DOI:**10.33099/2311-7249/2022-45-3-37-44**

УДК 355.4+623.4:004

Віталій Васильович Злакоман [1]
Валерій Валентинович Гордійчук *(кандидат технічних наук, старший дослідник)* [2]

[1] ***Операційне командування Повітряних Сил Збройних Сил України, Вінниця, Україна***
[2] ***Національний університет оборони України імені Івана Черняховського, Київ, Україна***

КОНЦЕПЦІЯ МУЛЬТИДОМЕННИХ ОПЕРАЦІЙ ДЛЯ ОБОРОНИ УКРАЇНИ: ТЕХНОЛОГІЧНИЙ АСПЕКТ

Форми, методи і засоби ведення війни в усі часи існування людства безпосередньо залежали від науково-технологічного прогресу. З освоєнням космосу, стрімким розвитком робототехніки, штучного інтелекту, інформаційних та комп'ютерних технологій суттєвих змін зазнали погляди провідних держав та воєнно-політичних блоків на питання концептуальних підходів до процесів планування і ведення операцій.

Сучасні війни і війни майбутнього розглядаються як багатовимірні та високотехнологічні. В основі міждержавної стратегічної конкуренції останнім часом спостерігається тенденція до збільшення ролі політичних, дипломатичних, економічних та інформаційних методів протиборства у конфлікті, а середовищем військових протистоянь розглядаються п'ять доменів: суша, море, повітряний простір, космічний простір та кіберпростір.

У зв'язку із цим, широкого розповсюдження серед країн-членів НАТО набуває поняття "мультидоменна операція" як найбільш ефективний інструмент досягнення оперативних і тактичних цілей. Перемога у сучасному конфлікті у більшій мірі стає залежною від технологічної переваги, аніж від чисельності армій і кількості бойової техніки. Основним завданням, що ставиться при розробці концепцій мультимедійної операції, розглядається можливість максимально ефективного застосування наявних сил та засобів з усіх доменів при найменших втратах. Досягнення поставленої мети виглядає можливим виключно за рахунок комплексного використання сучасних технологій: штучного інтелекту, швидкісних мереж та протоколів передачі даних, хмарних сховищ зберігання і обчислення даних, аутентифікації доступу, криптографічного захисту інформації, тощо.

В роботі розглянуто суть концепції мультимедійної операції, проведено аналіз сучасних технологій, які використовуються, або заплановані до використання провідними країнами для забезпечення концепцій мультимедійної операції, а також визначено можливі напрямки розробки концепції мультимедійної операції для оборони України на основі сучасних технологій.

Ключові слова: *міждержавна стратегічна конкуренція, воєнний конфлікт, мультидоменні операції, інформаційні технології, автоматизована система управління.*

Вступ

Аналіз подій останніх десятиліть вказує на поглиблення світової політичної кризи, загострення дипломатичних відносин та конфронтацію між окремими державами та воєнно-політичними блоками. На сьогоднішні питання міждержавної стратегічної конкуренції винесено на перший план оборонних доктрин більшості провідних країн світу, таких, як наприклад, Сполучені Штати Америки (США) [1].

З розвитком робототехніки, штучного інтелекту, військових, інформаційних та комп'ютерних технологій фундаментальних змін зазнали способи ведення збройної боротьби, а протистояння між країнами перейшли у багатовимірний простір і ведуться комплексно на всіх рівнях: стратегічному, оперативному та тактичному.

Стратегічна міждержавна конкуренція починається не на полі бою, а далеко за його межами: на політичному, дипломатичному, економічному, соціальному та інформаційному фронті.

Оперативні і тактичні збройні протистояння між арміями противників, які ще не так давно мали місце у тривимірному просторі (на суші, на морі та у повітрі), в наші дні знаходять своє розповсюдження також в інших середовищах: в космосі та кіберпросторі.

Постановка проблеми. Розширення середовища проведення військових операцій на тлі глобального технологічного прогресу та загострення міжнародних відносин створюють умови для перегляду діючих та створення нових концептуальних підходів до процесів планування і ведення бойових дій.

Провідними країнами НАТО на основі оцінки сучасних загроз своїй національній безпеці найбільш перспективним напрямком розглядається впровадження концепції ведення "мультидоменних операцій" (МДО).

У випадку з Україною, в умовах повномасштабної війни критично необхідним і важливим також є питання розроблення і

впровадження власної концепції, яка відповідатиме сучасним викликам та загрозам.

Аналіз останніх досліджень і публікацій. За результатами аналізу воєнно-політичної обстановки у світі, а також інформації з доступних джерел щодо поглядів у провідних країнах на війни майбутнього, найбільш перспективним напрямком розглядається впровадження концепції ведення МДО [1-10].

Термін "мультидоменна операція" вперше був використаний і описаний у 2018 році в публікації "Сухопутні війська США в мультидоменних операціях 2028" [2].

В зазначеній концепції поняття "мультидоменні операції" означає узгоджені за місцем і часом операції, які проводяться в декількох сферах (доменах) і оспорюваних просторах для подолання сильних сторін противника, пред'явивши йому декілька оперативних та/або тактичних дилем шляхом комбінованого (змішаного) застосування визначених військ (сил), залучених до побудови мультидоменного угруповання, в тісній взаємодії сил і засобів між різними сферами, з метою досягнення визначеної оперативної і тактичної мети (рис. 1) [5].

Рис. 1. Концепція мультидоменних операцій

За межами армії США, зокрема в інших країнах-членах НАТО, поняття МДО є більш загальним, і очевидно, що для різних країн має різне значення. Існують також пов'язані поняття, наприклад "мультидоменна бойова хмара", яка розглядається як намагання створити зв'язки між керованими та некерованими платформами з підтримкою ШІ [3].

На стадії розробки власної концепції МДО знаходиться також Стратегічне Командування Міністерства оборони Великобританії, яке розглядає її як інструмент досягнення визначених цілей шляхом безперешкодної спільної інтегрованої роботи усіх міністерств, відомств, союзників та партнерів [4].

За прикладом більш потужних партнерів, розгляд і розробка національних концепцій, а також можливості їх спільної інтеграції здійснюється іншими країнами-членами НАТО [6, 7].

Певні ознаки мультидоменних операцій були практично продемонстровані під час військового вторгнення в Сирію російською федерацією та в ході повномасштабного збройного вторгнення в Україні [11, 12].

За досвідом розвинених країн, з метою створення умов для найбільш ефективного застосовування наявних ресурсів держави для оборони в ході відсічі існуючої збройної агресії з боку російської федерації та запобігання її виникненню в майбутньому, стратегічно важливим питанням для України є розроблення власної концепції МДО, технологічним базисом якої має стати єдина АСУ, побудована з використанням сучасних інформаційних технологій: ШІ, швидкісних мереж і протоколів передачі даних, хмарних сервісів збереження і обробки даних, криптографічного захисту інформації, тощо.

Мета статті. Проаналізувати сучасний стан впровадження і технології реалізації концепцій МДО в провідних країнах світу, визначити технологічні аспекти розроблення концепції МДО для оборони України.

Для дослідження проблем означених в роботі, використано методи стратегічного аналізу, зокрема: метод екстраполяції, SWOT-аналіз, емпіричних досліджень.

Виклад основного матеріалу дослідження

1. Суть концепції мультидоменних операцій.

Розроблення концепції МДО в США було обумовлено внесеними змінами в Стратегію національної оборони 2018 року [8], в якій зазначено, що головною загрозою національній безпеці є міждержавна конкуренція, а не тероризм, як було визначено в попередньому документі. Зміщення акцентів відбувається у зв'язку зі зміною поведінки важливих стратегічних конкурентів, в першу чергу Китаю і росії, які своєю зовнішньою політикою демонструють бажання сформувати світовий порядок, який відповідатиме їхній авторитарній моделі – з правом вето на рішення у сфері безпеки, а також дипломатичні та економічні дії інших країн.

Зазначені противники намагаються використовувати умови оперативного середовища для досягнення своїх цілей, не вдаючись до збройного конфлікту. Протистояння ведеться шляхом впливу на дипломатичні та економічні процеси, ведення гібридної та інформаційної війни (через засоби масової інформації, соціальні мережі, кібератаки, тощо), а також фактичного застосування регулярних збройних сил. Таке протистояння серед країн заходу отримало термін "гібридне", або "не конвенційна війна". Створюючи нестабільність всередині країн і альянсів, Китай і росія стимулюють виникнення політичних протиріч, що призводить до стратегічної невизначеності, знижують швидкість реакції та спільного прийняття рішень союзниками. Завдяки цим діям створюються умови, за яких досягнення політичних цілей відбувається без розв'язання збройного конфлікту [2].

З іншого боку, основні стратегічні конкуренти

США продовжують використовувати набутий досвід проведення військових операцій та функціонування доктрин, синтезуючи новітні технології, та здійснюють розгортання засобів боротьби в усіх сферах в багаторівневому вимірі – на суші, на морі, у повітрі, в космосі та в кіберпросторі. В концепції "Сухопутні війська США в мультидоменних операціях 2028" начальник штабу Сухопутних військ США генерал Марк Міллі наголошує на необхідності безперервного розвитку та гнучкої адаптації до сучасних умов протистояння, а даний документ розглядає лише як перший крок в доктринальній еволюції армії США, як основу для подальшого обговорення, аналізу та розвитку [9].

Результатом п'ятирічної роботи над удосконаленням концепції МДО стала публікація у жовтні 2022 року нової доктрини МДО армії США, яка прийшла на заміну публікації від 2017 року та отримала назву "Field Manual 3-0. Operations" [5]. Командування армії США наголосило на тому, що зазначена доктрина стане ключовим керівництвом для збройних сил на період до 2030 року.

Таким чином, мультидоменні (багатосферні) операції – це комплексне застосування спроможностей наявних об'єднаних мультифункціональних сил в усіх сферах та вимірах з метою створення відносної переваги і її використання для досягнення визначеної мети – перемоги над противником. Застосування потенціалу об'єднаних сил в усіх доменах дозволяє досягти визначеної мети з найменшими втратами в кожному з них. Мультидоменні операції є своєрідною формою ведення збройної боротьби спільною кампанією наявних сил. До порогу виникнення збройного конфлікту МДО застосовуються для стримування противника, демонстрації готовності збройних сил до участі в бойових діях. В ході ведення бойових дій МДО застосовуються як асиметрична відповідь та виконують завдання: по зближенню з противником, подолання його оперативної побудови, захоплення критичних об'єктів та ділянок місцевості, знищення противника, здійснення контролю над населенням та ресурсами до досягнення стійких політичних рішень. Усі сучасні операції по своїй суті мають ознаки мультидоменних і проводяться у багатовимірному середовищі (рис. 2). Так, сухопутні війська в ході бойових дій постійно використовують авіацію та флот для переміщення військ, а можливості космосу та кіберпростору, які вони не контролюють – для організації і забезпечення супутникового зв'язку, навігації, отримання розвідданих, а також ведення розвідки та спостереження [10].

За межами США в інших країнах-членах НАТО поняття МДО розглядається з різним розумінням, але, незалежно від того, який зміст вкладають різні держави в поняття МДО, присутнє єдине розуміння необхідності розробки нових технічних рішень, які відповідали б сучасним викликам, пов'язаним із майбутніми високотехнологічними війнами. Безпосередньо в штаб-квартирі Верховного головнокомандувача об'єднаних збройних сил НАТО в Європі в червні цього року було проведено засідання по переходу до мультидоменних операцій як логічний розвиток війни, в ході якого керівником Об'єднаного воєнного центру наголошено на необхідності розробки понятійного апарату для МДО. В першу чергу це стосується питань використання космосу та кіберпростору. Основним завданням розглядається можливість об'єднання усіх видів інформації з урахуванням використання новітніх технологій для полегшення процесів прийняття рішень командувачами. Для цього, зокрема, в систему колективної підготовки командувачів та штабів, окрім навчання веденню операцій в традиційних фізичних просторах (на суші, на морі та в повітрі) включено визнані НАТО інші домени: космос та кіберпростір. Кінцевою метою підготовки передбачається, що будь-який офіцер об'єднаного штабу в командній структурі НАТО повинен чітко розуміти питання створеної системи управління та кінцеву мету мультидоменної операції в цілому, а також бути спроможним виконувати визначені функції в однотипних штабах. Так би мовити, бути спроможним ефективно взаємодіяти з іншими офіцерами та виконувати завдання, спілкуючись зрозумілою для всіх операційною термінологією [3].

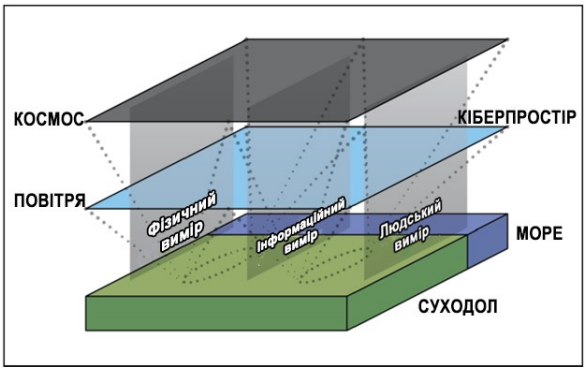

Рис. 2. Сфери і виміри операційного середовища

Великобританія основні зусилля у даному напрямку визначила на вирішенні можливості здійснення схожої концепції – багатодоменної інтеграції (MDI) між трьома рівнями: органами державної влади, багатодоменним середовищем ведення операцій та союзниками (рис. 3) [7]:

Основним завданням MDI розглядається можливість забезпечення безперебійної спільної роботи всієї системи оборони з іншими державними установами та союзниками шляхом [6]:

інтегрування в єдину систему всього доступного обладнання і технологій в усіх сферах;

створення та удосконалення ІТ-мереж, що дозволить забезпечити обмін потоками даних з датчиків в усіх доменах;

використання технології ШІ та хмарних обчислень для найбільш швидкої обробки інформації і надання її особам, відповідальним за прийняття рішень в усіх органах державної влади;

інтегрування усіх існуючих інформаційних державних систем з інформаційними системами партнерів і союзників з метою уникнення їх дублювання;

навчання персоналу спільним діям та використанню сучасних розробок під час комплексних навчань з партнерами та союзниками;

розробки завчасних планів спільних дій з партнерами і союзниками, а не реагування на загрози за необхідності.

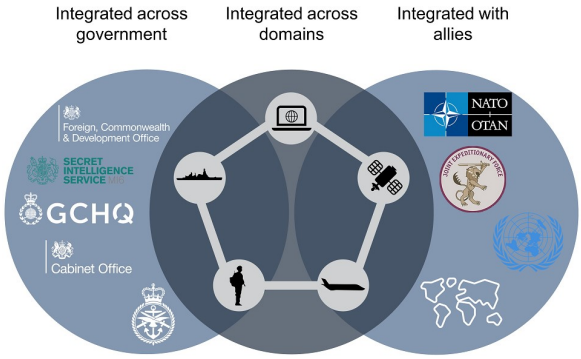

Рис. 3. Концепція багатодоменної інтеграції (MDI) у Великобританії

У своїй статті [11] Рейнольд Дінсдейл зауважує, що ще в 2015 році елементи проведення МДО чітко прослідковувались в ході воєнної кампанії з вторгнення російської федерації в Сирію. Російські сили для досягнення визначеної мети вели ефективні бойові дії в усіх п'яти доменах. Практично одночасно відбувалось застосування крилатих ракет для нанесення ударів з району Каспійського моря, накопичення підводних човнів-ракетоносіїв в Середземному морі, створення складної та інтегрованої системи протиповітряної оборони, налагодження ланцюгів логістичного постачання з використанням порту Тартус і авіабази Хмеймім, ведення повітряної розвідки та цілевказання з використанням авіації та БПЛА, ведення інформаційної кампанії в засобах масової інформації з виправданням дій політичних режимів путіна і АСАДА (рис. 4).

Рис. 4. Застосування концепції МДО російською федерацією в Сирії

В огляді "Гібридна війна – гібридна відповідь?" [12] політичні та військові діячі НАТО зауважують на комплексному застосуванні росією у війні проти України інструментів гібридної війни. Визначену політичну мету російська федерація спробувала досягти невійськовими засобами за рахунок інформаційного, політичного, дипломатичного, економічного, правового впливу та використання регулярних збройних сил без засобів розпізнавання під виглядом незадоволеного місцевого населення та загонів самооборони.

У даний спосіб було здійснено спробу встановлення контролю над Україною без безпосереднього військового втручання, фактично не оголошуючи війни та не порушуючи норми міжнародного законодавства. Не досягнувши мети невійськовими засобами, рф 24 лютого 2022 року розпочала повномасштабне військове вторгнення, яке містило усі ознаки МДО:

масований одночасний ракетний удар по об'єктам військової інфраструктури, пунктам управління та позиціям засобів протиповітряної оборони;

застосування авіації з метою досягнення переваги у повітрі та десантування повітряних десантів;

масштабний наступ підрозділів сухопутних військ з різних напрямків;

кібернетичну атаку на інформаційно-телекомунікаційні системи сил оборони України;

придушення роботи засобів навігації та супутникового зв'язку;

радіоелектронне подавлення наземного і повітряного радіообладнання.

2. Технологічний аспект концепції мультидоменних операцій.

США та НАТО. Проведення сучасних МДО передбачає, в першу чергу, протистояння в області останніх технологічних досягнень, тому їх технічна складова має містити передові технології, які забезпечать ефективну систему ситуаційної обізнаності та управління військами. Такі складові покладені в основу нового Меморандуму про взаєморозуміння між Сухопутними військами та Військово-Повітряними Силами збройних сил США, який отримав назву Об'єднане вседоменне управління (Joined All-Domain Command and Control – JADC2) [3]. Для Військово-Повітряних Сил США проведення МДО полягає у використанні найсучасніших засобів та систем управління, зв'язку, розвідки і спостереження (C4ISR) під міткою мультидоменного управління і контролю (MDC2), доктринально визначених як об'єднані вседоменні операції (JADO). В Об'єднаному комітеті штабів триває спільна робота з розробки інтегрованого сервісу об'єднаної вседоменної системи управління, таких як MDC2 та JADC2 [3].

Найбільш пріоритетним напрямком модернізації армії США в найближчий час розглядається удосконалення АСУ військами. Для реалізації цієї ідеї було сформовано Командування Сухопутних Військ США Майбутнього (Army Futures Command – AFC). До його складу входить Командування розвитку бойових спроможностей (Combat Capabilities Development Command –

CCDC), яке складається з семи Центрів. Основним завданням цього командування визначено формування концепції майбутнього, а також синхронізація і інтеграція науково-технічних підрозділів в рамках заходів по створенню збройних сил майбутнього. Ключовим напрямком роботи зазначених структур є подальший розвиток єдиної інформаційної мережі, що повністю захищена від впливу противника. Технічні деталі цих процедур є конфіденційними. Відомо лише, що розробники концентруються на чотирьох напрямках модернізації АСУ військами: безпосереднє створення і удосконалення єдиної мережі; створення спрощеного набору командних застосунків; покращення взаємодії між елементами армії, партнерами та союзниками; забезпечення живучості командних пунктів [17].

З метою обміну інформацією про дослідження кіберзахисних можливостей для МДО і покращення оперативної сумісності між Центром розвитку систем управління, зв'язку, кібербезпеки, розвідки та спостереження (Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) Center) Командування розвитку бойових спроможностей Командування Сухопутних Військ США Майбутнього та Міністерством оборони Естонії створено багатопрофільну робочу групу з операцій у кіберпросторі, завданням якої є визначення можливості для експериментів і демонстрації функціональної сумісності [15].

Своєчасний і швидкий обмін даними між різними суб'єктами і штабами, що залучені до проведення МДО, є запорукою успіху. Це можна забезпечити шляхом вибору оптимальної архітектури обміну даними. Необхідно запровадити гнучку структуру оперативної сумісності та оперативного управління, оскільки операції проводитимуться в динамічному середовищі та з обмеженими ресурсами. Системи розвідки (ISR), що розробляються в даний час для виявлення і супроводу цілей в глибині поля бою, будуть далі розвиватися, як і засоби знищення цілей, які стали б більш точними і могли б працювати з іще більшої відстані. Розвідувальні системи будуть все глибше інтегровані в єдину мережу, яка дозволяла б отримувати інформацію від різноманітних датчиків, безпілотних розвідувальних платформ, а також наземних, морських, повітряних підрозділів і супутників у космосі. Для успішного проведення МДО потрібні не тільки військова складова і можливості партнерів, а й усі інші доступні невійськові засоби, що можуть сприяти досягненню мети [1].

В 2020 році в НАТО було проведено і опубліковано спеціальне дослідження "Тренди в науці і технологіях 2020-2040" [17]. Ключовим завданням Альянсу визначено забезпечення живучості системи стратегічного і оперативного управління, зв'язку, розвідки і спостереження (C4ISR). Але, відкрито ведуться розмови лише про розробки тактичного рівня, які можна придбати переважно всередині Альянсу. Одним із найбільш надійних вважається пакет програмних продуктів SitaWare датської компанії Systematic, який забезпечує впровадження автоматизованого управління на рівні підрозділу. Дане рішення забезпечує управління і обмін інформацією в режимі реального часу від штабу до окремого екіпажу чи солдата. SitaWare здатна об'єднати інформацію поля бою в єдину операційну картину, що дозволяє командиру і його штабу правильно оцінювати поточну обстановку. Відомо, що такі системи успішно зарекомендували себе в операціях НАТО і були закуплені майже двома десятками країн [17].

Росія. В лютому місяці 2021 року міністр оборони рф шойгу заявив, що головним напрямком розвитку армії стає впровадження технологій штучного інтелекту в озброєння, які визначають перспективний склад збройних сил, а також розвиток систем АСУ [17].

За інформацією з відкритих джерел, з 2018 року на озброєнні армії росії з'явилась мобільна АСУ оперативно-стратегічного рівня "Акация-М", яка використовує так званий мережецентричний принцип управління, в якому всі структурні елементи зав'язані в єдину мережу. Це дозволяє на практиці реалізувати ідею створення ровідувально-вогневих і розвідувально-ударних контурів, синхронізувати в режимі реального часу цикли розвідки, планування та ураження противника. АСУ військами власного виробництва "Акация" складає технічну основу всієї АСУ збройних сил рф. Вона використовується для прискореного аналізу сил противника, власних сил і формування плану бойових дій. Фактично відбувається миттєве моделювання різноманітних сценаріїв, а ШІ автоматично пропонує найбільш прийнятний для зазначених умов варіант. Крім того, з різним ступенем деталізації, рішення доводиться до усіх підрозділів. Таким чином, навіть окремі екіпажі і розрахунки перебувають в єдиному цифровому полі, отримуючи усю необхідну інформацію (рис. 5).

Заявлено, що АСУ військами "Акация-М" забезпечує оперативно-стратегічне і оперативне управління збройними силами рф. Оперативно-тактичне і тактичне управління військами здійснюють комплекси Єдиної системи управління тактичної ланки (ЕСУ ТЗ) "Созвездие-М2" для сухопутних військ і "Андромеда-Д" для повітряно-десантних військ [17].

Рис. 5. Організація взаємодії в єдиній інформаційній мережі АСУВ "Акація"

Як зазначено [16], ЕСУ ТЗ призначена для комплексного управління військами з використанням систем навігації, а також супутникових та безпілотних систем наведення. ЕСУ ТЗ прийнята на озброєння в 2018 році, незважаючи на те, що роботи над її розробкою розпочалась більше двадцяти років тому на початку 2000-х. В РФ заявляють, що ЕСУ ТЗ – це єдина система управління боєм, яка включає у себе 11 підсистем, що здійснюють управління системами радіоелектронної боротьби, артилерії, протиповітряної оборони, інженерним і матеріально-технічним забезпеченням, а також єдину інформаційну мережу, в яку інтегровані різноманітні види зв'язку, у тому числі радіорелейний, тропосферний і цифровий [16].

Україна. За досвідом провідних країн, з урахуванням існуючих загроз національній безпеці, основними завданнями при розробці та впровадженні концепції МДО для оборони України слід розглядати створення умов для:

максимально ефективного використання усіх наявних ресурсів держави для ведення війни в багатовимірному просторі: на суші, на морі, в повітрі, в космосі та в кіберпросторі;

удосконалення процесів планування та ведення операцій, спрощення процесів прийняття управлінських рішень;

підвищення ефективності, оперативності та стійкості управління силами оборони України;

підвищення ефективності взаємодії між складовими сил оборони в ході підготовки (стримування) збройного конфлікту та під час його ведення.

Сучасні бойові дії характеризуються швидкою зміною умов обстановки, відповідно і обмеженим часом для прийняття рішень. Від оперативності, гнучкості та ефективності управління залежать результати виконання тактичних і оперативних завдань. Тому, на етапі підготовки, а також під час ведення операцій потрібно створити такі умови, за яких командувачі об'єднаними силами матимуть:

єдину спрощену доктринальну базу з питань ведення операцій;

навчений та підготовлений особовий склад підпорядкованих штабів;

постійний доступ до інформації про стан та положення противника і своїх військ в режимі реального часу.

Тому, подальшу роботу із впровадження сучасної концепції ведення операцій пропонується провести у наступних напрямках:

упорядкування діючої нормативно-правової бази;

проведення навчання особового складу штабів та внесення змін в організаційно-штатні структури;

розроблення єдиної (з інтегрованими підсистемами та інформаційними система) АСУ військами і взаємодії (або інтегрування існуючих) та проведення технічного оснащення підрозділів.

За прикладом США, роботу у даному напрямку доцільно розпочати з розроблення єдиної доктрини для СО України, яка буде чітко визначати основні складові МДО, а саме:

типи операцій, цілі і принципи їх проведення;

сили і засоби, що можуть залучатись;

масштаби проведення операцій;

порядок планування операцій;

єдиний порядок бойового забезпечення проведення операцій;

порядок управління і взаємодії в ході підготовки і ведення операцій (в першу чергу: спрощений та більш гнучкий процес передачі підрозділів в оперативне підпорядкування іншим командувачам; чітке розмежування повноважень і відповідальності командувачів під час прийняття рішень та віддання наказів (розпоряджень); спрощена процедура відпрацювання і доведення наказів та розпоряджень, взаємодії та обміну інформацією між різними складовими і органами місцевого самоврядування).

Другим важливим кроком є питання навчання особового складу підпорядкованих штабів концептуальним підходам до проведення МДО в системі колективної підготовки за прийнятими у країнах НАТО стандартами.

Технічним аспектом впровадження концепції МДО для СО України є розроблення єдиної АСУ військами і взаємодії та проведення технічного оснащення підрозділів.

З урахуванням зазначених потреб та стану розвитку інформаційних і комп'ютерних технологій, єдина АСУ і взаємодії повинна відповідати наступним вимогам:

використовувати єдину базу даних з максимальною швидкістю роботи та проведення обчислень;

забезпечувати кіберзахищенність, збереження інформації та шифрування даних;

забезпечувати процедуру надійної верифікації та ідентифікації користувачів, чітке розмежування прав доступу до інформації;

мати максимально простий та інтуїтивно зрозумілий інтерфейс.

Міністр оборони України Олексій Резніков повідомив, що з 6 грудня 2022 року на озброєння Збройних Сил України прийнято автоматизовану систему управління бойовими діями "Дзвін АС" (рис. 6) [14].

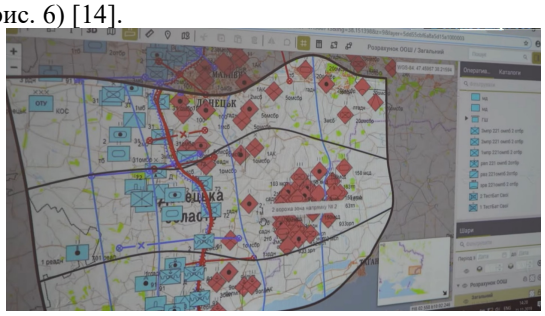

Рис. 6. Автоматизована система управління бойовими діями "Дзвін АС"

Як заявлено, можливості цієї автоматизованої системи управління та контролю бойовими діями стратегічного, оперативного і частково тактичного ("бригада") рівнів дозволяють:

у напівавтоматичному та автоматичному режимах генерувати документи бойового

управління;

створювати та відслідковувати картографічну інформацію;

отримувати вичерпні дані про власні війська; отримати наявні розвіддані; отримати дані про війська противника, їх поточне і перспективне забезпечення;

проводити розрахунки співвідношення сил і засобів, оптимальності їх застосування у різних сценаріях.

На сьогоднішній день також завершено проведення дослідно-конструкторських робіт (ДКР) інших АСУ, які в перспективі можливо інтегрувати в єдину АСУ Збройних Сил України. Це АСУ авіацією та протиповітряною обороною Повітряних Сил "Ореанда ПС" і АСУ тактичної ланки управління "Простір". Незавершеними залишились багато розробок АСУ для інших родів військ та сил, серед яких: "Логістика ІТ", "Регламент ІТ", "Базис", "Сфера", "Радник" [17].

Суттєвим недоліком усіх перелічених вище розробок є низький рівень відповідності автоматизації процесів сучасному рівню розвитку технологій. За своїми функціональними можливостями зазначені технології відносяться більше до засобів інформатизації (певною мірою автоматизовані інформаційні системи), а не автоматизації.

Щоб зазначені чи перспективні АСУ відповідали вимогам сучасного бою (операції) необхідно забезпечити відповідні:

пропускну здатність (час передачі інформації + час для прийняття рішення + час переміщення + час бойового розгортання < встановленого терміну на виконання завдання);

стійкість та прихованість (живучість + розвідзахищеність + завадостійкість + перешкодозахищеність після впливу противника мають забезпечити мінімально необхідну для виконання завдань швидкість доставки та обробки інформації);

безпеку передачі даних (конфіденційність + доступність + цілісність інформації);

обчислювальні технології та потужності для зберігання та обробки великих масивів даних.

Виконання зазначених вимог дозволить вигравати війни сучасності та майбутнього, але для їх забезпечення необхідне впровадження проривних технологій вже зараз, в цьому сенсі потрібно бути як мінімум на крок попереду противника. Прикладами таких технологій можуть бути: п'яте покоління мобільних мереж або п'яте покоління бездротових систем 5g; розподілена база даних створена за технологією блокчейну (blockchain); мобільні пакетні радіомережі, які не мають фіксованої інфраструктури – це мережі стаціонарних (Ad Hoc) і мобільних (MANET) абонентів; різноманітні технології на базі штучного інтелекту; нові способи використання супутникового зв'язку, зокрема з допомогою сузір'я комерційних супутників на низькій та середній орбітах; так звана технологія "бойової хмари" для підключення будь-якого датчика до будь-якого оператора у всіх доменах; тощо.

Висновки й перспективи подальших досліджень

На фоні існуючих політичних, дипломатичних, економічних та військових протиріч між провідними світовими державами, а також технологічного прогресу, розвитку військових, інформаційних та комп'ютерних технологій і штучного інтелекту сучасні війни та війни майбутнього розглядаються як такі, що вийшли за межі ведення в звичайному трирівневому вимірі (на суші, на морі та у повітрі). Вони знайшли своє поширення також в інших середовищах: у космосі та кіберпросторі. Тому, планування і проведення майбутніх військових операцій переважною більшістю розглядається як одночасна комплексна протидія противнику у багатовимірному просторі в усіх доменах. У військовій термінології країн НАТО даний тип операцій описується як "мультидоменні операції".

За результатами проведеного аналізу сучасного стану впровадження і технології реалізації концепцій МДО в провідних країнах світу можна зробити наступні висновки:

сучасні виклики та загрози національній безпеці України потребують від військового та політичного керівництва нашої держави швидкого та ефективного реагування на усі зміни, що відбуваються у світі, і пріоритетним питанням у цьому напрямку є розробка і впровадження власної концепції МДО для СО;

з урахуванням повномасштабної війни проти російської федерації; обраного політичного та військового курсу інтеграції з провідними західними країнами; швидкого оснащення сил оборони України зразками озброєння та військової техніки країн-членів НАТО основним вектором розвитку військових технологій для СО України є розробка власної єдиної АСУ управління і взаємодії, яку в перспективі можливо буде інтегрувати до подібних систем Альянсу.

Проведення подальших досліджень із заданого питання слід здійснювати у трьох основних напрямках:

удосконалення доктринальної нормативно-правової бази з питань проведення МДО;

організації системи підготовки персоналу за прийнятими у НАТО принципами, при цьому, в ході планування заходів колективної підготовки використовувати можливості технології штучного інтелекту з метою здійснення математичного моделювання нових сценаріїв навчань, що включають оперативні дилеми на основі існуючих світових політичних, економічних, соціальних та культурних міркувань та протиріч;

розроблення єдиної АСУ управління і взаємодії для СО України, побудованої з використанням сучасних технологій: штучного інтелекту, швидкісних мереж і протоколів передачі даних (таких як: розподілена однорангова Mesh-мережа, Ad hoc і MANET мережі з випадковими стаціонарними і мобільними абонентами, мереж мобільного зв'язку п'ятого покоління 5G), хмарних сервісів збереження і обробки даних, криптографічного захисту інформації (наприклад, технологія блокчейну), тощо.

Література

1. Multi-Domain Battle: Evolution of Combined Arms for the 21st Century (2025-2040). Version 1.0, December 2017. URL: https://www.tradoc.army.mil/wp-content/uploads/10/ MDB_Evolutionfor21st.pdf. **2. Andrew Feickert**. Defense Primer: Army Multi-Domain Operations (MDO) // Congressional Research Service, November 21, 2022. URL: https://sgp.fas.org/crs/natsec/IF11409.pdf. **3.** Understanding Multi-Domain Operations in NATO // The Three Swords Magazine 37/2021, p.91-94. URL: https://www.jwc.nato.int/ application/files/1516/3281/0425/issue37_21.pdf.
4. Andrew Tunnicliffe. Multi-domain operations in the future battlespace // Army Technology, September 12, 2022. URL: https://www.army-technology.com/analysis/multi-domain-operations-in-the-future-battlespace/.5. **Jan Judson.** US Army adopts new multidomain operations doctrine // October 10, 2022. URL: https://www.defensenews.com/ land/2022/10/10/us-army-adopts-new-multidomain-operations-doctrine/. **6. Donatas Palavenis.** Options for Small NATO Countries to Prepare for Multi-Domain Operations // Small Wars Journal, June 16, 2022. URL: https://smallwarsjournal.com/jrnl/art/options-small-nato-countries-prepare-multi-domain-operations. **7.** Guidance. Multi-Domain Integration // January 17, 2022. URL: https://www.gov.uk/guidance/multi-domain-integration. **8.** Summary of the 2018 National Defense Strategy of The United States of America. Sharpening the American Military's Competitive Edge. URL: https://dod.defense.gov/Portals/1/Documents/pubs/ 2018-National-Defense-Strategy-Summary.pdf. **9.** The US Army in Multi-Domain Operations 2028 // TRADOC Pamphlet 525-3-1, December 6, 2018. URL: https://api.army.mil/ e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf. **10.** Field Manual 3-0 Operations // Headquarters Department of the Army, Washington DC, October 01, 2022. – 280 pages. URL: https://irp.fas.org/doddir/army/fm3-0.pdf. **11. Ranald Dinsdale.** Multi-Domain Integration Demystified // October 11, 2021. URL: https://stratcommand.blog.gov.uk/ 2021/10/11/multi-domain-integration-demystified/.
12. Hybrid war - hybrid response? // NATO Review, July 1, 2014. URL: https://www.nato.int/docu/review/ articles/2014/07/01/hybrid-war-hybrid-response/index.html.
13. Застосування Сухопутних військ Збройних Сил України у конфліктах сучасності: Збірник тез доповідей науково-практичної конференції 18 листопада 2021 року. – Львів: НАСВ, 2021. – 210 с. URL: https://slyusar.kiev.ua/Slyusar_Lviv_2021_1.pdf.
14. Система управління "Дзвін АС" стала на озброєння України // Мілітарний, 08.12.2022. URL: https://mil.in.ua/ uk/news/systema-upravlinnya-dzvin-as-stala-na-ozbroyennya-ukrayiny/. **15. Edric Thompson.** US Army and Estonia sign historic agreement for collaborative research in cyber defense, September 14, 2020. URL: https://www.army.mil/us_army_estonia_sign_agreement.
16. Чому Україна не готова до війни майбутнього? // Оборонно-промисловий кур'єр, 29.03.2021. URL: https://opk.com.ua/чому-україна-не-готова-до-війни-майбут. **17. Raja Datta.** Security for Mobile Ad Hoc Networks// Science Direct. Handbook on Securing Cyber-Physical Critical Infrastructure, 2012, p. 95-98. URL: https://www.sciencedirect.com/book/9780124158153/handbook-on-securing-cyber-physical-critical-infrastructure.

CONCEPTION OF MULTIDOMAIN OPERATIONS FOR THE DEFENSIVE OF UKRAINE: TECHNOLOGICAL ASPECT

***Vitalii Zlakoman*[1]**
***Valerii Hordiichuk* *(Candidate of Technical Sciences, Senior fellow)*[2]**

[1]Air Force Operational Command of the Armed Forces of Ukraine, Vinnytsya, Ukraine
[2]National Defense University of Ukraine named after Ivan Chernyakhovskyi, Kyiv, Ukraine

Forms, methods and means of warfare in all times of human existence directly depended on scientific and technological progress. With the development of space, the rapid development of robotics, artificial intelligence, information and computer technologies, the views of leading states and military-political blocs on the issue of conceptual approaches to the processes of planning and conducting operations have undergone significant changes.

Modern wars and future wars are multidimensional and high-tech. At the core of interstate strategic competition, there has recently been a tendency to increase the role of political, diplomatic, economic and information methods of confrontation, and the environment of military confrontations considered on five domains: land, sea, air space, outer space and cyberspace.

In connection with this, the concept of "multi-domain operation" (MDO) is becoming widespread among NATO member states as the most effective tool for achieving operational and tactical goals. Victory in the modern conflict is becoming more dependent on technological superiority than on the number of troops and the number of combat equipment. The main task that is set in the development of MDO concepts is considering the possibility of the most effective use of available forces and means from all domains with the least losses. Achieving the set goal seems to be possible only due to the complex use of modern technologies: artificial intelligence (AI), high-speed networks and data transfer protocols, cloud storage and possibility of big data processing, access authentication, cryptographic protection of information, etc.

The paper examines the essence of the MDO concept, analyzes modern technologies that are used or planned to be used by leading countries to ensure MDO concepts, and identifies possible directions for developing the MDO concept for the defense of Ukraine based on advance technologies.

Keywords: *interstate strategic competition, military conflict, multi-domain operations, information technologies, automated control system.*