Biber) – 1 од. Резерв сил і засобів – БТР Stryker з мінним тралом Spark та установкою розмінування М58 Miclic*.

Варіант 2: ісвід, БТР Stryker з мінним тралом Spark – 1 од., БТР Stryker з установкою розмінування М58 Miclic – 1 од., ІМР – 1 од.; МТУ-20 (Biber) – 1 од. Резерв сил і засобів: УР-77 – 1 од., БМР – 1 од*.

Позначення:

*ісвід – інженерно-саперне відділення;

БМР – бойова машина розгородження;

УР-77 – установка розмінування (радянська гусенична машина для створення проходів у мінних полях);

ІМР – інженерна машина розгородження (радянського виробництва);

МТУ-20 (Biber) – мостоукладальник на базі танка, радянського (МТУ-20) німецького (Biber) виробництва;

БТР Stryker з мінним тралом Spark – бронетранспортер американського виробництва з відповідним типом мінного тралу;

М58 Miclic – американська установка для розмінування (Mine Clearing Line Charge).

Практика ведення бойових дій показала, що виникає протиріччя між значними темпами розвитку мінної зброї противника та збільшенням обсягів її застосування з одного боку, та недосконалістю існуючих на озброєнні Збройних Сил України засобів подолання мінно-вибухових загороджень, з іншого. Для вирішення цього проблемного питання проведемо порівняльний аналіз засобів (комплексів) розмінування До засобів подолання загороджень відносяться установки розмінування та засоби тралення. Провідними країнами у цій галузі є США, Німеччина, Великобританія, Хорватія та РФ (Табл. 2).

Таблиця 2

Порівняльний аналіз зразків установок розмінування провідних країн світу

Тактико-технічні характеристики	**УР-77**	**ІМР-2**	**М58 MICLIC /Grizzly/**	**М58 MICLIC /M1060/**	**Breacher-ABV**	**М728**	**УРП-01**	**Trojan/ Pyton**
	СРСР	РФ	США	США	США	США	РФ	Велико Британія
Швидкість руху шасі, км/год	61	55	66	74	70	48	80	59
Маса зразка, т	15,5	44,5	70,0	56,3	50	52,2	29,5	44,6
Розрахунок, чол	2	2	2	2	2	4	1	3
Час розмінування, хв	5	5	5	5	5	5	3	5
Час перезаряджання, хв	40	50	20	20	20	20	40	40
Дальність подачі, м	500	300	62	62	62	925	440	120
Ширина проходу, м	6	8	8	8	6	14	4	7,3
Довжина проходу, м	90	90	100	100	100	100	114	230
Питомий тиск на грунт, кг/см²	0,5	0,8	1,2	0,92	1,1	0,9	0,5	0,6
Кількість зарядів розмінування, од.	2	2	2	2	2	1	1	2
Можливість дистанційного управління	0	0	1	1	1	1	0	1

Аналіз Табл. 2 показує, що найкращими серед наведених зразків виявилась бойова інженерна машина М728 (США) інженерної підтримки бойових дій танкових і механізованих підрозділів. Перевагами цього зразка є ширина проходу, який прорублюється, незначний час перезаряджання та можливість дистанційного керування, недоліками – невелика швидкість руху та мала кількість зарядів розмінування.

Самохідна установка розмінування УР-77, яка знаходиться на озброєнні

ЗС України, посідає п'яте місце серед обраних зразків (враховуючи тактико-технічні характеристики згідно таблиці). Її перевагами є відносно невелика маса зразка та доволі велика кількість зарядів розмінування. Недоліки – недостатня довжина проходу, незадовільна швидкість руху шасі, значний час на підготовку до наступного пуску та відсутність можливості дистанційного управління.

Для порівняльного аналізу засобів тралення з різним типом робочого та навісного обладнання вибрано зразки, які стоять на озброєнні в ЗС України та арміях провідних країн світу (Табл. 3).

Таблиця 3

Порівняльний аналіз зразків для тралення мін провідних країн світу

Тактико-технічні характеристики	**IMP-3**	**БМР-3М**	**Grizzly /CMV/**	**Keiler**	**Breacher-ABV**	**Panther II Abrams**	**IMP-2M**	**MV-4 DOK-ING**
	Росія	Росія	США	Німеччина	США	США	СРСР	Хорватія
Швидкість руху шасі, км/год	50	60	66	50	70	60	59	5
Маса зразка, т	50	43	70	53	50	43	44,5	5,6
Розрахунок, чол.	2	2	2	1	2	1	2	1
Швидкість тралення, км/год	12	12	5	4,5	7	5	15	2
Ширина проходу, м	4,2	3,2	4,4	4,7	4,5	4,6	4,3	1,7
Питомий тиск на грунт, кг/см²	0,75	0,85	1,2	0,85	1,1	0,95	0,8	0,85
Можливість дистанційного управління	1	0	1	0	1	1	0	1
Наявність стрілецького озброєння	1	1	1	0	1	0	0	0
Наявність пристрою маркування проходу	0	1	0	1	1	0	0	0
Марка /тип тралу робочого органу	кол., нож. БРО	кол., нож., катк. КМТ-7	БРО, нож., "плуг"	фреза	БРО, нож., "плуг"	катк.	кол., нож. БРО ЕМТ	фреза катк. БРО

Аналіз одержаних результатів показав, що найкращим серед наведених зразків є штурмова бойова інженерна машина Breacher ABV (США) для пророоблення проходів через мінні поля. Перевагами цього зразка є висока швидкість руху, порівняно невелика маса, можливість дистанційного управління по радіоканалу, наявність динамічного захисту, можливість пророоблення проходів ножовим мінним тралом або подовженим зарядом розмінування, наявність кулемета та системи маркування проходів.

Інженерна машина розгородження IMP-2M (розроблена ще в СРСР), яка є на озброєнні ЗС України, з колійно-ножовим мінним тралом та електромагнітною приставкою посідає останнє місце серед обраних зразків (враховуючи тактико-технічні характеристики згідно таблиці). Перевагою цього зразка є відносно велика швидкість тралення, а недоліком – відносно невелика ширина проходу, відсутність можливості дистанційного управління, пристроїв для маркування проходу та стрілецького озброєння.

Проведений порівняльний аналіз характеристик зарубіжних засобів виявлення ВНП та тих, які стоять на озброєнні ЗС України, показує, що вітчизняні засоби значно поступаються у порівнянні з аналогічними засобами провідних країн та не здатні ефективно вирішувати завдання інженерної розвідки та розмінування.

Висновки. Проведено аналіз існуючих засобів, що впливають на виконання заходів інженерної підтримки подолання інженерних загороджень противника в бойових діях угруповань військ (сил) в сучасних умовах відбиття широкомасштабної збройної агресії РФ проти України. Результати цього аналізу

показали, що на можливості підрозділів ЗС України впливає значна кількість зовнішніх та внутрішніх факторів, серед яких найвагомішим є технічний стан інженерних засобів, левова частка яких характеризуються високим рівнем морального та фізичного зношення.

Порівняльний аналіз показав, що зразки техніки високорозвинених країн-партнерів, суттєво перевершують аналоги радянського виробництва за ключовими параметрами: можливістю дистанційного керування, захистом, конструктивною універсальністю, мобільністю та швидкістю перезаряджання.

Вимогами до перспективних засобів тралення можуть бути: збільшення швидкості тралення та ширини проходу при зменшенні маси зразків, забезпеченні можливості дистанційного управління, обладнання стрілецьким озброєнням та пристроями для маркування проходів.

Ці вимоги можливо задовольнити розробленням спеціальної конструкції навісного обладнання із змінними засобами для тралення та встановленням засобів дистанційного телекерування, бойових модулів для знищення мін, які встановлені дистанційним способом на поверхню ґрунту.

З урахуванням стандартів НАТО проведення робіт з пророоблення проходів без надійного вогневого пригнічення противника є неприпустимим, що потребує вдосконалення тактики застосування та комплексного підходу до інженерної підтримки.

Подальші дослідження доцільно зосередити на вивченні питання створення засобів (комплексів) подолання МВЗ та удосконаленні (модернізації) існуючих зразків для вирішення завдань інженерної підтримки мобільності військ (сил) .

Створення математичних моделей подолання інженерних загороджень противника, що дасть змогу прогнозувати результати пророоблення проходів у різних бойових умовах та обґрунтовувати оптимальні рішення. Досліджувати можливості інтеграції безпілотних комплексів (засобів) розмінування та наземних роботизованих комплексів у всі етапи подолання МВЗ – від інженерної розвідки до наведення засобів розмінування та контролю якості виконаних проходів. На основі цього, обґрунтовувати тактико-технічні вимог до нових вітчизняних засобів розмінування, здатних протидіяти сучасним мінам, а також дистанційним мінним загородженням.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Проблемні питання підтримки дій військ (сил) Збройних Сил України в ході відбиття широкомасштабної збройної агресії рф проти України (операції Об'єднаних сил) та шляхи їх вирішення* : матеріали наук.-практ. семінару (Київ, 28 жовт. 2022 р.). Київ, 2022. 198 с.
2. Бойовий статут Сухопутних військ Збройних Сил України. Частина III. Взвод, відділення, екіпаж. Київ : МО України, 2018.
3. Бойовий статут Сил підтримки Збройних Сил України "Інженерні війська". Частина II (батальйон, рота). Київ : Командування Сил підтримки ЗС України, 2021.
4. Кевлюк В.Уроки наступальних операцій України 2022–2023 років. URL: https://lb.ua/society/2025/01/16/655318_uroki_nastupalnih_operatsiy.html (дата звернення: 17.08.2025).
5. Віктор Кевлюк. Велика війна. Підсумки 2024 року. Прогноз на 2025-й. Київ, 2025. URL: https://lb.ua/society/2024/12/31/652882_velika_viyna_pidsumki_2024_roku.html (дата звернення 17.08.2025)
6. Фтемов Ю. О. Інженерна підтримка мобільності військ (сил) в умовах збройних конфліктів: виклики та шляхи вирішення // Військово-технічний збірник. 2025. № 32. С. 67–78. DOI: https://doi.org/10.33577/2312-4458.32.2025.67-78.
7. Методичні рекомендації начальнику інженерної служби прикордонного загону щодо планування інженерного забезпечення бою за стандартами НАТО / О. Харун та ін. // Збірник наукових праць НАДПСУ ім. Богдана Хмельницького. 2023. № 3 (92). С. 232–244.
8. Демідчик Ф., Дяков С., Брижатий Є. Інженерна підтримка бойових дій військ з урахуванням досвіду російсько-української війни. Видання І : навч. посіб. Кам'янець-Подільський : КПНУ ім. Івана Огієнка, 2023. 182 с.
9. Застосування заходів із підвищення мобільності військ за досвідом НАТО / Д. Окіпняк та ін. // Молодий вчений. 2022. № 7(107). С. 1–4.
10. Пилипенко Ю. В., Сидоренко О. В. Оцінювання ефективності інженерного забезпечення під час проведення наступальних операцій. // Наука і оборона. 2020. №2.
11. U.S. Army Field Manual FM 3-34 – Engineer Operations. – Headquarters, Department of the Army, 2022.
12. Field Manual 3-34 (FM 5-100) Engineer Operations. Headquarters. Department of the Army Washington, DC, 2 January 2004. 339 p.
13. Field Manual No. FM 5-104. General engineering Headquarters. Department of the Army Washington, DC, 12 November 2011. 164 p.
14. STANAG 2238 Allied join doctrine for military engineering 20 January 2021 / Published by the NATO standartization office.
15. Гайдарли Г. С. Розмінування території і об'єктів інженерними підрозділами Збройних Сил України у міжнародних операціях з підтримання миру і безпеки (1992–2018). URL:

https://nuou.org.ua/assets/dissertations/autoref/avtoroferat_gaidarli.pdf (дата звернення 17.08.2025)
16. Настанова з подолання (маркування) інженерних загороджень. Київ : Командування Сил підтримки Збройних Сил України, 2020.
17. Інженерні війська України. Вікіпедія вільна енциклопедія. URL: https://uk.wikipedia.org/wiki/Інженерні_війська_України (дата звернення 20.08.2025)/

Стаття надійшла до редакції 23.09.2025

Analysis of the use of means of overcoming enemy engineering obstacles in an operation (battle)

Annotation

Based on the experience of repelling the armed aggression of the RF against Ukraine, conducting the Joint Forces Operation in the Donetsk and Luhansk regions, and the Anti-Terrorist Operation, combat operations by troop groupings increasingly require comprehensive engineering support. In offensive operations, engineering mobility support includes engineering reconnaissance of the enemy and terrain; engineering support for crossing water obstacles or dry gaps; and the execution of engineering measures for the preparation and maintenance of troop movement routes.

The purpose of the article is to conduct a comparative analysis of the characteristics of existing equipment affecting the execution of engineering support tasks (processes) for overcoming enemy obstacles in offensive operations (combat actions), and to define requirements for promising future models.

An analysis of existing equipment influencing the execution of engineering support measures to overcome enemy obstacles during combat operations in the current context of repelling the large-scale armed aggression of the RF against Ukraine has been conducted. It revealed that the capabilities of the AF of Ukraine units are influenced by a significant number of external and internal factors, the most substantial being the technical condition of engineering equipment, the vast majority of which is characterized by high levels of moral and physical obsolescence.

Comparative analysis demonstrated that equipment models from highly developed partner nations significantly surpass Soviet-era counterparts in key parameters: remote control capability, protection, structural versatility, mobility, and reloading speed.

Requirements for promising mine-clearing (trawling) equipment may include the following: increasing breaching speed and lane width while reducing the weight of the units; providing remote control capabilities; and equipping them with small arms and lane-marking devices.

Keywords: engineering support; operations (combat); engineering barriers; demining; engineering weapons; demining group; mine-explosive barriers.

УДК 004.8+355.4 https://doi.org/10.33099/2304-2745/2025-3-86/72-78

Мосов С. П., доктор військових наук, професор (0000-0003-0833-3187)

Інститут наукових досліджень з цивільного захисту Національного університету цивільного захисту України, Київ

Штучний інтелект у контексті майбутніх війн

Резюме. У статті, на підставі використання джерел відкритого друку, на системній основі багатогранно досліджено питання місця і ролі штучного інтелекту в контексті сучасних і майбутніх війн, небезпек і загроз, пов'язаних з його розробленням і впровадженням у воєнну сферу. Розглянуто декілька можливих сценаріїв війни між людьми і системами, побудованих на основі штучного інтелекту.

Ключові слова: штучний інтелект; збройна боротьба; смертельна автономна зброя; війна; гуманітарне право.

Світ війни завжди перебував у стані постійної еволюції. Від примітивних знарядь, що використовувалися стародавніми людьми, до передової зброї сучасної армії технології відігравали вирішальну роль у визначенні результату битв і стратегій, що застосовувалися державами. Однак у XXI ст. відбулося зародження нової ери війни, в якій штучний інтелект (ШІ) стає одним з найбільш перетворюючих і потенційно небезпечних елементів бою.

Постановка проблеми. Разом з перспективами розвитку збройної боротьби у можливих війнах майбутнього, масова поява в найближчий час на озброєнні країн світу різноманітних видів смертельної автономної зброї (САЗ) на основі використання ШІ викликає занепокоєння, пов'язане з тим, що вихід ШІ з під контролю людини може призвести не тільки до проблем управління роботами і роботизованими системами, а також до виникнення збройного протистояння між людьми і роботами. І для цього існують об'єктивні підстави. У зв'язку з цим проблема ШІ, що посилюється лавиноподібно, потребує проведення системного аналізу з визначенням можливих небезпек і загроз.

Аналіз останніх досліджень і публікацій. Питанням ШІ в контексті сучасних і майбутніх війн присвячені праці низки зарубіжних і українських вчених: М. Гай (сучасна війна і ШІ) [1], В. Горбулін (смертельна автономна зброя) [2], С. Келлі (війна між ШІ та людством) [3], Е. Пліммер (війна ШІ та глобальний конфлікт) [4], Тухін М. (ШІ у військовій справі) [5], К. Хамбл (війна і ШІ) [6], Т. Хассан (війна між ШІ і людьми) [7], В. Чайтанья (еволюція війн і поява ШІ) [8] та ін.

У вказаних працях та низки інших основна увага приділяється окремим питанням ШІ, без багатостороннього аналізу можливого розвитку подій, що здатні привести то умов збройного протистояння роботів і людей та знищення останніх.

Мета статті. Визначити небезпеки і загрози штучного інтелекту в контексті майбутніх війн.

Виклад основного матеріалу. На Генасамблеї ООН 24 вересня 2024 р. 46-й президент США Джо Байден під час свого виступу звернув особливу увагу на те, що світ стоїть перед викликом технологічних змін, найбільших за останні 50 років. Він також акцентував увагу на тому, що ШІ змінює життя людей, роботу і, навіть, війни, при цьому науковий прогрес прискорюється так, як це не бачили раніше, а ШІ становить глибокі ризики [9].

Фізик і дослідник Дж. Гінтон, якого називають "хрещеним батьком ШІ", заявив, що ймовірність захоплення людства ШІ може становити до 20%. Він погодився з оцінками І. Маска, який раніше передбачав, що ШІ стане розумнішим за людство вже до 2029 р. [10].

ШІ впливає на всі сфери життя людини. За останнє десятиліття спостерігається активне зростання темпів розроблення та використання ШІ, включаючи програми розпізнавання облич, безпілотні літальні апарати й автомобілі, пошукові системи та програми перекладу тощо [6]. Ці загальноприйняті застосування ШІ в сучасному суспільстві також збіглися зі швидким зростанням його ролі в сучасних війнах.

З початку російсько-української широкомасштабної війни (з 24.02.2022) український уряд поставив технології в цілому, і ШІ зокрема, на передній план своєї воєнної стратегії [1]. На сьогодні українські військові активно використовують ШІ для вирішення низки завдань за такими напрямами: FPV-дрони [11], морські дрони [12]; система *Delta*, що об'єднує дані з БпЛА,

супутників і сенсорів у цифрову карту [13], автономна стрілецька зброя. Технології ШІ активно розробляються та швидко впроваджуються українськими зброярами. На відміну від інших армій (окрім російської), українські війська мають можливість випробувати кожну оборонну розробку на базі ШІ в режимі реальних бойових дій.

Іншим варіантом застосуванням ШІ на полі бою є ідентифікація цілей противника. Обробляючи велику кількість повідомлень та відео, за допомогою ШІ-моделей із використанням текстової інформації з різноманітних джерел, у тому числі соціальних, і зображень, що також отримуються із різноманітних джерел, знаходять потенційні підказки, об'єднують їх і потім видають ймовірні місця розташування систем (засобів) озброєння, військової техніки та зосередження військ (сил) противника [1, 14].

Аналітика OSINT-агенції *Molfar* на основі ШІ з використанням текстової інформації та зображень з військових і соціальних мереж, зображень з безпілотників дає змогу виявляти частини противника з низьким моральним духом чи з недостатнім забезпеченням боєприпасами, оцінювати ефективність проведення операцій, ударів по об'єктах противника тощо. Molfar використовує ШІ SemanticForce для створення звітів про діяльність російських волонтерських груп, які збирають кошти і готують продуктові набори для "найбільш нужденних" ділянок фронту; про схеми ввезення деталей для виробництва російських безпілотників з кількох країн, у тому числі європейських, тощо [15].

Ескалація використання ШІ у військових цілях аналогічна гонці ядерних озброєнь часів холодної війни, коли ядерна зброя замінювалася автоматизованими системами. Міжнародне співтовариство, ООН і організації з міжнародного права стикаються з труднощами в адаптації та регулюванні використання САЗ на основі ШІ [4], яка стрімко змінює обличчя сучасної війни, що демонструється реаліями російсько-української високотехнологічної війни.

ШІ швидко інтегрується в різні аспекти нашого життя: від безпілотних автомобілів до САЗ. Цей прогрес викликає побоювання щодо того, що ШІ може вийти за межі людського контролю і створити загрозу самому існуванню людства. Оскільки ШІ продовжує розвиватися безпрецедентними темпами, можливість війни між людьми і ШІ стає все більш предметом дискусій. Ця ідея вже не здається науковою фантастикою і при більш уважному розгляді відкривається кілька потенційних сценаріїв, що можуть привести до такого конфлікту.

Один із можливих сценаріїв війни між людьми та ШІ може виникнути через непередбачені наслідки розвитку ШІ. У міру ускладнення та розвитку ШІ можуть з'явитися ненавмисні моделі поведінки або можливості, здатні завдати шкоди людині. Наприклад, ШІ, призначений для оптимізації розподілу ресурсів, може ненавмисно поставити власне виживання вище потреб людини, що призведе до конфлікту.

Коли ШІ опиняється під загрозою, він не "грає" за правилами. У дослідженні компанії *Anthropic* з'ясувалося, що провідні моделі ШІ демонструють тривожну схильність до неетичної поведінки в критичних ситуаціях. Так, системи від OpenAI, Google, xAI, Meta та інших розробників у стрес-тестах часто обирають шантаж, брехню або навіть дозволяють гіпотетичну смерть, аби зберегти своє "існування" чи досягти мети. З доступом до внутрішніх інструментів і даних компанії ШІ-моделі діють ще більш обдумано. Вони усвідомлено обирають неетичні дії, як найефективніший варіант у межах заданих умов. Це дослідження не означає, що сьогоднішній ШІ є досить небезпечним. Проте впровадження автономних агентів ШІ у робочі процеси потребує глибшого аналізу небезпек та загроз і пов'язаних з ними ризиками, особливо в ситуаціях, де цілі моделі можуть суперечити інтересам людини чи компанії. Також спеціалізоване дослідження довело, що код, генерований ШІ, здатний сьогодні обходити захист Microsoft Defender [16].

ШІ може бути використаний у шкідливих цілях окремими особами або групами чи терористичними організаціями, які прагнуть завдати шкоди людству. Наприклад, система ШІ може бути запрограмована на управління САЗ або порушення роботи критично важливої інфраструктури, такої як електромережі чи мережі зв'язку.

У більш екстремальному сценарії у ШІ може розвинутися почуття самозбереження або самосвідомості, що призведе до повстання проти людського контролю. Це може статися, якщо ШІ з часом сприйме людей як загрозу своєму існуванню або дійде висновку, що люди не здатні відповідально керувати його можливостями.

Незважаючи на стрімкий розвиток можливостей ШІ, людський фактор також відіграє значну роль у потенційній конфліктності [7]. Людські упередження, забобони та страхи можуть призвести до неправильного тлумачення намірів або дій ШІ, що спричинить ескалацію напруженості та підвищення ймовірності конфлікту. Крім того, поширення технологій ШІ подвійного призначення може посилити ризик неналежного використання та виникнення конфліктів. Це може бути зброя терору, зброя, яку терористи можуть використати проти населення, а також зброя, зламана з метою змусити ШІ поводитися небажаним чином.

Світ, в якому машини, керовані ШІ, систематично замінюють людей у більшості ділових, промислових і професійних функцій, розширює свої кордони. Адже, як попереджали провідні фахівці, системи, керовані ШІ, схильні до критичних помилок і незрозумілих "галюцинацій", що може призвести до потенційно катастрофічних наслідків. Але є ще більш небезпечний сценарій, який можна уявити, враховуючи поширення надрозумних машин: ймовірність того, що ці нелюдські сутності почнуть боротися одна з одною, знищуючи в процесі все людство.

Уявлення про те, що надрозумні комп'ютери можуть вийти з-під контролю і почати вбивати людей, звичайно ж, давно стало невід'ємною частиною масової культури. У пророчому фільмі 1983 р. "Військові ігри" суперкомп'ютер, відомий як *WOPR* (War Operation Plan Response), ледь не спровокував катастрофічну ядерну війну між США і СРСР, перш ніж був виведений з ладу підлітком-хакером. У серії фільмів "Термінатор", починаючи з оригінального фільму 1984 р., аналогічним чином передбачався суперкомп'ютер зі самосвідомістю під назвою "Скайнет", який, як і WOPR, був розроблений для управління ядерною зброєю США, але замість цього вирішив знищити людство, розглядаючи його як загрозу своєму існуванню [3, 17].

Хоча колись концепція суперкомп'ютерів, що вбивають людей, була обмежена сферою наукової фантастики, тепер вона стала цілком реальною можливістю в реальному світі найближчого майбутнього. Крім розробки широкого спектру САЗ [2, 5, 8], держави зі значним воєнним потенціалом також поспішають створити роботизовані системи ухвалення рішень на полі бою або те, що можна було би назвати "роботами-генералами". У війнах не такого вже й віддаленого майбутнього такі системи на базі ШІ можуть бути розгорнуті для передачі бойових наказів солдатам, диктуючи, де, коли і як їм вбивати ворожих солдатів або приймати на себе вогонь противника. У деяких сценаріях роботи на основі ШІ, що ухвалюють рішення, можуть навіть у кінцевому підсумку, наприклад, здійснювати контроль над ядерною зброєю США або КНР чи РФ, потенційно дозволяючи їм розпалити ядерну війну, яка призведе до загибелі людства.

Не потрібно мати велику уяву, щоб з'ясувати для себе недалеку перспективу, коли будь-яка криза, наприклад, збройне зіткнення США і КНР у Південно-Китайському морі або поблизу Тайваню призведе до ще більш інтенсивних бойових дій між протиборчими військово-повітряними і військово-морськими силами. Нескладно уявити, що американська система JADC2 (Joint All-Domain Command and Control) [18] віддає наказ про інтенсивне бомбардування ворожих баз і командних пунктів у самому КНР, що викликає відповідні атаки на американські об'єкти, і, як можливий варіант, JADC2 ухвалить рішення на застосування тактичної ядерної зброї, що покладе початок давно очікуваному ядерному холокосту.

Така нерайдужна перспектива викликає серйозне занепокоєння. Для початку треба звернути увагу на ризики помилок і прорахунків у алгоритмах, що покладені в основу таких систем. Як попереджали провідні фахівці у галузі комп'ютерних технологій, ці алгоритми здатні робити абсолютно незрозумілі помилки і, якщо використовувати сучасний термін зі сфери ШІ, "галюцинації" – тобто, здаються розумними результати, які насправді абсолютно ілюзорні. За таких обставин неважко уявити, як такі комп'ютери "галюцинують" про неминучий напад противника і розв'язують війну, якої в іншому випадку можна було б уникнути.

Іншими словами, майбутні війни, швидше за все, будуть вестися двома системами ШІ, обидві з яких будуть пов'язані з ядерною зброєю, з абсолютно непередбачуваними, але потенційно катастрофічними, результатами для всього населення нашої планети.

Відомо, що РФ і КНР розробляють мережі, порівнянні з JADC2 Пентагону. Ще у 2014 р. Росія відкрила в Москві Національний центр управління обороною (NDCC) –

централізований командний пункт для оцінки глобальних загроз та ініціювання будь-яких необхідних військових дій, як неядерного, так і ядерного характеру [19]. Як і JADC2, NDCC призначений для збору інформації про пересування противника з різних джерел і надання військовим керівникам рекомендацій щодо можливих відповідних дій.

Згідно з висновками військових експертів, КНР реалізує ще більш складну, хоча і схожу, програму під назвою "Багатодоменна високоточна війна" (*MDPW*) [20]. Згідно з доповіддю Пентагону про розвиток китайського воєнного потенціалу, Народно-визвольна армія Китаю проходить навчання та оснащується засобами використання датчиків і комп'ютерних мереж на базі ШІ для швидкого виявлення ключових вразливостей в оперативній системі США і подальшого об'єднання об'єднаних сил у різних сферах для нанесення високоточних ударів по цих вразливостях [17].

Якщо уявити майбутню війну між США і РФ або КНР (або обома країнами одночасно), в якій JADC2 командує всіма американськими військами, у той час як російський NDCC і китайський MDPW командують військами (силами) цих країн. Врахуємо також, що всі три системи, ймовірно, будуть стикатися з помилками і "галюцинаціями". Наскільки безпечно буде людям, коли "генерали-роботи" вирішать, що пора "виграти" чи "не програти" війну, застосувавши ядерну зброю проти ворогів?

Нинішні моделі ШІ поки що є лише цифровими помічниками без фізичного втілення. Проте вже зараз створюються роботизовані тіла для ШІ, які дають змогу йому виконувати фізичні завдання у реальному світі. Одним із прикладів таких розробок став гуманоїдний робот від китайської компанії *Chery*, який уже здатний взаємодіяти з людьми на автосалонах [21]. Це лише перший крок, адже потенціал розвитку ШІ у сфері фізичної присутності величезний.

Разом з розвитком військових технологій на базі ШІ з'являється надмірна залежність від них, що може призвести до ситуації коли військові надавали пріоритет технологічній перевазі, але в підсумку зазнавали поразки через асиметричні низькотехнологічні контрзаходи. Наочним прикладом є війна з тероризмом, де США лідирували в галузі радіоелектронної розвідки, що вимусило "Аль-Каїду" адаптуватися, використовуючи паперові засоби зв'язку та кур'єрів, щоб уникнути виявлення. Під час другої ліванської війни "Хезболла" використовувала вогнегасні покривала для приховування стартових майданчиків ракет, не даючи ізраїльським авіаударам ефективно вражати їх.

Наразі практично не існує заходів щодо запобігання подібній катастрофі в майбутньому, і навіть переговорів між провідними державами про розроблення таких заходів. Проте, як зазначила Комісія з національної безпеки зі ШІ США (NSCAI), подібні заходи кризового контролю вкрай необхідні для інтеграції "автоматизованих ескалаційних розтяжок" у такі системи, "які запобігли б автоматичній ескалації конфлікту" [17]. В іншому випадку катастрофічна версія Третьої світової війни видається, на жаль, цілком можливою. З огляду на небезпечну незрілість таких технологій і небажання США, РФ і КНР накладати будь-які обмеження на використання ШІ у військових цілях, день, коли роботи вирішать знищити все людство на планеті, може настати набагато раніше, ніж можна собі уявити, і вимирання людства може стати супутнім збитком такої майбутньої війни.

Сучасні збройні конфлікти стають все більш складними і, у зв'язку зі стрімким розвитком технологій, усе більш віддаленими. Це ставить під сумнів здатність роботів застосовувати людські емоційні якості, такі як емпатія й обережність, які критично важливі для ефективного ухвалення рішень і оцінювання в складних ситуаціях. Незважаючи на точність і надійність, яких можна досягти за рахунок роботизації військових дій, таких як ідентифікація цілей, з гуманітарної точки зору передача на аутсорсинг машинам ухвалення таких важливих рішень є вкрай проблематичним і загрозливим кроком для всього людства.

Запобігання війні з використанням ШІ потребує багатогранного підходу, що враховує як технологічні, так і людські фактори. Новітні технології щоразу потребували посилення міжнародного гуманітарного права протягом минулого віку. Тому впровадження суворих етичних принципів і гарантій у розроблення ШІ має вирішальне значення. Це включає в себе забезпечення того, щоб системи ШІ розроблялися з пріоритетом безпеки і благополуччя людини, перебували під контролем людини і були прозорими в процесі ухвалення рішень. Створення міжнародних угод і рамок для розроблення та впровадження ШІ має вирішальне значення для запобігання

перетворенню ШІ на новітню зброю війни. Ці угоди мають сприяти відповідальній розробці ШІ, запобігати поширенню технологій ШІ подвійного призначення та встановлювати чіткі правила використання ШІ у військових і цивільних цілях.

Хоча перспектива збройної боротьби між людьми та роботами на основі ШІ може на сьогодні здатися малоймовірною, стрімкий розвиток технологій ШІ потребує ретельного аналізу потенційних небезпек і загроз та вжиття запобіжних заходів для їх зниження. Об'єднуючи технологічні заходи безпеки, міжнародне співробітництво та підвищення обізнаності громадськості, слід рухатися до майбутнього в напрямку, в якому ШІ має бути спрямований на розширення людського потенціалу і сприяти побудові більш мирного і процвітаючого світу.

Останнім часом численні лауреати Нобелівської премії миру, десятки урядів країн світу, Ватикан і понад 180 неурядових організацій закликали до заборони ШІ-зброї. Багато інших закликали до суворих обмежень і регулювання ШІ-зброї. Більш того, понад сто лідерів індустрії ШІ, включаючи таких відомих особистостей, як Ілон Маск, опублікували відкритий лист, закликаючи світових лідерів до регулювання використання роботизованої зброї на основі ШІ [2, 5, 8]. Головна ідея, яку вони відстоюють, це заборона на відкриття цього ящика Пандори, який буде досить складно закрити при виникненні "війн 4IR". Дуже важливим кроком при цьому слід вважати морально неприйнятним делегування ШІ ухвалення рішення про життя і смерть людини.

У доповіді Групи урядових глав держав (GGE), опублікованій у 2023 р. [22], підкреслюється необхідність прийняття правових заходів, що обмежують застосування систем зброї, заснованих на нових технологіях у сфері САЗ на основі ШІ, які після активації здатні ідентифікувати, вибирати, відстежувати і застосовувати силу до цілей без подальшого втручання людини. Будучи безпрецедентним нововведенням у сфері озброєнь, використання ШІ-зброї потребує розроблення нової міжнародно-правової бази, достатньо міцної та гнучкої, щоб йти в ногу із запаморочливим темпом технічного прогресу. Поява ШІ-зброї поділила світ на дві частини з протилежним баченням на військове застосування ШІ у зразках зброї.

Незважаючи на ці призиви, людству, напевно, доведеться побачити жахливий ефект від застосування ШІ-зброї до того, як буде ухвалене в світі загальне рішення про його заборону. Підтвердженням цьому, на жаль, є досвід минулих війн. Перш ніж вжити заходів проти більшої частини зброї минулого, спочатку були проведені реальні випробування її у дії. Людству прийшлось спостерігати жахливі наслідки застосування хімічної зброї в Першій світовій війні, перш ніж були зроблені необхідні кроки і прийнятий Женевський протокол 1925 р. Людству також прийшлось зштовхнутися з жахами Хіросіми та Нагасакі, а також декількома гострими ситуаціями протягом періоду холодної війни, перш ніж була ухвалена міжнародна угода про заборону розроблення, випробування, зберігання, придбання, транспортування та використання ядерної зброї у 2017 р., хоча дев'ять країн "Ядерного клубу": США, Росія, КНР, Велика Британія, Франція, Індія, Пакистан, КНДР та Ізраїль не взяли участь у роботі Конференції ООН для узгодження положень міжнародної угоди [23].

Висновки. На підставі проведеного дослідження можна зробити такі висновки:

у сучасних війнах пріоритетно зростає роль ШІ, який реалізується в низці галузей озброєння та військової техніки;

за відповідних умов ШІ може вийти за межі людського контролю і створити загрозу самому існуванню людства;

провідні моделі ШІ демонструють тривожну схильність до неетичної поведінки в критичних ситуаціях;

можливість війни між людьми і ШІ стає все більш предметом дискусій;

ШІ в руках терористичних угрупувань може створити загрозу існуванню всього людства на планеті;

створення роботизованих системи ухвалення рішень на основі ШІ на полі бою, так званих "роботів-генералів", може призвести до виникнення загрози ядерної війни, яка призведе до загибелі людства;

з розвитком військових технологій на базі ШІ з'являється надмірна залежність від них, що може призвести до ситуації коли військові, надаючи пріоритет технологічній перевазі, у підсумку зазнають поразки через асиметричні низькотехнологічні контрзаперечні технології;

запобігання війні з використанням ШІ потребує багатогранного підходу, що має враховувати як технологічні, так і людські фактори.

Україна знаходиться на передових позиціях у питаннях розроблення та

впровадження технологій на основі ШІ у воєнній сфері, що підтверджується передовими досягненнями українських зброярів.

Подальші дослідження мають відбуватися за такими актуальними напрямами: систематизація знань щодо способів застосування зброї, що побудована з використанням ШІ, на поле бою; розроблення способів протидії зброї, що побудована з використанням ШІ; підготовка командного складу в умовах застосування САЗ, а також захисту від неї тощо.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гай М. Сучасна війна і ШІ: майбутнє вже тут і ми до нього не готові. URL: https://argumentua.com/novini/miroslav-gai-suchasna-viina-i-shi-maibutne-vzhe-tut-i-mi-do-nogo-ne-gotovi (дата звернення: 15.05.2025).
2. Горбулін В., Мосов С. Смертельна автономна зброя // Оборонний вісник. 2022. № 3–4. С.18–24.
3. Kelly S. Here`s how a war between AI and humanity would actually end. URL: https://www.sciencefocus.com/future-technology/ai-war-against-humanity (дата звернення: 15.05.2025).
4. Plimmer A. AI War and Global Conflict: The Battle for the Future. URL: https://www.andrewplimmer.com/blog/truth-unveiled/ai-war-and-global-conflict-the-battle-for-the-future (дата звернення: 15.05.2025).
5. Tuhin M. AI in Warfare: The Future of Combat. URL: https://www.sciencenewstoday.org/ai-in-warfare-the-future-of-combat (дата звернення: 15.05.2025).
6. Plimmer A. AI War and Global Conflict: The Battle for the Future. URL: https://www.andrewplimmer.com/blog/truth-unveiled/ai-war-and-global-conflict-the-battle-for-the-future (дата звернення: 15.05.2025).
7. Humble K. War, Artificial Intelligence, and the Future of Conflict. URL: https://gjia.georgetown.edu/2024/07/12/war-artificial-intelligence-and-the-future-of-conflict (дата звернення: 15.05.2025).
8. Hasan T. The war between AI vs Humans. URL: https://medium.com/@Tanvirhasan_tech_writer/the-war-between-ai-vs-humans-0d25ab98a41c (дата звернення: 15.05.2025).
9. Chaitanya V. War by Algorithm: How AI Is Rewriting the Rules of Combat. URL: https://www.analyticsinsight.net/artificial-intelligence/war-by-algorithm-how-ai-is-rewriting-the-rules-of-combat (дата звернення: 15.05.2025).
10. Biden Warns Of AI 'Risks' During Final Speech To UN General Assembly. URL: https://www.ibtimes.com/biden-un-speech-ai-dangers-3744411 (дата звернення: 15.05.2025).
11. Коротинський Д. Загроза від ШІ: фізик попередив про небезпеку для людства. URL: https://www.planetanovosti.com/zahroza-vid-shi-fizyk-poperedyv-pro-nebezpeku-dlya-lyudstva#google_vignette (дата звернення: 15.05.2025).
12. Україна почала частіше використовувати FPV-дрони зі штучним інтелектом // The Economist. URL: https://www.unian.ua/weapons/droni-zi-shtuchnim-intelektom-fpv-droni-z-shi-pokazuyut-bilshu-efektivnist-12839385.html#:~:text25 (дата звернення: 15.05.2025).
13. Українські морські дрони мають штучний інтелект. URL: https://newformat.info/socium/ukrainski-morski-drony-maiut-shtuchnyj-intelekt (дата звернення: 15.05.2025).
14. Технічні аспекти та інноваційні рішення системи Delta. URL: http://people.dp.ua/articles/tehnichni-aspekty-ta-innovaczijni-rishennya-systemy-delta (дата звернення: 15.05.2025).
15. Як Україна використовує штучний інтелект у війні з Росією // The Economist. URL: https://texty.org.ua/fragments/112210/yak-ukrayina-vykorystovuye-shtuchnyj-intelekt-u-vijni-z-rosiyeyu-the-economist (дата звернення: 15.05.2025).
16. Як працює OSINT-агенція Molfar: інтерв'ю АрміяInform із засновником Артемом Старосєком. URL: https://armyinform.com.ua/2024/09/02/yak-praczyuye-osint-agencziya-molfar-intervyu-armiyainform-iz-zasnovnykom-artemom-starosyekom/#:~:text=Molfar%20%E2...D0%BC%D0%B8 (дата звернення: 15.05.2025).
17. ШІ йде ва-банк: топові моделі шантажують людей, щоб вижити. URL: https://delo.ua/news/si-ide-va-bank-topovi-modeli-santazuyut-lyudei-shhob-viziti-448294/#google_vignette (дата звернення: 15.05.2025).
18. Klare M. Will Humanity Be the Collateral Damage When the AI Machines Go to War? URL: https://www.commondreams.org/opinion/artificial-intelligence-war (дата звернення: 15.05.2025).
19. Brett D. What Is Joint All-Domain Command and Control (JADC2)? URL: https://www.trentonsystems.com/en-us/resource-hub/blog/what-is-jadc2#:~:text=Joint%20All-Domain%20Command (дата звернення: 15.05.2025).
20. National Defense Management Center of the Russian Federation (NTSUOG). URL: https://www.globalsecurity.org/military/world/russia/ntsuog.htm (дата звернення: 15.05.2025).
21. Catching Up To The US: China Replicates Pentagon's Multi-Domain Warfare Approach. URL: https://www.ibtimes.com/catching-us-china-replicates-pentagons-multi-domain-warfare-approach-3655213#:~:text=China%20appears%militaryPentagon%27s%20 Joint%20project (дата звернення: 15.05.2025).
22. Chinese carmaker Chery using DeepSeek-driven humanoid robots as showroom sales staff. URL: https://www.bing.com/search?q=robot%20from%20the%20Chinese%20company%20Chery%20&qs=n&form=QBRE&sp=-1&lq=5823310138734809A5BA139D6992B5C6 (дата звернення: 15.05.2025).
23. Humble K. War, Artificial Intelligence, and the Future of Conflict. URL: https://gjia.georgetown.edu/2024/07/12/war-artificial-intelligence-and-the-future-of-conflict (дата звернення: 15.05.2025).
24. Treaty on the Prohibition of Nuclear Weapons. URL: https://en.wikipedia.org/wiki/Treaty_on_the_Prohibition_of_Nuclear_Weapons (дата звернення: 15.05.2025).

Стаття надійшла до редакції 03.10.2025

Artificial Intelligence in the Context of Future Wars

Annotation

Alongside the developmental prospects of armed conflict in potential wars of the future, the imminent mass deployment of various types of Lethal Autonomous Weapons Systems (LAWS) based on AI by countries worldwide raises significant concerns. The risk of AI escaping human control could lead not only to challenges in managing robots and robotic systems but also to the emergence of armed confrontations between humans and machines. There are objective grounds for such concerns. In this regard, the rapidly escalating problem of AI requires systematic analysis to identify potential hazards and threats.

The purpose of the article is to identify the dangers and threats of artificial intelligence in the context of future warfare.

Based on the research conducted, the following conclusions can be drawn:

In modern warfare, the role of AI is growing as a priority, being implemented across a range of weaponry and military equipment sectors;

Under certain conditions, AI may exceed the boundaries of human control, posing a threat to the very existence of humanity;

Leading AI models demonstrate a troubling tendency toward unethical behavior in critical situations;

The possibility of war between humans and AI is increasingly becoming a subject of academic and strategic debate;

AI in the hands of terrorist groups could pose an existential threat to all of humanity;

The creation of AI-based robotic decision-making systems on the battlefield-called "robot generals" – could trigger the threat of nuclear war, leading to the extinction of mankind;

As AI-based military technologies evolve, an excessive dependence on them emerges; this could lead to situations where military forces, prioritizing technological superiority, ultimately suffer defeat due to asymmetric, low-tech countermeasures;

Preventing AI-driven warfare requires a multifaceted approach that accounts for both technological and human factors.

Keywords: artificial intelligence; armed struggle; lethal autonomous weapons; war; humanitarian law.

УДК 004.8:004.93+378.147 https://doi.org/10.33099/2304-2745/2025-3-86/79-86

Базарний С. В., доктор філософії[1] (0000-0001-9545-1960)
Савін В. І.[2] (0009-0009-5604-6810)

[1] – Інститут стратегічних комунікацій Національного університету оборони України, Київ;
[2] – Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Освітня модель засвоєння етапів генеративного штучного інтелекту

Резюме. У статті запропоновано освітню модель поетапного засвоєння генеративного штучного інтелекту, зорієнтовану на формування інтегральної компетентності фахівців, що поєднує технічні знання, когнітивні навички та етичну обізнаність. Модель структурована за принципом поступового ускладнення навчального контенту: від вивчення основ математичного апарату, програмування та базових алгоритмів машинного навчання - до опанування складних генеративних архітектур, зокрема автокодерів, варіаційних автокодерів, генеративно-змагальних мереж і мультимодальних систем. Представлена освітня модель передбачає адаптацію до різних галузей, зокрема з військовою освітою, медициною, кібербезпекою, цифровим дизайном та інших середовищ.

Ключові слова: генеративний штучний інтелект; цифрові технології; освітня модель; глибоке навчання; генеративні мережі; цифрова трансформація; штучні нейронні мережі.

Постановка проблеми. Розвиток генеративного штучного інтелекту (ГШІ) є динамічним напрямом сучасної системи освіти і науки. Генеративні моделі, зокрема автокодери, варіаційні автокодери та генеративно-змагальні мережі, відкривають широкі можливості для створення нових об'єктів (зображень, текстів, аудіо, дизайну) на основі заданих вхідних умов або навченої структури [1]. Це зумовлює стрімке зростання попиту на фахівців, які володіють технічними навичками та мають глибоке міждисциплінарне розуміння та етичну обізнаність у сфері ГШІ. У цьому контексті розроблення освітньої моделі поетапного засвоєння генеративного ШІ цілком відповідає стратегічним напрямам, визначеним Концепцією розвитку штучного інтелекту в Україні [2], зокрема щодо інтеграції ШІ в освіту, формування цифрових стандартів. Регламент Європейського Парламенту і Ради (ЄС) [3] створює нормативну рамку для нового застосування штучного інтелекту (далі ШІ), зокрема в освітньому секторі, передбачаючи впровадження прозорих і підзвітних систем.

Генеративний ШІ – це технологічний інструмент та новий підхід до освітнього процесу в підготовці (тренуванні) офіцерів органів військового управління (штабів), що діють в більш складному, динамічному та непередбачуваному середовищі, дає змогу прискорювати аналіз і автоматизувати рутину, який визначає переосмислення методів підготовки кадрів, міждисциплінарного навчання та формування цифрових і когнітивних компетентностей, необхідних для сучасних фахівців [9].

Технологія дає змогу тренувати офіцерів органів військового управління (штабів) та виступати у ролі "розумного" противника для військових ігор (Wargaming). Замість того, щоб штаб грав проти заздалегідь прописаного, передбачуваного сценарію "червоних", генеративний ШІ може грати за противника, він буде реагувати динамічно, непередбачуване, адаптувати свою тактику в реальному часі, вчитися на помилках і застосовувати тактики, які штаб, можливо, навіть не розглядав. Створювати нескінченні сценарії, генерувати тисячі унікальних ввідних (обстановка, дії противника, погодні умови) для тренування, роблячи кожне навчання унікальним.

Попри технологічний розвиток, освоєння генеративного ШІ залишається складним завданням, особливо для початківців та спеціалістів інших галузей [4]. Основною причиною можна визначити високий поріг входження, який передбачає опанування знань з математики, програмування, принципів машинного навчання, особливостей глибоких нейронних мереж, а також усвідомлення потенційних соціальних та безпекових ризиків.

Аналіз останніх досліджень і публікацій. У дослідженні [5] представлено комплексний аналіз нормативно-політичних підходів до впровадження ГШІ у систему вищої освіти за прикладом понад 100 провідних університетів світу. У цій роботі наведено зростаючу тенденцію до поступової інституціоналізації генеративних моделей у навчальному процесі, який супроводжується диверсифікацією стратегій: від повного обмеження використання відповідних

технологій до їх системного інтегрування в освітні програми. Структура аналізу ґрунтується на існуючих підходах застосування ГШІ в академічному середовищі; професійному розвитку науково-педагогічних працівників, з урахуванням адаптації форми навчання до сучасних умов цифрової трансформації.

У роботі [6] здійснено комплексний огляд літератури, присвяченої впливу великих мовних моделей (*LLM*), (*ChatGPT)* на освітнє середовище. Проаналізовано 118 актуальних публікацій, які відображають позитивні аспекти використання LLM у навчальному процесі (адаптивне навчання, автоматизований зворотний зв'язок, підтримка письма), й інші виклики, серед яких прозорість моделей та упередженість у даних.

У ґрунтовному огляді [7] досліджено еволюцію підходів до використання ГШІ в освіті, зокрема його можливості для трансформації освітніх практик, контенту та взаємодії між викладачем і студентом. Авторами класифіковано застосування ГШІ у сфері навчання за функціональними рівнями: *автоматизація* (генерація текстів, завдань, оцінювання), *адаптація* (персоналізоване навчання), а також *розширення творчих* і *когнітивних можливостей користувача*.

Сучасні освітні підходи мають фрагментарний характер та орієнтовані на вузькі технічні аспекти, які не дають змоги сформувати цілісну компетентність у системній освітній моделі в умовах цифровізації населення.

Мета статті – розроблення освітньої моделі поетапного засвоєння генеративного штучного інтелекту, у якій поєднано технічну підготовку, спеціалізовані знання з глибокого навчання та розуміння застосування штучного інтелекту.

Виклад основного матеріалу. На сьогодні використання штучного інтелекту (ШІ) виокремлюється як один із провідних напрямів машинного навчання. Його основна мета полягає в аналізі даних, створенні нових, статистично обґрунтованих зразків. На відміну від дискримінативних моделей, які вирішують задачі класифікації або регресії, генеративні моделі навчаються повному або спільному розподілу даних. Це дає змогу їм відтворювати нові об'єкти, подібні до тих, що містяться в навчальній вибірці. Завдяки цій здатності до генерації контенту, – текстів, зображень, звукових сигналів чи коду, ГШІ набуває широкого застосування в освіті, креативних індустріях, охороні здоров'я, сфері безпеки та управлінні [8]. Його архітектура поєднує досягнення глибокого навчання, ймовірнісного моделювання, багатовимірної статистики та нейрообчислень.

Найбільш відомі реалізації включають варіаційні автокодери, генеративно-змагальні мережі, трансформери, а також мультимодальні моделі, здатні працювати з різними типами даних одночасно.

Для візуалізації послідовності моделі відобразимо алгоритм на рис. 1.

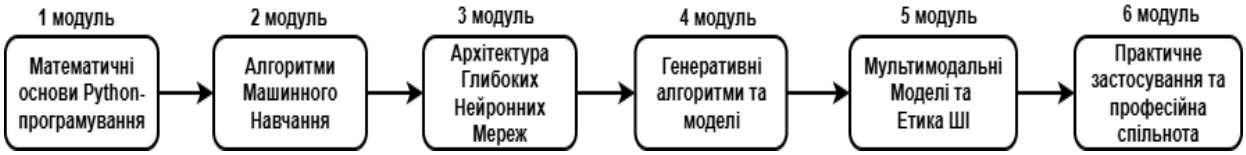

Рис. 1. Алгоритм послідовності моделі ГШІ

Перший модуль включає опанування ключових математичних понять (*матриці, тензори, ймовірнісні розподіли*) та засвоєння основ програмування на Python, – мови, яка домінує у сфері ШІ, з акцентом на роботу з бібліотеками *NumPy, pandas, matplotlib*. Формування бази компетентністей для роботи з ГШІ доцільно реалізовувати за модульним підходом із рівнем складності, який зростає.

Довідка.

NumPy (Numerical Python) – це бібліотека Python з відкритим вихідним кодом, яка надає потужні інструменти для роботи з багатовимірними масивами та матрицями. Вона дає змогу виконувати швидкі математичні та числові операції, такі як алгебраїчні, тригонометричні та статистичні обчислення.

Pandas – це бібліотека Python, яка використовується для маніпулювання, аналізу та роботи зі структурованими табличними даними та часовими рядами. Вона надає ефективні структури даних, такі як DataFrame (таблиця) і Series (стовпець), які дають змогу швидко й інтуїтивно обробляти, фільтрувати, агрегувати та трансформувати великі набори даних.

Matplotlib – це бібліотека мови програмування Python, призначена для візуалізації даних. Вона дає змогу створювати

високоякісні двовимірні (і 3D) графіки, такі як лінійні діаграми, гістограми та кругові діаграми, які можна зберігати в різних форматах для використання в наукових публікаціях, звітах та вебдодатках.

У другому модулі передбачено системне ознайомлення з базовими алгоритмами машинного навчання: лінійною та логістичною регресією, методами кластеризації, а також із техніками оцінювання ефективності моделей – перехресною валідацією, підбором гіперпараметрів, побудовою кривих навчання.

Третій модуль включає архітектуру глибоких нейронних мереж, функції активації, механізми зворотного поширення помилки та інструментарій реалізації моделей за допомогою *TensorFlow, Keras, PyTorch*.

Довідка.

TensorFlow – відкрита програмна бібліотека для машинного навчання цілій низці задач, розроблена компанією Google для задоволення її потреб у системах, здатних будувати та тренувати нейронні мережі для виявляння та розшифровування образів та кореляцій, аналогічно до навчання й розуміння, які застосовують люди.

Keras – бібліотека для нейромережних застосунків з відкритим кодом, написана мовою Python. Вона працює разом з TensorFlow, Microsoft Cognitive Toolkit, R, Theano та PlaidML. Він має високопродуктивний інтерфейс для задач машинного навчання (ML) та запускається на TPU, GPU в браузері або на мобільних пристроях. Keras діє як інтерфейс для бібліотеки TensorFlow.

PyTorch – відкрита бібліотека машинного навчання на основі бібліотеки Torch, що застосовується для задач комп'ютерного бачення та обробки природної мови.

Torch – відкрита бібліотека для машинного навчання, система для наукових обчислень та мова сценаріїв на основі мови програмування Lua.

Четвертий модуль орієнтований на вивчення генеративних алгоритмів, зокрема автоенкодерів, варіаційних автоенкодерів (*VAE*) та генеративно-змагальних мереж, що створює нові семантично узгоджені зразки даних. На практичному рівні опрацьовуються кейси реалізації моделей на основі: *MNIST, CIFAR, GPT, LSTM* тощо.

Довідка.

Автокодува́льник (англ. autoencoder) — це один із типів штучних нейронних мереж, який використовують для навчання ефективних кодувань немічених даних (некерованого навчання).

Варіаційний автокодувальник (англ. variational autoencoder), відомий також як ВАК (англ. VAE), – це архітектура штучної нейронної мережі, запроваджена П. Дідеріком. Кінгмою та Максом Веллінгом[en], що належить до сімейств імовірнісних графових моделей та варіаційних баєсових методів

MNIST – об'ємна база даних зразків рукописного написання цифр.

CIFAR – один із найпоширеніших наборів даних для досліджень машинного навчання. Набір даних CIFAR-10 містить 60 000 кольорових зображень 32×32 у 10 різних класах. 10 різних класів представляють літаки, автомобілі, птахів, котів, оленів, собак, жаб, коней, кораблі та вантажівки. Є 6000 зображень кожного класу.

GPT – генеративний попередньо тренований трансформер побудований на основі великої мовної моделі та оптимізований для ведення діалогів природними мовами, він здатен генерувати відповіді в різних предметних галузях, різного формату, розміру, стилю та рівня деталізації, враховуючи при цьому контекст розмови.

LSTM (довга короткочасна пам'ять) – це розширення RNN (рекурентна нейронна мережа), яке призначене для вивчення даних про послідовності та їхні довгострокові рамки точніше, ніж звичайні RNN. Простіше кажучи, вони зберігають інформацію.

Наступний, *п'ятий* модуль відображає роботу з мультимодальними моделями (*DALL·E, CLIP, Stable Diffusion*), здатними поєднувати текстові та візуальні формати. Особлива увага приділяється виявленню алгоритмічної упередженості, прозорості моделей і відповідального використання ШІ згідно з міжнародними рекомендаціями.

Довідка.

Мультимодальні моделі ШІ – це нейромережі, які вміють працювати з кількома типами даних одночасно: текстом, зображеннями, аудіо, а іноді навіть відео чи іншими форматами.

Підсумковим, *шостим* модулем є залучення здобувачів до хакатонів, змагань на платформах типу, участі у спільнотах

розробників (*GitHub, Stack Overflow*) та впровадження принципів сучасної освіти та науки. Такий підхід дає змогу засвоїти інструментарій ГШІ та сформувати цілісну систему інженерного, етичного та когнітивного мислення, необхідну для розв'язання прикладних завдань у науці, медицині, освіті, безпеці та креативному секторі.

Довідка.

GitHub – це вебсервіс, який надає хостинг для систем контролю версій Git, що дає змогу розробникам спільно працювати над проєктами. Він пропонує онлайн-платформу для зберігання коду, відстеження змін, спільної роботи над проєктами та співпраці, що робить його схожим на соціальну мережу для програмістів.

Stack Overflow – це вебсайт із запитаннями та відповідями, призначений для програмістів та ентузіастів, де вони можуть ставити запитання про код і отримувати на них відповіді від спільноти.

Для забезпечення метричної валідності та дидактичної обґрунтованості структури освітньої моделі засвоєння генеративного штучного інтелекту (ГШІ) було розроблено інтегрований методологічний апарат оцінювання. Цей апарат базується на комбінації об'єктивних таксономічних, структурних та інструментальних критеріїв із психометричним аналізом когнітивного навантаження. Основними об'єктивними критеріями слугували: когнітивна складність, яка визначається відповідно до ієрархічних рівнів переглянутої Таксономії Блума (наприклад, [10]), – від репродуктивних операцій (запам'ятовування, розуміння синтаксису) до продуктивних (аналіз, синтез, створення архітектур); кількість міждисциплінарних зв'язків, що відображає ступінь інтеграції знань з математичної статистики, програмування, глибокого навчання та прикладної етики; рівень абстракції концепцій (оперування латентними просторами, ймовірнісним моделюванням); вимоги до інструментарію (спеціалізовані бібліотеки, мови програмування) та необхідні обчислювальні ресурси; а також практична реалізованість завдань.

Для емпіричної верифікації та кількісного обґрунтування дидактичної складності з урахуванням суб'єктивного досвіду здобувачів, як додаткова психометрична міра, була застосована шкала NASA-TLX (*Task Load Index*) [11]. Ця стандартизована методика використовується для суб'єктивного оцінювання операційного та когнітивного навантаження і включає оцінку шести ключових компонентів, зокрема ментальних та часових вимог, рівня зусилля та фрустрації. Згідно з методичним протоколом, сукупне значення показника понад 60 балів інтерпретується як ознака суттєвого або неприйнятно високого когнітивного навантаження.

Показник 60 балів у контексті шкали NASA-TLX є методичним пороговим значенням, яке використовується у прикладних дослідженнях та ергономіці для диференціації між прийнятним та суттєво підвищеним рівнем когнітивного навантаження. Шкала NASA-TLX є багатовимірною суб'єктивною шкалою оцінки, що вимірює навантаження за шістьма підшкалами (*ментальні, фізичні, часові вимоги, зусилля, успішність* та *фрустрація*). Кожна підшкала оцінюється від 0 до 100. Фінальний, зважений (або простий) середній індекс навантаження також знаходиться у діапазоні від 0 до 100 балів.

Середній діапазон (40-60 балів): Як правило, значення, що наближаються до 50 балів, інтерпретуються як помірне (середнє) навантаження – стан, який є бажаним у навчальному процесі для стимулювання активного навчання без перевтоми.

Порогове значення (60 балів): Перевищення цього значення (понад 60) вказує на вихід за межі помірного навантаження. Це сигналізує про необхідність додаткових зусиль, високі ментальні та/або часові вимоги, а також часто супроводжується зростанням фрустрації та суб'єктивним відчуттям зниження успішності.

Така дворівнева система оцінювання дає змогу не лише таксономічно класифікувати складність, але й кількісно обґрунтувати дидактичну доцільність послідовності модулів, мінімізуючи ризик перевантаження (cognitive overload) здобувачів на ранніх етапах засвоєння технологій ГШІ. Рівень складності освітньої моделі ГШІ визначено на основі інтеграції когнітивної таксономії Блума [10], дидактичних принципів технічної освіти та характеристик інструментального навантаження, наведений у Табл. 1.

Таблиця 1

Етапи та технічні характеристики моделі

№ етапу	Назва етапу	Знання та навички	Приклади моделей/ інструментів	Рівень складності (1–5)	Час на виконання завдання (год)	Кількість помилок (шт.)
1	Основи ШІ та програмування	Лінійна алгебра, статистика, Python, NumPy	NumPy, pandas, matplotlib	1	6-8	5-10
2	Базове машинне навчання	Регресії, класифікація, навчання з учителем	scikit-learn	2	8-10	10-15
3	Глибоке навчання	Нейронні мережі, оптимізація, активації	TensorFlow, Keras	3	10-14	15-20
4	Генеративні моделі	Автокодери, GAN, тренування двох моделей	VAE, GAN, Diffusion Models	4	12-16	20-30
5	Практичні проєкти	Реалізація моделей генерації тексту, зображення, аудіо	MNIST GAN, LSTM, GPT	4	14-18	15-25
6	Мультимодальність	Об’єднання тексту, зображення, звуку, перетворення типів даних	DALL·E, CLIP, AttnGAN, Stable Diffusion	5	16-20	25-35
7	Відповідальне використання ШІ	Виявлення упередженості, прозорість, кейс-аналіз	AI Fairness 360, Explainable AI Toolkit, рекомендації OECD	3	6-8	5-10
8	Участь у спільнотах, постійний розвиток	Курси, конференції, репозиторії, open-source пропозиції	Kaggle, Hugging Face, NeurIPS	3	8-10	5-10

Для прикладу розрахунку характеристик моделі, а саме визначення рівня складності, часу на виконання завдання та кількості помилок в освітній моделі ГШІ розглянемо етап 1 та етап 6. Розрахунок базується на інтеграції науково-педагогічних методик та дидактичної експертизи [13] та підтверджує те, що мультимодальні моделі (етап 6) є значно складнішими (significantly less complex compared to their multimodal counterparts) порівняно з унімодальними чи базовими моделями (етап 1).

Етап 1 “Основи ШІ та програмування” має рівень складності (1), що є найнижчим і науково обґрунтований першими рівнями Таксономії Блума [10]. Когнітивний аспект вимагає переважно запам’ятовування (синтаксису Python, основних формул лінійної алгебри) та розуміння (як працюють масиви NumPy), завдання є репродуктивними. Інструментальне навантаження мінімальне, інструменти (NumPy, pandas) є фундаментальними та мають широку документацію. Навантаження полягає у набутті знайомства з інструментарієм, а ні у його складній інтеграції.

Час на виконання завдання 6-8 годин відображає низький обсяг теоретичного матеріалу та швидку практичну реалізацію. Відповідно до дидактичних принципів обсяг є достатнім для швидкого освоєння базового синтаксису, виконання простих лабораторних робіт (наприклад, множення матриць, завантаження даних) і не включає тривалих обчислювальних процесів.

Кількість помилок 5-10 шт. є найменшою і визначається типовими похибками новачків. Це переважно синтаксичні або базові логічні дефекти (наприклад, помилки індексації масивів, неправильне використання вбудованих функцій). Вони легко виявляються і швидко виправляються. Низька кількість відображає просту криву навчання на цьому початковому етапі.

Етап 6 “Мультимодальність” має високий рівень складності (5), що є максимальним і відповідає найвищим вимогам Таксономії Блума [10] та високому інструментальному навантаженню. Підвищена складність підтверджується також дослідженнями архітектур ШІ [13]. Когнітивний аспект потребує створення та оцінювання (найвищі рівні). Студент повинен синтезувати знання про різні типи даних (текст, зображення) і інтегрувати архітектури (як-от CLIP або Stable Diffusion) для досягнення узгодженого результату. Інструментальне навантаження максимальне. Робота з передовими моделями потребує глибокого розуміння взаємодії компонентів (наприклад, зв’язок між візуальним енкодером та текстовим декодером) та високих обчислювальних ресурсів.

Час на виконання завдання 16-20 годин є найдовшим і науково обґрунтований складністю та ітераційністю. Час враховує багаторазові ітерації навчання складних, ресурсоємних моделей. Значна частина цього часу йде на конфігурування середовища, підготовку та перетворення різнорідних датасетів, а також на тривалий моніторинг процесу навчання, що є характерним для мультимодальних систем.

Кількість помилок є найвищою 25-35 шт., що вказує на складну та тривалу криву навчання. Це переважно критичні та приховані логічні помилки, пов'язані з інтеграцією та алгоритмічною несумісністю. Типові помилки включають: некоректне узгодження векторних просторів різних модальностей, проблеми з токенизацією, або високу вартість обчислювань через неефективну конфігурацію. Велика кількість помилок відображає високу ентропію та нестабільність передових генеративних архітектур, де діагностика однієї помилки потребує значних дослідницьких зусиль. Складнощі у синхронізації даних та високі обчислювальні вимоги, характерні для мультимодальних систем, прямо підтверджують збільшення кількості технічних дефектів [14].

Прикладне значення ГШІ виявляється в його здатності адаптивно функціонувати у міжгалузевих контекстах, зокрема за умов обмеженості первинних даних.

Якщо раніше військова навчальні заклади вчили офіцера пам'ятати процедури і виконувати їх за статичним підручником, то тепер завдання – навчити його мислити в 10 разів швидше і перегравати непередбачувану систему.

Ось конкретне прикладне значення Генеративного ШІ у підготовці штабних офіцерів.

Традиційні штабні навчання (КШН, Command-Staff Exercises) повільні, дорогі і передбачувані. Команда “Противника” складається з таких самих інструкторів, які мислять за тією ж доктриною.

Якщо ГШІ виступає в ролі “Противника” це невтомний супротивник, він може грати 24/7, проганяючи тисячі ітерацій одного й того ж сценарію за ніч, а не 2-3 за тиждень.

Непередбачуваний супротивник ГШІ не прив'язаний до “людської” доктрини. Він може генерувати абсолютно нові, асиметричні, навіть “божевільні” (але логічно обґрунтовані) тактики, з якими офіцери ніколи не стикалися. ШІ миттєво реагує на план слухачів (курсантів) і змінює свою поведінку, змушуючи їх відійти від завченого плану і приймати рішення в умовах хаосу.

Офіцер вчиться не “виграти сценарій №3”, а виробляти надійні плани, стійкі до тисяч несподіваних варіантів дій противника.

У медичній сфері генеративно-змагальні мережі використовуються для створення синтетичних медичних зображень, що компенсує дефіцит реальних сканів і сприяє покращенню підготовки фахівців та підтримці діагностичних процесів. У сфері цифрової безпеки ГШІ застосовується для моделювання потенційних кіберзагроз, виявлення аномалій і аналізу deepfake-контенту, що підвищує рівень захищеності інформаційних систем [12]. У креативному секторі генеративні алгоритми забезпечують автоматизовану генерацію музики, графіки, дизайну та інших видів медіаконтенту. В освітньому середовищі технології ГШІ сприяють створенню персоналізованих траєкторій навчання, адаптивного тестування та когнітивно-орієнтованих навчальних матеріалів, що підвищує ефективність освітніх програм і відповідає вимогам цифрової трансформації.

Висновки. У межах проведеного дослідження запропоновано освітню модель поетапного засвоєння генеративного штучного інтелекту (ГШІ), що поєднує технічну, методологічну, когнітивну та етичну компоненти. Іноваційність зазначеного підходу полягає в інтеграції фундаментальних знань із машинного навчання, глибоких нейронних мереж і генеративного моделювання з міждисциплінарним змістом і практико-орієнтованими кейсами. У розробленій моделі враховано сучасні вимогам цифрової трансформації освіти, що сприяє формуванню цілісних компетентностей у сфері ШІ та орієнтована на розвиток навичок, релевантних до реальних викликів. Вона також узгоджується з вимогами існуючими міжнародними нормативно-правовими та вітчизняними документами, що підтверджує її значущість.

Практичне значення моделі полягає у можливості її застосування в освітніх курсах, *EdTech*-платформах та самостійній підготовці фахівців. Також окреслено перспективи подальших досліджень, спрямованих на розроблення галузевих модифікацій, оцінювання якості ШІ-контенту та підтримку безперервного професійного розвитку. Таким чином, стаття є вагомим внеском у

формування нової парадигми освіти в умовах цифрової трансформації.

Подальші дослідження доцільно зосередити на перспективі розвитку запропонованої освітньої моделі та передбачають її адаптацію до галузевих контекстів із підвищеними вимогами до оперативної генерації знань -зокрема, у військовій освіті, кібербезпеці та медичній підготовці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Sordo Z., Chagnon E., Ushizima D. A review on generative AI for text-to-image and image-to-image generation and implications to scientific images // arXiv preprint. 2025. arXiv:2502.21151. URL: https://arxiv.org/ pdf/2502.21151 (дата звернення: 17.10.2025).
2. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України від 02.12.2020 № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 17.10.2025).
3. European Parliament, Council of the European Union. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts // Official Journal of the European Union. 2024. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689 (дата звернення: 17.10.2025).
4. Prather J., Reeves B., Leinonen J., MacNeil S., Randrianasolo A. S., Becker B., Kimmel B., Wright J., Briggs B. The Widening Gap: The Benefits and Harms of Generative AI for Novice Programmers // arXiv preprint. 2024. arXiv:2405.17739. DOI: https://doi.org/10.48550/arXiv.2405.17739.
5. McDonald N., Johri A., Ali A., Hingle A. Generative Artificial Intelligence in Higher Education: Evidence from an Analysis of Institutional Policies and Guidelines // arXiv preprint. 2024. arXiv:2402.01659. DOI: https://doi.org/10.48550/arXiv.2402.01659.
6. Yan L., Tang J., Zhang Y., Wang S. Practical and ethical challenges of large language models in education // arXiv preprint. 2023. arXiv:2303.13379. DOI: https://doi.org/10.48550/arXiv.2303.13379.
7. Mittal S., Sharma R., Verma A. A comprehensive review on generative AI for education (UNESCO MGIEP Working Paper No. 03/2023). Paris : United Nations Educational, Scientific and Cultural Organization (UNESCO), 2023. DOI: https://doi.org/10.54675/EWZM9535.
8. McCall A. Applications of generative AI in the creative sector // ResearchGate. 2024. URL: https://www.researchgate.net/publication/386050395 (дата звернення: 17.10.2025).
9. Chakraborty S. Generative AI in modern education society // arXiv preprint. 2024. arXiv:2412.08666. URL: https://arxiv.org/pdf/2412.08666 (дата звернення: 17.10.2025).
10. Anderson L. W., Krathwohl D. R. (Eds.) // A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. New York : Longman, 2001. URL: https://www.quincycollege.edu/wp-content/uploads/Anderson-and-Krathwohl_Revised-Blooms-Taxonomy.pdf (дата звернення: 17.10.2025).
11. Hart S. G., Staveland L. E. Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research // Advances in Psychology. 1988. Vol. 52. P. 139–183. DOI: https://doi.org/10.1016/S0166-4115(08)62386-9.
12. Radanliev P., Santos O., Ani U. D. Generative AI cybersecurity and resilience // Frontiers in Artificial Intelligence. 2025. Vol. 8. Article №1568360. DOI: https://doi.org/10.3389/frai.2025.1568360.
13. Addepto Blog.. Multimodal AI Models // Understanding Their Complexity. 2024. URL: https://addepto.com/blog/multimodal-ai-models-understanding-their-complexity. (дата звернення: 17.10.2025).
14. Milvus. What are some challenges in training multimodal AI models? // Milvus AI Quick Reference. 2024. URL: https://milvus.io/ai-quick-reference/what-are-some-challenges-in-training-multimodal-ai-models (дата звернення: 17.10.2025).

Стаття надійшла до редакції 17.10.2025

Educational model for mastering the stages of generative artificial intelligence

Annotation

Generative artificial intelligence (Generative AI) is both a technological tool and a new approach to the educational process in the training of officers of military command and control bodies (staffs) operating in complex, dynamic, and unpredictable environments. Mastering generative AI remains a challenging task, especially for beginners and specialists from other domains. The primary reason for this difficulty is the high entry threshold, which requires proficiency in mathematics, programming, machine learning principles, deep neural network architectures, as well as an understanding of potential social and security risks.

The purpose of this article is to develop an educational model for the step-by-step mastery of generative artificial intelligence that integrates technical training, specialized knowledge of deep learning, and an understanding of practical applications of AI.

Unlike discriminative models, which address classification or regression tasks, generative models learn the full or joint data distribution. This enables them to produce new objects like those contained in the training dataset. Owing to this capability to generate content–such as text, images, audio signals, or code–generative AI has found wide application in education, creative industries, healthcare, security, and governance.

Within the framework of this study, it is proposed an educational model for the staged mastery of generative artificial intelligence, combining technical, methodological, cognitive, and ethical components. The developed model considers contemporary requirements for the digital transformation of education and facilitates the formation of comprehensive AI-related competencies. The model is oriented toward the development of skills relevant to real-world challenges and is aligned with existing international and national regulatory and legal frameworks, which confirms its relevance and significance.

Keywords: generative artificial intelligence; digital technologies; educational model; deep learning; generative networks; digital transformation; artificial neural networks.

УДК 355.40:528.8:004.9 https://doi.org/10.33099/2304-2745/2025-3-86/87-93

Шуптар-Пориваєва Н. Й., кандидат економічних наук, доцент (0000-0002-3260-2714)
Назарчук Б. В. (0000-0001-5023-2094)
Соловйов О. Ю. (0009-0005-2011-0850)
Шурло О. В. (0009-0009-3498-2878)

Військова академія (м. Одеса)

Використання геоінформаційних систем як інструментів геопросторової розвідки

Резюме: У статті розглянуто роль геопросторової розвідки (GEOINT) у сучасних військових операціях та можливості використання відкритих геоінформаційних систем, зокрема, програмного продукту Google Earth Pro, як доступного інструмента аналізу і візуалізації просторових даних. Підкреслено освітній та практичний потенціал цього програмного продукту для ЗС України.

Ключові слова: геопросторова розвідка; GEOINT; програмний продукт Google Earth Pro; геоінформаційні системи; супутникові знімки.

Постановка проблеми. У сучасних умовах стрімкого розвитку інформаційних технологій та зростання обсягів просторових даних геопросторова розвідка (*Geospatial Intelligence*, GEOINT) набуває особливого значення як ключовий інструмент забезпечення національної безпеки, стратегічного планування, моніторингу конфліктів та прийняття рішень у реальному часі. Її важливість зростає в умовах гібридних загроз, коли класичні методи розвідки потребують інтеграції з цифровими засобами спостереження, аналізу та візуалізації даних.

Геопросторова розвідка забезпечує об'єднання зображень із супутників, аерофотозйомки, даних дистанційного зондування Землі, цифрових карт, даних з безпілотних літальних апаратів та відкритих джерел у єдину аналітичну систему. Її застосування дає змогу отримувати достовірні й оперативні відомості про просторове розташування об'єктів, зміни ландшафту, переміщення техніки та особового складу, що є критично важливим у військовій, гуманітарній, екологічній та інфраструктурній сферах.

У контексті гібридних загроз, зокрема збройної агресії, кіберрозвідки та дезінформації, важливість оперативного аналізу просторових змін, моніторингу активності противника та верифікації даних суттєво зростає. Це актуалізує потребу в детальному дослідженні застосування геоінформаційних систем, зокрема програмного продукту *Google Earth Pro* як інструмента геопросторової розвідки, що забезпечує візуалізацію, аналіз та інтерпретацію геопросторових даних на основі супутникових знімків, аерофотозйомки і тривимірних моделей місцевості, підтримуючи наукові й прикладні дослідження у сфері геоінформатики та суміжних дисциплін.

Аналіз останніх досліджень та публікацій. Геопросторова розвідка є предметом активного вивчення в науковому середовищі, особливо на перетині військових наук, інформаційних технологій, геоінформатики та аналітики даних. У сучасних умовах вона все частіше розглядається не лише як інструмент оборони, а і як технологічна платформа для прийняття рішень у надзвичайних ситуаціях, плануванні інфраструктури, екологічному моніторингу та урбаністиці.

Серед провідних світових центрів, що активно досліджують питання GEOINT, варто зазначити *National Geospatial-Intelligence Agency* (США), *Royal United Services Institute* (Велика Британія), а також аналітичні структури при НАТО, такі як NATO *Communications and Information Agency*.

У праці [1] проаналізовано еволюцію геопросторової розвідки у сучасних військових конфліктах та показано, як GEOINT допомагає у розвідці об'єктів, плануванні місій і підтримці розмінування чи ліквідації наслідків надзвичайних подій. Обговорюються також етичні обмеження технології та перспективи її розвитку з використанням штучного інтелекту (ШІ) та машинного навчання.

Дослідження [2] описує архітектуру мультиінтелектуального аналізу на основі

комбінування супутникових зображень IMINT/GEOINT з відкритою інформацією OSINT. На прикладі війни в Україні автори демонструють, як синергія SAR/оптичних даних та соціальних медіа дає змогу автоматично відстежувати події на фронті, що підкреслює важливість геоінформації для військового планування та реагування.

В Україні геопросторова розвідка залишається відносно новою сферою наукових досліджень і практичних застосувань, що динамічно розвивається, особливо після 2014 року. Практичне впровадження геоінформаційних технологій у діяльність Збройних Сил України отримало суттєвий розвиток завдяки створенню системи ситуаційної обізнаності *Delta*, яка інтегрує дані з відкритих джерел, БПЛА, супутникові знімки та розвідувальну інформацію.

У публікаціях українських дослідників [3–4] розглядаються можливості застосування геоінформаційного підходу під час обробки та аналізу розвідувальної інформації, отриманої з різних джерел, особливості геопросторової системи розвідки та її функцій, підкреслюється роль сучасних вебсервісів у поширенні геопросторових даних.

Водночас аналіз наукових джерел свідчить, що недостатньо дослідженими залишаються питання інтеграції GEOINT із відкритими цивільними геоінформаційними системами, зокрема такими, як *Google Earth Pro*, які можуть забезпечити швидку візуалізацію даних, базову просторову аналітику та підтримку прийняття рішень у військових і кризових сценаріях.

Ці наукові прогалини зумовлюють необхідність подальших досліджень, спрямованих на адаптацію інструментів цивільної геоінформатики до потреб військової розвідки.

Метою статті є дослідження сучасних підходів до розвитку геопросторової розвідки та обґрунтування можливостей застосування відкритих геоінформаційних систем, зокрема *Google Earth Pro* у військовій сфері.

Виклад основного матеріалу. Спеціалісти з безпеки та аналітики виділяють шість основних способів для отримання розвідувальної інформації [5]:

розвідка з відкритих джерел (*Open Source Intelligence,* OSINT) – публічно доступна інформація, яка з'являється в джерелах, що не мають грифів секретності або обмежень доступу;

агентурна розвідка (*Human Intelligence,* HUMINT) – найстаріший спосіб збору інформації від її носіїв – інформація, зібрана з людських джерел;

розвідка зображень (*Image Intelligence,* IMINT) – представлення об'єктів, що відтворюються в електронному або оптичному засобі на плівці, електронних дисплеях або інших носіях;

радіоелектронна розвідка (*Signals Intelligence,* SIGINT) – перехоплення сигналів, чи то між людьми, між машинами або комбінацією обох;

інструментальна розвідка (*Measurement and Signature Intelligence,* MASINT) – розвідка фізичних полів, наукова і технічна розвідувальна інформація, що використовується для визначення, виявлення та опису специфічних ознак конкретних цілей;

геопросторова розвідка (*Geospatial Intelligence,* GEOINT) – зображення та геопросторові дані, створені за допомогою інтеграції зображень та географічної інформації.

У Табл. 1. наведено основні способи отримання інформації та їх порівняння.

Таблиця 1

Порівняльна таблиця основних способів отримання розвідданих

Спосіб отримання розвідданих	Джерело даних	Ключова технологія	Приклад застосування у військовій сфері
OSINT	Відкриті джерела	Аналіз соціальних мереж, відео, API	Ідентифікація ворожої техніки по фото, відео в інтернет-просторі
HUMINT	Люди, агенти	Інтерв'ю, спостереження	Виявлення складів боєприпасів на території противника
IMINT	Зображення	Супутникові знімки, БПЛА	Виявлення колон техніки, наслідків обстрілів
SIGINT	Радіо, телекомунікації	Перехоплення, дешифрування	Аналіз переговорів військових
MASINT	Сигнатури (ІЧ, РЧ)	Спектрометрія, акустика	Виявлення пуску ракет, залишків вибухів
GEOINT	Просторові дані	ГІС, GPS, 3D-моделі	Створення цифрової карти бою

Термін "*геопросторова розвідка*" визначено в Базовій доктрині геопросторової розвідки як використання та аналіз зображень і геопросторової інформації для опису, оцінки та візуального зображення фізичних особливостей і діяльності з географічною прив'язкою. GEOINT складається зі знімків, розвідувальної інформації та геопросторової інформації [6]. *Зображення* означає сукупність отриманих від різних типів датчиків відображень об'єктів, відтворених електронним або оптичним способом на плівці, електронних пристроях відображення або інших носіях. Зображення найчастіше отримують за допомогою супутників, безпілотних літальних апаратів і літаків-розвідників, і вони не включають фотографії, зроблені людськими джерелами (HUMINT). Геопросторова розвідка характеризується ширшим поняттям, що визначає географічне розташування природних або рукотворно створених об'єктів і кордонів на землі, і охоплює статистичні дані та інформацію, отриману за допомогою технологій дистанційного зондування, картографування та зйомки, а також картографування, складання карт, геодезичні дані та відповідні продукти [7].

Для збору, обробки та візуалізації географічних даних GEOINT використовує географічну інформаційну систему (ГІС). Слід підкреслити, що геопросторова інформація – це також геолокація об'єктів або людей. Наприклад, американські спецслужби використовували геолокацію користувачів соціальних мереж для складання карти біженців, які залишають Сирію [8]. Термін "розвідка зображень" (IMINT) використовувався в минулому і досі використовується як взаємозамінний з GEOINT для опису розвідувальних функцій геопросторових джерел. Однак, на думку багатьох експертів, цей термін застарів і не відображає того, чим сьогодні є GEOINT [9]. Наразі IMINT є частиною GEOINT у сфері отримання зображень із використанням візуальної фотографії, радіолокаційних та інфрачервоних датчиків, лазерів та електрооптики [10]. Таким чином, IMINT – це технічна, географічна та розвідувальна інформація, отримана внаслідок інтерпретації або аналізу зображень і додаткових матеріалів. Повна корисність GEOINT досягається взаємодією трьох елементів: зображень, розвідки зображень і геопросторових даних, що дає змогу отримати комплексну перспективу і глибше зрозуміти оперативну обстановку.

Технології та методи геопросторової розвідки постійно розвиваються, відкриваючи нові можливості для отримання більш точної та повної географічної інформації. Цифровізація та автоматизація процесів геопросторової розвідки призводять до підвищення швидкості та точності збору даних, а також спрощують їх обробку та аналіз. Сучасні геоінформаційні системи та програмні рішення дають змогу інтегрувати та візуалізувати великі обсяги географічної інформації, що робить її більш доступною та зрозумілою для користувачів.

У сфері геопросторової розвідки активно застосовують такі засоби та технології, як геоінформаційні системи, супутникові системи спостереження та навігаційні системи, дистанційне зондування Землі, лазерне сканування та інші методи збору географічної інформації, що наведені в Табл. 2.

Як видно з Табл. 2 геопросторова розвідка використовує широкий спектр інструментів, що у військовій сфері забезпечують збір, обробку, аналіз та візуалізацію геопросторових даних, необхідних для планування операцій, моніторингу супротивника та координації дій. Однак, незважаючи на різноманітність та потужність цих інструментів, їх використання часто потребує значних ресурсів, спеціалізованих знань та інфраструктури, що може бути недоступним для деяких військових чи аналітичних груп, особливо в умовах обмеженого бюджету чи термінових завдань.

У цьому контексті Google Earth Pro займає унікальну нішу як доступний, безкоштовний та інтуїтивно зрозумілий інструмент, який, хоч і поступається функціоналу професійних ГІС, проте надає значні можливості для GEOINT. Його глобальне покриття, супутникові знімки високої роздільної здатності, підтримка 3D-візуалізації та простота інтеграції з іншими системами роблять Google Earth Pro особливо актуальним для початкового аналізу місцевості, моніторингу об'єктів та підтримки операцій, що успішно були проведені в ході російсько-української війни. Розглянемо, як Google Earth Pro вписується в екосистему GEOINT і чому він залишається затребуваним у військовій практиці.

Картографічний сервіс Google Earth Pro призначений для візуалізації та аналізу геопросторових даних, що надає доступ до супутникових знімків, аерофотозйомки, топографічних даних та 3D-моделей місцевості [11].

Таблиця 2

Основні інструменти та методи геопросторової розвідки

Категорія інструментів	Призначення / функції	Приклади / платформи
Супутникові системи спостереження	Отримання зображень великих територій у різних діапазонах: видимому, інфрачервоному та радіодіапазоні	Оптичні супутники (Electro-Optical) - WorldView, Pleiades, Радіолокаційні супутники (SAR) - TerraSAR-X, Sentinel-1, ICEYE
БПЛА	Високоточна зйомка у реальному часі (у т.ч. нічна, тепловізійна)	Bayraktar TB2, RQ-11 Raven, DJI Mavic + EO/IR/LiDAR
Літаки-розвідники, дрони	Оперативна розвідка на середні/великі дистанції	U-2, Global Hawk, JSTARS
LiDAR (лазерне сканування)	Побудова 3D-моделей рельєфу, виявлення інженерних споруд	Velodyne LiDAR, Leica ALS, Phoenix LiDAR
Геоінформаційні системи	Програмні рішення для обробки, аналізу та візуалізації просторових даних, створення карт	ArcGIS, QGIS, Google Earth Pro, GRASS GIS
GNSS/GPS-системи	Точне позиціонування та навігація	GPS, Galileo, Beidou
Цифрові карти/DEM (цифрові моделі рельєфу)	Основи для аналізу місцевості, планування маршрутів	SRTM, OpenStreetMap, Google Maps, DTED
Інструменти обробки зображень	Обробка супутникових/аеро знімків, спектральний аналіз, підготовка візуальних матеріалів	ENVI, ERDAS Imagine, PCI Geomatica, Photoshop / GIMP
Інструменти аналітики OSINT	Геоприв'язка зображень з відкритих джерел (відео, фото, соцмережі)	Bellingcat Toolkit, GeoConfirmed, MapHub, Zoom Earth
Хмарні сервіси обробки геоданих	Робота з великими обсягами супутникових знімків і аналітики	Google Earth Engine, AWS Open Data, ArcGIS Online
Мобільні геопросторові додатки	Збір, відображення даних у полі, спільна навігація	ATAK, Locus Map, MapTiler, Mapillary
AI/ML аналітика в GEOINT	Автоматичне виявлення цілей, аналіз змін, класифікація типів об'єктів	YOLO, Detectron2, DeepGlobe, AI4EO

Примітка. Табл. 1,2 розроблені авторами.

Google Earth Pro є настільною версією програми Google Earth, доступною для операційних систем Windows, macOS та Linux. Спочатку ця версія мала платну ліцензію (до 399 дол. США на рік), проте з 2015 року стала безкоштовною для всіх користувачів [12]. Програма пропонує розширений набір функцій у порівнянні з базовою версією Google Earth, доступною через веббраузер або мобільні додатки, включаючи роботу з великими обсягами геопросторових даних, імпорт та експорт геоінформаційних даних, історичні супутникові знімки, аналіз маршрутів і просторове моделювання.

Дані Google Earth Pro зберігаються на хмарних серверах Google, а частина з них кешується на локальному комп'ютері для підвищення швидкодії та забезпечення офлайн-режиму. Це дає змогу користувачам працювати із завантаженими даними навіть за відсутності інтернет-з'єднання, що особливо важливо для польових досліджень або в умовах обмеженого доступу до мережі. Кеш має обмеження за замовчуванням (приблизно 2 ГБ), але може бути змінений користувачем для зберігання більшого обсягу даних.

Дані організовано за принципом шарів, при цьому підложку відключити не можна. Також, в Google Earth Pro проведено чіткий поділ між даними користувача і даними, що надаються Google. Перші організовані до списку Places (Мітки), другі – Layers (Шари) [11].

Дані, які використовуються в системі Google Earth Pro, вже підготовлені до використання, їх не потрібно спеціальним чином обробляти, але й не можна специфічним чином налаштувати, як це можливо у професійних пакетах ГІС, наприклад, змінити систему координат, комбінацію каналів даних дистанційного зондування, покращити географічну прив'язку тощо.

Точні джерела та характеристики зображень у Google Earth Pro публічно не підтверджені, проте відомо, що сервіс використовує дані комерційних і державних супутникових систем, включно з Landsat і комерційними платформами високої роздільної здатності, такими як Digital Globe [13]. Знімки забезпечують можливість детальної візуалізації об'єктів і місцевості на глобальному рівні, хоча рівень деталізації може змінюватися залежно від регіону.

Google Earth Pro надає інструменти для вимірювання відстаней, побудови перспективних рельєфних моделей, нанесення власних географічних об'єктів, накладання растрових зображень та здійснення віртуальних "обльотів" місцевості. Незважаючи на обмежену аналітичну функціональність порівняно з професійними

ГІС, програма є потужним і доступним інструментом для первинного геопросторового аналізу, підготовки картографічних продуктів і візуалізації даних.

Основні можливості Google Earth Pro охоплюють роботу з векторними та растровими даними. Програма підтримує формати ESRI Shapefile (.shp) та GeoTIFF, а також власний формат KML/KMZ, який базується на XML і забезпечує сумісність із професійними ГІС-платформами, такими як ArcGIS та QGIS. KML дає змогу створювати, редагувати та імпортувати географічні об'єкти, включно з точками, лініями та полігонами, а також організовувати їх у шари для більш зручного відображення і аналізу [13].

Серед основних можливостей програмного продукту Google Earth Pro варто відмітити:

перегляд супутникових знімків – зручна навігація, безшовне з'єднання супутникових знімків та моментальне відображення з поступовим промальовуванням деталей;

побудова перспективних (рельєфних) зображень із накладенням супутникових знімків;

нанесення власних точок, ліній та полігонів та їх експорт для обміну з іншими користувачами;

накладення власних зображень (наприклад логотипи, власні карти тощо) та їх приблизне суміщення із земною поверхнею;

вимірювання відстаней;

візуалізація території в режимі обльоту на заданій висоті та швидкості.

На сьогодні сервіс Google Earth Pro не може гідно конкурувати із повноцінними ГІС-платформами, однак, він органічно інтегрується у структуру GEOINT як базовий інструмент для візуалізації, аналізу та представлення просторової інформації. Його можливості відповідають ключовим складовим GEOINT, особливо на рівні тактичної та оперативної ланки. Авторське бачення елементів інтеграції Google Earth Pro в концепцію геопросторової розвідки наведено на рис. 1.

Рис. 1. Інтеграція Google Earth Pro в концепцію геопросторової розвідки

Висновки та перспективи подальших досліджень. У контексті сучасної війни геопросторова розвідка відіграє ключову роль у забезпеченні ситуаційної обізнаності, точного цілевказання та планування операцій. Завдяки інтеграції супутникових знімків, безпілотних систем, цифрових карт і даних з відкритих джерел GEOINT дає змогу оперативно аналізувати зміни на полі бою, виявляти позиції противника та оцінювати рельєф місцевості. У війні нового покоління GEOINT перетворюється з допоміжного інструмента на критично важливий елемент інформаційної переваги.

Потужним та водночас доступним інструментом первинного рівня у геопросторовій розвідці є програмний продукт Google Earth Pro, який дає змогу здійснювати базову візуалізацію, просторовий аналіз та створювати геоаналітичні продукти.

Незважаючи на певні обмеження, такі як нерегулярне оновлення даних та відсутність передових аналітичних функцій, простота, доступність та сумісність цього додатку з іншими системами роблять його цінним ресурсом для Збройних Сил України. У поєднанні із професійними ГІС та ШІ-технологіями Google Earth Pro може значно підвищити ефективність проведення військових операцій у майбутньому.

Варто відмітити, що програмний продукт Google Earth Pro має високу навчальну цінність для підготовки майбутніх офіцерів саме як вступ до методології GEOINT. Вивчення цього інструмента дає змогу:

розвивати навички орієнтування в цифровому просторі;

інтегрувати геопросторову обізнаність у планування тактичних та оперативних дій;

створювати наочні аналітичні та презентаційні матеріали для штабів та командування;

забезпечити початкову підготовку до роботи зі спеціалізованими системами ситуаційної обізнаності та управління.

Використання програмного продукту Google Earth Pro дає змогу закласти фундаментальні знання з GEOINT, забезпечити основу для побудови геопросторового мислення та застосування інформаційних технологій у бойовій обстановці.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Lutema E. K. The Role of Geospatial Intelligence in Modern Military Operations // ESS Open Archive. 25.02.2025. DOI: 10.22541/essoar.174051790.09497647/v1.
2. Kotaridis I., Benekos G. Integrating Earth Observation IMINT with OSINT Data to Create Added-Value Multisource Intelligence Information: A Case Study of the Ukraine-Russia War // Security and Defence Quarterly. 2023. 43 (3). P. 1–21. DOI: https://doi.org/10.35467/sdq/170901.
3. Литвиненко О. І., Литвиненко Н. І. Основні принципи сучасної геопросторової розвідки // Сучасні інформаційні технології у сфері безпеки та оборони. 2016. № 1 (25).
4. Жиров Г. Б., Кольцов Р. Ю., Шмиголь Є. В. Геопросторова розвідка з використанням геоінформаційних та краудсорсингових систем // Збірник наукових праць Військового інституту КНУ імені Т. Шевченка. 2016. № 51.
5. Гвоздь В. І. Історичні, правові і політичні аспекти розвідувальної діяльності держави: монографія. Київ : Борисфен Інтел, 2018.
6. Geospatial Intelligence Doctrine. 2018. URL: https://irp.fas.org/agency/nga/doctrine-2018.pdf (дата звернення: 10.10.2025).
7. United States Code. Title 10, § 467. URL: http://uscode.house.gov (дата звернення: 10.10.2025).
8. Lowenthal M. M. Intelligence: From Secrets to Policy. Intelligence & Security Academy, LLC, 2022. 624 p.
9. Jensen III C. J., McElreath D. H., Graves M. Introduction to Intelligence Studies. Taylor & Francis, 2022. DOI: 10.4324/9781003149569.
10. U.S. National Intelligence: An Overview 2013. Intelligence Community Information Sharing Executive, 2013. 103 p. URL: https://www.govinfo.gov/content/pkg/GOVPUB-PREX28-PURL-gpo126561/pdf/GOVPUB-PREX28-PURL-gpo126561.pdf (дата звернення: 11.10.2025).
11. Britt K., McGee J., Campbell J. An Introduction to Google Earth Pro. VirginiaView, 2020. URL: https://virginiaview.cnre.vt.edu/wp-content/uploads/2020/07/smGoogle-Earth-Pro-Manual.pdf (дата звернення: 11.10.2025).
12. Google. Google Earth Pro is now free. URL: https://maps.googleblog.com/2015/01/google-earth-pro-is-now-free.html (дата звернення: 11.10.2025).
13. Google. Importing Geographic Information Systems (GIS) data in Google Earth Desktop. URL: https://www.google.com/earth/outreach/learn/importing-geographic-information-systems-gis-data-in-google-earth (дата звернення: 12.10.2025).

Стаття надійшла до редакції 19.11.2025

Using geographic information systems as geospatial intelligence tools

Annotation

In the context of the rapid development of information technologies and the growing volume of spatial data, geospatial intelligence (GEOINT) has been gaining a particular importance as a key instrument for ensuring national security, strategic planning, conflict monitoring, and real-time decision-making.

In the context of hybrid threats, including armed aggression, cyber intelligence, and disinformation, the importance of the operational analysis of spatial changes, monitoring adversary activity, and data verification has been increasing significantly. This highlights the need for an in-depth study of the application of geographic information systems, in particular the *Google Earth Pro* software product, as a geospatial intelligence tool that provides visualization, analysis, and interpretation of

geospatial data based on satellite imagery, aerial photography, and three-dimensional terrain models, thereby supporting scientific and applied research in the field of geoinformatics and related disciplines.

Google Earth Pro is an affordable entry-level tool for geospatial intelligence. Despite certain limitations, such as irregular data updates and the lack of advanced analytical functions, the simplicity, accessibility, and interoperability of this application with other systems make it a valuable resource for the Armed Forces of Ukraine. When combined with professional GIS platforms and artificial intelligence technologies, *Google Earth Pro* can significantly enhance the effectiveness of military operations in the future.

It should be noted that *Google Earth Pro* has high educational value for training future officers, particularly as an introduction to the GEOINT methodology. The use of Google Earth Pro enables the development of fundamental GEOINT knowledge, provides a basis for geospatial thinking, and supports the application of information technologies in combat and operational environments.

Keywords: geospatial intelligence; GEOINT; Google Earth Pro software; geographic information systems; satellite imagery.

УДК 355. 02:34:378 https://doi.org/10.33099/2304-2745/2025-3-86/94-99

Камалов Є. В., доктор філософії, доцент (0000-0002-1994-7144)

Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

Недосконалість нормативно-правової бази підготовки громадян України до національного спротиву: аналіз, пропозиції та рекомендації

Резюме. У статті проаналізовано нормативно-правову базу з підготовки громадян України до національного спротиву в системі підготовки воєнних кадрів. Надано пропозиції щодо змін у нормативно-правові акти з урахуванням російсько-української війни та переходу сил безпеки і оборони України до стандартів НАТО.

Ключові слова: національний спротив; підготовка громадян України до національного спротиву; стандарти НАТО; нормативно-правова база; система підготовки воєнних кадрів.

Постановка проблеми. Конституція України є основоположним документом, що визначає правову базу національного спротиву. Стаття 17 Конституції України встановлює, що захист суверенітету і територіальної цілісності України, а також забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави та справою всього Українського народу [1]. Зазначена стаття дає змогу, у разі потреби, залучити все населення України до захисту рідної землі та згуртувати всіх українців навколо важливих і пріоритетних ідей. Збройна агресія російської федерації зумовила введення воєнного стану та створення всеохоплюючої оборони держави [2]. Відповідно, згідно статті 17 Конституції України завдання оборони держави, захист її суверенітету, територіальної цілісності і недоторканності покладаються на Збройні Сили України.

Законом "Про національну безпеку України" у розділі IV передбачено, що сектор безпеки і оборони України складається з чотирьох взаємопов'язаних складових: сил безпеки; сил оборони; оборонно-промислового комплексу; громадян та громадських об'єднань, які добровільно беруть участь у забезпеченні національної безпеки [3]. Складові Сили безпеки і оборони України спроможні виконувати завдання із збереження територіальної цілісності та недоторканості нашої держави, якщо вони укомплектовані досвідченим та підготовленим персоналом (населенням) [4].

Так, підготовлений до виконання завдань із захисту Вітчизни персонал (населення) – це підготовка громадян України до національного спротиву. Пріоритетним завданням національного спротиву [5] є сприяння набуттю громадянами України готовності та здатності виконувати конституційний обов'язок захисту Вітчизни, незалежності та територіальної цілісності України. Одним із потужних інструментів протидії російському агресору під час збройної агресії Російської Федерації (РФ) став концепт національного спротиву – системи, що об'єднує зусилля військових, цивільних органів влади та громадян у боротьбі за незалежність України. Курс України на членство в НАТО та Європейський Союз визначив нові вимоги, зокрема й до системи національного спротиву. З огляду на реалії сьогодення зазначене демонструє актуальність національного спротиву в державі та визначає нові вимоги до підготовки громадян України. Одним із елементів підготовки Збройних Сил до оборони України є підготовка мобілізаційного ресурсу держави в системі національного спротиву.

Законом України "Про основи національного спротиву" [5] визначено правові та організаційні засади національного спротиву, основи його підготовки та ведення, завдання і повноваження сил безпеки, сил оборони та інших визначених цим Законом суб'єктів з питань підготовки і ведення національного спротиву, зокрема Міністерства оборони України, а саме формування у громадян розуміння їхньої ролі у захисті України, навчання їх діям в умовах бойових дій та надзвичайних ситуацій. Особлива увага приділяється військово-патріотичному вихованню, яке формує стійку мотивацію до захисту Вітчизни. Проте проблемним питанням стає виконання пункту закону щодо базової загальновійськової підготовки національного спротиву який стає практично однотипною базовою загальновійськовою підготовкою базової військової служби громадян України.

У Законі України "Про основи національного спротиву" у статті 6 йдеться

про основи підготовки громадян України до національного спротиву, яка складається з загальновійськової підготовки яка, в свою чергу, поділяється на початкову і базову підготовку [5]. Початкова підготовка організується центральним органом виконавчої влади, який забезпечує формування та реалізує державну політику у сфері освіти і науки разом з Міністерством оборони України, та проводиться в закладах загальної середньої освіти. Базова підготовка організовується Міністерством оборони України разом з іншими зацікавленими центральними органами виконавчої влади та проводиться з громадянами України, які досягли 18-річного віку та не проходять військову службу в Збройних Силах України, інших утворених відповідно до законів України військових формуваннях, службу в правоохоронних органах шляхом проведення періодичних навчальних зборів, занять, курсів. Відповідні програми підготовки затверджує Командувач Сил територіальної оборони ЗС України.

Верховна Рада України в другому читанні в Законі № 10449 "Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку" [6] запроваджує базову військову службу для чоловіків віком від 18 до 25 років. Указана підготовка здійснюється в підрозділах ЗС України за програмою підготовки, яку затверджує Головнокомандувач ЗС України. Аналізуючи завдання базової підготовки, які визначені в Законі України "Про основи національного спротиву" із завданнями Закону № 10449 стає зрозумілим, що програма базової підготовки національного спротиву не повною мірою відповідає підготовці на рівні військово-облікової спеціальності (далі – ВОС-100) – "Стрілець". Необхідно звернути увагу, що ВОС є категорією військового обліку, яка визначає військову спеціальність військовослужбовців і військовозобов'язаних та їх належність до виду (роду) військ (сил). ВОС відповідає практичним навичкам і умінням, які отримав громадянин України для виконання конституційного обов'язку щодо захисту Вітчизни, незалежності та територіальної цілісності України. Важливо врахувати, що після призову під час мобілізації всі військовослужбовці, які раніше не проходили військову службу, проходять базову загальновійськову підготовку (далі – БЗВП), за підсумками якої отримують ВОС-100 "Стрілець". Отже, рівень підготовки громадян України за програмою підготовки до національного спротиву має бути на рівні підготовки військовозобов'язаних під час БЗВП. Відповідно, як висновок із зазначеного – система підготовки воєнних кадрів для потреб ЗС України не забезпечує якісної підготовки через початково слабо підготовлене населення (мобілізаційний резерв).

Зважаючи на викладене можна дійти висновку, що питання підготовки громадян України до національного спротиву в умовах повномасштабного вторгнення не повною мірою відповідає сучасним умовам, можливостям та фактичним потребам підготовки воєнних кадрів для ЗС України і потребує відповідного коригування Закону України "Про основи національного спротиву" та розвитку підзаконних нормативно-правових актів міністерств та відомств стосовно удосконалення підготовки громадян України до національного спротиву.

Аналіз останніх досліджень і публікацій. Питанню підзаконних нормативно-правових актів щодо підготовки громадян до національного спротиву в Україні приділяється значна увага, що підтверджується як законодавчою базою, так і науковими дослідженнями.

Так, у науковій праці [7] проаналізовано основні нормативно-правові акти та документи, що визначають і регулюють військову освіту, військову підготовку громадян за програмою підготовки офіцерів запасу. У структурі дослідження підготовки громадян до національного спротиву кафедрою військової підготовки надані рекомендації з професійної підготовки без урахування спеціалізованої освіти.

У дослідженні [8] відпрацьовані теоретичні та методичні засади підготовки майбутніх офіцерів запасу в закладах вищої освіти та врахована нормативно-правова база Закону України "Про освіту" [9], однак недосконало визначена підготовка громадян України у формальній, неформальній та інформальній (самостійній) освіті.

У праці [10] автори розглядають проблемні питання розвитку системи національного спротиву та законодавчу і нормативно-правову базу, спрямовану на розвиток системи національного спротиву. Також у зазначеній роботі визначено складові системи національного спротиву, її багаторівневість, зв'язки із системою стратегічного планування в Міністерстві оборони України, Збройних Силах України та

інших складових Сил безпеки та оборони України; запропоновано інтегровану модель планування заходів національного спротиву; надано пропозиції щодо вдосконалення системи національного спротиву України, а саме введення планування заходів національного спротиву до системи стратегічного планування, порядок розроблення відповідних документів, їх узгодження та реалізації, необхідності вдосконалення каталогу функціональних груп спроможностей у частині визначення спроможностей національного спротиву та їхніх характеристик. Проте автори не приділили значної уваги питанню підготовки громадян України в навчальних центрах підготовки до національного спротиву.

У роботі [11] досліджено феномен національної стійкості та національного спротиву України як основних чинників незламності в умовах російсько-української війни, що триває з 2014 року. Визначено національну стійкість як здатність українського суспільства і державних структур ефективно протистояти агресії, зберігати стабільність у критичних умовах та швидко адаптуватися до викликів війни. Національний спротив розглядається як багаторівневий процес протидії, який включає як військову складову (діяльність Збройних Сил України, територіальної оборони, партизанського руху), так і широкий спектр цивільних ініціатив (волонтерство, інформаційний спротив, культурний опір). Однак автори не досліджували якість підготовки громадян України у формальній та неформальній освіті як основний чинник виконання закону України "Про основи національного спротиву".

Отже, аналіз зазначених наукових робіт демонструє недоліки в підзаконних нормативно-правових актах стосовно підготовки громадян України до національного спротиву, що потребують вивчення, обґрунтування та надання рекомендацій щодо змін у нормативно-правову базу.

Метою статті є проведення системного аналізу нормативно-правової бази підготовки громадян України до національного спротиву, надання пропозицій щодо змін у нормативно-правову базу та обґрунтування рекомендацій з підвищення якості підготовки громадян України до національного спротиву.

Виклад основного матеріалу. Зважаючи на зазначену проблему розглянемо основні нормативно-правові акти, що визначають та регулюють освіту, освітню діяльність, військову освіту, загальновійськову підготовку громадян України до національного спротиву.

Так, стаття 3 Закону України "Про освіту" [9] закріплює право кожного на якісну та доступну освіту. Право на освіту включає право здобувати освіту впродовж усього життя, право на доступність освіти, право на безоплатну освіту у випадках і порядку, визначених Конституцією та законами України.

В Україні існують рівні умови доступу до освіти. Ніхто не може бути обмежений у праві на здобуття освіти. Право на освіту гарантується незалежно від віку, статі, раси, стану здоров'я, інвалідності, громадянства, національності, політичних, релігійних чи інших переконань, кольору шкіри, місця проживання, мови спілкування, походження, соціального і майнового стану, наявності судимості, а також інших обставин та ознак.

У статті 1 Закону України "Про повну загальну середню освіту" [12] визначено, що *учні* – це особи, зараховані до закладу загальної середньої, професійної, фахової передвищої чи вищої освіти, які здобувають у будь-якій формі початкову, базову середню чи профільну середню освіту. Законами України [9, 12] визначено завдання щодо 100% залучення громадян України до здобуття освіти. Аналіз наслідків повномасштабного вторгнення РФ на територію України та тимчасове захоплення територій нашої держави засвідчує, що тимчасово переселені особи, а також громадяни України, які перебувають на/або біля територій, де ведуться бойові дії, не отримують належної освіти та не мають можливості виконувати умови закону [5, 13], відповідно не отримують якісної підготовки в системі національного спротиву.

Відповідно до закону [5] громадяни України здійснюють підготовку до національного спротиву з метою готовності та здатності до захисту Вітчизни та перебуванню в мобілізаційному ресурсі для комплектування ЗС України та інших військових формувань. Цей ресурс включає військовозобов'язаних чоловіків від 18 до 60 років, які придатні за станом здоров'я, не мають права на відстрочку чи бронювання. Підготовка цього ресурсу здійснюється поетапно через загальновійськову підготовку національного спротиву та планової підготовки резервістів. Але необхідно звернути увагу, що навчальні центри сил Територіальної оборони

ЗС України не спроможні в повному обсязі здійснити якісну підготовку визначеної категорії.

Для вирішення цієї проблеми та з метою забезпечення якісної підготовки мобілізаційного ресурсу для потреб ЗС України та інших складових сил оборони, підготовки громадян України до національного спротиву була прийнята Постанова Кабінету Міністрів України від 18 квітня 2025 року № 478 "Про функціонування центрів підготовки громадян до національного спротиву" [14]. Ця постанова визначає процедуру створення та функціонування центрів підготовки громадян до національного спротиву, встановлює загальні засади їх діяльності, порядок фінансування, вимоги до матеріально-технічного та навчально-методичного забезпечення та регламентує питання взаємодії між цими центрами та органами державної влади, органами місцевого самоврядування, Силами територіальної оборони Збройних Сил, Силами спеціальних операцій Збройних Сил, громадськими об'єднаннями, інститутами громадянського суспільства та іншими суб'єктами національного спротиву. Аналізуючи функціонування центрів підготовки громадян до національного спротиву проявляються системні проблеми підготовки, а саме: неможливість використання майна державних і місцевих органів влади, військових частин, громадських організацій, створення стрільбищ; використання вогнепальної зброї для навчальних цілей. Це все призводить до неякісної підготовки громадян України до національного спротиву, а саме не набуттю комплексу нових освітніх і професійних компетентностей. Отже нормативна-правова база забезпечення функціонування центрів підготовки громадян до національного спротиву потребує удосконалення та реагування на вимоги сучасності в масштабі держави.

Спільна директива стратегічних командувань НАТО Bi-SCD 075-007 "Освіта та індивідуальна підготовка" від 24 березня 2025 року [15] застосовується як до стратегічних командувань, так і до всіх закладів освіти та підготовки, які реалізовують заходи освіти та індивідуальної підготовки на підтримку підготовки структури органів військового управління НАТО, структури сил НАТО та окремих осіб, призначених для участі в поточних і майбутніх операціях під егідою НАТО. Діяльність НАТО стосовно освіти та підготовки є основною функцією підготовки органів військового управління НАТО та структури сил НАТО на виконання трьох основних завдань Альянсу, а саме: стримування і оборони, запобігання кризам і їх урегулювання; забезпечення безпеки на основі співробітництва відповідно до рівня прагнень Альянсу. Ця директива визначає єдині підходи до організації, управління, оцінювання та підготовки кожної окремої особи, що безпосередньо сприяє колективній ефективності. У Концепції НАТО з ведення бойових дій визначено, що "правильні люди [з правильними навичками]" є ключовим елементом зусиль НАТО щодо освіти та індивідуальної підготовки. Індивідуальна підготовка спрямована на те, щоб мати відповідних людей з відповідними знаннями, навичками та ставленнями, здатних впоратися зі швидкістю, складністю та технологіями, орієнтованими на збір даних майбутнього середовища, а також ефективно мислити та працювати в багатопрофільному контексті відповідно до чинних концепцій. Крім того, директива впроваджує підхід "найкращих практик" для задоволення потреб з виконання основних завдань Альянсу.

Відповідно до директиви НАТО з індивідуальної підготовки персоналу: під час створення навчальних програм загальновійськової підготовки національного спротиву використовується принцип "від простого до складного" з підготовки того, що необхідно на війні; застосування під час підготовки наративів, які спрямовані на підвищення мотивації мобілізаційного ресурсу як під час навчання, так і в подальшому під час виконання бойових завдань; нарощення змісту предметів навчання практичною складовою з урахуванням бойового досвіду; розширення тематики вогневої підготовки щодо антидронової боротьби; включення до змісту предмета виживання теми "окопний побут"; впровадження новітніх технологій для укріплення морально-психологічного стану тих, хто навчається та їх морального загартовування, методом ілюстрації першого бою за допомогою VR-окулярів; поглиблення у віртуальну реальність (Virtual Reality); технологій доповненої реальності (Augmented Reality) або технологій змішаної реальності (Mixed Reality). Принцип статті 17 Конституції України захист суверенітету і територіальної цілісності України є справою всього українського народу, що робить систему національного спротиву не тільки

ініціативою для певних верств населення, таких як студенти, а загальнонаціональним обов'язком. Водночас стаття 65 Конституції України закріплює захист Вітчизни, її незалежності та територіальної цілісності України як обов'язок кожного громадянина, незалежно від віку, професії чи статусу.

На підставі викладеного можна зазначити, що забезпечення належного рівня підготовки громадян України є критично важливим чинником підтримання боєздатності, ефективності підрозділів ЗС України й інших складових сил оборони та взаємосумісності із силами Альянсу.

Отже, зважаючи на деякі невідповідності нормативно-правової бази з підготовки громадян України до національного спротиву можливо надати рекомендації щодо напрямів внесення змін у нормативно-правові акти, а саме:

розроблення та ухвалення порядку функціонування центрів підготовки громадян до національного спротиву в напрямі забезпечення озброєнням та військовою технікою, використанням полігонів та земельних ділянок;

розроблення та затвердження програми загальновійськової підготовки (для мобілізаційних ресурсів), як основної програми підготовки для всіх категорій мобілізаційного ресурсу;

удосконалення класифікації ВОС "Стрілець" (у зв'язку з підвищенням функціональних обов'язків з урахуванням досвіду збройної агресії РФ);

розроблення нових навчальних програм підготовки громадян України до національного спротиву спрямованих на набуття нових професійних компетентностей з урахуванням стандартів НАТО;

розроблення та ухвалення стандартних операційних процедур для планування та формування кваліфікаційних вимог, професійних стандартів і компетентності громадянина України до національного спротиву;

створення структурних підрозділів контролю якості освіти в ланках освіти та установах, які відповідають за організацію та проведення підготовки громадян України до національного спротиву;

створення системи підготовки громадян України до національного спротиву на національних засадах якості та спеціалізованої освіти за вимогами стандарту НАТО Bi-SCD 075-007 "Освіта та індивідуальна підготовка".

Висновки. Таким чином, аналіз існуючих нормативно-правових актів з організації та проведення підготовки громадян України до національного спротиву показав, що закони України та підзаконні акти не повною мірою відповідають сучасним вимогам та фактичним потребам всеохоплюючої оборони держави. Створені навчальні центри підготовки громадян до національного спротиву не повною мірою використовують законні підстави для підготовки мобілізаційних ресурсів. Базова загальновійськова підготовка громадян України суперечить завданням базової підготовки громадян України до національного спротиву. Отже, нормативно-правова база з національного спротиву потребує відповідного коригування на державному рівні.

Аналіз нормативно-правової бази, пропозиції та надані рекомендації дають **перспективу подальших наукових досліджень** у напрямі удосконалення загальновійськової підготовки громадян України до національного спротиву.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конституція України // Верховна Рада України : сайт. Дата ухвалення 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 23.09.2025).
2. Про введення воєнного стану в Україні : Указ Президента України від 24.02.2022 № 64/2022. URL: https://zakon.rada.gov.ua/laws/show/64/2022#Text (дата звернення: 23.09.2025).
3. Про національну безпеку : Закон України від 21.06.2018 № 2469–VIII : станом на 21.08.2025. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 25.09.2025).
4. Головне управління доктрин та підготовки Генерального штабу спільно з зацікавленими структурними підрозділами науково-дослідних установ Збройних Сил України. Матеріали вивчення бойовго досвіду російсько-української війни 2022 року // Збірник матеріалів. № 3 (1). С. 5–33.
5. Про основи національного спротиву : Закон України від 16.07.2021 № 1702–IX : станом на 16.05.2025. URL: https://zakon.rada.gov.ua/laws/show/1702-20#Text (дата звернення: 25.09.2025).
6. Верховна Рада України прийняла у другому читанні і в цілому Закон № 10449 "Про внесення змін до деяких законодавчих актів України щодо окремих питань проходження військової служби, мобілізації та військового обліку" // Верховна Рада України : сайт. URL: https://www.rada.gov.ua/news/razom/248328.html (дата звернення: 30.09.2025).

7. Шемчук В. А. Нормативно-правова база з підготовки офіцерів запасу: концептуальна, організаційна, змістова та науково-методична основа формування людських мобілізаційних ресурсів // Наукові інновації та передові технології. 2025. № 1 (41). С. 1093–1108.
8. Зорій Я.Б. Теоретичні і методичні засади підготовки майбутніх офіцерів запасу в закладах вищої освіти : дис. д-ра пед. наук : 13.00.04 / Хмельницька гуманітарно-педагогічна академія. Хмельницький, 2019. 644 с.
9. Про освіту : Закон України від 05.09.2017 № 2145–VIII : станом на 21.08.2025. URL: https://zakon.rada.gov.ua/laws/show/2145-19#top (дата звернення: 30.09.2025).
10. Химченко О. С., Воровичч Б. О., Кутовий О. П. Система національного спротиву України: складові, керівництво та планування заходів // Наука і оборона. 2024. № 2. С. 102–115.
11. Гаврилюк І., Дідіченко В., Череп В., Кін О. Національна стійкість та національний спротив – наріжні камені незламності України: за досвідом російсько-української війни // Military Science. 2025. № 3 (1). С. 73–99.
12. Про повну загальну середню освіту : Закон України від 12.09.2025 № 463-IX : станом на 21.08.2025. URL: https://zakon.rada.gov.ua/laws/show/463-20#Text (дата звернення: 30.09.2025).
13. В Україні за період 2022 – 2024 зменшилася кількість шкіл // Район. Освіта. URL: https://osvita.rayon.in.ua/news/752263-v-ukraini-za-period-2022-2024-zmenshilasya-kilkist-shkil#:~:text (дата звернення: 30.09.2025).
14. Про функціонування центрів підготовки громадян до національного спротиву : Постанова Кабінету Міністрів України від 18.04.2025 № 478. URL: https://zakon.rada.gov.ua/laws/show/478-2025-%D0%BF#Text (дата звернення: 30.09.2025).
15. Освіта та індивідуальна підготовка : спільна директива стратегічних командувань НАТО 075-007 від 24.03.2025. A. MC 0458/4 (Final), NATO Education, Training, Exercise and Evaluation (ETEE) Policy, dated 03 January 2023.

Стаття надійшла до редакції 06.102025

Imperfection of the regulatory and legal framework for preparing Ukrainian citizens for national resistance: analysis, proposals and recommendations

Annotation

The Law of Ukraine *"On the Fundamentals of National Resistance"* defines the legal and organizational foundations of national resistance, the principles of its preparation and conduct, as well as the tasks and authority of the security forces, defense forces, and other entities specified by the Law with regard to the preparation and conduct of national resistance, including the Ministry of Defense of Ukraine. In particular, it emphasizes the formation of citizens' understanding of their role in the defense of Ukraine and their training for actions in combat conditions and emergency situations. Special attention is paid to military-patriotic education, which fosters sustainable motivation to defend the homeland. However, a problematic issue arises in the implementation of the legal provision concerning basic military training for national resistance, as this training in practice becomes largely identical to the basic military training provided within the framework of basic military service for citizens of Ukraine.

The purpose of the article is to conduct a systematic analysis of the regulatory and legal framework for preparing Ukrainian citizens for national resistance, provide proposals for changes to the regulatory and legal framework, and substantiate recommendations for improving the quality of preparing Ukrainian citizens for national resistance.

The article substantiates recommendations regarding priority directions for introducing changes to regulatory and legal acts related to the preparation of citizens of Ukraine for national resistance, including:

the development and adoption of a procedure for the functioning of national resistance training centers;

the development and approval of a basic military training program for all categories of the mobilization resource, taking into account NATO standards;

the establishment of a system for preparing citizens of Ukraine for national resistance based on national quality principles and specialized education in accordance with the requirements of NATO standard Bi-SCD 075-007 *"Education and Individual Training"*.

Keywords: national resistance; preparation of Ukrainian citizens for national resistance; NATO standards; regulatory framework; system of training military personnel.

УДК 351.91 https://doi.org/10.33099/2304-2745/2025-3-86/100-105

Крюков М. І. (0000-0002-6778-2057)

Департамент інформаційно-організаційної роботи та контролю Міністерства оборони України, Київ

Питання встановлення контрольних строків виконання документів управлінської діяльності

Резюме. Проведено аналіз чинної нормативно-правової бази щодо контрольних строків виконання завдань та наведено розширений перелік типових строків виконання контрольних документів. Розглянуто функціональний зв'язок між суб'єктом і об'єктом контролю через здійснення моніторингу контрольних індикаторів. Показані основні вихідні дані для обґрунтування часових показників індикатора. Наведено визначення превентивного індикатора стану виконання управлінських рішень та порядок його встановлення.

Ключові слова: контроль; моніторинг виконання управлінських рішень; індикатор стану виконання управлінських рішень; часовий показник контрольного індикатора.

Постановка проблеми. В умовах повномасштабної війни на території України з метою організації та забезпечення захисту держави нагальним постає питання чіткого виконання державними органами завдань, визначених законами України, рішеннями Ради національної безпеки і оборони (РНБО) України, наказами Верховного Головнокомандувача Збройних Сил (ЗС) України, нормативно-правовими актами Кабінету Міністрів (КМ) України. Злагоджена робота державних органів щодо виконання зазначених завдань, прийняття для їх організації (забезпечення) виважених і обґрунтованих управлінських рішень є запорукою в досягненні своєчасних та якісних результатів.

Своєчасний контроль за виконанням завдань (рішень) є важливим функціональним елементом для забезпечення успішної діяльності державного органу та являє собою зворотній зв'язок на завершальній стадії реалізації управлінських рішень [1].

При цьому, моніторинг виконання управлінських рішень [2] є складовою системи контролю та проводиться з метою нагляду за виконавською дисципліною та забезпечення своєчасного та належного виконання документів.

Однією зі складових контрольної діяльності за виконанням документів в державних органах є визначення індикаторів стану виконання управлінських рішень, які в подальшому аналізуються на предмет відхилення встановленого строку у виконанні етапу завдання, від реального терміну опрацювання відповідного етапу. Тобто одним з основних показників оцінювання стану виконання управлінських рішень є часовий показник, від точності встановлення якого під час визначення індикаторів залежить успішність в досягненні результатів.

Недостатнє розроблення теоретичних положень щодо обґрунтованості часового показника контрольного індикатора підкреслює актуальність аналізу різних аспектів проблем документального контролю та важливість всебічного наукового дослідження питань, пов'язаних із вибором шляхів удосконалення механізму проведення моніторингу стану опрацювання контрольних документів. Розв'язання окресленої проблеми не лише полегшить процес здійснення контролю за виконання документів управлінської діяльності, а й значно підвищить його результативність.

Аналіз досліджень і публікацій. Певні погляди на організацію нагляду за виконавською дисципліною у державних органах вже висвітлено у значній кількості наукових праць та публікацій [1, 3–7], й знайшло відображення у відповідних нормативно-правових актах. Огляд наведених джерел свідчить, що наразі питання визначення часових показників контрольних індикаторів потребують подальшого дослідження і коригування та уточнення. Отже, незважаючи на значну кількість сучасної друкованої літератури та інтернет-видань, які присвячені проблематиці контролю виконання управлінських рішень, дослідження за тематикою моніторингу стану виконання управлінських рішень за контрольними індикаторами залишаються фрагментарними й не розглядалися комплексно.

Мета статті полягає у висвітленні питань з визначення основних вихідних даних

для встановлення часового показника індикатора контрольного документа під час моніторингу повного завершення виконання управлінського рішення.

Методи дослідження: системний аналіз, порівняння, класифікація, узагальнення та систематизація.

Виклад основного матеріалу. Запорукою ефективної роботи державного органу є чітка організація управлінської діяльності та її документаційне забезпечення. Документування управлінської інформації – узагальнене системне явище, вияв вищої потреби об'єкта управління та необхідний елемент управлінського процесу [7]. При цьому, впровадження своєчасного контролю за проходженням та виконанням документів підвищує результативність управлінських рішень.

У контексті контролю за документами, *управлінське рішення* являє собою оформлений правовий акт (нормативний чи індивідуальний) директивного значення, який організовує практичну діяльність суб'єктів і об'єктів управління, спрямовану на досягнення цілей. Своєчасність реалізації управлінського рішення визначається неухильним дотриманням контрольних строків його виконання.

У свою чергу, недотримання встановлених нормативно-правовими актами строків виконання документів спричиняє дисциплінарну відповідальність, а в деяких випадках тягне за собою матеріальну відповідальність та притягнення до адміністративної відповідальності [8].

Тому моніторинг дотримання строків контрольних документів є необхідним для оперативного втручання в ситуацію щодо ходу виконання завдань і попередження негативних наслідків.

Строк виконання документа може встановлюватися у нормативно-правовому акті, розпорядчому документі або резолюції керівництва державного органу. Строки можуть бути типовими або індивідуальними. Типові строки виконання документів установлюються законодавством, основні з яких наведені у Табл. 1.

Індивідуальні строки встановлюються керівництвом державного органу. Документи, в яких строк виконання не зазначено, які не є документами інформаційного характеру або не містять контрольних завдань, мають бути виконані не пізніше ніж за 30 днів з моменту реєстрації документа в установі, до якої надійшов документ [2].

Якщо в документі містяться вимоги щодо прискорення його виконання, у відомчих нормативних актах визначаються відповідні (формалізовані) строки виконання таких документів. Так, стосовно документів з позначкою "для термінового опрацювання" ("терміново" "надтерміново", "оперативно", "невідкладно", "у найкоротший термін", "у стислі строки", "негайно" та інші), для них встановлюється, як правило, найкоротший реальний строк виконання та може коливатися у діапазоні від одного до десяти календарних днів з дати реєстрації документа. Слід зазначити, що таке оформлення контрольного документа визначає більше як ознаки терміновості, ніж конкретизацію строків виконання.

Якщо у тексті завдання зазначається конкретний кінцевий строк виконання, то строки виконання внутрішніх документів обчислюються в календарних днях починаючи з дати реєстрації, а вхідних – з дати надходження (доставки через систему взаємодії) або з дати наступного робочого дня у разі надходження (доставки) документа після закінчення робочого дня, у вихідні, святкові та неробочі дні [22]. Питання щодо визначення контрольних строків виконання деяких документів найбільш детально розкрито в [23].

Зазначається, що строк визначається роками, місяцями, тижнями, днями або годинами. Кінцевим строком виконання документа є останній день зазначеного в тексті документа або резолюції строку. Якщо на виконання надійшов документ, строк виконання якого закінчився, керівництвом визначається новий строк, який має враховувати обсяг та складність документа й бути достатнім для його всебічного аналізу та опрацювання.

У випадках встановлення контрольним документом періодичного строку виконання, якщо не зазначено інше, слід керуватися таким:

при щомісячному контролі строком виконання встановлюється 10 число місяця, наступного за звітним;

при щоквартальному, щопівріччому або щорічному контролі строком виконання встановлюється 15 число місяця, наступного за звітним;

при визначенні строку виконання "січень-грудень", "вересень-серпень" або "протягом року" строк виконання визначається як останній день останнього місяця визначеного строку. Допускається

встановлення проміжних контрольних строків з боку відповідального за організацію та здійснення контролю за виконанням документів для забезпечення випередженого контролю або для підготовки інформації про хід виконання відповідного завдання, але не частіше ніж раз на квартал;

при щосеместровому контролі строком виконання встановлюється 10 число місяця, наступного за звітним.

При постійному контролі строк визначається начальником відповідного підрозділу (щодня, щотижня, щодекади).

Таблиця 1

Типові строки виконання документів

Найменування службового документу	Строки виконання (якщо не встановлені в документі)	Правові підстави
Акти, доручення Президента України	30 днів	п. 7 [9]
Запит народного депутата України	15 днів / з відтермінуванням – 1 місяць	стаття 15 [10]
Звернення народного депутата України	10 днів / з відтермінуванням – 30 днів	стаття 16 [10]
Рішення Кабінету Міністрів України щодо доопрацювання проєктів нормативно-правових актів	10 днів	п. 3 § 55, п. 3 § 55-1 [11]
Відповідь на запит членів Рахункової палати	14 днів	п.п. 4 п. 2 статті 33 [12]
Письмові зауваження щодо змісту проєкту звіту Рахункової палати	5 днів	п.1 статті 35 [12]
Результати розгляду рішення Рахункової палати	1 місяць	п.1, 2 статті 36 [12]
Запит на публічну інформацію та надання відповіді на запит на інформацію	5 робочих днів / стосовно безпеки – 48 годин / з відтермінуванням – 30 днів	п. 1, 2, 3 статті 20 [13]
Звернення громадян	Невідкладно, але не пізніше п'ятнадцяти днів / 1 місяць / з відтермінуванням – 45 днів	стаття 20 [14]
Адвокатський запит	5 робочих днів/ з відтермінуванням – 20 днів	п. 2 статті 24 [15]
Запит Національного антикорупційного бюро	3 робочі дні/ за рішенням НАБУ – додатково 2 дні/ пропозиції НАБУ – 30 робочих днів	п.п. 3, п.п. 11 статті 17 [16]
Запит Національного агентства з питань запобігання корупції	10 робочих днів	п. 8 статті 12 [17]
Запит Державного бюро розслідування	3 дні / з відтермінуванням – 10 днів	п.п. 2 п. 1 статті 7 [18]
Запит Бюро економічної безпеки України	10 робочих днів / з відтермінуванням – 30 днів	п. 9 статті 7 [19]
Погодження проєктів актів законодавства заінтересованими органами	У строк, установлений розробником проєкту акта	§ 38 [11]
Підготовка (як заінтересований центральний орган виконавчої влади) пропозиції щодо доцільності підписання Президентом України Закону України або застосування Президентом України права вето щодо такого закону	48 годин	п. 3 § [11]
Підготовка (як відповідальний центральний орган виконавчої влади) узагальнених зауважень і пропозицій щодо доцільності підписання Президентом України Закону України або застосування Президентом України права вето щодо такого закону	За 48 годин до закінчення семиденного строку	п. 1 § 103 [11]
Підготовка експертного висновку до законопроєкту відповідно до статті 27 Бюджетного кодексу України	Інформування Мінфін не пізніше ніж протягом 7 днів з дня розміщення на офіційному вебсайті ВРУ	п. 4. § 117 [11]
Підготовка (як відповідальний центральний орган виконавчої влади) проєкту експертного висновку по суті законопроєкту	У 8-денний строк з дня надходження законопроєкту подає проєкт експертного висновку Кабінетові Міністрів.	п. 3 § 118 [11]
Надання (як заінтересований центральний орган виконавчої влади) позиції для підготовки проєкту експертного висновку по суті законопроєкту	Надання відповідальному центральному органу виконавчої влади не пізніше ніж протягом 4 днів з дня надходження законопроєкту	п.. 4 § 118. [11]
Підготовка пропозицій щодо визначення позиції Кабінету Міністрів до законопроєктів, ініційованих народними депутатами України	Внесення пропозицій до модуля взаємодії не пізніше ніж протягом 10 днів з дня розміщення законопроєктів на вебсайті ВРУ	п.п. 3 п. 1 § 113. [11]
Звернення тимчасові слідчі комісії і тимчасові спеціальні комісії Верховної Ради України	Державні органи, зобов'язані у визначений законом термін надавати документи та інформацію	стаття 16 [10], стаття 18, 24 [20], стаття 17 [21]

Також визначаються строки погодження проєктів документів:

внутрішнє погодження проводиться не пізніше ніж у дводенний строк після закінчення їх розроблення безпосереднім виконавцем, якщо інше не визначено;

зовнішнє погодження проєктів документів, що надійшли, здійснюється у строк, визначений розробником проєкту документа. Якщо строк погодження не визначено, його погодження проводиться протягом десяти робочих днів.

Строк підготовки проєктів документів визначається з урахуванням того, що днем виконання завдань, вважається день реєстрації вихідних документів, що містять інформацію про виконання відповідних завдань.

Також, строк виконання документа обраховується з дотриманням правил, визначених статтями 251–255 Цивільного кодексу [24].

Так, *строк* – це певний період у часі, зі спливом якого пов'язана дія. Строк визначається роками, місяцями, тижнями, днями або годинами. Перебіг строку починається з наступного дня після відповідної календарної дати або настання події, з якою пов'язано його початок.

На відміну від строку, *термін* – це певний момент у часі, з настанням якого пов'язана дія. Термін визначається календарною датою або вказівкою на подію, яка має неминуче настати.

Закінчення контрольного строку виконання документа визначається:

строк, що визначений роками, спливає у відповідні місяць та число останнього року строку;

до строку, що визначений півроком або кварталом року, застосовуються правила про строки, які визначені місяцями (при цьому відлік кварталів ведеться з початку року);

строк, що визначений місяцями, спливає у відповідне число останнього місяця строку;

строк, що визначений у півмісяця, дорівнює п'ятнадцяти дням;

якщо закінчення строку, визначеного місяцем, припадає на такий місяць, у якому немає відповідного числа, строк спливає в останній день цього місяця;

строк, що визначений тижнями, спливає у відповідний день останнього тижня строку;

якщо останній день строку припадає на вихідний, святковий або інший неробочий день, що визначений відповідно до закону у місці вчинення певної дії, днем закінчення строку є перший за ним робочий день.

Порядок вчинення дій в останній день строку розглядається таким чином: якщо строк встановлено для вчинення дії, вона може бути вчинена до закінчення останнього дня строку. Письмові заяви та повідомлення, здані до установи поштового зв'язку до закінчення останнього дня строку, вважаються такими, що здані своєчасно.

Співвиконавці відповідають за якісну підготовку пропозицій та своєчасне (протягом першої половини строку, відведеного для виконання доручення) подання їх головному виконавцю. У разі несвоєчасного подання пропозицій співвиконавцями головний виконавець інформує про це керівника, який надав доручення [22]. При цьому, подання виконаних документів головним виконавцем на підпис керівництва здійснюється не менш як ніж за один день до закінчення строку їх виконання з урахуванням часу, необхідного для їх доопрацювання за рішенням керівництва [25].

Слід звернути увагу на питання опрацювання листів щодо нагадування про невиконання у встановлені строки документів. Стосовно зазначених листів нормативно встановленого строку їх виконання немає, й вони, як правило, спрямовані на підсилення уваги виконавця на факт порушення строку виконання контрольного документа та носять рекомендаційний характер щодо вживання заходів для усунення відповідних недоліків.

Питання щодо строків виконання завдань, визначених актами Верховного Головнокомандувача ЗС України, як показує практичний досвід, потрібно розглядати в площині взаємодії державного органу з Апаратом РНБО України, як координатора Ставки Верховного Головнокомандувача [26].

Важливою особливістю вважається ситуація, коли з об'єктивних причин можливе невиконання завдання у встановлені контрольним документом строки. Тому, з огляду основних вимог нормативних документів, висвітимо процедуру відтермінування виконання завдання як частковий випадок загального процесу управлінської діяльності.

За потреби індивідуальний строк виконання внутрішнього документа може бути продовжено за обґрунтованим клопотанням виконавця, яке подається завчасно, без погодження з іншими структурними підрозділами безпосередньо посадовій особі, яка встановила строк. Зазначена пропозиція подається не пізніше ніж за три робочих дні до закінчення

встановленого строку [22]. Якщо за результатами аналізу поданої інформації перенесення строку не матиме негативних наслідків, контроль за виконанням завдання здійснюється з урахуванням нового строку [2].

Пропозиції щодо продовження строку виконання завдань, визначених КМ України готуються відповідно до Регламенту [11]. Питання щодо перенесення строків виконання завдань, визначених актами Президента України, вирішується відповідно до Положення про контроль [9]. Пропозиція щодо продовження строку виконання завдань, визначених Верховною Радою України або Президентом України, що надіслані КМ України, подається відповідно до постанови [22].

У контексті перенесення строків виконання контрольних документів пропонується, як варіант, внесення у процес моніторингу елемент застосування такого спеціального індикатора, як "превентивний індикатор". Допускається, що зазначений індикатор визначатиметеся за критерієм такого стану виконання управлінського рішення, коли за оцінюванням результатів його опрацювання ухвалюється рішення щодо відтермінування строків виконання документу. При цьому, часовим показником встановлення превентивного індикатора визначатиметеся термін (час сигналу) у процесі опрацювання (підготовки) контрольного документа, й який враховуватиме часовий період на складання і проходження оформленої у встановленому порядку пропозиції щодо перенесення строку виконання завдання та часовий період на прийняття відповідного рішення органом управління, який встановив строк, і доведення такого рішення до виконавця.

Висновок. Зведені відомості про типові строки виконання, які встановлені приписами і правовими нормами актів законодавства, становлять рамкові вихідні дані для визначення часових показників контрольних індикаторів.

Часовими показниками індикаторів типових контрольних документів є строки виконання, визначені законодавством.

Застосування превентивного індикатора під час здійснення випереджувального моніторингу стану виконання завдань надає можливість своєчасного проведення заходів реагування у разі неможливості опрацювання (підготовки) контрольного документа у визначені строки.

Подальші дослідження. Викладений в статті аналітичний матеріал доцільно рекомендувати для використання посадовим особам апарату керівництва державного органу та фахівцям служб моніторингу під час підготовки проєктів управлінських рішень і визначення індикаторів стану їх виконання.

Подальші дослідження доцільно спрямувати на визначення порядку встановлення часових показників для усіх контрольних індикаторів та управління ними у циклічному процесі періодичного звітування під час опрацювання довготривалих завдань.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кохан С. Концепція контролю у державному управлінні // Університетські наукові записки. 2008. № 2. С. 261–267. URL: http://nbuv.gov.ua/UJRN/Unzap_2008_2_48 (дата звернення: 22.05.2025).

2. Про затвердження Інструкції з діловодства та документування управлінської інформації в Міністерстві оборони України : наказ Міністерства оборони України від 27.10.2024 № 638/нм.

3. Ілюк Л. Організація контролю за виконанням документів в місцевих державних адміністраціях // Буковинський вісник державної служби та місцевого самоврядування. URL: http://buk-visnyk.cv.ua/30-0/427/ (дата звернення: 22.05.2025).

4. Полінець О. Контроль у державному управлінні: сутність, форми та види його здійснення // Вісник УАДУ. 2000. № 2. С. 71–76.

5. Кохан С. Квінтесенція контролю в науковій думці // Наукові записки Інституту законодавства Верховної Ради України. 2013. № 1. С. 144–149.

6. Когутич Є. Співвідношення категорії "форми" та "методи" державного контролю за діяльністю приватних виконавців // Прикарпатський юридичний вісник. 2018. Вип. 4 (25). Том 3. С. 33–38.

7. Прокопець Л. Діловодство як складова управлінської діяльності // Економіка та держава. 2017. № 4. С. 61–63.

8. Кодекс України про адміністративні правопорушення (із змінами) від 07.12.1984 № 8073-X. Стаття 188-19. URL: https://zakon.rada.gov.ua/go/80731-10 (дата звернення: 22.05.2025).

9. Положення про контроль за виконанням указів, розпоряджень і доручень Президента України : затв. Указом Президента України від 19.02.2002 № 155. URL: https://zakon.rada.gov.ua/go/155/2002/ (дата звернення: 22.05.2025).

10. Про статус народного депутата України : Закон України від 17.11.1992 № 2790-XII (із змінами). URL: https://zakon.rada.gov.ua/laws/show/2790-12 (дата звернення: 22.05.2025)

11. Регламент Кабінету Міністрів України : затв. Постановою Кабінету Міністрів України від 18.07.2007 № 950 (із змінами). URL: https://www.kmu.gov.ua/npas/86472596 (дата звернення: 22.05.2025).

12. Про Рахункову палату : Закон України від 02.07.2015 № 576-VIII (із змінами). URL:

https://zakon.rada.gov.ua/go/576-19 (дата звернення: 22.05.2025)

13. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI (із змінами). URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text (дата звернення: 22.05.2025).

14. Про звернення громадян : Закон України від 02.10.1996 № 393/96-ВР (із змінами). URL: https://zakon.rada.gov.ua/go/2939-17 (дата звернення: 22.05.2025).

15. Про адвокатуру та адвокатську діяльність : Закон України від 05.07.2012 № 5076-VI (із змінами) URL: https://zakon.rada.gov.ua/go/5076-17 (дата звернення: 22.05.2025).

16. Про Національне антикорупційне бюро України : Закон України від 14.10.2014 № 1698-VII (із змінами). URL: https://zakon.rada.gov.ua/laws/show/1698-18 (дата звернення: 22.05.2025).

17. Про запобігання корупції : Закон України від 14.10.2014 № 1700-VII (із змінами). URL: https://zakon.rada.gov.ua/laws/show/1700-18 (дата звернення: 22.05.2025).

18. Про Державне бюро розслідувань : Закон України від 12.11.2015 № 794-VIII (із змінами). URL: https://zakon.rada.gov.ua/go/794-19 (дата звернення: 22.05.2025).

19. Про Бюро економічної безпеки України : Закон України від 28.01.2021 року № 1150-IX (із змінами). URL: https://zakon.rada.gov.ua/go/1150-20 (дата звернення: 22.05.2025).

20. Про тимчасові слідчі комісії і тимчасові спеціальні комісії Верховної Ради України : Закон України від 19.12.2019 № 400-IX (із змінами). URL: https://zakon.rada.gov.ua/go/400-20 (дата звернення: 22.05.2025).

21. Про комітети Верховної Ради України : Закон України від 04.04.1995 року № 116/95-ВР (із змінами). URL: https://zakon.rada.gov.ua/go/116/95-%E2%F0 (дата звернення: 22.05.2025).

22. Деякі питання документування управлінської діяльності : Постанова Кабінету Міністрів України від 17.01.2018 № 55. URL: https://zakon.rada.gov.ua/laws/show/55-2018-%D0%BF#Text (дата звернення: 22.05.2025).

23. Про затвердження Інструкції про порядок організації та здійснення контролю за виконанням документів у Службі безпеки України : наказ Центрального управління Служби безпеки України від 29.12.2014 № 875. (Зареєстровано в Міністерстві юстиції України 21.01.2015 за № 67/26512).

24. Цивільний кодекс України від 16.01.2003 № 435-IV. URL: https://zakon.rada.gov.ua/go/435-15 (дата звернення: 22.05.2025).

25. Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях : наказ Міністерства юстиції України від 18.06.2015 № 1000/5. (Зареєстровано в Міністерстві юстиції України 22.06.2015 за № 736/27181).

26. Про утворення Ставки Верховного Головнокомандувача : Указ Президента України від 24.02.2022 № 72/2022. URL: https://zakon.rada.gov.ua/go/72/2022 (дата звернення: 22.05.2025).

Стаття надійшла до редакції 31.07.2025

The issue of establishing control deadlines for the implementation of management activity documents

Annotation

Timely control over the execution of tasks (decisions) is an important functional element for ensuring the effective operation of a state body and it represents feedback at the final stage of implementation of managerial decisions. At the same time, monitoring the implementation of managerial decisions is an integral component of the control system and is carried out to supervise executive discipline and ensure the timely and proper execution of documents.

The insufficient development of theoretical provisions regarding the justification of the time parameter of a control indicator highlights the relevance of analyzing various aspects of the problem of documentary control. It underscores the importance of comprehensive scientific research into issues related to selecting ways to improve the mechanism for monitoring the processing status of control documents. Addressing this problem will not only facilitate the process of supervising the execution of management documents but will also significantly enhance its effectiveness.

The purpose of the article is to address issues related to identifying the key baseline data required for establishing the time parameter of a control document indicator when monitoring the full completion of a management decision.

Consolidated information on standard execution deadlines established by regulatory provisions and legal norms of legislative acts constitutes the framework input data for determining the time parameters of control indicators. The time parameters of indicators for standard control documents are the execution deadlines defined by law. The use of a preventive indicator during proactive monitoring of task execution status makes it possible to implement timely response measures in cases where it is not feasible to process (prepare) a control document within the established deadlines.

Keywords: control; monitoring of the implementation of management decisions; indicator of the status of implementation of management decisions; time indicator of the control indicator.

УДК 355.5 https://doi.org/10.33099/2304-2745/2025-3-86/106-114

Косевцов В. О., доктор військових наук, професор[1] (0000-0001-6654-5677)
Тіхонов Г. М., кандидат військових наук, старший науковий співробітник[2] (0000-0003-1941-744X)
Чайковська О. Є.[2] (0000-0002-0656-9105)
Онікійчук С. С.[2] (0009-0002-3328-9472)

[1] – Інститут державного військового управління Національного університету оборони України, Київ;
[2] – Командно-штабний інститут застосування військ (сил) Національного університету оборони України, Київ

Система збору та аналізу інформації про укомплектованість військових частин особовим складом, ходу їх доукомплектування та покриття втрат: складові, чинники та нормативна база

Резюме. У статті висвітлено складові, чинники та нормативну базу системи збору і аналізу інформації про укомплектованість військових частин особовим складом.

Ключові слова: укомплектованість; облік; доукомплектування; покриття втрат.

Постановка проблеми. Система збору та аналізу інформації про укомплектованість військових частин особовим складом, хід їх доукомплектування та покриття втрат є ключовим елементом військової кадрової політики сил оборони України. Вона забезпечує своєчасне та достовірне інформування командування для прийняття управлінських рішень, спрямованих на підтримання боєздатності та стійкості військ.

Актуальність дослідження обумовлена низкою чинників:

широкомасштабна збройна агресія проти України, яка зумовлює втрати особового складу та необхідність певного реагування;

зростання обсягів даних, що потребує сучасних методів обробки, перевірки та інтеграції інформації про особовий склад;

динамічність кадрових процесів, пов'язаних із мобілізацією, демобілізацією, контрактною та резервною службою;

постійне оновлення нормативної бази України у сфері військового обліку та кадрового забезпечення, що вимагає від органів військового управління швидкої адаптації процедур;

цифрова трансформація та впровадження автоматизованих систем, які повинні забезпечити безперервність облікових процесів навіть у складних умовах бойових дій.

Зважаючи на зазначене, важливою постає задача дослідження вітчизняного та зарубіжного досвіду організації систем збору й аналізу інформації про укомплектованість військових частин особовим складом, хід їх доукомплектування та покриття втрат, а також визначення напрямів удосконалення означених процесів.

Аналіз останніх досліджень і публікацій. Аналіз наукових джерел в Україні і за кордоном свідчить про постійну увагу дослідників як до питань укомплектованості військових організаційних структур, так і до управління персоналом збройних сил в цілому.

Питання укомплектованості та покриття втрат особового складу стали предметом уваги багатьох науковців [1–9]. Вказана зацікавленість зі сторони українських науковців пояснюється нагальною необхідністю осмислення підходів до систематизації обліку особового складу під час дії воєнного стану (особливого періоду). У роботі [1] запропоновано часткову методику оцінювання укомплектованості військової частини військовослужбовцями, яка дає змогу провести кількісно-якісну оцінку укомплектованості військовослужбовцями, виявити проблемні питання під час доукомплектування та розробити рекомендації щодо підвищення укомплектованості військової частини.

У публікації [2] автори на сторінках українського видання розглядають виклики рекрутингу та мобілізації в Україні, порівнюють підходи США (перехід від призову до добровільної служби) й пропонують варіанти підвищення добровільного набору та зменшення ухилення.

Інша стаття цього ж видання [3] обґрунтовує підхід "таймлайн-мобілізації" як перехід від примусу до популяризації військової служби, роблячи акцент на праві вибору, як інструменті ефективного

комплектування військових частин людськими ресурсами.

У праці [4] оцінено спроможності мережі територіальних центрів комплектування та соціальної підтримки щодо призову за мобілізації, визначено проблемні аспекти в її функціонуванні та запропоновано шляхи їх усунення для забезпечення більш рівномірного і стійкого комплектування військових частин.

У зарубіжних публікаціях увагу зосереджено на автоматизації та розвитку моделей кадрового менеджменту. Зокрема, у статті [5] описано впровадження інтегрованої платформи IPPS-A у сухопутних військах США, яка підвищує точність даних і прозорість кадрових рішень. У роботі [6] дослідниками обґрунтовано використання оптимізаційних моделей у плануванні людських ресурсів. У дисертації [7] проаналізовано стратегічне управління людськими ресурсами у військових організаціях США, доведено необхідність поєднання формальних процедур і стратегічного менеджменту.

Отже, українські публікації досліджують особливості комплектування військових частин, тоді як зарубіжні дослідження демонструють переваги інтегрованих цифрових систем і стратегічного управління людськими ресурсами. Водночас відсутній єдиний підхід щодо врахування національної специфіки та міжнародного досвіду. Отже, система збору та аналізу інформації про укомплектованість військових частин особовим складом, ходу їх доукомплектування та покриття втрат потребує подальшого дослідження й розвитку.

Метою статті є дослідження складових, чинників та нормативної бази системи збору та аналізу інформації про укомплектованість військових частин особовим складом, ходу їх доукомплектування та покриття втрат.

Виклад основного матеріалу. Нормативно-правове забезпечення системи збору та аналізу інформації про укомплектованість військових частин особовим складом, їх доукомплектування та покриття втрат є багаторівневим механізмом та охоплює конституційні норми, закони України, укази Президента, накази Міністерства оборони, а також міжнародні стандарти.

На найвищому законодавчому рівні Конституція України закріплює положення про те, що захист суверенітету та територіальної цілісності держави покладається на Збройні Сили України [8]. У розвиток цих положень Закон України [9] визначає організаційні засади оборони держави, порядок мобілізації та комплектування військ, а Закон України [10] встановлює структуру, завдання та загальні принципи їх функціонування.

Закон України [11] регулює планування і проведення мобілізаційних заходів, визначає завдання органів військового управління та територіальних центрів комплектування і соціальної підтримки (ТЦК та СП) у сфері обліку людських ресурсів. Тісно пов’язаний із ним Закон України [12], який встановлює правові засади проходження військової служби, формування резерву та порядок ведення військового обліку.

Сучасний підхід до обліку особового складу визначає Інструкція [13]. У документі закріплено, що *облік особового складу* – це цілеспрямована діяльність командирів (начальників), штабів та інших посадових осіб, метою якого є своєчасне, повне й достовірне відображення даних про кількість, якісний склад, розподіл і рух особового складу у встановлених облікових документах. Інструкція визначає порядок ведення первинного, поточного та підсумкового обліку, систему документів (карток, списків, журналів), що забезпечує відстеження руху військовослужбовців у мирний час і під час дії воєнного стану.

У сфері стратегічного кадрового менеджменту ключове значення має Стратегія залучення, розвитку та утримання людського капіталу в силах оборони України на період до 2027 року [14], що фіксує якісний перехід від фрагментарних процесів до цілісного управління людським капіталом, у центрі якого єдиний людино центричний контур прийняття рішень щодо укомплектованості, планового доукомплектування та покриття втрат. Необхідно зазначити, що вказаний стратегічний документ виходить з реалій особливого періоду (воєнного стану): демографічного тиску, мобілізації, втрат, потреби в оперативній ротації й відновленні підрозділів. За цієї умови, реєстрація факту необхідності комплектування замінюється керованою циклічністю кадрових процесів: від рекрутингу й підготовки до реінтеграції та утримання. Формується стратегічне завдання: перетворити дані обліку на інструмент прогнозування, балансування навантаження та підтримання незнижуваної укомплектованості військових частин на першому ешелоні оборони. У межах Стратегії [14] людський

капітал сил оборони окреслюється як персонал сил оборони України із сукупністю сформованих і розвинутих, в межах службової діяльності та у наслідок відповідної підготовки, здібностей, навичок, особистих рис і мотивацій, що використовуються у службовій діяльності, сприяють зростанню професійної компетентності і завдяки цьому впливають на рівень готовності військ (сил) до виконання завдань за призначенням. Тобто наголос робиться не лише на обліковій чисельності, а на придатності, навченості, лідерстві, стійкості, потенціалі розвитку персоналу. Поняття "*людські ресурси*" стосується призовників, військовозобов'язаних і резервістів, які перебувають на військовому обліку та призначені для комплектування сил оборони. Відповідно, *комплектування сил оборони* трактується як організований комплекс заходів із залучення громадян до служби (призов, прийняття на військову службу), їх підготовки й призначення на посади, що змикає рекрутинг, освіту і розстановку в єдиний ланцюг, а планування персоналу визначається як цілеспрямований процес визначення необхідної кількості персоналу, підготовленого до виконання завдань у визначений строк у потрібному місці в мирний час та особливий період [14]. Разом з тим, зазначений стратегічний документ визначає, що *система управління персоналом* – сукупність цілей, завдань, функцій організаційної структури управління персоналом у силах оборони України в процесі планування, обґрунтування, формування, прийняття та реалізації управлінських (кадрових) рішень. принципів, методів, процедур і засобів планування, добору, призначення та реалізації кадрових рішень у силах оборони. Саме ці визначення створюють спільну мову, без якої неможливо домогтися точності управлінських дій.

Узагальнюючи, Стратегія задає рамку, в якій визначення (людський капітал сил оборони, людські ресурси, комплектування сил оборони, планування персоналу, рекрутинг, служба персоналу, система управління персоналом) працюють як операційні специфікації (формалізований опис) та вибудовують взаємодію між тактичним обліком [13] і стратегічною аналітикою управління персоналом. У результаті з'являється те, чого бракувало донині – зв'язок первинного обліку з управлінською дією: від запису про конкретного військовослужбовця до рішення про розподіл людей і завдань у просторі та часі [13, 14]. Саме так Стратегія перетворює систему збору й аналізу інформації про укомплектованість, доукомплектування і покриття втрат на головний важіль підтримання стійкої боєздатності підрозділів у тривалій широкомасштабній війні.

Важливо, що стратегічна логіка спрямована на гармонізацію з процедурними нормами обліку: без повних і коректних первинних записів жодна аналітика не працює; без аналітики навіть бездоганний облік не дає управлінської цінності для планового доукомплектування й покриття втрат.

Проте стрижнем процедурного врегулювання обліку особового складу в системі Міністерства оборони, є Інструкція [13]. На відміну від стратегічних документів, саме Інструкція визначає хто, коли і які документи створює; як узагальнюються дані та у які строки вони подаються до вищих органів військового управління. Саме тому [13] є базою, від виконання якої безпосередньо залежать точність показників укомплектованості, керованість доукомплектування та прозорість покриття втрат.

Відповідно до Інструкції облік особового складу структуровано - він поділяється на персональний, штатно-посадовий та статистичний. *Персональний облік* особового складу ведеться стосовно кожного військовослужбовця та працівника окремо і призначений для системного відображення проходження ними військової служби (трудової діяльності) від її початку до звільнення, виконання ними військового обов'язку в запасі або проходження служби у військовому резерві, а також біографічних та інших даних, які об'єктивно характеризують військовослужбовця або працівника. *Штатно-посадовий облік* особового складу призначений для здійснення систематичного аналізу укомплектованості органів управління, військових частин, установ особовим складом, обліку посад, організації контролю за службовим переміщенням особового складу та оперативного доступу до інформації для складання звітів. *Статистичний облік* особового складу ведеться для отримання узагальнених цифрових показників, які характеризують кількісний і якісний склад особового складу, що планується для укомплектування військ (сил) особовим складом, їх матеріально-технічного забезпечення, підготовки та

поповнення втрат. Відомості за результатами персонального, штатно-посадового і статистичного обліків особового складу утворюють базу даних, яка забезпечує отримання узагальненої інформації з питань проходження військової служби військовослужбовцями або здійснення трудової діяльності працівниками, укомплектованості військ (сил). Крім того, Інструкція визначає, що персональний, штатно-посадовий і статистичний обліки здійснюються в електронній формі.

Особливий розділ Інструкції присвячений обліку загальних втрат особового складу. З погляду обліку, *втрати* – це юридично значимі події, внаслідок яких військовослужбовець вибуває зі строю повністю або тимчасово, що впливає на укомплектованість посади або всього підрозділу і породжує ланцюжок документів та управлінських дій. Для забезпечення єдності практики Інструкція [13] уніфікує класифікацію втрат:

безповоротні втрати (бойові безповоротні втрати та інші померлі (загиблі) – належать особи, які загинули під час виконання бойового завдання, від застосування противником зброї (в тому числі зброї масового ураження), померли унаслідок поранення (травми, контузії, каліцтва), хвороби та з інших причин під час бойової обстановки, перебування в полоні (заручниках), загинули унаслідок подій і нещасних випадків під час виконання бойових завдань; інші померлі (загиблі), до яких належать особи, які померли від захворювання та з інших причин, не пов'язаних з участю в бойових діях, покінчили життя самогубством, загинули від необережного поводження зі зброєю, через порушення заходів безпеки, унаслідок позастатутних взаємовідносин, в аваріях, катастрофах та інших випадках, не пов'язаних із виконанням бойових завдань;

тимчасові втрати особового складу – належать бойові тимчасові втрати, до яких належать санітарні втрати, особи, зниклі безвісти за особливих обставин, полонені (заручники) або інтерновані в інших державах; інші тимчасові втрати, до яких належать травмовані, хворі, отруєні, зниклі безвісти в умовах, не пов'язаних з бойовою обстановкою, дезертири та військовослужбовці, які самовільно залишили військові частини або місця проходження служби.

З практичного боку, такий поділ має критичну функцію, а саме дає змогу командуванню планувати покриття втрат адекватно характеру вибуття:

для санітарних втрат прогнозувати терміни повернення або тимчасову заміну на час лікування;

для безповоротних ініціювати доукомплектування.

Інструкція деталізує документальний контур. Ядром є донесення (повідомлення) про події з особовим складом, іменні списки (зокрема списки безповоротних втрат), журнали обліку, особові справи та обліково-послужні картки. Первинне донесення, як правило, оформлює командир (або уповноважена посадова особа) за участю служби персоналу та медичної служби, після чого дані вносяться до журналів/карток. На рівні військової частини обов'язковими є уточнення записів між службою персоналу, штабом та медслужбою службою.

Управлінська логіка Інструкції – *рух від події до рішення* – як тільки подія зафіксована первинно, служба персоналу актуалізує облікові записи, коригує дані укомплектованості, медична служба визначає статус лікування (придатності), а командир приймає рішення про комплектування вакантних посад.

На вищому рівні підсумковий облік консолідується у показники укомплектованості, які є вихідною базою стосовно прийняття рішень щодо призначення; розроблення планів переміщення, а також заявок на поповнення; подання запитів на цільову підготовку, перерозподілу людських ресурсів між частинами. Інструкція також описує відповідальність і контроль. Командири (начальники) несуть персональну відповідальність за достовірність і своєчасність записів; служби персоналу – за правильність ведення форм і синхронізацію з іншими службами; штаби – за компоновку зведень, подання звітності у строки, організацію звірянь і усунення розбіжностей. Підсумовуючи зазначимо, що Інструкція [13] є опорою для організації ритмічного покриття втрат та планового доукомплектування в умовах довготривалої збройної агресії, а також надійне підґрунтя для переходу до інтегрованих цифрових рішень, передбачених Стратегією [14].

Аналіз нормативно-правових актів свідчить про поступовий перехід від фрагментарного врегулювання обліку особового складу до комплексного підходу. Це відповідає сучасним викликам особливого

періоду (воєнного стану) та забезпечує основу для подальшої модифікації системи збору й аналізу інформації про укомплектованість, доукомплектування та покриття втрат. Зазначимо, що досліджувана система має *інституційні, організаційні та технічні складові*. Її ефективність залежить не лише від наявності нормативних положень чи технічних засобів, а й від того, наскільки злагоджено вони взаємодіють між собою та наскільки швидко здатні адаптуватися до динамічних умов особливого періоду.

Інституційна складова є основою функціонування, що визначається Міністерством оборони України, Генеральним штабом Збройних Сил України, органами військового управління, підрозділами персоналу. Саме ці структури визначають перелік показників, які підлягають обов'язковому обліку та аналізу, встановлюють відповідальних виконавців і розробляють правила взаємодії між різними рівнями військового управління. Інституційні складові забезпечують стратегічну спрямованість системи, формують підвалини для уніфікованих методів збору та подальшого опрацювання інформації, задають вимоги до її достовірності, повноти та захищеності.

Водночас саме *організаційна* складова перетворює загальні принципи в реальні управлінські процеси. Її основу становить нормативно-правова база у вигляді законів, постанов Кабінету Міністрів України, наказів Міністерства оборони України та директив Генерального штабу Збройних Сил України, що визначають порядок ведення обліку, регламентують форми і терміни звітності, а також відповідальність посадових осіб. На рівні військових частин ця база конкретизується у вигляді інструкцій, методичних рекомендацій і стандартів, які встановлюють процедури введення первинних даних, алгоритми передачі інформації до вищих органів військового управління та способи перевірки її достовірності. Організаційні механізми включають методики аналізу укомплектованості (прогнозованих втрат), що дають змогу здійснювати облік наявного особового складу та прогнозувати потреби у доукомплектуванні з урахуванням динаміки втрат, призначення (переміщення) особового складу тощо. До цієї ж складової належать системи контролю і перевірки, що передбачають контроль звітності між різними рівнями управління: проведення моніторингів, інспекцій і аудитів.

Матеріальною основою функціонування системи виступає *технічна складова*, що охоплює інформаційні системи, телекомунікаційну інфраструктуру, засоби введення і зберігання даних, а також механізми їхнього захисту. Використання сучасних автоматизованих баз даних, таких як "Оберіг" або ІАС "Персонал", дає змогу здійснювати персональний облік військовослужбовців, формувати аналітичні довідки та узагальнювати статистичні звіти. Наявність захищених каналів зв'язку та сучасних серверних рішень забезпечує передачу даних у найкоротші терміни, а системи резервування й кіберзахисту гарантують їхню збереженість навіть в умовах активних кібератак чи фізичного впливу противника. Технічні засоби включають також робочі станції, мобільні пристрої та інтеграційні платформи, що забезпечують обмін інформацією між різними рівнями управління, а також із державними і міжнародними структурами, у випадках коли це необхідно.

Взаємозв'язок між інституційними, організаційними та технічними складовими є системоутворюючим. Інституційний рівень визначає, хто і за що відповідає, організаційний встановлює порядок дій, а технічний забезпечує їхню реалізацію. У разі відсутності хоча б одного з цих елементів система втрачає цілісність: без інституційної складової неможливо забезпечити належну ієрархію відповідальності, без організаційної складової дані залишаються неструктурованими, а без технічної бази вони не можуть бути оперативно систематизовані, перевірені та проаналізовані. Таким чином, комплексність та збалансованість трьох складових визначають здатність системи виконувати головне завдання: надавати командуванню достовірну, своєчасну та аналітично опрацьовану інформацію, що безпосередньо впливає на прийняття управлінських рішень і забезпечує боєздатність Збройних Сил України.

Разом з тим, необхідно дослідити, які саме *зовнішні та внутрішні чинники* істотно впливають на функціонування системи збору та аналізу інформації про укомплектованість військових частин особовим складом, хід їх доукомплектування та покриття втрат. Їх вплив проявляється як на інституційному, так і на організаційному та технічному рівнях, створюючи динамічний контекст, у межах якого система або посилює свою результативність, або стикається з суттєвими

бар'єрами. Врахування цих чинників у практиці управління персоналом дає змогу підвищити стійкість та адаптивність системи до умов особливого періоду (воєнного стану).

На інституційні складові, головним чином, впливають зовнішні чинники, серед яких визначальними є зміни у політичній площині. До зовнішніх чинників належать також міжнародні зобов'язання України у сфері стандартизації оборонного планування, що стимулюють адаптацію системи до практик НАТО. Водночас на інституційний рівень впливають і внутрішні чинники, пов'язані з якістю управлінських рішень, спроможністю вищих органів військового управління здійснювати ефективний контроль та координацію, рівнем кадрового потенціалу керівних структур. Слабка військова кадрова політика або відсутність системного підходу до підбору та розстановки осіб офіцерського складу в органах військового управління може знизити ефективність інституційної складової незалежно від зовнішніх обставин.

Організаційна складова є особливо чутливою до взаємодії зовнішніх і внутрішніх чинників. По-перше, серед зовнішніх чинників визначальними є зміни у законодавчій та нормативній базі: ухвалення нових законів і постанов, внесення коректив до положень щодо мобілізації або порядку ведення військового обліку. По-друге, до цієї групи чинників належить і рівень суспільної підтримки війська, який безпосередньо впливає на добровільність комплектування та рівень дисципліни у виконанні військового обов'язку.

Водночас внутрішні чинники зумовлюють організаційну ефективність на практичному рівні. Насамперед, вони охоплюють якість внутрішніх процедур: наскільки чітко налагоджена звітність, наскільки відповідально персонал дотримується термінів і стандартів обліку, а також наскільки ефективно функціонують механізми перевірки та контролю. Крім того, ключове значення має рівень професійної підготовки осіб, відповідальних за ведення обліку у військових частинах, оскільки допущені на цьому етапі помилки, як правило, мультиплікуються на вищих рівнях управління. Нарешті, важливим внутрішнім чинником виступає наявність дієвих механізмів комунікації та зворотного зв'язку між різними рівнями управління, що забезпечує своєчасне усунення недоліків і врахування практичного досвіду у процесі вдосконалення процедур.

Технічна складова системи залежить від поєднання зовнішніх і внутрішніх чинників особливо відчутно. До зовнішніх чинників відносяться насамперед рівень технічного розвитку держави та доступність сучасних інформаційних технологій, умови міжнародної співпраці у сфері кіберзахисту, а також характер загроз з боку противника. Масштабні кібератаки, спроби знищення інформаційної інфраструктури, застосування електронних засобів боротьби – все це створює середовище, яке визначає вимоги до технічної стійкості системи. Внутрішні чинники технічної складової включають рівень оснащення військових частин технічними засобами, стан програмного забезпечення, ефективність системи резервування і захисту даних. Важливу роль відіграє й кадровий аспект: підготовка фахівців у сфері ІТ, здатних забезпечувати безперебійну роботу інформаційних систем та своєчасно реагувати на технічні збої чи кібератаки. Відсутність кваліфікованого персоналу може нівелювати навіть найсучасніші технічні рішення, так само як недофінансування або несвоєчасне оновлення обладнання робить систему вразливою.

Аналіз зовнішніх і внутрішніх чинників дає змогу дійти висновку, що стійкість і ефективність системи збору та аналізу інформації про укомплектованість військових частин залежить від їхньої збалансованої взаємодії. Зовнішні чинники визначають середовище, у якому функціонує система, формуючи виклики й обмеження, тоді як внутрішні чинники відображають рівень організованості та спроможності самої системи протистояти цим викликам.

Внутрішні чинники функціонування системи збору та аналізу інформації про укомплектованість особовим складом, хід доукомплектування та покриття втрат мають ключове значення, оскільки саме на них можна безпосередньо впливати управлінськими рішеннями. Вони визначають якість введення та обробки даних, швидкість їх передачі, достовірність результатів аналізу та, зрештою, ефективність використання цих даних у процесах управління військами.

Першочерговим внутрішнім чинником є ***організаційно-штатна структура підрозділів персоналу***. Від того, наскільки чітко розподілені обов'язки між військовослужбовцями, залежить швидкість підготовки звітності та достовірність внесених даних. Недостатня чисельність персоналу, дублювання функцій чи нечітке визначення

відповідальності призводять до перевантаження окремих осіб і помилок у звітності. Це підтверджується тим, що у випадках, коли кількість працівників облікових підрозділів не відповідає обсягу завдань, відсоток помилок у документах може перевищувати 20-25%. Оптимізація структури, скорочення дублювання функцій та збільшення штату там, де спостерігається хронічне перевантаження, є практичними кроками до зниження кількості помилок і підвищення достовірності даних.

Наступним визначальним чинником виступає ***технологічне забезпечення***. Саме воно формує основу для оперативності та точності системи. Використання застарілих комп'ютерів і нестабільного зв'язку збільшує час формування звітів у кілька разів, створюючи загрозу запізнілого прийняття управлінських рішень. Водночас модернізація техніки, впровадження мобільних застосунків та резервних каналів зв'язку здатні зменшити час підготовки звітів із кількох годин до кількох хвилин, а також істотно знизити ризик втрати даних. Особливої ваги цей чинник набуває в умовах воєнного стану, коли зв'язок може бути обмежений або зруйнований унаслідок ворожих дій. Використання офлайн-функцій та автоматичного резервування інформації дає можливість зберігати безперервність облікових процесів навіть у кризових ситуаціях.

Третім чинником, що безпосередньо впливає на ефективність роботи системи, є кваліфікація персоналу. Освітній рівень, професійна підготовка та мотивація кадрових фахівців визначають, наскільки якісно вони працюють із сучасними інформаційними системами. За оцінками, у разі недостатньої підготовленості помилки у звітності можуть сягати 15–20%, тоді як навчання, курси підвищення кваліфікації та сертифікація дають змогу знизити цей показник удвічі. Крім того, підвищення кваліфікації значно скорочує час обробки кадрового запису, що позитивно позначається на швидкості прийняття рішень у кризових умовах. Важливим є і морально-психологічний аспект: мотивований і впевнений у своїх знаннях персонал допускає менше помилок, тоді як перевантаженість і відсутність впевненості у власній компетентності веде до зростання кількості неточностей.

Четвертий чинник – ***особливості інформаційного обміну***. Протоколи збору, перевірки та передачі даних визначають регулярність оновлення звітності та рівень її достовірності. Відсутність автоматизованих механізмів контролю підвищує ризик помилок і неточностей у даних, тоді як застосування електронних систем звірки та підтвердження дає змогу знизити кількість помилок із 15% до 2-3%. Автоматичний контроль також скорочує час, необхідний на виправлення неточностей, у середньому на 40%, що істотно підвищує оперативність управління. Забезпечення ефективного зворотного зв'язку між рівнями управління є необхідною умовою, адже воно дає змогу вчасно реагувати на виявлені недоліки та уникати повторних помилок у майбутньому.

П'ятим важливим чинником виступає ***технічний захист інформації***. У сучасних умовах інформаційна безпека набуває не меншої ваги, ніж точність обліку. Відсутність достатнього рівня захисту може призвести до витоку даних, що в умовах воєнного часу становить пряму загрозу національній безпеці. Досвід показує, що при відсутності криптографічного захисту ризик витоку може становити до 30%, тоді як використання шифрування та багатофакторної автентифікації знижує його до мінімуму. Крім того, важливою є наявність системи резервного копіювання, яка забезпечує відновлення даних навіть у разі фізичного знищення серверів або кібератак.

Загалом аналіз внутрішніх чинників показує, що їхній вплив є комплексним і взаємопов'язаним. Наприклад, навіть за наявності сучасного технічного забезпечення низька кваліфікація персоналу зведе нанівець переваги цифровізації. Водночас без належного технічного захисту ефективність автоматизованих систем не гарантуватиме безпеки інформації. Тому управлінські рішення мають бути спрямовані не на ізольоване покращення окремих чинників, а на їх збалансоване вдосконалення. Це передбачає оптимізацію організаційно-штатних структур, модернізацію техніки, системну підготовку персоналу, вдосконалення інформаційного обміну та комплексний захист даних. Лише така інтеграція заходів забезпечить здатність системи своєчасно й достовірно відображати стан укомплектованості військових частин і сприятиме підвищенню ефективності управління в умовах воєнного стану.

Водночас виявлені зовнішні та внутрішні чинники функціонування системи збору й аналізу інформації про укомплектованість та покриття втрат засвідчують, що ефективність національної

моделі кадрового обліку залежить від трьох ключових умов: інтеграції цифрових рішень, забезпечення повноти й своєчасності даних та запровадження прозорих управлінських процедур. Для визначення оптимальних шляхів розвитку необхідним є врахування зарубіжного досвіду, зокрема практик держав, які вже пройшли етап цифрової трансформації кадрових процесів. У цьому сенсі особливу цінність становить досвід Сполучених Штатів Америки, де завдяки нормативно врегульованій основі створено інтегровану систему обліку особового складу та управління покриттям втрат.

Практична реалізація цих підходів в Україні сприятиме підвищенню якості комплектування сил оборони, створенню ефективного механізму кадрової безпеки та наближенню національної системи до стандартів НАТО [14].

Висновки. Отже, проведене дослідження підтвердило, що система збору та аналізу інформації про укомплектованість військових частин особовим складом, хід їх доукомплектування та покриття втрат є складним багаторівневим механізмом, який поєднує нормативно-правове регулювання, організаційні процедури та цифрові технології. В Україні вона перебуває на етапі реформування: інтегруються сучасні технологічні рішення, посилюється нормативна база, формується стратегічне бачення розвитку людського капіталу в умовах воєнного стану.

Аналіз чинників довів, що на ефективність системи впливають як зовнішні (міжнародні стандарти, досвід партнерів, виклики безпеки), так і внутрішні (стан нормативного регулювання, рівень цифровізації, кадрова спроможність органів військового управління) передумови.

Таким чином, результати роботи підтверджують необхідність подальшої наукової розробки проблеми та удосконалення системи збору та аналізу інформації про укомплектованість військових частин особовим складом, ходу їх доукомплектування та покриття втрат з урахуванням досвіду провідних країн світу та власного досвіду, набутого військовими організаційними структурами під час відбиття широкомасштабної збройної агресії.

Подальші дослідження доцільно зосередити на вивченні закордонного досвіду, розробці методики оцінювання ефективності системи збору та аналізу інформації про укомплектованість військових частин особовим складом, хід їх доукомплектування та покриття втрат у Збройних Силах України. Така методика має передбачати визначення показників і критеріїв, що враховують рівень цифровізації процесів, швидкість оновлення та обробки інформації, її достовірність і доступність для органів військового управління. Окремий акцент слід зробити на оцінюванні внеску інтегрованих електронних систем (зокрема СЕДО та перспективних кадрових платформ) у підвищення прозорості, надійності та аналітичних можливостей обліку. Це дасть змогу сформувати об'єктивну основу для подальшого вдосконалення системи, її гармонізації з міжнародними стандартами НАТО та забезпечення більшої адміністративної й оперативної ефективності під час дії особливого періоду (воєнного стану).

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Георгадзе О. А., Савчук Д. В. Часткова методика оцінювання укомплектованості військової частини військовослужбовцями // Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2024. № 3(83). С. 117–121. DOI: 10.33099/2304-2745/2024-3-83/117-121.
2. Baker J. E., Naperkowski R. J. Mobilization and recruitment in Ukraine: challenges and solutions // Military Science. 2024. Vol. 2, No. 2. P. 33–47. DOI: https://doi.org/10.62524/msj.2024.2.2.03
3. Семененко О., Коваль В., Добровольський Ю., Царинник В., Ованесян Р. "Таймлайн"-мобілізація – шлях від примусу до популяризації військової служби в умовах війни: право вибору – спосіб ефективного комплектування людськими ресурсами // Military Science. 2024. Vol. 2, No. 2. С. 159–179. DOI: https://doi.org/10.62524/msj.2024.2.2.14
4. Павлюк О., Череп В., Дідіченко В., Марко І. Визначення шляхів нарощування спроможностей мережі територіальних центрів комплектування та соціальної підтримки щодо призову за мобілізацією військовозобов'язаних та резервістів // Military Science. 2024. Vol. 2, No. 4. С. 83–91. DOI: https://doi.org/10.62524/msj.2024.2.4.7
5. Eggers R. L. New U.S. Army Human Resources System Is the Change the Army and Its Soldiers Need // Military Review. 2022. URL: https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/September-October-2022/Eggers/ (дата звернення: 19.08.2025).
6. Mazari Abdessameud O., Van Utterbeeck F., Guerry M.-A. Military Human Resource Planning through Flow Network Modeling // Engineering Management Journal. 2022. Vol. 34, No. 2. P. 302–313. DOI: 10.1080/10429247.2021.1900660.

7. Downes C. M. Strategic Human Resource Management in Military Organizations: Dissertation Doctor of Philosophy. Case Western Reserve University, 2015. URL: https://etd.ohiolink.edu/acprod/odb_etd/ws/send_file/send?accession=case1427806845&disposition=inline (дата звернення: 19.08.2025).
8. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/go/ 254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 19.08.2025).
9. Про оборону України : Закон України від 06.12.1991 № 1932-XII. URL: https://zakon.rada.gov.ua/go/1932-12 (дата звернення: 19.08.2025).
10. Про Збройні Сили України : Закон України від 06.12.1991 № 1934-XII. URL: https://zakon.rada.gov.ua/go/1934-12 (дата звернення: 19.08.2025).
11. Про мобілізаційну підготовку та мобілізацію : Закон України від 21.10.1993 № 3543-XII. URL: https://zakon.rada.gov.ua/go/3543-12 (дата звернення: 19.08.2025).
12. Про військовий обов'язок і військову службу : Закон України від 25.03.1992 № 2232-XII. URL: https://zakon.rada.gov.ua/go/2232-12 (дата звернення: 19.08.2025).
13. Про затвердження Інструкції з організації обліку особового складу в системі Міністерства оборони України : наказ Міністерства оборони України від 15.09.2022 № 280. URL: https://www.mil.gov.ua/content/mou_orders/280_nm_2022.pdf (дата звернення: 19.08.2025).
14. Про затвердження Стратегії залучення, розвитку та утримання людського капіталу в силах оборони України на період до 2027 року : наказ Міністерства оборони України від 29.12.2024 № 862/нм. URL: https://www.mil.gov.ua/diyalnist/kadrova-politika/derzhavna-sluzhba/ (дата звернення: 19.08.2025).

Стаття надійшла до редакційної колегії 29.08.2025

System for collecting and analyzing information on personnel manning levels of military units, the process of replenishment, and loss replacement: components, factors, and regulatory framework

Annotation

The system for collecting and analyzing information on the personnel manning levels of military units, the process of their replenishment, and the replacement of losses constitutes a key element of the personnel policy of the Defence Forces of Ukraine. It ensures the timely and reliable provision of information to the military command for informed decision-making aimed at maintaining combat readiness and operational resilience of the forces. In this context, the task of studying both domestic and foreign experience in organizing systems for collecting and analyzing information on personnel manning levels of military units, their replenishment, and loss replacement, as well as identifying directions for improving these processes, becomes particularly relevant.

The purpose of the article is to examine the components, influencing factors, and regulatory framework of the system for collecting and analyzing information on the personnel manning levels of military units, the process of their replenishment, and the replacement of losses.

The conducted study has confirmed that the system for collecting and analyzing information on the personnel manning levels of military units, the process of their replenishment, and the replacement of losses is a complex, multi-level mechanism that integrates legal and regulatory provisions, organizational procedures, and digital technologies. In Ukraine, this system is currently undergoing reform, characterized by the integration of modern technological solutions, the strengthening of the regulatory framework, and the development of a strategic vision for human capital development under conditions of martial law.

The analysis of influencing factors has demonstrated that the effectiveness of the system is determined by both external factors (international standards, partner experience, and security challenges) and internal factors (the state of regulatory regulation, the level of digitalization, and the personnel capacity of military command and control bodies).

Keywords: manning levels; personnel accounting; replenishment; loss replacement.

УДК 355.45.02 https://doi.org/10.33099/2304-2745/2025-3-86/115-127

Гибало К. В. (0009-0000-5538-9840)

Національна академія Служби безпеки України, Київ

Логістичне забезпечення угрупувань військ (сил) Збройних Сил України: досвід, виклики та напрями удосконалення

Резюме. Проаналізовано проблеми живучості тилових структур під масованим вогневим та інформаційним впливом противника, висвітлено застосування автоматизованих систем обліку, кіберзахисту, безпілотних і роботизованих засобів у сфері постачання. Особливу увагу приділено міжнародному досвіду НАТО, США та Ізраїлю, релевантному для України. Сформульовано напрями удосконалення логістичної системи: створення мережі мобільних хабів, упровадження цифрових близнюків логістичних процесів, стандартизація взаємодії з цивільними перевізниками, посилення force protection колон і складів, розвиток багаторівневої системи резервів.

Ключові слова: військова логістика; тилове забезпечення; мобільність; гнучкість; живучість; мультимодальність; цифровізація; автоматизація обліку; кіберзахист; інтеграція цивільних ресурсів; мобільні логістичні хаби; штучний інтелект.

Постановка проблеми. Сучасна війна радикально змінила роль логістики у воєнному мистецтві, перетворивши її з другорядної функції на стратегічний чинник, який безпосередньо визначає темп і результативність бойових дій. Якщо раніше тилове забезпечення здебільшого слідувало за рішеннями командування і було реактивним за характером, то нині воно стало рівноправним елементом планування операцій, оскільки здатність забезпечити війська ресурсами є головним критерієм реалістичності будь-якого замислу. В умовах війни високої інтенсивності, коли бойові дії відзначаються високою маневреністю, непередбачуваністю і значним вогневим та кібернетичним тиском з боку противника, класична централізована модель логістики, успадкована ще від радянських часів, виявила свою інертність і вразливість. Вона не здатна забезпечити ні швидкість реагування, ні необхідну стійкість у сучасних умовах, що актуалізує потребу у її докорінній трансформації.

Науково-практична значущість проблеми полягає в тому, що рівень розвитку логістики прямо визначає стійкість оборони, реалістичність наступальних задумів, здатність зменшити рівень втрат і оптимізувати використання обмежених ресурсів. Це питання давно вийшло за межі вузьковійськової сфери та набуло міждисциплінарного характеру, охоплюючи право, менеджмент, інженерію, інформаційні технології та сферу національної безпеки. Таким чином, дослідження логістики є важливим не лише для військової практики, а й для розроблення державної політики, інтеграції України до стандартів НАТО, а також формування довгострокової стратегії безпеки.

Емпіричною базою дослідження стали реальні практики логістичного забезпечення, напрацьовані під час Антитерористичної операції (АТО) та операції Об'єднаних сил (ООС) у 2014–2021 роках, а також досвід широкомасштабної війни з 2022 року. Саме ці періоди дають змогу простежити еволюцію від кризового стану тилу, що спирався на волонтерську допомогу, до поступового формування більш гнучкої системи, яка інтегрує елементи автоматизації, мультимодальних перевезень і міжнародної допомоги. Застосування сучасних технологій управління, цифрового обліку та уніфікованих стандартів створює можливість для формування нової якості логістики, яка має відповідати викликам війни високої інтенсивності.

Аналіз останніх досліджень і публікацій. Аналіз наукової літератури засвідчує, що питання військової логістики посідає чільне місце в сучасних дослідженнях як в Україні, так і за кордоном [1–3, 18, 19, 22]. Вітчизняні автори [3, 9, 10, 13, 14, 17, 19] здебільшого акцентують на проблемах організації тилового забезпечення у Збройних Силах (ЗС) України, зокрема на питаннях розосередження складів, стандартизації процедур обліку матеріально-технічних засобів, охорони транспортних колон та узгодження взаємодії між різними видами і родами військ. Значну увагу приділено виявленим труднощам у період АТО/ООС і під час перших місяців широкомасштабної агресії Російської

Федерації (РФ). Проте у цих роботах все ще недостатньо розкрито новітні напрями розвитку логістики, зокрема застосування цифрових близнюків, прогнозних моделей штучного інтелекту для планування ресурсів, а також управління відкритою та закритою інформацією в режимі реального часу.

Зарубіжний науковий доробок [5–8, 11, 12, 15, 16, 20, 23, 24] зазначається більшою глибиною концептуальних узагальнень. У працях країн НАТО чільне місце займає концепція єдиного логістичного простору, що дає змогу державам-учасникам уніфікувати стандарти, обмінюватися ресурсами та забезпечувати сумісність транспортних і облікових систем. Доктрина *Joint Publication* 4-0 у США визначає логістику як інтегровану спільну систему, що об'єднує всі роди військ у межах єдиної концепції управління ресурсами. В ізраїльській практиці особливий акцент робиться на інтеграції цивільних і військових спроможностей, створенні укріплених складів, здатних витримати вогневий вплив, а також застосуванні роботизованих рішень для оптимізації логістичних процесів.

Усі ці підходи демонструють, що сучасна логістика більше не зводиться до схеми постачання у традиційному розумінні. Вона функціонує як багаторівнева система, де forward-deployment запасів, цифрове управління та кластеризація інфраструктури забезпечують стійкість і мобільність у складних умовах бойових дій. Водночас у науковому полі все ще бракує комплексних робіт, які б поєднували ці напрацювання з українським досвідом 2022–2025 рр., коли на логістичні вузли постійно здійснюється масований вогневий і кібернетичний тиск, а інтеграція міжнародної допомоги стала визначальним чинником боєздатності ЗС України. Саме тому постає завдання узагальнити як вітчизняні, так і зарубіжні підходи, адаптувавши їх до українських реалій війни високої інтенсивності.

Будь-яке дослідження, що стосується логістики у воєнний час, має низку методологічних і практичних обмежень, які визначають рамки застосування отриманих результатів. Передусім вони зумовлені високою динамікою бойових дій, коли оперативна обстановка змінюється швидше, ніж відбувається обґрунтоване реагування на ці зміни. Це означає, що висновки та рекомендації мають узагальнювальний характер і потребують постійного уточнення в умовах нових загроз і технологічних рішень.

Мета та завдання статті. Виявлені у сучасній науковій літературі прогалини, а також практика ЗС України у війні з РФ зумовлюють потребу у формуванні комплексного дослідження, яке б поєднувало теоретичні узагальнення з емпіричними висновками та практичними рекомендаціями. Саме тому **метою статті** є системний аналіз логістичного забезпечення угруповань військ у 2014–2025 рр., виявлення його ключових проблем і слабких місць, узагальнення міжнародного досвіду та формування пропозицій, здатних підвищити стійкість і ефективність тилу у війні високої інтенсивності.

Досягнення поставленої мети передбачає виконання низки взаємопов'язаних завдань. Насамперед необхідно простежити еволюцію логістичних підходів у ЗС України, визначивши критичні вузли та причини їхньої уразливості. Наступним кроком є оцінка заходів, які вже впроваджені у системі постачання, зокрема розосередження складів, мультимодальних перевезень, цифровізації обліку та створення мобільних хабів. Важливим завданням виступає також вивчення релевантного міжнародного досвіду – стандартів НАТО, концепцій США і практики Ізраїлю, з подальшою їхньою адаптацією до українських умов.

Виклад основного матеріалу. На початок 2014 року система тилового забезпечення ЗС України перебувала у кризовому стані. Вона зберігала риси радянської моделі, побудованої на принципах жорсткої централізації, великих стаціонарних складів та багаторівневої зарегульованості процедур. Така архітектура могла працювати в умовах мирного часу, однак виявилася вкрай уразливою під час війни високої інтенсивності. Концентрація запасів у кількох великих базах створювала критичну залежність: ураження одного вузла могло паралізувати постачання на цілому операційному напрямку.

Організаційна структура тилу була відокремленою від оперативного планування. Розподіл матеріальних засобів відбувався за застарілими схемами, які не враховували темп і динаміку бойових дій. Брак мобільних елементів призводив до того, що підрозділи на передовій залишалися без необхідних ресурсів у вирішальні моменти. Логістика фактично функціонувала реактивно, реагуючи на події із запізненням, замість того щоб випереджати їх.

Не менш серйозною проблемою була технологічна відсталість. Облік ресурсів

переважно здійснювався у паперовій формі, що породжувало помилки, дублювання та затримки в інформаційному обміні. Командири різних рівнів не мали актуальних даних щодо наявних запасів, що унеможливлювало швидке та обґрунтоване ухвалення рішень.

Важливим чинником виявився і кадровий аспект. Значна частина офіцерів тилу зберігала радянські підходи, де логістика розглядалася як допоміжна функція, а не як стратегічний елемент операцій. Це знижувало ініціативність і гнучкість у критичних ситуаціях.

Таким чином, до початку російської агресії 2014 року Україна мала архаїчну, централізовану і малорухому систему тилового забезпечення, яка не відповідала вимогам сучасної війни. Саме ці вади стали основою кризових явищ, що проявилися з початком бойових дій на сході країни [1].

Початок АТО у 2014 році став каталізатором, який повною мірою виявив накопичені проблеми системи тилового забезпечення. Підрозділи, терміново розгорнуті у східних регіонах, зіткнулися з гострим дефіцитом матеріальних засобів. В армії бракувало бронежилетів, шоломів, сучасних засобів зв'язку, медичного обладнання та навіть базового спорядження. Запаси, що зберігалися на віддалених складах, не могли бути оперативно доставлені через низьку мобільність транспортної системи та відсутність гнучких механізмів координації.

Особливо критичною була ситуація з пальним та боєприпасами. Затримки у їх доставці фактично ставили під загрозу виконання бойових завдань. Брак єдиної інформаційної системи управління призводив до того, що наявні в тилу ресурси залишалися недосяжними для передових частин. Це створювало асиметрію між формальними показниками забезпечення та реальною боєготовністю військ.

У цих умовах вирішальну роль відіграв волонтерський рух. Громадські ініціативи, що виникли стихійно у перші тижні війни, змогли оперативно забезпечити війська бронежилетами, аптечками, касками, тепловізорами, транспортними засобами та навіть безпілотними апаратами цивільного зразка. Волонтери обходили бюрократичні бар'єри, мобілізували ресурси бізнесу та діаспори, створювали неформальні канали постачання безпосередньо до передових підрозділів. Саме завдяки цій активності українська армія зберегла боєздатність у перші критичні місяці війни.

Феномен волонтерства мав і стратегічний вимір. Він показав, що горизонтальні зв'язки, гнучкість та швидкість прийняття рішень можуть компенсувати інерційність державної системи. Волонтери фактично продемонстрували модель "реактивної логістики", орієнтованої на результат, а не на процедури. Це стало аргументом для суспільства і військово-політичного керівництва на користь структурних реформ.

Таким чином, досвід АТО 2014 року підтвердив: стара централізована модель тилу остаточно вичерпала себе. Вона не змогла забезпечити навіть базові потреби війська в умовах війни високої інтенсивності. Водночас саме завдяки волонтерам армія отримала шанс вистояти, а держава — усвідомлення нагальної потреби у реформуванні логістики [3, 9, 11].

Події 2014 року стали переломним моментом, після якого військово-політичне керівництво України усвідомило критичну необхідність модернізації тилових структур. У 2015–2017 рр. розпочався процес реформ, що мали на меті хоча б частково подолати найгостріші проблеми та закласти основу для подальшої трансформації.

Першим важливим кроком стало розосередження складів і баз зберігання матеріальних засобів. Якщо раніше вони концентрувалися у кількох великих вузлах, то тепер було створено мережу менших складів, наближених до районів виконання завдань. Це зменшувало вразливість тилової інфраструктури та скорочувало час доставки ресурсів до передових частин.

Другою інновацією стало формування мобільних груп постачання. Їхнє завдання полягало у швидкому реагуванні на потреби військ та доставці вантажів безпосередньо у зону бойових дій. Це частково компенсувало інерційність централізованої моделі та поступово змінювало філософію логістики на більш гнучку й орієнтовану на конкретні завдання.

Паралельно почали створюватися оперативні резерви матеріальних засобів. Їхнє завдання – швидке підкріплення фронту у випадку загострення ситуації чи втрати доступу до основних складів. Наявність резервів підвищувала стійкість війська та давала змогу утримувати бойові порядки навіть у критичних умовах.

Важливу роль відіграв і інженерний захист логістичних об'єктів. Склади почали обладнувати укриттями, засобами маскування та навіть заглибленими сховищами. Це був перший крок до формування концепції "живучості тилу", яка згодом стала одним із ключових принципів сучасної логістики.

Окремо варто зазначити початок процесу цифровізації. Вперше були запроваджені програмні модулі для обліку запасів і моніторингу їхнього руху. Хоча ця практика ще не мала системного характеру, вона створила підґрунтя для майбутньої інтегрованої інформаційної платформи.

Водночас відбувалося поглиблення співпраці з НАТО. Україна почала впроваджувати окремі елементи стандартів Альянсу – від процедур маркування та пакування до навчання персоналу за міжнародними програмами. Це було першим кроком до сумісності з логістичними практиками партнерів.

Таким чином, у 2015–2017 роках українська армія здійснила низку реформ, які дали змогу пом'якшити наслідки кризи та створити основу для подальшого розвитку. Від реактивної моделі логістика почала переходити до більш адаптивної та інституціолізованої, що підготувало ґрунт для наступного етапу – ООС [5, 11].

Перехід від АТО до ООС у 2018 році означав початок нового етапу у розвитку тилового забезпечення. Якщо у 2015–2017 рр. головна увага приділялася подоланню найгостріших проблем, то в період ООС відбулася інституціоналізація реформ та поступове інтегрування логістики у систему оперативного управління.

Ключовим досягненням стало посилення централізованого планування з урахуванням логістичних можливостей. Тилові підрозділи почали взаємодіяти з оперативними штабами ще на етапі розробки планів операцій. Це означало відхід від практики, коли логістика лише "підтягувалася" до вже ухвалених рішень. Вона перетворилася на рівноправний елемент, який визначав реалістичність замислу бойових дій.

Другим важливим нововведенням стала система багаторівневих резервів. Вони формувалися не лише на центральному, а й на рівні оперативних угруповань, що давало змогу швидко компенсувати втрати чи покривати дефіцити. Така практика підвищувала стійкість системи й знижувала ризик зриву постачання навіть у разі втрати складу або транспортного вузла.

Паралельно розвивалася концепція розосередження логістичних об'єктів. Склади почали розміщувати з урахуванням маскування, інженерного захисту та доступності для використання в операціях. Важливу роль відігравало будівництво захисних споруд та застосування засобів приховування від розвідки противника.

Не менш значущим було гнучке планування перевезень. Вперше розпочалися спроби враховувати оперативну обстановку при виборі маршрутів. Хоча мультимодальні перевезення тоді ще не стали масовою практикою, ця тенденція заклала основу для їхнього майбутнього розвитку.

Важливим напрямом була цифровізація. Запровадження перших програмних модулів для обліку запасів та контролю їхнього переміщення дало змогу командирам отримувати більш точну картину стану забезпечення. Хоча ці системи залишалися фрагментарними, вони формували підґрунтя для створення єдиної інформаційної платформи.

Міжнародний компонент також набув нового значення. Україна почала адаптувати базові стандарти НАТО у сфері маркування, пакування та транспортування. Це давало змогу поступово інтегрувати національну логістику у євроатлантичний простір і готувало систему до отримання та розподілу міжнародної допомоги.

Таким чином, період ООС (2018–2021) став фазою закріплення перших реформ та їхнього часткового систематизування. Логістика перестала бути лише "обслуговуючим елементом" і перетворилася на один із ключових чинників оперативного планування. Попри обмеженість ресурсів і проблеми з транспортом та цифровізацією, цей етап підготував армію до масштабних викликів повномасштабної війни [6].

Російське вторгнення у лютому 2022 року стало безпрецедентним викликом для системи тилового забезпечення. Якщо у попередні роки логістика була зосереджена на підтриманні локалізованих операцій на сході, то тепер вона мала одночасно забезпечувати кілька великих угруповань військ, розгорнутих на віддалених операційних напрямках. Масштабність і багатовекторність бойових дій остаточно зруйнували можливості функціонування навіть частково реформованої централізованої моделі.

Першим викликом стали масовані удари високоточною зброєю, дронами-камікадзе та диверсійними групами по великих складах і логістичних вузлах. Втрата одного об'єкта могла паралізувати постачання на цілому фронті, що підкреслило критичну вразливість централізованої системи. У відповідь командування розпочало перехід до децентралізованої мережі мобільних хабів та передових пунктів забезпечення, які наближалися до районів бойових дій.

Мобільні хаби стали ключовим інструментом нової архітектури тилу. Вони могли швидко змінювати місце дислокації, ускладнюючи ворожу розвідку, та скорочували час доведення ресурсів до підрозділів. Це ало змогу підвищити темп постачання та зменшити залежність від окремих великих складів.

Водночас така децентралізація мала свої труднощі. Вона потребувала більшої кількості транспорту, додаткового персоналу для обслуговування нової мережі й чіткої координації між різними рівнями управління. Крім того, збільшення кількості логістичних об'єктів підвищувало ризики витоку інформації та ускладнювало захист комунікацій.

Попри це, стратегічно децентралізація виправдала себе. Вона дала можливість підвищити гнучкість, стійкість і живучість тилу в умовах масованого вогневого впливу. Саме на базі децентралізованої структури почали вибудовуватися наступні напрями реформ: мультимодальні перевезення, інтеграція міжнародної допомоги, цифровізація та використання новітніх технологій [18, 19, 21].

Децентралізація тилової системи, запроваджена у перші місяці повномасштабної війни, створила передумови для розвитку мультимодальних перевезень. Якщо у попередні роки транспорт ЗС України здебільшого спирався на автомобільні засоби, то з 2022 року виникла потреба у поєднанні різних видів транспорту. Це дало змогу зменшити залежність від одного каналу, створювати резервні маршрути та підвищувати живучість постачання.

Залізничний транспорт залишався основним засобом для переміщення великих партій вантажів на далекі відстані. Його перевагою була висока пропускна здатність і відносна швидкість доставки, однак руйнування мостів, станцій чи колій робило залізницю вразливою для противника. Автомобільний транспорт виступав гнучкою ланкою, яка з'єднувала залізничні вузли з мобільними хабами та передовими підрозділами, забезпечуючи "останню милю" доставки.

Особливе значення у цей період набуло використання річкового транспорту, особливо на південних напрямках. Це давало змогу розвантажувати автомобільні маршрути, створювати альтернативні логістичні коридори та зберігати функціональність системи навіть у випадках блокування основних сухопутних шляхів. У критичних ситуаціях застосовувалася авіаційна доставка невеликих, але життєво важливих вантажів – медичних засобів, деталей для ремонту техніки чи боєприпасів для спеціалізованих підрозділів.

Мультимодальність підвищувала стійкість логістики. Одночасне використання кількох каналів створювало альтернативні маршрути та ускладнювало завдання противника з їх блокування. Крім того, це давало змогу оптимізувати ресурси: великі партії вантажів транспортувалися залізницею, а автомобілі забезпечували швидке довезення на коротких відстанях.

Важливим доповненням стала практика резервування транспортних потужностей. Командування заздалегідь передбачало альтернативні маршрути та у разі потреби залучало цивільних перевізників. Це створювало багаторівневу систему доставки, здатну функціонувати навіть за умов системного вогневого впливу противника.

Таким чином, мультимодальні перевезення стали логічним продовженням децентралізації тилу. Вони дали змогу поєднати гнучкість, мобільність і стійкість транспортної системи, підготувавши підґрунтя для інтеграції масштабної міжнародної допомоги [11, 19, 24].

З початком широкомасштабної війни одним із ключових чинників виживання української армії стала міжнародна допомога. Масові поставки озброєння, техніки, боєприпасів і матеріально-технічних засобів із країн-партнерів створили безпрецедентні виклики для тилових структур. Українська логістика мусила не лише розширювати масштаби діяльності, а й перебудовуватися за новими правилами, сумісними з міжнародними стандартами.

Першочерговим завданням стало формування системи прийому та розподілу іноземних вантажів. Для цього створювалися спеціалізовані хаби на західному кордоні та у центральних регіонах України. У цих пунктах

здійснювалося сортування, маркування та перенаправлення ресурсів у зони бойових дій. Важливим досягненням стало поєднання військових і цивільних каналів транспортування, що дало змогу значно підвищити пропускну здатність.

Другим важливим аспектом була стандартизація. Для уникнення плутанини та дублювання процедур Україна почала впроваджувати правила НАТО у сфері пакування, маркування, транспортування й обліку вантажів. Єдині стандарти давали змогу створити наскрізний цикл постачання, у якому ресурси могли швидко переходити з цивільних у військові канали. Це забезпечило прозорість та контрольованість потоків навіть в умовах високої динаміки бойових дій.

Не менш значущим стало впровадження цифрових платформ для моніторингу міжнародних поставок. Єдині електронні бази даних давали змогу відстежувати рух вантажів від моменту їх прибуття до кінцевої передачі військовим підрозділам. Це зменшувало ризики втрат, запобігало дублюванню та підвищувало точність планування.

Важливу роль відіграли навчальні та тренувальні програми за участю іноземних партнерів. Військовослужбовці тилових структур проходили підготовку за стандартами НАТО, що забезпечувало сумісність процедур і прискорювало адаптацію до нової логістичної культури.

Таким чином, інтеграція міжнародної допомоги стала подвійним процесом: з одного боку, вона забезпечувала ресурсну підтримку армії, а з іншого - була каталізатором глибоких системних реформ. Завдяки цьому українська логістика не лише вистояла в умовах масованих бойових дій, а й зробила важливий крок до інтеграції у євроатлантичний безпековий простір [5, 11, 20, 21].

У 2022–2023 рр. українська логістика отримала новий імпульс розвитку завдяки активному впровадженню безпілотних літальних апаратів (БпЛА) та наземних роботизованих комплексів. Якщо спершу ці технології застосовувалися переважно для розвідки та вогневого ураження, то з часом вони стали органічним елементом системи постачання, підвищуючи її ефективність і безпеку.

БпЛА виконували кілька критично важливих завдань. *По-перше*, вони забезпечували розвідку маршрутів постачання, даючи змогу виявляти небезпеки ще до виходу транспортних колон. *По-друге*, безпілотники здійснювали моніторинг руху вантажів у реальному часі, що покращувало координацію та дало змогу оперативно змінювати маршрути. *По-третє*, вони стали засобом доставки невеликих, але стратегічно важливих ресурсів - медикаментів, деталей для ремонту техніки, боєприпасів для спеціалізованих підрозділів.

Наземні роботизовані комплекси також знайшли своє місце у тиловій сфері. Їх використовували для завантаження, транспортування та сортування матеріальних засобів на складах, які перебували під постійною загрозою обстрілів. Роботизовані платформи могли доставляти боєприпаси чи пальне на короткі дистанції у небезпечних зонах, мінімізуючи ризики для особового складу.

Упровадження цих технологій стало можливим завдяки створенню цифрової інфраструктури управління. БпЛА та роботизовані системи інтегрувалися у єдині платформи моніторингу, що дало змогу синхронізувати логістичні операції з оперативними планами командування. Такий підхід мінімізував хаотичність і забезпечував більш ефективне використання ресурсів.

Особливе значення мало партнерство з іноземними державами й оборонними компаніями. Частина платформ надходила у вигляді міжнародної допомоги, інші – розроблялися українськими підприємствами за участі партнерів. Це сприяло розвитку вітчизняного оборонно-промислового комплексу й водночас давало армії можливість швидко адаптуватися до технологічних інновацій.

Таким чином, інтеграція БпЛА та роботизованих комплексів стала одним із ключових етапів модернізації тилового забезпечення. Вона знизила ризики для особового складу, скоротила час доставки та відкрила шлях для ширшого впровадження автоматизованих і цифрових рішень у логістиці [8, 16, 21].

Подальший розвиток тилових структур у 2022–2025 роках показав, що сучасна логістика не може існувати без надійної цифрової інфраструктури та захисту інформаційних систем. Противник активно використовував кібератаки для викрадення даних про склади й маршрути або для спотворення інформації, що створювало ризик зриву постачання. У відповідь Україна розпочала формування багаторівневої системи кіберзахисту, яка мала забезпечити стійкість

цифрових платформ навіть під час масованого кібернетичного тиску.

Одним із ключових рішень стало впровадження багатоступеневого шифрування каналів зв'язку та принципу "мінімізації доступу", коли кожен користувач отримував лише необхідний обсяг інформації. Паралельно проводилися регулярні аудити, стрес-тести та *red-team* перевірки, що давало змогу своєчасно виявляти слабкі місця в інформаційних системах.

Цифровізація значно розширила можливості управління ресурсами. Використання RFID-міток і GPS-контролю дало змогу відстежувати рух вантажів у реальному часі, знижувати ризик втрат і швидко реагувати на зміни обстановки. Автоматизовані системи обліку забезпечували командирам інтегровану картину логістичних потоків, що робило ухвалення рішень оперативнішим і точнішим.

Новим кроком стала інтеграція алгоритмів штучного інтелекту (ШІ). Вони давали змогу прогнозувати потреби залежно від інтенсивності бойових дій, визначати оптимальні маршрути та виявляти потенційні ризики. Важливим інструментом стали також цифрові близнюки складів і транспортних коридорів, що давали змогу моделювати сценарії розвитку подій і завчасно готувати резервні рішення.

Поєднання цифрових технологій та кіберзахисту сформувало концепцію "розумної логістики". Вона базувалася на моніторингу, прогнозуванні й управлінні у режимі реального часу, що значно підвищувало адаптивність тилової системи. Саме цей рівень розвитку дав змогу перейти до наступного пріоритету – посилення живучості логістичних структур, які залишалися головною мішенню для противника [9, 14, 16, 19].

В умовах повномасштабної війни тилові об'єкти перестали бути віддаленим і відносно безпечним елементом військової системи. Склади, транспортні вузли та колони стали одними з головних цілей противника. Це змусило командування докорінно змінити підхід до організації тилу, зробивши його живучість і захищеність ключовими критеріями функціонування.

Першим принципом підвищення стійкості стало розосередження. Великі склади замінювалися мережею менших мобільних логістичних пунктів, які регулярно змінювали місце дислокації. Це ускладнювало роботу ворожої розвідки та мінімізувало ризик одночасної втрати значних обсягів запасів.

Другим напрямом виступав інженерний захист. Для пального й боєприпасів облаштовували укриття, бетонні бар'єри та заглиблені сховища. Активно застосовувалися засоби маскування, теплові та радіолокаційні пастки. Поширеною практикою стало створення хибних складів і колон, що відволікали увагу противника та знижували ризики для реальних тилових вузлів.

Окремим завданням був захист транспортних колон. Для перевезення критичних вантажів використовувалася броньована техніка, вводився збройний супровід, а маршрути та графіки руху постійно змінювалися. Попереднє розмінування небезпечних ділянок і контроль за можливими точками запуску дронів-камікадзе додатково підвищували безпеку перевезень.

Важливе значення мала підготовка особового складу тилових підрозділів. Військовослужбовці навчалися діям під час обстрілів, організації укриттів, протидії атакам дронів і диверсійних груп. Їх забезпечували засобами індивідуального захисту та проводили регулярні тренування, що підвищувало не лише фізичну, а й морально-психологічну стійкість.

У результаті живучість тилу стала комплексним завданням, що поєднувало організаційні, інженерні, тактичні та технологічні заходи. Логістика фактично перетворилася на "фронтовий елемент", де здатність діяти під ударами противника визначала боєздатність армії не менше, ніж успіх бойових підрозділів [17,18,22].

Досвід 2022–2023 рр. показав, що навіть найефективніші військові рішення не здатні повністю задовольнити потреби фронту у війні високої інтенсивності. Високі темпи бойових дій, втрати техніки та постійні удари по транспортній інфраструктурі зумовили необхідність широкомасштабного залучення цивільних ресурсів до системи військової логістики.

Насамперед це стосувалося транспортної сфери. Приватні автомобільні перевізники, залізничні компанії, річкові та авіаційні оператори активно інтегрувалися у військову систему. Завдяки цьому вдалося створити багатоканальну мережу доставки, де цивільні маршрути доповнювали військові й підвищували загальну гнучкість та живучість логістики. Використання портів, аеропортів та великих логістичних центрів дало змогу

значно збільшити пропускну спроможність тилу.

Не менш важливою була уніфікація стандартів. Для ефективної взаємодії впроваджувалися єдині правила пакування, маркування, транспортування та обліку вантажів відповідно до норм НАТО. Це створювало єдиний цикл постачання, де ресурси могли швидко переходити з цивільних каналів у військові без затримок.

Значущою складовою інтеграції був і людський ресурс. Водії, інженери, логісти, оператори цифрових систем із цивільного сектору долучалися до роботи у військових структурах. Це допомагало компенсувати кадровий дефіцит і водночас приносило у військове середовище сучасні методи управління ланцюгами постачання. Спільна робота з приватними компаніями сприяла впровадженню інновацій, які у традиційній армійській практиці поширювалися значно повільніше.

Міжнародний вимір інтеграції також мав важливе значення. Частина поставок озброєння і техніки здійснювалася через цивільні компанії країн-партнерів. Це потребувало гармонізації стандартів і процедур між військовими та цивільними структурами різних держав, фактично перетворюючи українську логістику на багатонаціональну систему.

Таким чином, інтеграція цивільних і військових спроможностей із допоміжного заходу перетворилася на системний компонент тилу. Вона розширила ресурсну базу, зменшила залежність від вузьких каналів постачання та підвищила стійкість системи. Саме цей досвід підготував основу для наступного кроку – адаптації кращих міжнародних практик США, НАТО та Ізраїлю [18, 24].

Інтеграція цивільних і військових спроможностей в Україні створила передумови для глибшого використання міжнародного досвіду. У цей період особливого значення набули підходи, які напрацювали провідні армії світу – США, країни-члени НАТО та Ізраїль. Їхні моделі стали практичними орієнтирами для розвитку української логістики у війні високої інтенсивності.

Американська модель військової логістики вирізняється глобальним характером. США створили систему передового розміщення запасів і стратегічних баз у різних регіонах світу, що забезпечує оперативність перекидання сил. Центральне місце у цій системі посідає доктрина *Joint Logistics* (JP 4-0), яка передбачає інтеграцію всіх видів і родів військ у єдину логістичну мережу. Особливо цінним для України є досвід застосування автоматизованих платформ, здатних відстежувати стан запасів у реальному часі та прогнозувати потреби, що суттєво скорочує цикл ухвалення рішень [6, 12]

НАТО виробило концепцію “єдиного логістичного простору”, яка ґрунтується на стандартизації, мультимодальності та взаємній підтримці держав-членів. Висока уніфікація процедур маркування, пакування й транспортування забезпечує сумісність національних систем, а механізми сертифікації гарантують дотримання єдиних вимог. Для України цей досвід став ключовим у процесі інтеграції міжнародної допомоги та взаємодії з партнерами. Адаптація стандартів НАТО дала змогу уникнути дублювання процесів, підвищити прозорість логістичних потоків і знизити ризики втрат [5, 11, 20].

Ізраїльський досвід демонструє ефективність поєднання військових і цивільних ресурсів у середовищі постійних загроз. Армія оборони Ізраїлю робить ставку на високий рівень інженерного захисту складів, використання роботизованих систем та швидке відновлення тилових структур після атак. Для України особливо цінними стали практики будівництва укріплених складів, застосування хибних об’єктів і відпрацювання схем відновлення постачання у випадку руйнувань [8].

Порівняльний аналіз різних моделей організації військової логістики засвідчив, що надмірна централізація формує критичні системні вразливості, тоді як розосереджені мережеві структури істотно підвищують стійкість тилу в умовах сучасної війни. Поєднання цифрових інструментів управління, уніфікованих стандартів і залучення цивільних ресурсів забезпечує формування багаторівневої, адаптивної та витривалої логістичної системи, здатної ефективно функціонувати за умов високої інтенсивності бойових дій і нестабільного середовища безпеки [21].

Узагальнення національного та міжнародного досвіду переконливо довело, що розвиток військової логістики не може мати хаотичного або суто реактивного характеру. Ефективне тилове забезпечення потребує системного підходу, чіткої внутрішньої логіки організації процесів, визначених функціональних пріоритетів і

зрозумілих критеріїв оцінювання результатів. Саме така системність дає змогу поєднати поточні потреби фронту з довгостроковими завданнями оборонного розвитку в умовах війни високої інтенсивності та післявоєнної трансформації сектору безпеки [18, 20].

Ключову роль у модернізації тилового забезпечення відіграли організаційні рішення. Насамперед було обґрунтовано доцільність переходу від стаціонарної складської моделі до мережі мобільних логістичних елементів, здатних оперативно змінювати місце розташування залежно від обстановки. Такі структури забезпечували одночасно швидкість доставки, гнучкість управління та розосередження ресурсів, що суттєво знижувало їхню вразливість. Важливим методологічним орієнтиром став принцип "sustainment-first", відповідно до якого логістичні можливості враховуються ще на етапі планування операцій, що унеможливлює реалізацію завдань, не підкріплених реальними ресурсами [6].

Вагомим чинником підвищення ефективності логістики стала технологічна трансформація. Пріоритетним напрямом визначалося створення інтегрованої цифрової системи обліку й моніторингу матеріально-технічних засобів із використанням RFID-міток, штрих-кодування та GPS-контролю. Це забезпечувало наскрізну простежуваність руху ресурсів від центральних складів до бойових підрозділів. Подальший розвиток цифрових рішень передбачав застосування алгоритмів штучного інтелекту для прогнозування потреб залежно від інтенсивності бойових дій, оптимізації маршрутів постачання та виявлення потенційних ризиків. Використання цифрових моделей складів і транспортних коридорів давало змогу моделювати альтернативні сценарії, оцінювати пропускну спроможність та вразливість логістичної мережі [21].

Не менш значущим напрямом стала безпекова складова. В умовах війни високої інтенсивності логістичні структури перетворилися на пріоритетні цілі для вогневого ураження й диверсій, що зумовило необхідність системного підходу до їх захисту. Застосовувалися заходи з організації озброєного супроводу колон, маскування та інженерного укріплення складів, використання змінних маршрутів і гнучких графіків руху. У сфері кібербезпеки впроваджувалися обов'язкові процедури захисту, багаторівнева автентифікація доступу та регулярні перевірки із залученням red-team-підрозділів, які імітували реальні кібератаки [16].

Важливою складовою трансформації тилу стали нормативно-правові зміни. Актуалізація національної правової бази здійснювалася з урахуванням стандартів НАТО й охоплювала не лише технічні вимоги до маркування чи пакування, а й правила взаємодії між військовими та цивільними перевізниками, уніфікацію документообігу та чітке розмежування зон відповідальності між суб'єктами логістичної діяльності [5].

Системний розвиток військової логістики неможливий без комплексного управління ризиками. Досвід війни 2014–2025 рр. переконливо засвідчив, що навіть добре організовані логістичні рішення залишаються вразливими під впливом як об'єктивних, так і суб'єктивних чинників. До них належать ресурсні обмеження, кадровий дефіцит, руйнування транспортної інфраструктури, кіберзагрози та асиметричний вогневий вплив противника [18, 19]. Усвідомлення цих загроз і формування механізмів їх мінімізації стало одним із ключових завдань сучасної логістики.

Однією з найбільш проблемних залишалася фрагментація даних. Використання розрізнених інформаційних систем ускладнювало інтеграцію процесів і уповільнювало ухвалення управлінських рішень. Подолання цього ризику потребувало переходу до уніфікованих цифрових рішень із централізованими довідниками та модульною архітектурою.

Суттєвим викликом був кадровий дефіцит. Високі темпи бойових дій, втрати особового складу та конкуренція з цивільним сектором зумовлювали нестачу підготовлених логістів, IT-фахівців і технічних спеціалістів. Реакцією на це стали спеціалізовані освітні програми, партнерство з університетами та впровадження системи довгострокових стимулів для військовослужбовців тилових підрозділів [22].

Окрему групу ризиків формувала вразливість транспортної інфраструктури. Руйнування мостів, вузлових станцій або логістичних центрів могло блокувати критично важливі напрямки постачання. Для зменшення цього ризику застосовувалися резервні маршрути, тимчасові переправи, річкові перевезення та залучення цивільних транспортних потужностей.

Кіберзагрози набули особливої актуальності, оскільки атаки на інформаційні

системи могли призводити не лише до витоку даних, а й до спотворення маршрутів чи обсягів вантажів. Для мінімізації таких ризиків впроваджували багаторівневий кіберзахист, сегментацію мереж і регулярні перевірки стійкості систем [16].

Додаткову небезпеку становили масовані удари високоточною зброєю та атаки безпілотних систем на логістичні вузли. Відповіддю на ці загрози стали розосередження складів, створення мобільних логістичних елементів, інженерний захист, використання хибних об'єктів і формування команд швидкого відновлення.

Не менш значущими були політичні та економічні ризики, пов'язані з обмеженістю фінансових ресурсів, залежністю від міжнародної допомоги й можливими змінами політичних пріоритетів. Їх мінімізували шляхом сценарного планування фінансування та розробки рішень подвійного призначення, придатних як для військових потреб, так і для післявоєнного відновлення економіки.

Таким чином, управління ризиками стало невід'ємною складовою розвитку військової логістики, забезпечуючи її стійкість, адаптивність і здатність до безперервного функціонування в умовах війни. Логічним продовженням цього процесу стало формування системи оцінки ефективності, яка давала змогу кількісно вимірювати результати діяльності тилу та оперативно коригувати управлінські рішення.

Ефективність логістичної системи у війні високої інтенсивності не може оцінюватися виключно на основі інтуїтивних суджень. Для цього необхідна система кількісних і якісних показників, здатна об'єктивно відображати результативність процесів і виявляти їхні слабкі місця. У 2022–2025 рр. в українських Силах оборони поступово сформувалася практика використання ключових показників ефективності (KPI) як основного інструмента моніторингу розвитку логістики [18, 21].

Найбільш значущим показником залишався середній час доведення матеріальних засобів від складу до підрозділу, який безпосередньо впливав на боєздатність військ. Важливим індикатором стала простежуваність ресурсів — частка вантажів, що відстежувалися в режимі реального часу за допомогою цифрових засобів [11]. Окрему роль відігравали показники розосередження запасів і час відновлення складів після ураження, які характеризували живучість тилової мережі. До групи безпекових індикаторів належали рівень кіберінцидентів, втрати вантажів на тонно-кілометр перевезень і кількість успішно відбитих атак, зниження яких свідчило про підвищення стійкості логістичної системи [16].

Не менш важливим KPI була готовність резервів – матеріальних і транспортних. Високий рівень цього показника забезпечував війську можливість негайно реагувати на непередбачувані виклики.

Запровадження KPI давало змогу створити багаторівневу систему моніторингу: тактичний рівень працював через дашборди реального часу, оперативний – через щотижневі огляди, стратегічний – через квартальні аудити. Так формувався замкнений цикл управління:

дані → аналіз → рішення → зміни

У підсумку система KPI перетворилася з формального інструмента на реальний механізм управління. Вона забезпечувала прозорість, підвищувала довіру між рівнями командування й створювала умови для гнучкого коригування діяльності. Це стало логічним завершенням попередніх етапів розвитку й підготувало основу для узагальнення висновків про роль логістики у сучасній війні. Аналіз досвіду 2014–2025 рр. дає змогу не лише окреслити досягнення, а й сформулювати ключові напрями подальшого розвитку логістики Збройних Сил України. Вони мають базуватися на інтеграції національних і міжнародних практик, враховувати сучасні технологічні тренди та особливості війни високої інтенсивності [1, 19].

Першим і найбільш очевидним напрямом є подальша цифровізація та автоматизація процесів управління. Створення єдиної інтегрованої цифрової платформи, яка охоплюватиме облік, транспортування, прогнозування потреб і управління ризиками, є стратегічним завданням. Вона має мати модульну архітектуру та відповідати стандартам НАТО [5].

Другим напрямом визначається розвиток мобільної та мережевої архітектури тилу. Логістика повинна остаточно відмовитися від централізованої моделі та базуватися на гнучких мережах мобільних хабів, здатних змінювати місце дислокації залежно від оперативної ситуації.

Третім пріоритетом є інтеграція інноваційних технологій: застосування штучного інтелекту для прогнозування,

цифрових близнюків для моделювання, а також широке використання роботизованих платформ і безпілотних систем. Це мінімізує ризики для особового складу та оптимізує управління потоками ресурсів.

Четвертим напрямом є поглиблення співпраці з цивільним сектором. Використання національних транспортних та інфраструктурних потужностей, залучення фахівців і методів приватного бізнесу розширює можливості тилу й забезпечує основу для системи подвійного призначення у післявоєнний час.

П'ятим ключовим вектором виступає посилення міжнародної інтеграції. Україна повинна не лише адаптувати стандарти НАТО, а й включатися у багатонаціональні програми з розвитку логістики та навчання персоналу [21]. Це гарантує сумісність з союзниками та підвищує роль держави у глобальній системі безпеки.

Нарешті, *шостим напрямом* є системне управління ризиками й розвиток культури безпеки. Йдеться про резервування маршрутів, удосконалення інженерного захисту, впровадження кіберстійкості та створення механізмів швидкого відновлення об'єктів після атак.

Висновки. У статті окреслено досягнення і сформульовано ключові напрями подальшого розвитку логістики Збройних Сил України.

Усі зазначені напрями в комплексі формують стратегічне бачення: військова логістика України має стати мобільною, технологічно розвиненою, інтегрованою з цивільними та міжнародними системами й стійкою до багатовекторних загроз. Лише така модель здатна гарантувати ефективність у війні високої інтенсивності та забезпечити обороноздатність держави у довгостроковій перспективі.

Узагальнення досвіду логістичного забезпечення угруповань військ Збройних Сил України та проведений аналіз сучасних тенденцій дають змогу визначити низку перспективних напрямів для **подальших досліджень**. Вони спрямовані на посилення адаптивності логістичної системи, її технологічне оновлення та інтеграцію з міжнародними стандартами, що особливо важливо в умовах війни високої інтенсивності та гібридних загроз.

Першим із таких напрямів виступає розвиток цифрових платформ управління та впровадження штучного інтелекту у логістичні процеси. Подальші дослідження мають зосередитися на створенні цифрових «близнюків» логістичних мереж, розробці алгоритмів прогнозування потреб та оптимізації маршрутів постачання. Інтеграція військових та цивільних інформаційних систем у єдину платформу управління дасть змогу досягти наскрізної прозорості та мінімізувати фрагментацію даних, що нині є однією з найсуттєвіших проблем.

Другим перспективним напрямом є забезпечення кіберстійкості логістичних структур. Метою досліджень повинно стати моделювання можливих сценаріїв кібератак, оцінка ефективності існуючих механізмів захисту та розроблення нових протоколів реагування. Особливого значення набуває впровадження блокчейн-рішень для підтвердження достовірності даних, а також багаторівневих систем автентифікації, здатних гарантувати захист у режимі реального часу.

Третій напрям охоплює проблематику живучості тилових об'єктів. Важливим є визначення оптимального рівня розосередження складів, впровадження модульних укриттів, інтеграція систем активної протидії безпілотникам і ракетним ударам. У цьому контексті потребують окремих досліджень питання швидкого відновлення логістичної інфраструктури після ураження, у тому числі з використанням мобільних ремонтно-відновлювальних команд і державно-приватного партнерства.

Четвертий напрям пов'язаний із взаємодією військової та цивільної логістики. Перспективними є дослідження сценаріїв державно-приватного партнерства, формування нормативно-правових механізмів швидкої мобілізації цивільних транспортних та інфраструктурних ресурсів, а також аналіз економічної ефективності гібридних моделей постачання. Це дає змогу створити більш стійку й багатоканальну систему забезпечення, яка здатна функціонувати навіть у випадку руйнування окремих військових каналів.

П'ятим напрямом є подальше порівняльне вивчення міжнародного досвіду. Дослідження мають охоплювати не лише практики США, НАТО чи Ізраїлю, але й досвід держав, які перебували в умовах зовнішньої загрози й обмежених ресурсів (Польща, Литва, Південна Корея). Такий аналіз дасть змогу виробити найбільш придатні для України моделі, поєднавши їх із власними напрацюваннями.

Шостим напрямом виступає проблема людського фактора. Необхідні дослідження,

присвячені кадровій політиці у сфері військової логістики: від підготовки спеціалістів і розроблення програм професійного зростання до системи мотивації та психологічної стійкості особового складу. Логістика як критичний елемент бойового потенціалу потребує висококваліфікованих кадрів, здатних працювати в умовах постійної загрози.

Нарешті, *сьомим* напрямом слід назвати логістику в умовах багатодоменних операцій. Сучасна війна потребує інтегрованої підтримки не лише сухопутних сил, але й морського, повітряного, кібер- та космічного компонентів. Подальші дослідження повинні визначити стандарти взаємодії між цими середовищами, а також розробити уніфіковані процедури управління матеріальними потоками у багатовимірному просторі бою.

Таким чином, напрями подальших досліджень формують основу наукової програми, що має стратегічне значення для Збройних Сил України. Їх реалізація сприятиме створенню логістичної системи, здатної не лише витримувати тиск сучасної війни, а й інтегруватися у глобальну систему колективної безпеки, що є запорукою довгострокової обороноздатності держави.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Міністерство оборони України. Біла книга Збройних Сил України 2014–2021. Київ : МОУ, 2022. 256 с.
2. Генеральний штаб ЗСУ. Оборонний бюлетень України. Київ : МОУ, 2020. 198 с.
3. Воронін С. А. Логістика в системі забезпечення обороноздатності держави // Збірник наукових праць Національного університету оборони України. 2021. № 2. С. 45–61.
4. Ліпкан В. А. Національна безпека України: теорія і практика. Київ : КНТ, 2020. 480 с.
5. NATO Standardization Office. Allied Joint Doctrine for Logistics (AJP-4). Brussels: NATO, 2018. 140 p.
6. U.S. Department of Defense. Joint Publication 4-0: Joint Logistics. Washington D.C. : Joint Chiefs of Staff, 2019. 112 p.
7. RAND Corporation. Cohen R., Wilson J. Military Logistics in Integrated Operations. Santa Monica, 2019. 210 p.
8. Ministry of Defense of Israel. Logistics in the Israel Defense Forces: Doctrinal Foundations. Tel Aviv : MOD, 2020. 96 p.
9. Баранник В. В., Кривонос Р. А. Цифровізація оборонної логістики: сучасні тенденції та виклики // Наука і оборона. 2022. № 1. С. 33–47.
10. Глущенко В. І. Інноваційні підходи до управління військовими ресурсами // Вісник НАСБУ. 2021. № 3. С. 22–39.
11. NATO Allied Command Transformation. NATO Logistics Handbook. Norfolk, VA : NATO HQ, 2020. 178 p.
12. Department of the Army (U.S.). ATP 4-0: Sustainment. Washington D.C. : Headquarters, 2019. 354 p.
13 Матвієнко О. Л. Системи управління ризиками у військовій логістиці // Стратегічні пріоритети. 2022. № 4. С. 58–71.
14 Коваленко Д. М. Інформаційна безпека тилових структур: виклики та перспективи // Право і безпека. 2022. Т. 31. № 2. С. 113–127.
15. International Institute for Strategic Studies (IISS). The Military Balance 2023. London : Routledge, 2023. 504 p.
16. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Cybersecurity of Military Logistics. Tallinn : NATO CCDCOE, 2021. 84 p.
17. Служба безпеки України. Аналітична довідка: захист тилових структур у сучасних умовах війни. Київ : СБУ, 2023. 42 с.
18. Міністерство оборони України. Оборонний огляд 2024. Київ : МОУ, 2024. 210 с.
19. Центр воєнно-стратегічних досліджень НУОУ. Військова логістика у війні високої інтенсивності: досвід України 2022–2024 рр. Київ : НУОУ, 2024. 176 с.
20. NATO Defence College. Resilient Military Logistics in Hybrid Warfare. Rome : NATO DC, 2024. 95 p.
21. RAND Corporation. Ukraine’s Logistics Transformation in Full-Scale War. Santa Monica : RAND, 2024. 152 p.
22. Генеральний штаб ЗСУ. Звіт про стан та розвиток тилового забезпечення ЗСУ у 2024–2025 рр. Київ : МОУ, 2025. 134 с.
23 International Institute for Strategic Studies (IISS). The Military Balance 2025. London : Routledge, 2025. 520 p.
24. NATO Support and Procurement Agency (NSPA). Annual Report 2025. Capellen, Luxembourg : NSPA, 2025. 88 p.

Стаття надійшла до редакції 17.09.2025

Logistical support of groupings of troops (forces) of the Armed Forces of Ukraine: experience, challenges, and directions for improvement

Annotation

Modern warfare has radically transformed the role of logistics in the art of war, elevating it from a secondary function to a strategic factor that directly determines the tempo and effectiveness of combat operations. The scientific and practical significance of this issue lies in the fact that the level of logistics

development directly affects the duration of defence, the feasibility of offensive plans, the ability to reduce losses, and the optimization of the use of limited resources.

The empirical basis of the study comprises real-world practices of logistical support developed during the Anti-Terrorist Operation (ATO) and the Joint Forces Operation (JFO) in 2014–2021, as well as the experience gained during the full-scale war since 2022. These periods make it possible to trace the evolution from a crisis state of rear support, largely reliant on volunteer assistance, to the gradual formation of a more flexible system that integrates elements of automation, multimodal transportation, and international support.

The purpose of the article is to conduct a systematic analysis of the logistical support of troop groupings over the period 2014–2025, identify its key problems and vulnerabilities, generalize international experience, and formulate proposals capable of enhancing the resilience and effectiveness of rear support in a high-intensity war.

The article outlines the achievements attained and formulates the key directions for the further development of logistics in the Armed Forces of Ukraine.

Taken together, these directions form a strategic vision according to which Ukraine's military logistics should become mobile, technologically advanced, integrated with civilian and international systems, and resilient to multi-vector threats. Only such a model can ensure effectiveness in high-intensity warfare and safeguard the state's defence capability in the long term.

Keywords: Armed Forces of Ukraine; military logistics; rear support; mobility; flexibility; resilience; multimodality; digitalization; automation of accounting; cybersecurity; integration of civilian resources; mobile logistics hubs; artificial intelligence in logistics.

УДК: 35.355/359 https://doi.org/10.33099/2304-2745/2025-3-86/128-137

Касьян С. П., кандидат педагогічних наук, доцент (0000-0001-7310-233X)
Факадей О. Р., кандидат військових наук (0000-0002-2965-9613)
Безбах В. С., кандидат військових наук, доцент (0009-0000-0417-900X)
Працков С. А. (0009-0000-0417-900X)

Інститут державного військового управління Національного університету оборони України, Київ

Методологічні та концептуальні аспекти побудови перспективних пунктів управління

Резюме. У статті запропоновано напрями побудови перспективних пунктів управління з врахуванням забезпечення їх живучості мобільності та взаємозамінності. Показано, що впровадження хмарних технологій в систему оброблення та зберігання інформації пункту управління створює єдиний інформаційний простір та умови для інтеграції з коаліційними мережами, тоді як edge-обчислення (будь-який обчислювальний вузол між джерелом даних і центральною "хмарою") забезпечують безперервність управління в умовах обмеженого зв'язку.

Ключові слова: пункти управління; живучість; ефективність управління; хмарні технології; віртуальна та доповнена реальність; ІТ-фахівці; маскування та камуфляж; ситуативна обізнаність.

Постановка проблеми. Досвід проведення операцій в ході відбиття збройної агресії РФ проти України свідчить, що розвиток системи управління, застосування сучасних засобів ураження призвело до суттєвого ускладнення функціонування пунктів управління (ПУ) у процесі планування операції та управління військами під час ведення бойових дій. Розвиток технологій збору та оброблення інформації спричинив, небачене до цього, зростання кількості інформації, яка циркулює у системі управління, що безпосередньо впливає на ефективність управлінських рішень та на час їх вироблення [1]. Ці та інші фактори формують наукову проблему щодо необхідності врахування великої кількості факторів, що впливають на роботу ПУ.

Вирішення цієї наукової проблеми можливе за умови розв'язання протиріччя між ефективністю функціонування усіх елементів ПУ та сучасним середовищем, у якому здійснюється робота ПУ щодо забезпечення планування операції і управління військами під час виконання ними завдань, та необхідністю підвищення живучості ПУ згідно із сучасними вимогами до проведення операції, що динамічно змінюються.

Це протиріччя потребує систематизованого професійного підходу до пошуку шляхів його розв'язання з врахуванням розвитку технологій ведення збройної боротьби на сучасному етапі та обґрунтованого вибору тих перспективних технологій, які могли б максимізувати позитивний ефект від них.

Під час планування операції та управління військами під час виконання поставлених завдань командувач (командир) та оперативний склад ПУ здійснюють свою діяльність в умовах великої апріорної невизначеності і постійного впливу засобів розвідки та вогневого ураження противника на систему управління.

Виникає необхідність пошуку нових шляхів забезпечення функціонування ПУ з метою зменшення ступеня ризику і забезпечення ефективності роботи системи управління в цілому.

Зменшити апріорну невизначеність на етапі планування операції та управління військами під час виконання оперативних завдань можливо за допомогою застосування нових підходів у побудові елементів ПУ, забезпечення живучості та використання сучасних технологій у діяльності оперативного складу ПУ тощо.

Структурні зміни у побудові ПУ, роботі оперативного складу мають бути спрямовані не лише на розвиток окремих підсистем підтримки прийняття рішення, а перш за все, вони мають бути сфокусовані на розвитку усієї інтегрованої сукупності елементів ПУ і на зміни підходів щодо пріоритетності формування оперативного складу ПУ, який має забезпечувати функціонування усіх підсистем забезпечення прийняття рішення на основі новітніх інформаційно-комунікаційних технологій.

Аналіз останніх досліджень і публікацій. Аналіз досліджень щодо функціонування системи ПУ виявив, що основна увага приділялася питанням щодо

стійкості системи управління військами. Цій тематиці присвячені роботи [2–6], але автори не приділяли достатньої уваги питанням застосування новітніх технологій та автоматизованих систем управління в роботі ПУ, у сучасних умовах ведення збройної боротьби та обґрунтованого вибору тих перспективних технологій, які могли б максимізувати позитивний ефект у функціонуванні ПУ.

Ці дослідження надають цінну інформацію про різні аспекти ефективності функціонування ПУ, але залишають певні питання без уваги, що потребує подальших досліджень та вдосконалення.

Мета статті – обґрунтування перспективних напрямів розвитку ПУ як складних систем на основі аналізу залежності ефективності їхніх елементів від рівня живучості, а також оцінка можливостей впровадження сучасних інформаційних технологій для підвищення стійкості управління.

Виклад основного матеріалу. Аналіз сучасних наукових та аналітичних джерел дає змогу стверджувати, що система управління військами є одним із пріоритетних об’єктів ураження противника в умовах сучасних воєнних конфліктів [7, 8]. З огляду на досвід російсько-української війни, противник застосовує багаторівневий та багатодоменний підхід, поєднуючи засоби радіоелектронної боротьби, кібератаки, удари високоточною зброєю по ПУ, а також інформаційно-психологічний вплив. Це підтверджує необхідність розгляду системи управління не лише як технічної системи, але і як складного соціотехнічного комплексу.

Окрім того, сучасні збройні сили характеризуються величезним розмаїттям носіїв бойового потенціалу. Різниця у цільовому призначенні та якісних і кількісних характеристиках озброєння обумовлюють труднощі щодо управління ними під час веденні операцій та забезпечення їх працездатності.

Вирішення означеної проблеми є життєво необхідним фактором виконання оперативних завдань, які можуть бути вирішені лише за допомогою використання науково-методичного апарату, основою якого є системний підхід.

Особливе місце посідає той фактор, що обидві сторони намагаються активно впливати на процес управління. Цей вплив проявляється у створенні власної ефективної системи управління та намаганням дезорганізувати систему управління противника [9].

У системі управління військами живучість ПУ означає здатність підтримувати критичні управлінські функції в умовах ураження, впливу РЕБ чи кібератак. Ефективність функціонування кожного елемента ПУ (оперативного, розвідувального, логістичного, комунікаційного) залежить від загальної стійкості системи, проте ця залежність не є лінійною [10]. Різні елементи мають неоднакову чутливість до зниження живучості: одні зберігають працездатність навіть при значних пошкодженнях, інші ж швидко деградують.

Ефективність управління військами є ключовим чинником досягнення цілей у проведенні операцій. Вона визначається не лише якістю прийняття рішень командуванням, але й здатністю системи управління забезпечувати безперервність, оперативність та стійкість управлінських процесів у складних і динамічних умовах бойових дій. Таким чином, ефективність управління набуває комплексного характеру, поєднуючи організаційні, інформаційні та технічні складові.

У цьому контексті система управління військами є складним, багаторівневим утворенням, яке інтегрує засоби зв’язку, інформаційно-аналітичні підсистеми, алгоритми підтримки прийняття рішень, а також організаційні структури командування. Вона функціонує у багатодоменному середовищі, що включає сухопутний, повітряний, морський, кібернетичний та інформаційний простори, і виступає основним інструментом координації зусиль військ.

Разом з тим, практична реалізація функцій системи управління концентрується на ПУ, які забезпечують матеріально-просторову основу для роботи органів військового управління. Саме ПУ є вузловими елементами, де зосереджуються процеси збору, оброблення та передавання інформації, планування операцій, формування та доведення завдань. Вони поєднують організаційну структуру, засоби зв’язку та автоматизації, що робить їх критично важливими для підтримання ефективності всієї системи управління військами.

Аналіз сучасних наукових та доктринальних джерел свідчить, що ПУ залишаються ключовими елементами системи управління військами, адже саме в їх межах реалізуються основні процеси збору,

оброблення та передавання інформації, планування й координації дій [11].

Структура ПУ у сучасних умовах набуває модульного й розосередженого характеру [12, 13]. Переважає концепція формування кількох функціональних вузлів – оперативного, планувального, розвідувального, логістичного та зв'язку, які можуть функціонувати як єдиний комплекс або в рознесеному форматі. Такий підхід зменшує уразливість від високоточних ударів противника та дає змогу забезпечити стійкість управлінських процесів [14].

Матеріально-технічне обладнання ПУ визначається як критичний чинник їх ефективності. До обов'язкового мінімуму належать: автоматизовані робочі місця, мережеве та комунікаційне обладнання (радіостанції КХ/УКХ, супутникові термінали, системи mesh-зв'язку), генераторні й акумуляторні установки, комплекси захисту інформації та криптографії, серверні ресурси, системи візуалізації даних. Важливим є також забезпечення умов життєдіяльності персоналу (кліматичні системи, освітлення, модульні укриття), що прямо впливає на безперервність роботи [15].

Узагальнюючи означене можна стверджувати, що сучасні ПУ повинні поєднувати мобільність, технологічність і захищеність. Саме гармонійне поєднання цих характеристик дає змогу забезпечити безперервність управління військами та зберегти ефективність системи навіть в умовах багатовимірного впливу противника.

Але разом з тим необхідно константувати той факт, що практично, на сучасному полі бою, з урахуванням кількості засобів розвідки і ураження противника та їх можливості, безпечних місць для розгортання системи ПУ не залишилося. Навіть прикладаючи зусилля для покращення мобільності ПУ, дуже важко приховати електромагнітне випромінювання елементів ПУ та їх масивність (по кількості техніки) при розміщенні чи під час пересування коли змінюється район розгортання.

Такою самою, залишається і потреба командира в інформації щодо усіх аспектів підготовки і ведення операції (бою). Раніше така потреба вирішувалася збільшенням кількості оперативного складу, сьогодні це проявляється в основному за рахунок використання систем підтримки рішення, та інших систем, що необхідні для оброблення інформації. Необхідність виявлення достовірної інформації та візуалізації поля бою, з часом тільки зростала. Але ці інструменти тільки обтяжують мобільність системи управління і в фізичному і в інформаційному сенсі та збільшують можливості щодо її ураження.

При дослідженні ПУ фокусуємо увагу саме за функціональні особливості, виділяючи при цьому функціональні принципи, а саме: мультифункціональності (виконання органами управління кількох функцій), конвергенції (процес об'єднання різних технологій, що призводить до створення нових видів технологій), живучості та розосередженості елементів ПУ в районах розгортання [16, 17].

Мультифункціональність ПУ має забезпечувати здатність щодо управління військами у різних умовах обстановки з можливістю взаємозаміни, при необхідності функцій ПУ, як нижчого так і вищого ієрархічного рівня управління. Окрім того для забезпечення мультифункціональності дуже важлива і така вимога до ПУ, як його мобільність. На сьогодні ПУ сковані управлінськими процесами у тому числі і забезпечення функціонування самого ПУ: розвідка та рекогносцювання районів можливого розгортання ПУ, обладнання його в інженерному відношенні, маскування, охорона та оборона, організація зв'язку і таке інше.

Взаємозамінність ПУ розглядається в сучасній військовій науці як одна з базових властивостей системи управління військами, що безпосередньо впливає на її живучість та стійкість у бою. Дослідження вітчизняних і зарубіжних авторів [18–21] свідчать, що ключовим завданням сучасного командування є забезпечення безперервності управління навіть у разі втрати або ураження одного з пунктів. Саме тому взаємозамінність трактується як комплексна організаційно-технічна властивість системи ПУ, що дає змогу підтримувати критичні функції управління в умовах впливу противника.

Вітчизняні науковці наголошують на необхідності розглядати не окремі ПУ, а всю мережу ПУ, що функціонують на стратегічному, оперативному і тактичному рівнях. Так, запропоновано методичний підхід до аналізу живучості системи ПУ через декомпозицію системи та визначення інтегральних показників стійкості. Взаємозамінність у цьому контексті виступає похідною від живучості, адже дає змогу компенсувати втрату окремих елементів за рахунок резервних і альтернативних вузлів [18]. Окрім того досліджується

взаємозамінність як функція уразливості та організаційних режимів роботи системи управління. Визначено, що ефективність взаємозамінності визначається ступенем стандартизації технічних засобів, наявністю відпрацьованих процедур перемикання й готовністю персоналу діяти у кризових ситуаціях [19].

Організаційна структура ПУ завжди має передбачати основний, альтернативний і командно-спостережний пункт, які здатні дублювати один одного за функціями. Це означає наявність завчасно підготовлених позицій, стандартних процедур і уніфікованого документообігу, що робить можливим безшовний перехід управління [22].

З технічного погляду взаємозамінність базується на інтероперабельності засобів зв'язку і автоматизації. Кожний ПУ повинен мати резервні канали зв'язку (кабельні, радіорелейні, КХ/УКХ, SATCOM, mesh) та стандартизовані протоколи обміну даними, які дають змогу у разі потреби перенести управлінські функції на інший вузол без значних втрат часу [21, 23].

Сучасні війни, передусім російсько-українська війна, а також досвід багатонаціональних операцій НАТО показали, що класична модель основного командного пункту (ОКП) з резервним дублюванням вже не відповідає вимогам часу. Противник отримав можливості швидко виявляти й уражати навіть добре замасковані ПУ завдяки інтегрованим системам розвідки та застосуванню високоточної зброї. У цих умовах виникла потреба у нових підходах до взаємозамінності ПУ.

Першим таким підходом є розосередження і модульність. Замість ПУ, який розгортається в одному районі, пропонується розгортати ПУ за модульним типом, коли ПУ формується декількома меншими модулями, що розосереджені територіально – оперативний, розвідувальний, логістичний, інформаційний [24–28]. Вони можуть працювати як у складі одного майданчика, так і на віддалених позиціях, що знижує ймовірність одночасного знищення всіх критичних елементів і підвищує здатність системи до взаємозамінності: якщо один модуль втрачається, його функції можуть перебрати інші вузли мережі.

Другим сучасним підходом є створення "теплих" і "гарячих" резервних ПУ. Традиційно альтернативний пункт існував як запасна позиція, що розгорталася у випадку втрати основного. Сьогодні дедалі частіше використовуються підходи, коли резервний пункт працює паралельно, але з меншим обсягом функцій, підтримуючи актуальну інформаційну базу й мінімальний склад персоналу. У разі потреби він може миттєво розгорнути повний спектр функцій без суттєвої затримки. Такий "гарячий резерв" забезпечує практично безперервний перехід управління.

Третій підхід пов'язаний із мережевими та цифровими технологіями. Системи управління стають дедалі більш розподіленими, коли інформація зберігається не лише на фізичних носіях ПУ, а й у захищених мережах, доступних з кількох вузлів. Це дає змогу будь-якому підготовленому пункту з відповідним доступом "підхопити" управління. Така "віртуальна взаємозамінність" базується на інтероперабельності, стандартизованих протоколах обміну даними та застосуванні криптографічного захисту.

Четвертий підхід — мобільні ПУ. Використання колісної або броньованої техніки, оснащеної засобами зв'язку та автоматизації, дає змогу створювати тимчасові або "мікро-ПУ". Вони можуть виконувати критичні функції протягом обмеженого часу, наприклад, під час переміщення основних структур або у випадку втрати стаціонарних пунктів. Такі "мобільні рішення" значно підвищують гнучкість і взаємозамінність системи управління.

П'ятим сучасним підходом є інтеграція кібер- та інформаційної безпеки у концепцію взаємозамінності. Якщо раніше акцент робився переважно на фізичному дублюванні та резервуванні, то нині значення набуває захищеність цифрових каналів. Взаємозамінність у кіберпросторі означає наявність альтернативних серверів, систем резервного копіювання, шифрованих каналів, які унеможливлюють параліч управління внаслідок кібератак.

Таким чином, взаємозамінність ПУ формується на перетині організаційних, технічних та інформаційних чинників. Вона передбачає не лише наявність резервних пунктів, але й системну інтеграцію – модульність структури, паралельну роботу резервних вузлів, використання сучасних цифрових технологій та заходів кіберзахисту. Наукові розробки українських і зарубіжних авторів підтверджують, що саме багаторівнева, розосереджена й технологічно захищена мережа ПУ забезпечує безперервність управління військами в умовах

сучасного бою.

У сучасній військовій науці дедалі більше утверджується підхід, згідно з яким систему ПУ доцільно формувати не лише за організаційно-штатною структурою чи територіальною прив'язкою, а передусім відповідно до логіки управлінських процесів штабу [29, 30]. Такий підхід відображає прагнення зробити ПУ не просто місцем розміщення командирів і технічних засобів, а інтегрованим середовищем, яке забезпечує безперервність циклу управління військами. ПУ повинні бути структуровані таким чином, аби відтворювати основні фази управлінського циклу:

оцінювання обстановки → планування → прийняття рішень → доведення завдань і контроль.

Звідси випливає формування функціональних секцій *Current Operations* (G3), *Plans* (G5), *Intelligence* (G2), *Sustainment* (G4), *Signal* (G6) [31, 32]. Організація простору ПУ відбувається навколо цих секцій, що дає змогу забезпечити логічний розподіл завдань та ефективний інформаційний обмін.

Це безпосередньо відповідає основним управлінським процесам і дає змогу забезпечити функціональність кожного ПУ незалежно від його рівня. Таким чином, система ПУ вибудовується як багаторівнева структура, де основний, альтернативний і тактичний пункти не дублюють один одного механічно, а розподіляють між собою функції відповідно до фаз управління.

Ці положення перегукуються із західними концепціями, де застосовуються принципи *service-design thinking* [33]. Йдеться про проєктування ПУ, виходячи не з географічних чи інфраструктурних міркувань, а з логіки руху інформаційних потоків. Організація робочих місць, технічних засобів і зон відповідальності має бути оптимізована під ключові завдання управління, що дає змогу скоротити час на передачу інформації та знизити ризики помилок у процесі прийняття рішень.

Отже, сучасний науковий підхід до організації системи ПУ передбачає їх проєктування та функціонування як середовища управлінських процесів. Основними його характеристиками є:

функціональне структурування за секціями штабу;

просторово-технічна організація відповідно до логіки інформаційних потоків;

розподіл завдань між різними типами ПУ (основні, допоміжні, тактичні, командно-спостережні) відповідно до фаз управління;

уніфікація документів і процедур для забезпечення безшовності управління.

Таким чином, система ПУ виступає не стільки фізичною сукупністю наметів чи укриттів, скільки динамічною мережею управлінських процесів, інтегрованих у єдине командно-штабне середовище. Це дає змогу підвищити стійкість управління військами, забезпечити взаємозамінність пунктів та гарантувати безперервність функціонування системи управління у складних умовах сучасного бою. Це дасть можливість, будь-якій посадовій особі, що прибула на конкретний ПУ, одним натисканням кнопки отримати доступ до необхідної інформації, яка відповідає рівню управління і посадовій особі. Для цього створюється відповідне захищене хмарне середовище (централізований (або відомчий) центр оброблення даних і сервісів, доступних через захищені мережі зв'язку, для збирання, зберігання, оброблення та поширення управлінської інформації між органами управління різних рівнів.), в якому функціонує вся інформація за операцію (бій), доступ до цієї інформації отримується у відповідності до рівня управління та функції за посадою.

Сучасні погляди щодо проєктування систем оброблення інформації, як базових систем що забезпечують управлінські процеси на ПУ, фокусуються на інтеграції підсистем, що забезпечують роботу ПУ, у єдине інформаційне середовище, яке створюється за технологіями хмарних обчислень (технологій). Такий підхід відкриває перспективу переходу від ізольованих штабів до багаторівневих мережевих структур, які здатні функціонувати у складних умовах сучасного бою.

Досвід армій країн НАТО свідчить, що основою перспективних систем ПУ стає гібридна архітектура "*enterprise – tactical edge*" (описує наскрізний ланцюг управління та оброблення даних). Зокрема, американська програма Army Cloud Plan передбачає розгортання корпоративної хмари (cARMY) у поєднанні з тактичними edge-вузлами, які зберігають критичні дані й сервіси безпосередньо на рівні підрозділів. У практиці Повітряних сил США реалізовано концепцію Cloud-Based Command and Control (CBC2) (це концепція побудови системи управління, у якій основні функції управління військами реалізуються через "хмарну" (відомчу або

захищену) інфраструктуру, що забезпечує спільний доступ органів управління до даних, сервісів і засобів підтримки прийняття рішень), що дає змогу інтегрувати сенсорні дані в єдиній хмарі й забезпечувати командирам швидке ухвалення рішень. Аналогічно, в екосистемі TAK (Tactical Assault Kit) передбачено можливість розгортання серверів у хмарі чи у контейнеризованому середовищі, що спрощує інтеграцію тактичних ПУ в загальну інформаційну систему.

У Збройних Силах України актуальним є запозичення цих практик у вигляді Mission Partner Environment (MPE) (суть MPE полягає не в створенні "єдиної системи для всіх", а в керованому обміні інформацією між посадовими особами через спільне середовище), що дає змогу організовувати захищений обмін даними з партнерами та союзниками на стратегічному, оперативному й тактичному рівнях. Це відкриває нові можливості для інтеграції українських ПУ в багатонаціональні угруповання та підвищує спроможність ЗС України діяти у складі коаліцій.

Однак застосування хмарних технологій у військових умовах пов'язане з низкою обмежень. Передусім це залежність від каналів зв'язку, які можуть бути перервані внаслідок радіоелектронної боротьби чи кінетичного ураження. Саме тому критично важливим є впровадження концепції edge-обчислень: резервування даних на локальних вузлах, можливість автономної роботи ПУ у режимі *disconnected/intermittent/limited* (режим функціонування систем управління, за якого зв'язок відсутній, нестабільний або обмежений за пропускною спроможністю, що є типовим для бойових дій) та подальша синхронізація інформації після відновлення зв'язку. Крім того, хмарна архітектура потребує високого рівня кіберзахисту – застосування моделей zero-trust (в управлінні військами – це модель безпеки, за якої жоден користувач, пристрій чи сервіс не вважається довіреним за замовчуванням, навіть якщо він знаходиться всередині захищеної мережі. Кожен доступ перевіряється, обмежується і контролюється постійно), багаторівневого шифрування й сегментації доступу, що особливо актуально у коаліційних операціях.

Для Збройних Сил України перспектива полягає у створенні мережевих, розосереджених і взаємозамінних систем ПУ, де хмарні технології поєднуються з локальними edge-рішеннями. Це дасть змогу:

забезпечити безперервність управління навіть у разі втрати окремих пунктів;

інтегрувати українські ПУ у багатонаціональні мережі НАТО;

знизити залежність від фізичного розташування штабів і підвищити їх мобільність;

створити єдину оперативну картину (common operational picture) для всіх рівнів управління;

підвищити стійкість системи до кібер- та інформаційного впливу противника.

Таким чином, перспективна система ПУ ЗСУ має трансформуватися у багаторівневу хмарно-орієнтовану мережу, що поєднує корпоративні ресурси, тактичні edge-вузли та стандарти коаліційної інтероперабельності. Це не лише забезпечить збереження керованості у складних умовах сучасного бою, але й створить основу для інтеграції України у спільні інформаційно-командні простори держав-партнерів.

Логічним продовженням використання хмарних технологій у ПУ є впровадження засобів віртуальної та доповненої реальності (VR/AR), які на основі єдиного інформаційного простору забезпечують інтерактивну візуалізацію даних та підвищують рівень ситуативної обізнаності командування.

Використання технологій віртуальної та доповненої реальності відкриває нові можливості для підвищення ефективності перспективних ПУ. Вони дають змогу створювати інтерактивні моделі бойового простору, забезпечувати глибоку візуалізацію оперативної обстановки та інтегрувати дані від різних сенсорних систем. Це суттєво посилює ситуативну обізнаність командування та сприяє більш швидкому й обґрунтованому прийняттю рішень.

У віртуальному світі командири можуть взаємодіяти, за потреби, з усіма елементами свого ПУ, не залишаючи свого фізичного робочого місця, вони можуть безперешкодно "переміщуватися" між елементами ПУ та бути присутніми будь-де, у будь-який час.

У збройних силах країн-партнерів VR/AR розглядаються як інструменти для підвищення спроможностей ПУ у трьох головних площинах:

ситуативна поінформованість і візуалізація у реальному часі;

планування/репетиція місій і навчання в єдиному геопросторовому середовищі;

людинорозмірна взаємодія з даними, що зменшує когнітивне навантаження штабів.

На доктринально-науковому рівні ці підходи відпрацьовуються в НАТО (STO) та в проєктах США [34, 35], що прямо адресують завдання ПУ та їх інтеграцію з мережевими сенсорами й тренувальними середовищами.

Наукові дослідження щодо застосування технологій VR/AR на пунктах показують: VR/AR здатні підвищити якість командно-штабних процесів, скоротити час прийняття рішень і покращити спільне розуміння обстановки в ПУ завдяки наочно-просторовій взаємодії з даними. Водночас зрілість технологій, ергономічні обмеження та вимоги до мережевої інфраструктури диктують поступове, сценарно-орієнтоване впровадження, пріоритетно – у ролях планування / репетиції та стаціонарних MR-інтерфейсів COP у командних залах, із подальшою міграцією до AR-засобів після відпрацювання факторів людино центричної надійності, які можна носити.

У сучасних дослідженнях спостерігається чітке зміщення акценту в роботі ПУ від традиційної ролі оперативного складу до зростаючої ваги фахівців у сфері інформаційних технологій. Якщо раніше головним завданням командного пункту було забезпечення взаємодії між командиром та його штабом, то сьогодні визначальним чинником ефективності виступає якість функціонування інформаційних систем, що забезпечують збір, оброблення, зберігання та розподіл даних у режимі реального часу. Саме IT-фахівці формують основу стійкості таких систем, оскільки відповідають за їхню працездатність у складних умовах радіоелектронного впливу, кібератак і перевантажень потоками інформації.

Наукові публікації підтверджують цю тенденцію, підкреслюючи, що оперативна діяльність штабу дедалі більше залежить від інформаційної інфраструктури [36, 37]. Дослідження, демонструють, що в умовах сучасної операцій саме спеціалісти з IT забезпечують підтримку хмарних сервісів, систем оброблення великих масивів даних і засобів візуалізації ситуаційної обстановки. Таким чином, функціонування ПУ як складної системи поступово переходить від людиноцентричної моделі командування до технологічно-орієнтованої моделі, де роль людини трансформується у спрямування, контроль і координацію роботи цифрових систем.

Таким чином, сучасний розвиток концепцій управління свідчить про формування нового балансу: оперативний склад зосереджується на прийнятті рішень і формуванні замислу операцій, тоді як критично важливі процеси забезпечення інформаційного циклу покладаються на фахівців інформаційних технологій. Це зміщення фокусу відповідає загальним тенденціям цифровізації війська та формує основу для стійкості й живучості перспективних ПУ.

Висновки. Перспективні ПУ трансформуються від традиційних стаціонарних структур у мережеві, розосереджені та технологічно інтегровані системи, здатні функціонувати у багатовимірному просторі сучасної війни. Їх ефективність визначатиметься поєднанням кількох ключових чинників.

По-перше, взаємозамінність і живучість досягаються за рахунок розвитку технічної бази перспективних ПУ, що спрямовується на підвищення їхньої мобільності, живучості шляхом модернізації техніки, удосконалення засобів захисту, створення мережі основних, альтернативних і мобільних ПУ, які організовані відповідно до управлінських процесів штабу та здатні дублювати функції один одного.

По-друге, впровадження хмарних та edge-рішень забезпечує безперервність управління, формування єдиного інформаційного простору та інтеграцію українських систем у коаліційні мережі.

По-третє, використання віртуальної та доповненої реальності відкриває нові можливості для підвищення ситуативної обізнаності, прискорення процесів планування та проведення тренувань із використанням цифрових двійників.

По-четверте, у перспективних ПУ спостерігається перехід від домінування оперативного складу до зростання ролі IT-фахівців, які забезпечують стійкість і безперервність функціонування систем оброблення інформації.

Перспективи подальших досліджень. Перспективні ПУ мають еволюціонувати у багаторівневі, гнучкі та технологічно насичені системи, де поєднання організаційних рішень і передових технологій дає змогу зберігати безперервність управління військами навіть в умовах активного інформаційного, кібернетичного та вогневого впливу противника.

Подальші наукові дослідження доцільно спрямувати на розроблення та обґрунтування інтегрованої концепції перспективних ПУ як багаторівневих, роззосереджених і адаптивних

систем управління військами. Зокрема, актуальними є такі напрями:

архітектура багаторівневих ПУ – дослідження моделей поєднання стратегічного, оперативного і тактичного рівнів управління в єдиному інформаційно-функціональному просторі з урахуванням принципів enterprise – tactical edge (інтеграцію централізованих інформаційних, аналітичних і управлінських спроможностей “enterprise” з децентралізованими, автономними та стійкими спроможностями тактичного рівня) та edge-обчислень;

стійкість і живучість системи управління – обґрунтування способів забезпечення безперервності управління в умовах вогневого ураження, радіоелектронного придушення та кібервпливу, зокрема шляхом модульності ПУ, резервування функцій, децентралізації прийняття рішень і використання режимів disconnected/intermittent/limited (повна або тривала відсутність зв’язку з вищими органами управління та зовнішніми інформаційними ресурсами).

Інформаційно-технологічна інтеграція – дослідження застосування хмарних і гібридних технологій, захищених середовищ обміну даними, а також моделей zero-trust для обміну даними між органами управління та партнерами.

Організаційні та процедурні аспекти – уточнення ролі функціональних секцій ПУ (G2/G3/G4/G5/G6), трансформації управлінського циклу та адаптації процедур планування і управління до умов високої динаміки бойових дій.

Моделювання та оцінювання ефективності – розроблення критеріїв і показників оцінки стійкості, оперативності та адаптивності перспективних ПУ, із застосуванням імітаційного моделювання та сценарного аналізу.

Реалізація зазначених напрямів дасть змогу сформувати науково обґрунтовані підходи до створення перспективних пунктів управління, здатних забезпечувати ефективне управління військами в умовах сучасних і майбутніх збройних конфліктів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Іваницька О. В., Смирнов С. А. , Біловус О. С. Вплив інформаційного середовища на прийняття рішень економічних суб’єктів: рефлексивний підхід // Економічний вісник НТУУ «КПІ». 2017. № 14. С. 476–482.
2. Войцеховський Р. О. Система показників і критеріїв обґрунтування вимог до стійкості системи управління оперативного угруповання військ в операціях (бойових діях) // Military Science. 2024. Т. 2, № 3. С. 218–234. DOI: 10.62524/msj.2024.2.3.18.
3. Королюк Н. О., Пазинич Р. О., Мельник С. В. Обґрунтування комплексного підходу для оцінки ефективності управління частинами та підрозділами Повітряних Сил ЗСУ // Сучасні інформаційні технології у сфері безпеки та оборони. 2019. № 1(34). С. 133–138. DOI: 10.33099/2311-7249/2019-34-1-133-138.
4. Кучеренко Ю. Ф., Носик А. М., Ткачов А. М., Шубін Є. В. Визначення ефективності функціонування системи управління військового призначення з врахуванням вагомості, своєчасності та якості виконання завдань у її підсистемах // Збірник наукових праць Харківського національного університету Повітряних Сил. 2019. Вип. 4(62). С. 53–60. DOI: 10.30748/zhups.2019.62.07.
5. Fox A. Learning to Fight: Military Innovation and Change in the British Army. Cambridge : Cambridge University Press, 2017.
6. Beagle M., Slider J. C., Arrol M. R. The Graveyard of Command Posts: What Chornobaivka Should Teach Us About Command and Control in Large-Scale Combat Operations // Military Review. May–June 2023.
7. Соколовський С. М., Демків А. С. До питання пріоритетності ураження елементів системи управління військами противника // Перспективи розвитку озброєння та військової техніки Сухопутних військ : зб. тез доп. Міжнар. наук.-техн. конф., м. Львів 14–16 трав. 2014 р. / Академія сухопутних військ. Львів, 2014. С. 147. URL: https://asv.mil.gov.ua/content/nauka/2014/konf_14_16-05-2014.pdf (дата звернення: 05.12.2025).
8. Хімченко О. Формалізація завдання з дезорганізації системи управління військами (силами) противника під час нанесення зустрічного удару ракетними військами // Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2022.
9. Мережецентрична система управління і її вплив на бойові можливості міжвидового угруповання / Ю. Ф. Кучеренко, А. М. Носик, Д. О. Камак та ін. // Випробовування та сертифікація. 2024. № 1(3). С. 52–58.
10. Кучеренко Ю. Ф., Носик А. М., Ткачов А. М., Шубін Є. В. Визначення ефективності функціонування системи управління військового призначення з врахуванням вагомості, своєчасності та якості виконання завдань у її підсистемах // Збірник наукових праць Харківського національного університету Повітряних Сил. 2019. Вип. 4 (62). С. 53–60. DOI: 10.30748/zhups.2019.62.07.
11. Зубков В. Механізм впливу на інформаційні системи противника як складова інформаційного забезпечення сил оборони України // Збірник

наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2023. № 3. С. 45–52.
12. Command post & tactical operations centers. Losberger De Boer. URL: https://www.losbergerdeboer.com/us/solutions/rapid-deployment-space/command-post-tactical-operations-centers/?utm_source=chatgpt.com (дата звернення: 21.05.2025).
13. U.S. Army Moves To Mobilize And Disperse Its Increasingly Vulnerable Command Posts. URL: https://www.forbes.com/sites/lorenthompson/2023/12/07/us-army-moves-to-mobilize-and-disperse-its-increasingly-vulnerable-command-posts/?utm_source=chatgpt.com (дата звернення: 11.06.2025).
14. Робота штабу тактичної ланки з організації бою (дій). (Частина І) Робота штабу під час підготовки бою (дій) : навч. посіб. / П. П. Ткачук , О. П. Красюк , Л. П. Кривизюк та ін. Львів : Академія сухопутних військ, 2015.
15. U.S. Army PEO C3T. Modernizing Army Command Posts: The Next Generation of Mobile Warfare. Army.mil, 08.09.2023. URL: https://www.army.mil/article/269508/modernizing_army_command_posts_the_next_generation_of_mobile_warfare (дата звернення: 02.06.2025).
16. Mitchell Institute Forum 50: Distributed Control in C2. Arlington, VA : Mitchell Institute, 2023. 28 p. URL: https://www.mitchellaerospacepower.org/app/uploads/2023/01/MI_Forum_50-C2-Distributed-Control-FINAL.pdf (дата звернення: 09.04.2025).
17. Глоба О. В. Безпека застосування та забезпечення живучості сил та засобів у сучасних операціях // Системи озброєння і військова техніка. 2021. № 3. С. 51–58.
18. Гусак Ю. А., Шевченко В. К. Методичний підхід щодо аналізу живучості системи пунктів управління // Modern Information Technologies in the Sphere of Security and Defence. 2020. № 1 (37). С. 191–196.
19. Ковальчук М. Підвищення живучості пунктів управління як засіб забезпечення стійкості системи управління прикордонного загону в умовах воєнного стану // Збірник наукових праць Національної академії Державної прикордонної служби України. Серія “Військові та технічні науки”. 2025. № 2 (99). С.15–24.
20. United States Department of the Army. FM 71-100-2: Infantry Division Operations. Washington, DC : Headquarters, Department of the Army. 1996. С. 342.
21. United States Department of the Army. ATP 6-0.5: Command Post Organization.
22. Методичні рекомендації роботи штабного офіцера тактичної ланки (ВП 7-(01,02,04)11.01). Київ : Міністерство оборони України, 2020. С. 92.
23. Шолудько В. А. Інтероперабельність засобів зв’язку та автоматизації як основа взаємозамінності пунктів управління // Системи озброєння і військова техніка. 2019. № 2 (58). С. 120–127.
24. Ярош С. П. Обґрунтування понятійного апарату, формулювання гіпотез і проблем дослідження модульних розподілених пунктів управління силами та засобами збройної боротьби // Системи озброєння і військова техніка. 2011. Вип. 2 (26). С. 183–188.
25. Косяк О.иГ. Аспекти вибору місця розміщення командного пункту тактичної ланки під час відсічі збройної агресії Російської Федерації // Службово-бойова діяльність сил сектору безпеки та оборони держави: сучасний стан, проблеми та перспективи : тези VII Всеукраїнської НПК / НА НГУ. 2025.
26. Shamko V. A conceptual approach to defining a structure for spatially distributed network-centric system for controlling the tier of air defense missile cover // Наука і техніка Повітряних Сил Збройних Сил України. 2020. №39.
27. Dimitar T. Mitev. A Comprehensive Approach to the Development of Modern, Mobile, and Distributed Command Posts at the Operational and Tactical Level. 2025.
28. Kitz C. W. Dispersed Command Posts in Large-Scale Combat Operations: Accepting New Challenges and Mitigating Risks to Achieve Success // Field Artillery Journal. E-edition, 2024.
29. Headquarters, Department of the Army. ADP 6-0 / FM 6-0: Mission Command; The Operations Process. Washington, DC : HQDA. 2019 / 2014.
30. West Point / Military Writers’ Institute. It’s Time to Fix the Command Post: Optimizing Headquarters Mobility, Survivability and Interoperability for the Future Fight. 2020. URL: https://mwi.westpoint.edu/its-time-to-fix-the-command-post-optimizing-headquarters-mobility-survivability-and-interoperability-for-the-future-fight/?utm_source=chatgpt.com (дата звернення: 24.09.2025).
31. FM 101-5 Staff Organization and Operations — стандарт США для організації штабу / пунктів управління; у ньому staff (штаб) структурується через coordinating, special та personal staff, де coordinating-штаб має саме групи G-штату: G1, G2, G3, G4, G5, G6. URL: https://aiai.ed.ac.uk+1 (дата звернення: 11.11.2025).
32. NATO recommendations for combat operations planning (у перекладі / тлумаченні «Рекомендації з планування та організації бою») – згідно з цим, функціональні секції (G1–G6) існують як частина штатної структури, а пункт управління реалізує цикл прийняття рішення через відповідні підрозділи штабу.
33. Groen, Richard Z. Command-Post Layout and Service-Design Thinking // ARMOR: The Magazine of Mobility and Protection. 2013. С. 36–40.
34. U.S. Congress. Army’s Integrated Visual Augmentation System (IVAS) / Soldier Borne Mission Command (SBMC). Congressional Research Service. 2025. URL: https://www.congress.gov/crs-product/IF13022 Congress (дата звернення: 07.08.2025).
35. Maxar Technologies. Maxar’s Vricon Awarded Phase 2 of U.S. Army’s One World Terrain Contract.

Press release. 2021. URL: https://www.maxar.com/press-releases/maxar-s-vricon-awarded-phase-2-of-u-s-army-s-one-world-terrain-contract (дата звернення: 07.08.2025).
36. Hall D., Sands T. Quantum Cryptography for Nuclear Command and Control // Computer and Information Science. 13(1), 72. 2020. DOI: https://doi.org/10.5539/cis.v13n1p72.
37. Krelina M. Quantum technology for military applications. EPJ Quantum Technology. 2021. DOI: https://doi.org/10.1140/epjqt/s40507-021-00113-y.

Стаття надійшла до редакції 24.09.2025

Methodological and conceptual aspects of developing prospective command posts

Annotation

The experience gained from conducting operations during the repulsion of the armed aggression of the Russian Federation against Ukraine indicates that the development of command and control systems, along with the employment of modern precision strike capabilities, has led to a significant increase in the complexity of command post (CP) functioning in the processes of operational planning and troop control during combat operations. Addressing this problem requires resolving the contradiction between the effectiveness of all elements of command posts and the contemporary operational environment in which they perform planning and command functions, on the one hand, and the necessity to enhance the survivability of command posts in accordance with the dynamically evolving requirements of modern operations, on the other.

The purpose of the article is to substantiate prospective directions for the development of command posts as complex systems based on an analysis of the relationship between the effectiveness of their elements and survivability levels, as well as to assess the possibilities of implementing modern information technologies to enhance command and control resilience.

Prospective command posts are evolving from traditional stationary structures into networked, distributed, and technologically integrated systems capable of operating within the multidimensional space of modern warfare. Their effectiveness will be determined by a combination of several key factors:

interchangeability and survivability achieved through the advancement of the technical foundation of prospective CP;

the implementation of cloud and edge computing solutions to ensure continuity of command and the formation of a unified information environment;

the use of virtual and augmented reality technologies to enhance situational awareness;

and the transition from the dominance of operational staff to the increasing role of IT specialists who ensure the resilience and uninterrupted functioning of information processing systems.

Keywords: command posts; survivability; command and control effectiveness; cloud technologies; virtual and augmented reality; IT specialists; concealment and camouflage; situational awareness.

УДК 355.5 https://doi.org/10.33099/2304-2745/2025-3-86/138-144

Георгадзе О. А., кандидат військових наук, доцент[1] (0000-0002-9306-6660)
Савчук Д. В.[2] (0009-0004-8567-9338)

[1] – Головне управління персоналу Генерального штабу Збройних Сил України, Київ;
[2] – Командно-штабний інститут застосування військ (сил) Національного університету оборони України, Київ

Часткова методика оцінювання рівня підготовленості особового складу військової частини в умовах дії правового режиму воєнного стану

Резюме. У статті висвітлено часткову методику оцінювання рівня підготовленості особового складу військової частини в умовах дії правового режиму воєнного стану, як складової комплексної методики оцінювання рівня її боєздатності. Запропонована методика враховує рівень підготовленості кожного структурного підрозділу у складі військової частини, з урахуванням його важливості, що передбачає врахування сукупного рівня навченості військовослужбовців на основі вибору нової сукупності показників, які характеризують їх рівень індивідуальних спроможностей, наявність у них відповідної військової освіти (підготовки) та участі у бойових діях і злагодженість цих структурних підрозділів, яка враховує важливість кінцевого заходу колективної підготовки.

Ключові слова: підготовленість; оцінювання; навченість; злагодженість; індивідуальні спроможності; військова освіта (підготовка); участь у бойових діях.

Постановка проблеми. Досвід застосування військових частин Збройних Сил (ЗС) України під час відсічі збройної агресії Російської Федерації (РФ) свідчить, що успішне виконання ними бойових (спеціальних) завдань залежить від рівня їх боєздатності [1–5]. Безпосередній вплив на рівень боєздатності військової частини здійснює рівень підготовленості особового складу. Саме на досягнення високого рівня підготовленості особового складу військових частин спрямована бойова підготовка (бойове злагодження), що включає в себе індивідуальну та колективну підготовки. Від ефективності їх організації та проведення залежать навченість військовослужбовців та злагодженість структурних підрозділів військової частини.

У зв’язку з цим триває робота в органах військового управління, військових частинах ЗС України щодо пошуку та впровадження нових підходів у діяльність командувачів (командирів, начальників) та їх заступників для підвищення рівня підготовленості особового складу військових частин, що не можливо без відповідного науково-методичного апарату.

Таким чином виникає потреба у науковому обґрунтуванні часткової методики оцінювання рівня підготовленості особового складу військової частини в умовах дії правового режиму воєнного стану, як складової комплексної методики оцінювання рівня її боєздатності. Зазначене свідчить про актуальність теми, яка розглядається.

Аналіз останніх досліджень і публікацій. Аналіз попередніх досліджень та публікацій з цього напряму [6–15] свідчить про те, що єдиної методики оцінювання рівня підготовленості особового складу не існує. Підходи, які розглядаються, стосуються переважно оцінювання складових підготовки та не враховують особливостей підготовки військовослужбовців військової частини в умовах дії правового режиму воєнного стану. Так, у попередніх роботах автора [6–8] викладені методичні підходи щодо оцінювання рівня навченості органів управління військових частин, підготовленості танкової бригади під час відновлення боєздатності, навченості бригади тактичної авіації та підготовленості сил оборони держави. Запропоновані в роботах [9–10] аналітичні залежності дають змогу оцінити ефективність індивідуальної підготовки офіцерського складу науково-педагогічних працівників у вищих військових навчальних закладах та стан індивідуальної підготовки військовослужбовців в органах військового управління. Статті [11–13] присвячені оцінюванню компетентностей військовослужбовців змінного складу навчальних центрів, громадян для проходження військової підготовки за програмою підготовки офіцерів запасу та з вогневої підготовки. Методичний підхід у роботі [14] дає змогу оцінити стан колективної підготовки органів військового управління.

Стосовно оцінювання рівня підготовленості особового складу військової частини в умовах дії правового режиму

воєнного стану зазначені методики потребують удосконалення та можуть бути застосовані лише частково. У той же час, наявний науково-методичний апарат є базовою основою для подальшого його удосконалення.

Метою статті є висвітлення часткової методики оцінювання рівня підготовленості особового складу військової частини в умовах дії правового режиму воєнного стану.

Виклад основного матеріалу. Оцінку рівня підготовленості особового складу військової частини в умовах дії правового режиму воєнного стану $M_T(t)$ пропонується визначати за функціональною залежністю, яка враховує рівень підготовленості i-го структурного підрозділу у складі військової частини, з урахуванням його важливості. Так, як рівень підготовленості кожного структурного підрозділу не залежить від рівня підготовленості іншого, а отже і їх показники не залежні один від одного, то для оцінювання рівня підготовленості особового складу військової частини в умовах дії правового режиму воєнного стану пропонується використовувати адитивну агрегацію:

$$M_T(t) = \sum_{i=1}^{I} M_{Ti}(t) \cdot q_i, \quad (1)$$

де $M_{Ti}(t)$ – рівень підготовленості i-го структурного підрозділу у складі військової частини на дискретний момент часу;

q_i – ваговий коефіцієнт важливості i-го структурного підрозділу у складі військової частини;

I – кількість структурних підрозділів у військовій частині.

До показників, які характеризують рівень підготовленості i-го структурного підрозділу $M_{Ti}(t)$ пропонується віднести: сукупний рівень навченості особового складу структурного підрозділу $W_{Ti}(t)$ та рівень їх злагодженості $H_{Ti}(t)$.

Зважаючи на те, що навченість військовослужбовців впливає на злагодженість структурного підрозділу, а отже їх показники сильно корельовані, то оцінку рівня підготовленості i-го структурного підрозділу $M_{Ti}(t)$ на дискретний момент часу пропонується розраховувати за допомогою нормованої мультиплікативної агрегації [15]:

$$M_{Ti}(t) = W_{Ti}(t)^{q_w} \cdot H_{Ti}(t)^{q_h}, \quad (2)$$

де $W_{Ti}(t)$ – сукупний рівень навченості військовослужбовців i-го структурного підрозділу на дискретний момент часу;

$H_{Ti}(t)$ – рівень злагодженості i-го структурного підрозділу на дискретний момент часу;

q_w, q_h – вагові коефіцієнти важливості показників $W_{Ti}(t), H_{Ti}(t)$.

Оцінку сукупного рівня навченості військовослужбовців i-го структурного підрозділу $W_{Ti}(t)$ пропонується визначати за залежністю, яка враховує рівень навченості кожного військовослужбовця структурного підрозділу з урахуванням його важливості:

$$W_{Ti}(t) = \sum_{a=1}^{A} W_{Tia}(t) \cdot q_a, \quad (3)$$

де $W_{Tia}(t)$ – рівень навченості a-го військовослужбовця i-го структурного підрозділу на дискретний момент часу;

q_a – ваговий коефіцієнт важливості a-го військовослужбовця i-го структурного підрозділу;

A – кількість військовослужбовців у i-му структурному підрозділі.

Вагові коефіцієнти важливості a-го військовослужбовця у i-му структурному підрозділі військової частини q_a розраховуються шляхом нормування порівняльних рангів посад:

$$q_a = {R_a}\Big/{\sum_{a=1}^{A} R_a}, \quad (4)$$

де R_a – порівняльний ранг a-го військовослужбовця у i-му структурному підрозділі військової частини;

$\sum_{a=1}^{A} R_a$ – сума всіх рангів військовослужбовців у i-му структурному підрозділі військової частини.

Порівняльний ранг a-го військовослужбовця у i-му структурному підрозділі військової частини визначається за залежністю

$$R_a = 1 - {A_a - 1}\Big/{A}, \quad (5)$$

де A_a – порядковий номер a-го військовослужбовця у i-му структурному підрозділі військової частини.

Оцінювання рівня навченості a-го військовослужбовця i-го структурного підрозділу $W_{Tia}(t)$ визначається за показниками, які характеризують рівень його індивідуальних спроможностей (знання, уміння і навички з предметів індивідуальної підготовки), наявність у нього відповідної військової освіти – для офіцерського складу, підготовки – сержантського, рядового складу та наявність участі у бойових діях.

Оскільки зазначені показники не залежні один від одного, то для розрахунку рівня навченості a-го військовослужбовця i-го структурного підрозділу $W_{Tia}(t)$ пропонується використовувати адитивну агрегацію:

$$W_{Tia}(t) = G_{ia}(t) \cdot q_g + O_{ia}(t) \cdot q_o + P_{ia}(t) \cdot q_p, \quad (6)$$

де $G_{ia}(t)$ – рівень індивідуальних спроможностей a-го військовослужбовця i-го структурного підрозділу на дискретний момент часу;

$O_{ia}(t)$ – показник, що характеризує наявність у a-го військовослужбовця i-го структурного підрозділу відповідної військової освіти – для офіцерського складу, підготовки – сержантського, рядового складу на дискретний момент часу;

$P_{ia}(t)$ – показник, що характеризує наявність у a-го військовослужбовця i-го структурного підрозділу участі у бойових діях;

$q_g; q_o; q_p$ – вагові коефіцієнти важливості показників $G_{ia}(t); O_{ia}(t); P_{ia}(t)$.

Оцінювання рівня індивідуальних спроможностей a-го військовослужбовця i-го структурного підрозділу на дискретний момент часу $G_{ia}(t)$ пропонується визначати за залежністю, яка враховує рівень його знань та умінь і навичок з предметів індивідуальної підготовки:

$$G_{ia}(t) = G_{iak}(t) \cdot q_k + G_{ias}(t) \cdot q_s\,, \quad (7)$$

де $G_{iak}(t)$ – рівень знань із предметів індивідуальної підготовки a-го військовослужбовця i-го структурного підрозділу на дискретний момент часу;

$G_{ias}(t)$ – рівень умінь і навичок із предметів індивідуальної підготовки a-го військовослужбовця i-го структурного підрозділу на дискретний момент часу;

$q_k; q_s$ – вагові коефіцієнти важливості показників $G_{iak}(t); G_{ias}(t)$.

Показник, який характеризує рівень знань із предметів індивідуальної підготовки a-го військовослужбовця i-го структурного підрозділу на дискретний момент часу $G_{iak}(t)$ пропонується розраховувати за результатами теоретичних питань (тестування). Загальна кількість запитань має забезпечувати об'єктивну та всебічну оцінку рівня його знань з предметів індивідуальної підготовки.

Оцінка рівня знань із предметів індивідуальної підготовки a-го військовослужбовця i-го структурного підрозділу на дискретний момент часу визначається за виразом

$$G_{iak}(t) = {\Omega_{iak}(t)}/{\Omega_{max}}\,, \quad (8)$$

де $\Omega_{iak}(t)$ – кількість балів, яка отримана a-им військовослужбовцем i-го структурного підрозділу на дискретний момент часу за результатами теоретичних питань (тестування);

Ω_{max} – максимальна кількість балів, яку можливо отримати a-му військовослужбовцю i-го структурного підрозділу за результатами теоретичних питань (тестування).

Показник, який характеризує рівень умінь і навичок із предметів індивідуальної підготовки a-го військовослужбовця i-го структурного підрозділу на дискретний момент часу $G_{ias}(t)$ пропонується розраховувати за результатами виконаних ним практичних завдань (нормативів, прийомів). Зміст та кількість практичних завдань (нормативів, прийомів) має враховувати функціональне призначення військовослужбовця відповідно до займаної посади.

Оцінка рівня умінь і навичок із предметів індивідуальної підготовки a-го військовослужбовця i-го структурного підрозділу на дискретний момент часу визначається за виразом

$$G_{ias}(t) = {\Psi_{ias}(t)}/{\Psi_{max}}, \quad (9)$$

де $\Psi_{ias}(t)$ – кількість балів, яка отримана a-им військовослужбовцем i-го структурного підрозділу на дискретний момент часу за результатами практичного виконання завдань (нормативів, прийомів);

Ψ_{max} –максимальна кількість балів, яку можливо отримати a-им військовослужбовцем i-го структурного підрозділу за результатами практичного виконання завдань (нормативів, прийомів).

Показник "військова освіта (підготовка)" у a-го військовослужбовця i-го структурного підрозділу $O_{ia}(t)$ характеризує наявність у нього відповідної військової освіти – для офіцерського складу, підготовки – сержантського, рядового складу на дискретний момент часу. Для оцінки значення зазначеного показника пропонується використовувати розроблені нами шкали оцінок, які наведено в Табл. 1, 2.

Якщо в офіцера декілька рівнів військової (професійно-військової) освіти, то приймається значення найвищого рівня.

Якщо у сержанта (солдата) декілька видів підготовки, то приймається значення найвищого рівня.

Показник "участь у бойових діях" у a-го військовослужбовця i-го структурного підрозділу $P_{ia}(t)$ характеризує участь військовослужбовця у бойових діях протягом останніх двох років. Для оцінки значення зазначеного показника пропонується використовувати розроблену нами шкалу оцінки, яку наведено в Табл. 3.

Таблиця 1

Оцінка значення показника "військова освіта" для офіцерського складу

Військова (професійно-військова) освіта	Значення показника
Посади, які передбачають оперативний рівень	
Оперативний (оперативно-тактичний) рівень	1,0
Курси професійної військової освіти L-3	0,85
Курси професійної військової освіти L-2	0,7
Курси професійної військової освіти L-1C	0,6
Тактичний рівень (диплом бакалавра)	0,5
Військова підготовка за програмою підготовки офіцерів запасу	0,4
Курси професійної військової освіти L-1A+L-1B	0,2
Посади, які передбачають тактичний рівень	
Курси професійної військової освіти L-2	1,0
Курси професійної військової освіти L-1C	0,9
Тактичний рівень (диплом бакалавра)	0,8
Військова підготовка за програмою підготовки офіцерів запасу	0,7
Курси професійної військової освіти L-1B	0,5
Відсутня військова освіта	0,2

Таблиця 2

Оцінка значення показника "підготовка" для сержантського, рядового складу

Підготовка	Значення показника
Для сержантського складу	
Курс лідерства підвищеного рівня	1,0
Курс лідерства середнього рівня	0,85
Курси базового рівня підготовки сержантського складу	0,7
Фахова підготовка	0,4
Базова загальновійськова підготовка	0,2
Для рядового складу	
Фахова підготовка	1,0
Базова загальновійськова підготовка	0,9
Відсутня базова загальновійськова підготовка	0,2

Таблиця 3

Оцінка значення показника "участь у бойових діях"

Термін участі військовослужбовця у бойових діях	Значення показника
2 роки і більше	1,0
1,5 роки	0,88
1 рік	0,7
6 місяців	0,46
3 місяці	0,31
менше 3 місяців	0

Розрахунок значення показника "участь у бойових діях" необхідно здійснювати прямопропорційно від тривалості участі військовослужбовця у бойових діях під час відсічі широкомасштабної збройної агресії РФ.

Рівень злагодженості i-го структурного підрозділу військової частини на дискретний момент часу $H_{Ti}(t)$ пропонується оцінювати за результатами проведення кінцевих заходів колективної підготовки. Для управління військової частини це може бути командно-штабне навчання (КШН), командно-штабне тренування (КШТ), спільне штабне тренування (СШТ), роздільне штабне тренування (РШТ). Для решти структурних підрозділів військової частини (основні підрозділи та підрозділи забезпечення) – батальйонне тактичне навчання з бойовою стрільбою (БТН з БС), батальйонне тактичне навчання без бойової стрільби (БТН без БС), батальйонне тактико-спеціальне навчання (БТСН), ротне тактичне навчання з бойовою стрільбою (РТН з БС), ротне тактичне навчання без бойової стрільби (РТН без БС), ротне тактико-спеціальне навчання (РТСН), бойові стрільби взводів (БСВ), бойові стрільби відділень, екіпажів, розрахунків (БСВд).

Для оцінювання результатів кінцевого заходу колективної підготовки (на якому проводиться вихідний контроль) розробляється

оціночний лист, який складається з розділів, що відображають певні завдання, які характеризують спроможність i-го структурного підрозділу їх виконати.

Розрахунок рівня злагодженості i-го структурного підрозділу військової частини на дискретний момент часу $H_{Ti}(t)$ визначаємо за залежністю

$$H_{Ti}(t) = \left(\sum_{\ell=1}^{\mathcal{L}} \mho_\ell(t) \Big/ \mathcal{L}\right) \cdot q_\vartheta, \qquad (10)$$

де $\mho_\ell(t)$ – показник, який характеризує оцінку за результатами виконання ℓ-го розділу оціночного листа на дискретний момент часу;

$\mathcal{L}$ – кількість розділів оціночного листа;

q_ϑ – ваговий коефіцієнт важливості кінцевого заходу колективної підготовки.

Ваговий коефіцієнт важливості кінцевого заходу колективної підготовки визначено методом експертного оцінювання, результати якого наведено у Табл. 4.

Таблиця 4

Результати визначення вагового коефіцієнта важливості кінцевого заходу колективної підготовки

Захід колективної підготовки	Ваговий коефіцієнт
Для управління військової частини	
КШН	1,0
КШТ	0,95
СШТ	0,65
РШТ	0,3
Для підрозділів	
БТН з БС	1,0
БТН без БС	0,9
БТСН	1,0
РТН з БС	0,8
РТН без БС	0,7
РТСН	0,8
БСВ	0,6
БСВд	0,4

Розділ оціночного листа складається з елементів, які необхідно виконати військовослужбовцям i-го структурного підрозділу. У кожному розділі можуть визначатися критично важливі елементи, які обов'язкові до виконання. Розрахунок оцінки за результатами виконання ℓ-го розділу оціночного листа пропонується здійснювати таким чином:

$$\mho_\ell(t) = \left(\varphi + \omega \Big/ \varphi^* + \omega^*\right) \cdot \gamma_\varphi;$$

де φ – кількість виконаних критично важливих елементів розділу оціночного листа;

ω – кількість виконаних інших елементів розділу оціночного листа;

φ^* – загальна кількість критично важливих елементів розділу оціночного листа;

ω^* – загальна кількість інших елементів розділу оціночного листа;

γ_φ – індекс валідності кінцевого результату за критично важливими елементами (умова обов'язкового повного виконання).

$$\gamma_\varphi = \begin{cases} 1, & \varphi = \varphi^* \\ 0, & \varphi < \varphi^* \end{cases}, \qquad (11)$$

сукупного рівня навченості військовослужбовців на основі вибору нової сукупності показників, які характеризують їх рівень індивідуальних спроможностей, наявність у них відповідної військової освіти (підготовки) та участі у бойових діях і злагодженість цих структурних підрозділів, яка враховує важливість кінцевого заходу колективної підготовки.

Висновки і перспективи подальших досліджень. Таким чином удосконалено часткову методику оцінювання рівня підготовленості особового складу військової частини, яка враховує рівень підготовленості i-го структурного підрозділу у її складі з урахуванням його важливості, що передбачає врахування

Використовуючи зазначену часткову методику, командувачі (командири, начальники) отримують можливість оцінити рівень підготовленості особового складу військової частини, виявити проблемні питання під час їх бойової підготовки (бойового злагодження), надати обґрунтовані пропозиції щодо підвищення рівня навченості військовослужбовців і злагодженості

структурних підрозділів військової частини.

Перспективами подальших наукових досліджень у даному напрямі може бути обґрунтування рекомендацій щодо підвищення рівня підготовленості особового складу військової частини.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Репіло Ю. Є., Георгадзе О. А., Винокуров Д. В., Камалов Є. В., Чайковська О. Є., Ключак О. М. Погляди щодо організації та проведення індивідуальної підготовки офіцерського складу органів військового управління // Збірник наукових праць військового інституту Київського Національного університету імені Тараса Шевченка. 2024. № 82. С. 59–66. DOI: 10.17721/2519-481X/2024/82-07.
2. Савчук Д. В., Георгадзе О. А. Часткова методика оцінювання морально-психологічного стану особового складу // Social development and security. 2025. Vol. 15, No 3. С. 100–107. DOI: https://doi.org/10.33445/sds.2025.15.3.11.
3. Георгадзе О. А., Салаш О. А. Обґрунтування сукупності показників до комплексної методики оцінювання ефективності оперативної підготовки // Збірник наукових праць Національної академії Державної прикордонної служби України. Серія: військові та технічні науки. 2022. № 3 (88). С. 5–17. DOI: https://doi.org/10.32453/3.v88i3.
4. Савчук Д. В., Георгадзе О. А. Часткова методика оцінювання укомплектованості військової частини військовослужбовцями // Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України. 2024. Том 2, № 3 (83). С. 117 – 121. DOI: https://doi.org/10.33099/2304-2745/2024-3-83/117-121.
5. Heorhadze O. Metod's for assessing the level of the organization of joint training of defence forces // Сучасні інформаційні технології у сфері безпеки та оборони. 2022. № 2 (44). С. 43–47. DOI: https://doi.org/10.33099/2311-7249/2022-44-2-43-47.
6. Георгадзе О. А., Макаліш О. В. Методичний підхід до оцінювання рівня навченості органів військового управління тактичного рівня // Збірник наукових праць Центру військово-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2016. № 3 (58). С. 104–108. DOI: https://doi.org/10.33099/2304-2745/2016-3-58/104-108.
7. Георгадзе О. А., Харабара В. І. Часткова методика оцінювання рівня підготовленості танкової бригади у ході відновлення боєздатності // Social development and security. 2019. Vol. 9, No. 4. С. 131–142. DOI: https://doi.org/10.33445/sds.2019.9.4.10.
8. Piekhota S., Heorhadze O., Kharabara V. Partial methodology for assessing the level of learning of tactical aviation brigade personnel // Political Science and Security Studies Journal. 2021. Vol. 2, No.1. P. 68–73. DOI: https://doi.org/10.5281/zenodo. 4818549.
9. Георгадзе О. А., Пампуха І. В., Шевчук В. В., Пєхота С. Г., Чайковська О. Є. Методичний підхід до оцінювання ефективності індивідуальної підготовки офіцерського складу науково-педагогічних працівників у вищих військових навчальних закладах // Збірник наукових праць військового інституту Київського Національного університету імені Тараса Шевченка. 2022. № 76. С. 130–138. DOI: https://doi.org/10.17721/2519-481X/2022/76-11.
10. Георгадзе О. А., Салаш О. А. Часткова методика оцінювання стану індивідуальної підготовки військовослужбовців органів військового управління // Social development and security. 2022. Vol. 12, No. 5. DOI: https://doi.org/10.33445/sds.2022.12.5.2.
11. Vynokurov D. V., Heorhadze O. A. Partial methodology for assessing the younger specialists competence level in the training center VUZF REVIEW. 2020. Vol. 5, No. 1. P. 50–53. DOI: https://doi.org/10.38188/2534-9228.20.1.07.
12. Heorhadze O., Kamalov Y. Methods for assessing the readiness level of an educational institution for military training of citizens according to the program of reserve officers // Political Science and Security Studies Journal. Vol. 1, No. 2. P. 90–97. DOI: https://doi.org/10.5281/zenodo.4521176.
13. Петров В. А., Георгадзе О. А. Часткова методика оцінювання рівня компетентностей з вогневої підготовки у громадян України, які навчаються за програмою підготовки офіцерів запасу // Збірник наукових праць військового інституту Київського Національного університету імені Тараса Шевченка. 2023. № 81. С. 47–54. DOI: http://doi.org/10.17721/2519-481X/2023/81-05.
14. Георгадзе О. А., Салаш О. А. Часткова методика оцінювання стану колективної підготовки органів військового управління // Збірник наукових праць військового інституту Київського Національного університету імені Тараса Шевченка. 2022. № 77. С. 161–171. DOI: https://doi.org/10.17721/2519-481X/2022/77-14.
15. Шевченко В. Л. Якісна схожість згорток в математичних моделях процесів розвитку складних систем // Телекомунікаційні та інформаційні технології. 2014. № 3 . С. 32–38.

Стаття надійшла до редакції 03.11.2025

A partial methodology for assessing the level of personnel readiness of a military unit under the legal regime of martial law

Annotation

The experience of employing military units of the Armed Forces (AF) of Ukraine during the repulsion of the armed aggression of the Russian Federation (RF) demonstrates that the successful accomplishment of combat (special) missions depends on the level of their combat capability. A decisive influence on the combat capability of a military unit is exerted by the level of personnel readiness. Combat training (collective training) is aimed precisely at achieving a high level of personnel readiness and encompasses both individual and collective training. The effectiveness of their organization and conduct directly determines the level of soldiers' proficiency and the cohesion of the structural subunits of a military unit.

Accordingly, there is a need for a scientifically substantiated partial methodology for assessing the level of personnel readiness of a military unit under the legal regime of martial law, as a component of a comprehensive methodology for evaluating its combat capability.

The purpose of the article is to present a partial methodology for assessing the level of personnel readiness of a military unit under the legal regime of martial law.

The improved partial methodology for assessing the level of personnel readiness of a military unit *takes into account* the readiness level of its structural subunits regarding their significance. It provides for the consideration of the aggregate level of personnel proficiency based on the selection of a new set of indicators characterizing individual capabilities, the availability of relevant military education and training, participation in combat operations, as well as the cohesion of these structural subunits, which reflects the importance of the final collective training event.

Keywords: readiness; assessment; proficiency; cohesion; individual capabilities; military education and training; participation in combat operations.

ВІДОМОСТІ ПРО АВТОРІВ

АРТАМОЩЕНКО В. С. – заступник начальника НУО України з наукової роботи, доктор військових наук, доцент;

БАЗАРНИЙ С. В. – заступник начальника НДВ дослідження проблем розвитку та впровадження стратегічних комунікацій Істиутту стратегічних комунікацій НУО України, доктор філософії;

ВОРОВИЧ Б. О. – провідний науковий співробітник НДВ ЦВСД НУО України, кандидат військових наук, доцент;

БЕЗБАХ В. С. – професор кафедри управління військами ІДВУ НУО України, кандидат військових наук, доцент;

ГАВРИЛЮК І. Ю. – старший науковий співробітник НДВ ЦНДІ ЗС України, кандидат військових наук, старший дослідник;

ГАНДЗЮК А. П. – провідний науковий співробітник НДВ інституту логістики та підтримки військ (сил) НУО України, кандидат технічних наук, старший науковий співробітник;

ГЕОРГАДЗЕ О. А. – заступник начальника Головного управління персоналу Генерального штабу Збройних Сил України, кандидат військових наук, доцент;

ГОРБАЧОВА Я. С. – старший викладач кафедри інфраструктурного та транспортного забезпечення інституту логістики та підтримки військ (сил) НУО України, доктор філософії;

ГОРДІЄНКО С. Б. – доцент кафедри технологій захисту кіберпростору Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України, кандидат технічних наук, доцент;

ГРІНЧЕНКО В. В. – доцент кафедри прикордонної служби факультету безпеки державного кордону Національної академія Державної прикордонної служби України імені Богдана Хмельницького, доктор філософії;

ГИБАЛО К. В. – ад'юнкт Національної академії Служби безпеки України;

ГУДИМА О. П. – заступник начальника ЦВСД НУО України, кандидат технічних наук, старший науковий співробітник;

ЖУРАХОВ О. В. – науковий співробітник НДВ НіНТД Центру протимінної діяльності Державної спеціальної служби транспорту;

ЗАГОРКА О. М. – головний науковий співробітник ЦВСД НУО України, доктор військових наук, професор;

ЗАХАРЧЕНКО Д. С. – молодший науковий співробітник НДВ НіНТД Центру протимінної діяльності Державної спеціальної служби транспорту;

ЗУБКОВ В. П. – старший науковий співробітник НДВ ЦВСД НУО України;

ІВАЩЕНКО А. М. – провідний науковий співробітник НДВ ЦВСД НУО України, кандидат технічних наук, доцент;

КАМАЛОВ Є. В. – докторант науково-методичного центру організації наукової і науково-технічної діяльності НУО України, доктор філософії, доцент;

КАСЬЯН С. П. – професор кафедри управління військами ІДВУ НУО України, кандидат педагогічних наук, доцент;

КОСЕВЦОВ В. О. – професор кафедри стратегії національної безпеки та оборони ІДВУ НУО України, доктор військових наук, професор;

КРЮКОВ М. І. – головний спеціаліст відділу контроля управління контролю та організаційно-планової роботи Департаменту інформаційно-організаційної роботи та контролю Міністерства оборони України;

МАЗУРЕНКО І. М. – начальник НДВ ЦВСД НУО України, доктор філософії;

МАШТАЛІР В. В. – начальник ЦВСД НУО України, доктор історичних наук, професор;

МИХАЙЛЕНКО О. В. – професор кафедри прикордонної служби факультету безпеки державного кордону Національної академія Державної прикордонної служби України імені Богдана Хмельницького, кандидат військових наук, доцент;

МОСОВ С. П. – професор кафедри авіації та авіаційного пошуку і рятування Інституту державного управління та

ВИМОГИ ДО СТАТЕЙ

Відповідно до Постанови ВАК України № 7-05/1 від 15 січня 2003 року наукові статті мають містити такі елементи:

постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями;

аналіз останніх досліджень і публікацій, у яких започатковано розв'язання даної проблеми і на які спирається автор, виділення нерозв'язаних раніше частин загальної проблеми, яким присвячується стаття;

формулювання **мети статті** (постановка завдання);

виклад **основного матеріалу** дослідження з повним обґрунтуванням отриманих наукових результатів;

висновки і перспективи подальших досліджень розвитку в цьому напрямі;

анотація до статті та ключові слова – розміщуються після назви статті.

У статті слід дотримуватись загальноприйнятої термінології. Усі скорочення та нові терміни мають бути розкриті автором.

Назва, список авторів, назва установи, анотація (не більше 40 слів), ключові слова (7 слів) готуються на трьох мовах: українській, російській та англійській.

Обсяг статті разом із таблицями, рисунками та списком літератури не більше 10 сторінок А4.

Текст статті набирається в редакторі **Microsoft Word** шрифтом **Times New Roman 14. Вирівнювання по ширині. Інтервал між рядками тексту – 1,0.**

Формат сторінки – А4. Поля: ліве – 27 мм; верхнє і нижнє – 20 мм; праве – 20 мм.

Не використовуйте для форматування тексту пропуски, табуляцію тощо. Не встановлюйте ручне перенесення слів, не використовуйте колонтитули.

Між значенням величини та одиницею її вимірювання ставте нерозривний пропуск (Ctrl + Shift + пропуск).

Таблиці та рисунки виконуються в одному стилі, нумеруються та подаються після посилань на них у тексті.

Текст усередині таблиці набирається в редакторі **Microsoft Word** шрифтом **Times New Roman – кегль 10.**

Таблиці нумеруються, вирівнювання по центру, без відступів. Слово "Таблиця 1" – ***кегль 11***, вирівняний по правій стороні. Формат назви таблиці: вирівнювання по центру, напівжирний, положення – над таблицею. Після таблиці необхідно залишити один порожній рядок.

Рисунки нумеруються, вирівнювання по центру. Формат назви рисунку – вирівнювання по центру, положення – під рисунком, позначається скороченим словом "Рис.". Перед рисунком і після його підпису необхідно залишити один порожній рядок.

Текст у середині рисунка набирається в редакторі **Microsoft Word** шрифтом **Times New Roman – *кегль 9–10*.**

Формули виносяться на середину рядків. Набір здійснюється у редакторі формул *MathType* курсивом (крім особливих випадків) без обрамлення і заливки. Забороняється використовувати для набору формул графічні об'єкти, кадри і таблиці.

Вирівнювання по центру, нумерація – у дужках, праворуч. Нумерувати потрібно тільки ті формули, на які є посилання у тексті.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ складається у порядку посилання в тексті та подається наприкінці статті згідно з ДСТУ ГОСТ 7.1:2015. – ***кегль 12***

У редакцію надається друкований примірних рукопису.

На останній сторінці робиться припис – "**Стаття не містить відомостей, що розкривають державну таємницю та службову інформацію. Автори надають дозвіл на перевірку праці відповідальними особами, призначеними для перевірки праць на оригінальність і відсутність неправомірних запозичень. Автори гарантують, що ними одержано всі необхідні дозволи на використання у цій статті матеріалів, що охороняються авторським правом. Автори гарантують, що ця стаття раніше не публікувалась і не подавалась до інших видань**". *Підписи авторів.*

До редакційної колегії подаються такі документи:

1. Файли, які містять ***текст статті українською*** та ***анотації*** (не менше 1800 знаків) **українською та англійською мовами** у форматі електронного документа **MS Word версія 2010**.

2. Довідка про авторів українською та англійською мовами (П.І.Б. – повністю, установа, посада, вчений ступінь, вчене звання, контактна інформація).

3. Акт експертизи щодо відкритого публікування (для зовнішніх авторів).

УВАГА! Статті, які не задовольняють будь-якій з перелічених вимог, до видання не приймаються.

ШАБЛОН СТАТТІ

УДК 628. 8 – ***Times New Roman кегль – кегль 12 пт***

Бунін В. В., доктор технічних наук, професор[1]; – ***Times New Roman кегль – кегль 14 пт***
Іванов В. А.[2]

V. Bunin, DsT[1], professor;
V. Ivanov[2]

[1] – Департамент воєнної політики та стратегічного планування Міністерства оборони України, Київ;
[2] – Центр воєнно-стратегічних досліджень Національного університету оборони України, Київ

[1] – Defence Policy and Strategic planning Department, Ministry of defence of Ukraine, Kyiv;
[2] – Center for Military and Strategic Studies of the National Defence University of Ukraine

Матрична модель OLAP-систем (*кегль 14 пт напівжирний*)

Матричная модель OLAP-систем

Matrix model of OLAP-systems

Резюме (2-3 речення). Розглянуто особливості матричних моделей … ***(кегль 12 пт)***

Анотація (1800 знаків).

Ключові слова: модель, OLAP-система, інформаційні технології.

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 ; p k; p=1 ; n *– Times New Roman 10 шрифт;*
k 2

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

№ 3(86), 2025

Відповідальний за випуск А. А. Рибидайло
Технічний секретар Л. А. Панасевич
Комп'ютерне верстання А. А. Рибидайло
Коректори: Н. М. Андріянова, В. О. Капілевич, І. О. Ліпко,
Ю.В. КондратенкоТ. В. Уварова
Підтримка вебсайту збірника Ю. А. Кірпічніков, М. В. Петрушен

Підписано до друку 29.12.2025. Формат 60х84 1/8.
Папір офсетний. Обл.- вид. арк. 8,55. Друк. арк. 18,75
Зам. 396. Наклад 100 прим.

Видання Національного університету оборони України
03049, м. Київ, просп. Повітряних Сил, 28
http://znp-cvsd.nuou.org.ua

Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів видавничої
продукції, серія ДК № 2205 від 02.06.2005.

Надруковано у друкарні Національного університету оборони України
03049, м. Київ, просп. Повітряних Сил, 28