УДК 341.32::355.488

С.П. Ярош

Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

СПОСОБИ АСИМЕТРИЧНОЇ ПРОТИДІЇ ЗБРОЙНИМ СИЛАМ, ПОБУДОВАНИМ ДЛЯ ВЕДЕННЯ МЕРЕЖЕЦЕНТРИЧНОЇ ВІЙНИ

В статті визначені поняття "асиметричне протиборство" та "асиметрична протидія", проаналізовані основні елементи, які забезпечують збройним силам побудованим за мережецентричною концепцією перевагу в сучасній війні, запропоновані традиційні та асиметричні способи протидії подібному противнику та сформульовані пропозиції щодо напрямків розвитку засобів боротьби з високотехнологічним противником в Україні.

Ключові слова: *противник, конфлікт, асиметрична протидія, спосіб, мережецентрична концепція.*

Воюют не числом, а уменьем!!... Быстрота и внезапность заменяют число... Удивить – значит победить! [18]
А.В. Суворов

Вступ

Постановка проблеми. Неспроможність більшості країн світу на рівних протистояти збройним силам з мережецентричною організацією спонукає їх шукати інші, нестандартні шляхи забезпечення власної безпеки, розробляти та впроваджувати нову стратегію з метою збільшення ефекту від застосування власних обмежених ресурсів. При цьому безпосередня розробка конкретних способів протидії угрупованням збройних сил з подібною організацією ускладнюється через недостатнє знання складу та структури, принципів побудови, форм і способів їх бойового застосування. Термін існування "мережецентричних" збройних сил достатньо нетривалий, якщо за початок брати військову операцію США 2003 року "Свобода Іраку", коли вперше в межах 4 механізованої дивізії 3 АК США було запроваджено використання автоматизованої системи управління FBCB2 побудованої за мережецентричними принципами, то це близько 10 років. Після цього в бойових умовах застосування військових формувань подібного або вищого рівня більше ніде не проводилось. Практичні випробування окремих нових елементів мережевих сил відбувається в ході навчань, а форм і способів бойового застосування сил і засобів, можливостей системи управління та розвідки створених в межах даної концепції – в ході воєнних конфліктів в Лівії (2011 року) та Афганістані (2001 – 2011 рр.). Останній став справжнім полігоном США для перевірки інновацій у військовій галузі в останнє десятиліття. Звичайно, більшість результатів досліджень, що проводяться в ході подібних заходів, мають закритий характер, а інформація, що надається у відкриті ЗМІ, дуже часто носить рекламний характер. Таким чином, виникає протиріччя між зародженням і бурхливим розвитком нової концепції побудови та застосування мережецентричних збройних сил, управління якими здійснюється в єдиному інформаційному просторі, та відсутністю науково обґрунтованих принципів, форм і способів організації протидії подібному противнику. Враховуючи цей факт, дослідження способів протидії збройним силам з мережецентричною організацією є актуальним завданням, особливо для країн, які сьогодні мають збройні сили з традиційною для XX століття структурою і не можуть собі дозволити їх повномасштабне реформування в напрямку модернізації, переозброєння та впровадження передових інформаційних технологій.

Аналіз літератури. Термін "асиметричність" досить часто використовується в сучасній літературі присвяченій воєнній тематиці [6, 9, 10, 15, 17, 21]. При цьому автори визначають за допомогою нього неоднозначні поняття, розглядаючи з обох боків воєнного протистояння різних за походженням, силою та озброєністю суб'єктів.

У [6], співавтором якої є видатний російський воєнний теоретик І.Н. Воробйов, розглядається трансформація принципів тактики загальновійськового бою. Під асиметричністю автори розуміють принцип тактики мережецентричних дій, який приходить на заміну принципу бойової активності притаманному сучасній тактиці ведення бою. Змістом даного принципу на їх погляд є: протидія противнику в захопленні вогневої та тактичної ініціативи, дія за принципом "першим розвідав – першим уразив"; застосування на всій глибині розташування противника високоточної зброї (ВТЗ) великої та малої дальності, спряження дій засобів ураження з системами розвідувально-інформаційного забезпечення; застосування малих розвідувально-ударних безпілотних літальних апаратів (БЛА), наземних розвідувально-ударних комплексів, роботів; випередження

противника у циклі розвідки, застосування мережевих принципів управління зброєю, застосуванням енергетичних ударів, зброї на нових фізичних принципах у сполученні з застосуванням зброї ближнього та дальнього бою з оптичними, лазерними та радіолокаційними системами наведення на ціль; активність бойових дій у всіх сферах – на землі, в повітрі, інформаційному просторі; утримання противника в постійній напрузі; збільшення в 3 – 7 разів глибини інформаційно-енергетичного впливу на противника та в 1,5 – 2 рази інтенсивності нанесення вогневого удару. Аналіз змісту наповнення запропонованого принципу свідчить швидше про рівні можливості сторін протиборства аніж про асиметричні.

У [9] на основі аналізу принципів та особливостей мережецентричної війни обґрунтовуються окремі напрямки розвитку засобів протидії високотехнологічному противнику. Робиться висновок про доцільність базування на ручному управлінні в тактичній ланці до досягнення паритету з противником в галузі розвитку мережецентричних технологій. Нажаль не розглядаються питання тактики протидії високотехнологічному противнику в ході конфлікту.

У [10] розкривається суть асиметричного підходу в розвитку воєнних технологій, яка полягає в ухиленні однієї зі сторін (яка не має достатньо ресурсів) від фронтального протистояння до концентрації зусиль в галузях де вдалося виявити уразливість та слабкість в озброєнні та організації потенційного противника, а також в плануванні та використанні елементів раптовості та технологічних сюрпризів. Також в даному джерелі в якості виду пасивної асиметрії пропонуються способи воєнно-технологічного розвитку, які здійснюються на перший погляд паралельно "світовим тенденціям", але за рахунок відмови від частини технологій та концентрації зусиль і ресурсів на тих, де з'являється можливість скоротити відставання. Хоча в статті автори досліджують не питання форм і способів протиборства в ході конфлікту між нерівними противниками, а проблеми розвитку озброєння, але роблять це з використанням асиметричного підходу, зміст якого цілком відповідає визначенню терміна "асиметрія".

В лекції [15] командувача американськими військами у Європі наведені погляди командування американської армії на характер війн у XXI столітті. При цьому одними з основних понять є поняття асиметричності та ідиосинкритичності. Під останньою розуміються нові способи використання нових або старих засобів збройної боротьби. Робиться висновок, що для правильної організації збройної боротьби в умовах асиметричних війн важливо правильно оцінити противника. Насамперед має значення, де й коли противник може одержати виняткові військові знання, важливі його унікальні можливості змінювати свої структури. А також важливо визначити й уважно вивчити свої уразливі місця. Але в якості асиметричного конфлікту розглядається протиборство з терористичними організаціями.

У [17] досліджуються питання застосування міжнародного гуманітарного права до нових типів конфліктів – "асиметричних". В якості "асиметричних" конфліктів розглядаються неміжнародні конфлікти між збройними силами держави та недержавними угрупованнями або терористами. Дослідження спрямоване на вивчення різних за способами та тривалістю протистоянь між указаними суб'єктами. Автори перевіряють гіпотезу про те, що асиметричність виникає не тільки тоді, коли існує нерівність воєнних потенціалів, а й тоді, коли одна сторона конфлікту дотримується норм міжнародного гуманітарного права (МГП), а інша використовує порушення норм цього права в якості засобів боротьби з переважаючими силами регулярної армії. Підсумовують роботу теза про відсутність юридичного поняття загальної або глобальної війни з тероризмом і висновок, що боротьба з терористичними угрупованнями не є новим типом війни. Результуючим висновком з аналізу змісту статті може бути положення про те, що застосування терміну "асиметрична війна" до боротьби з недержавними угрупованнями правомірне тільки тоді, коли вони добре організовані та здатні вести тривалі бойові дії.

У [21] авторами надається перелік слабких сторін збройних сил побудованих за традиційними принципами XX століття, на підставі аналізу воєнних конфліктів у зоні Перської затоки за участю США, визначаються фактори, які дозволили досягти підвищення ефективності застосування угруповань коаліційних збройних сил побудованих відповідно до концепції "мережецентричної війни". Один з розділів книги присвячений загрозам "асиметричної війни". Прийоми та способи ведення такої війни з боку противника, що наведені, носять явно терористичну спрямованість і суперечать нормам МГП. Разом з тим, деякі з них після певної обробки та інтерпретації можуть бути класифіковані як такі, що відповідають нормам війни. До них відносяться: нанесення ударів по структурам управління й безпеки ідеологічними, політичними і силовими засобами; створення союзів користувачів неофіційних мереж з іншими групами для нападу на країну-агресора, розхитування регіональних урядів, або зусиль у створенні націй; підтримка стратегії постійного виснаження агресора; використання засобів масової інформації (ЗМІ) й систем комунікації для розвідки й для інформаційної війни; заграваання й керування регіональними й зовнішніми ЗМІ; перенесення боротьби на територію противника; використання перебільшення й фальсифікації наслідків атак агресора, які викликали жертви серед цивільного населення й

непрямий збиток, дружнього вогню проти місцевих союзників, та інциденти, у яких країна-агресор може бути звинувачена в тім, що вони антинаціональні й антирелігійні; активне використання вибухових пристроїв; атаки ліній комунікації, тилових районів і заходів забезпечення; активне використання найбільш сучасних типів легкого озброєння, атаки з віддаленого місця розташування або використання пристроїв з таймерами; створення розподілених мереж бойового управління й розвідки. Але навіть ці прийоми та способи в більшості лежать поза площиною складових воєнного мистецтва.

Враховуючи проведений аналіз можна зробити висновок, що однозначного розуміння того, в яких випадках доречне використання при характеристиці воєнного протистояння терміна "асиметрична протидія" як і змісту самого поняття на сьогодні немає.

Мета статті визначити поняття "асиметрична протидія", правомірність і порядок його застосування для визначення способів протидії збройним силам з мережецентричною організацією, обґрунтувати напрямки запровадження такої протидії у випадку зіткнення з подібним противником і способи її реалізації.

Основна частина

Для визначення терміна "асиметрична протидія" розглянемо тлумачення таких понять, як "симетрія", "пропорційні величини", "асиметрія" і "протидія" наведені в тлумачному словнику [2].

Симетрія – розмірне, пропорційне розміщення якогось цілого щодо центру, середини. *Пропорційні величини* – величини, які залежать одна від одної таким чином, що збільшення або зменшення однієї з них викликає збільшення або зменшення іншої у стільки ж разів. *Асиметрія* – брак або порушення симетрії; несиметричність, нерозмірність. *Протиборство* – боротьба одне проти одного. *Протидія* – дія, що спрямована проти іншої дії, перешкоджає їй.

Останнє з наведених понять може бути уточнене з урахуванням розроблених вітчизняними воєнними вченими аксіоматичних основ теорії взаємодії в яких протидія визначається як антонім терміна взаємодія [11].

Протидія – дії суб'єктів (противників), що ведуться кожним із них шляхом активного (агресивного) впливу на противника з метою виконання кожним свого бойового завдання. Протидія здійснюється в умовах невизначеності щодо намірів і планів суб'єктів протидії. Головна ознака протидії – агресивний вплив на противника. Завдання противників можуть бути абсолютно чи частково протилежними [11].

З урахуванням аналізу змісту визначень даних понять під симетричним збройним протиборством слід розуміти збройну боротьбу сторін одна проти одної, при якій обидві сторони зіткнення характеризуються розмірними бойовими потенціалами [12].

Прикладами симетричного протиборства можуть служити перша та друга світові війни, війна в Кореї 1950 – 1953 рр. та ін. Подібні війни визначаються у [4] як збройні конфлікти, в яких групи, що суперничають, мають достатньо рівні сили, щоб зробити результат протиборства невизначеним.

У противагу симетричному, *під асиметричним збройним протиборством* будемо розуміти збройну боротьбу сторін одна проти одної, при якій одна із сторін зіткнення характеризується значно більшим бойовим потенціалом ніж інша.

Аналоги асиметричних протиборств нескладно віднайти в прийнятій класифікації війн [3, 4]. Це і збройні конфлікти сильних у воєнному відношенні країн з племенами, що перебувають на примітивному рівні розвитку, які класифікуються як умиротворяння, військові експедиції або освоєння нових територій; з невеликими державами – інтервенції або репресалії; із внутрішніми групами – повстання, заколоти або внутрішні конфлікти (громадянська війна). Подібні інциденти, якщо опір виявився досить сильним або тривалим за часом, можуть досягти достатнього розмаху, щоб бути класифікованими як "війна".

Прикладами асиметричних протиборств можуть служити війни коаліцій держав проти Югославії (1999 рік), талібів в Афганістані (2001 – 2011 рр.), режимів С. Хусейна в Іраку (2003 рік), М. Каддафі в Лівії (2011 рік).

Термін "асиметрична протидія" дозволяє поглибити розуміння терміна "асиметричне протиборство" і може застосовуватися для зазначення конкретних способів дій однієї із сторін у ході останнього у відповідь на дію іншої, як правило, носія значно більшого бойового потенціалу.

Під способами бойових дій будемо розуміти порядок і прийоми застосування сил і засобів для вирішення оперативних і бойових завдань в інтересах досягнення мети бойових дій [5].

Таким чином, визначення *асиметричної протидії* має такий вигляд – це нерозмірні за змістом, але відповідні за впливом на результат конкретного бою (бойового зіткнення) способи дій однієї із сторін у ході конфлікту у відповідь на дію іншої сторони, яка характеризувалася значно більшим прикладеним бойовим потенціалом.

Поставимо питання: "Що є поштовхом для появи нових форм і способів збройної боротьби?" Це або розробка зразків ОВТ з новими тактико-технічними характеристиками, або забезпечення можливості сумісного використання існуючих зразків ОВТ, від якого отримується синергетичний ефект. Мережецентричні концепції розвитку збройних сил високоіндустріальних країн світу втілюють

в собі обидва ці напрямки, на відміну від думки деяких експертів, які вважають головним їх змістом виключно зміну способу управління військами (силами) [8]. Основні елементи, які забезпечують збройним силам з мережецентричною організацією перевагу в сучасній війні, перелічені в табл. 1. Там же наведені уразливі місця кожного з елементів, визначені на підставі вивчення досвіду локальних війн і збройних конфліктів кінця XX – початку XXI століття [4, 20].

Таблиця 1

Елементи збройних сил з мережецентричною організацією, які роблять їх сильнішими за платформоцентричні збройні сили та їх найбільш уразливі компоненти

Елемент	Найбільш уразливі компоненти
система розвідки та спостереження, засоби якої працюють на різних фізичних принципах, просторово-розподілені в широкому діапазоні частот	система синхронізації; пункти ототожнення розвідувальної інформації; радіоелектронна апаратура чуттєва до впливу електромагнітного випромінювання
багатоканальна мережева багатократно дубльована захищена система передачі великих обсягів даних у масштабі часу близькому до реального	система синхронізації; термінали доступу до космічного сегменту системи; сервери; апаратура зв'язку; засоби комутації; центри управління локальною мережею (концентратори)
багаторівнева ієрархічна система управління, яка забезпечує оцінку обстановки, виробку замислу, прийняття рішення на застосування сил і засобів, контроль результатів застосування зброї по об'єктах противника	апаратура та лінії зв'язку; точки доступу до відкритої мережі Інтернет
нові міжвидові мобільні тактичні групи, що реалізують свої потенційні можливості на основі мережецентричних методів розвідки, управління й забезпечення (рис. 1)	застосування розосередженого бойового порядку; досить скромні бойові можливості без відповідних засобів підтримки
високоточні засоби вогневого ураження, які застосовуються як за планом, так і за заявкою підрозділів	приймачі системи визначення місцеположення; канали управління; головка самонаведення; велика ймовірність перевитрат боєприпасів за рахунок ударів по хибним цілям
велика кількість БЛА різного розміру та призначення	приймачі системи визначення місцеположення; канали управління БЛА; відсутність засобів самооборони
нова мобільна система забезпечення, що рухається разом з ударними силами	приймачі системи визначення місцеположення; апаратура зв'язку; відносно слабкі можливості щодо самооборони
особовий склад, навчений діяти в умовах мережецентричних бойових дій	велика впевненість в точних діях сусідів і сил підтримки; в більшості випадків видалення військовослужбовців з поля бою, винесення жахів війни у віртуальну реальність веде до того, що зіткнення з реальними жертвами суттєво впливає на свідомість військовослужбовців, які до них не звикли

Крім того характерними рисами збройних сил, що будуються для ведення мережецентричної війни, є такі: реформа збройних сил більшості країн світу проводиться в напрямку створення невеликих за чисельністю збройних сил (по суті поліцейських) неспроможних самостійно поза коаліцією вести широкомасштабну і саме головне тривалу війну [4, 20]; уразливість сучасних збройних сил від кіберзагроз набуває настільки серйозного значення, що в США, наприклад, прийнято рішення про допустимість нанесення по джерелу такої загрози удару вогневими засобами [1]; зростання залежності перемоги від своєчасності надходження та точності інформації (прикладом може служити бій за міст через р. Євфрат, названий американцями "Peach", під час війни в Іраку в 2003 р.); наявність центрів сили, які підвищують можливості інших сил і засобів збройної боротьби, і одночасно зводять нанівець усі переваги у випадку їх знищення, наприклад, космічна складова, яка відіграє провідну роль при організації зв'язку, забезпеченні навігації та веденні розвідки; зменшення кількості втрат особового складу з одночасним зростанням вартості перемоги через дорожнечу високоточних боєприпасів; реалізація концепції сумісного та взаємопов'язаного за часом і простором застосування космічних, повітряних, морських і наземних засобів розвідки та ураження.

У збройних силах побудованих за мережецентричною концепцією основним тактичним підрозділом стають бойові тактичні групи, склад яких змі-

нюється в залежності від мети застосування. На рис. 1 наведений варіант організаційно-штатної структури бойової тактичної групи (БТГ) у складі європейських сил швидкого реагування. Такі БТГ створені й в НАТО в рамках концепції підготовки до ведення мережецентричних бойових дій [14, 19].

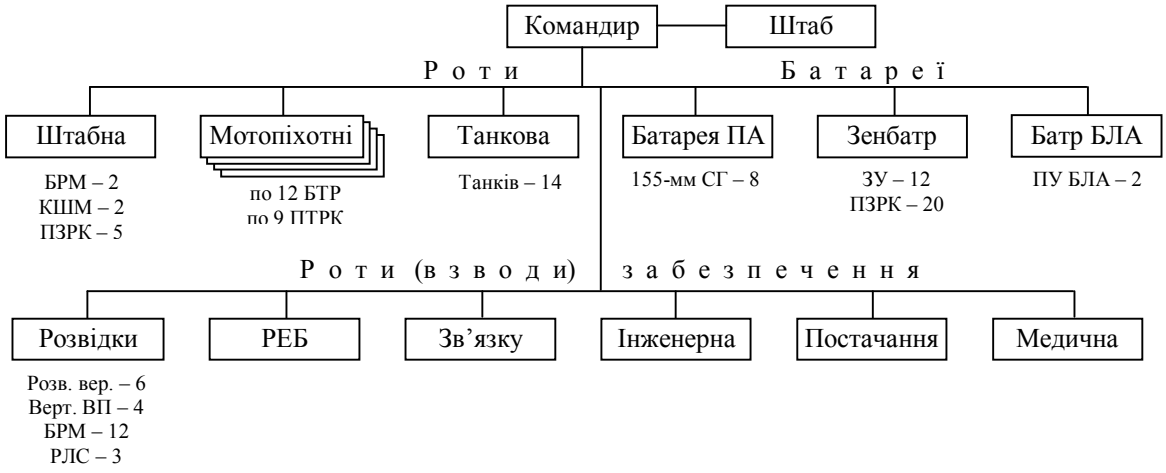

Рис. 1. Організаційно-штатна структура бойової тактичної групи в складі сил і засобів швидкого реагування ЄС (варіант)

У складі сил і засобів швидкого реагування Європейського Союзу створено 18 подібних високомобільних формувань чисельністю до 1,5 – 2,5 тис. чол. кожне. За необхідності вони повинні за 5 – 15 діб підготуватися до перекидання в район конфлікту та діяти там автономно впродовж місяця. Подібна організація покладена в основу реформування армій більшості високотехнологічних країн світу. Аналіз бойового потенціалу БТГ дозволяє зробити висновок про досить скромні можливості такої групи без вогневої підтримки частин авіації та кораблів ВМС, озброєних високоточною зброєю, у порівнянні з типовою окремою механізованою бригадою ЗС України.

Слід зазначити, що застосування способів асиметричної протидії не може привести до перемоги в конфлікті в цілому, але може дозволити на певний термін в певній області простору на рівних протистояти силам противника, які характеризуються значно більшим бойовим потенціалом, завдяки виведенню з ладу його систем розвідки, управління та всебічного забезпечення або послаблення впливу його високотехнологічних засобів ураження.

Які ж способи протидії високотехнологічному противнику можливо протиставити на сучасному етапі? Вони можуть бути умовно поділені на дві великих групи. Перша група об'єднує в собі способи обрані серед традиційних способів протидії, але найбільш ефективні у випадку асиметричного протиборства. Вони зведені у групи відповідно до часу їх застосування: при підготовці до відсічі агресії, в ході наступальної операції противника, під час систематичних бойових дій (або під час окупації території противником). Друга група містить саме асиметричні способи протидії, які відповідно до наведеного визначення забезпечують більший ефект від прикладення меншого за розміром бойового потенціалу.

Розглянемо ***способи протидії першої групи***.

При підготовці до відсічі агресії найбільш ефективними будуть такі способи протидії: організація районів оборони навколо крупних міст з завчасним створенням угруповань військ здатних не тільки відбити наступ, а й перейти у контрнаступ. (Основу таких угруповань повинні складати з'єднання і частини (підрозділи) в цілісній організаційно-штатній структурі зі своїми органами управління і забезпечення. Головні вимоги до такого угруповання: в керівництві – централізоване управління військами (силами), а в забезпеченні бойової діяльності – єдність систем розвідки, зв'язку, РЕБ, інженерного, тилового та технічного забезпечення); відпрацювання порядку ведення оборони при організації децентралізованого управління з наданням вирішальних повноважень в прийнятті рішень у ході воєнних дій командирам створених угруповань; інженерне обладнання території країни: будівництво удаваних позицій підрозділів зенітних ракетних військ; хибних сховищ для літаків на аеродромах базування з бетонним покриттям до них; створення (закупівля) макетів озброєння та військової техніки високого ступеня деталізації; мінування мостів через ріки, гребель ГАЕС, встановлення загороджувальних мінних постановок вздовж морського узбережжя; евакуація населення з місць можливого затоплення у випадку руйнування гребель на р. Дніпро, Дністер; влаштування розгалуженої мережі складів і пунктів постачання військ озброєння, медикаментів, продовольства.

У ході наступальної операції противника доцільно застосовувати: ухилення від фронтальних зіткнень з противником на відкритій місцевості для зведення до мінімуму переваги повітряного господарювання противника; перешкоджання оперативному дорозгортанню угруповання противника шляхом нанесення ударів по районам розгортання; створення рухомих мінних полів на базі автомобілів завантажених боєприпасами призначеними для утилізації з метою розстановки та дистанційного підриву їх на ракетонебезпечних напрямках під час удару крилатих ракет; максимум зусиль зосередити на маскуванні засобів ППО, які здебільшого використовувати для прикриття найбільш важливих об'єктів держави, угруповань військ, на захисті районів оборони навколо міст; підйом авіації в повітря з аеродромів базування з викриттям початку удару противника (підлітний час крилатих ракет морського базування за умови запуску їх з 43° півн. ш. акваторії Чорного моря становитиме для об'єктів розташованих вздовж чорноморського узбережжя 10 – 20 хв., для об'єктів в глибині країни – 30 – 70 хв.); маскування авіації після повернення з вильотів; знищення частини мостів для перешкоджання пересуванню сухопутних військ противника вглиб території країни; активне використання диверсійних груп; вимкнення на час бомбардувань ліній електропередач для зменшення ймовірності знищення енергосистеми держави внаслідок застосування противником графітової зброї; організація боротьби з розвідувально-диверсійними групами противника, які здійснюють збір інформації про результати ракетно-бомбових ударів з метою уточнення місцеположення і стану об'єктів ураження та виконують завдання в якості авіанавідників; перешкоджання просуванню противника з використанням природних водних, гірських (Карпати, Крим) і зведених оборонних рубежів; для укриття військової техніки використання території підприємств, які займаються видобутком і збагаченням стратегічної сировини (скандій, нікель, титанова, свинцево-цинкова, ртутна та алюмінієва руди) та за досвідом локальних війн, як правило, не потрапляють до списку цілей МРАУ.

Під час систематичних бойових дій здійснювати: перешкоджання нарощуванню угруповань противника; влаштування засідок; завдання ударів по комунікаціях противника з метою зриву заходів тилового та технічного забезпечення; застосування партизанської тактики на територіях захоплених противником: мінометних обстрілів, дій снайперів-одиночок, "мінної війни".

Перейдемо до розгляду прийомів і способів асиметричної протидії.

Головні завдання при організації протидії високотехнологічному противнику можливо сформулювати таким чином: 1) втягування противника в довготривалий конфлікт низької інтенсивності, що веде до зростання вартості перемоги, яку забезпечують дорогі в утриманні бойові системи та засоби формування мережевої архітектури; 2) введення противника в оману в ході повітряної наступальної операції щодо дійсного стану збройних сил і результатів масованих ракетно-артилерійських ударів, примушення його перейти до наземної фази операції для завдання йому втрат у живій силі та техніці; 3) першочергове виведення з ладу "центрів сили" противника, до яких відносяться: прикордонні командні пункти, повітряні командні пункти, об'єднані розвідувальні центри, літаки ДРЛВ і У, авіаносці та ін.

При цьому ***тактичні прийоми та способи асиметричної протидії*** збройним силам з мережецентричною організацією можуть бути умовно розділені за такими напрямками: застосування засобів ураження; застосування засобів РЕБ, застосування військ (сил), організація захисту своїх військ; організація управління військами та зброєю; програмний вплив на інформатизовані системи противника. Розглянемо їх більш докладно.

Застосування засобів ураження: ЗРК С-200В, С-300ПТ зменшити час використання своїх радіолокаційних засобів, включення здійснювати тільки за необхідності; мобільним комплексам ЗРВ і військ ППО СВ використовувати прийом "стрільба з засади"; раптове застосування установок реактивних систем залпового вогню та артилерійських підрозділів, що кочують, по площам, які завчасно пристріляні; широке використання засобів військ ППО СВ працюючих по цілях, які візуально спостерігаються, що примусить авіацію діяти з висот вище 3 000 м; використання ударної авіації для знищення кораблів носіїв крилатих ракет в Чорному морі та найближчих авіабазах противника, які будуть знаходитись в межах досяжності; застосування в якості рухомих засобів ураження автомобілів легкової групи вантажопідйомністю до 1000 кг, на які встановити зенітні кулеметні установки, міномети, протитанкові гранатомети, реактивні системи залпового вогню; застосування радіоуправляємих авіамоделей категорій F3, F4, F5 (за класифікацією FAI [3]) для боротьби таранним способом з розвідувальними "мікро" БЛА.

Застосування засобів РЕБ: створення широковіщального шторму – багаточисельних одночасних передач, які заповнюють усю доступну смугу пропускання мережі та можуть викликати уповільнення її роботи і навіть привести до її повної непрацездатності [7]; постановка завад супутниковим системам навігації в дециметровому діапазоні хвиль (на частотах

L1 = 1575,42 МГц,
L2 = 1227,60 МГц,
L5 = 1176,45 МГц);

одночасне вимкнення всіх РЛС і включення великої кількості хибних випромінюючих джерел, в якості яких можуть бути використані навіть звичайні мікрохвильові печі; активне використання великої кількості малорозмірних передавачів завад, що закидаються, закидання здійснювати за допомогою, аеростатів, РСЗВ, артилерії; використовувати передавачі завад, які вмикаються за таймером або дистанційно.

Застосування військ (сил): використання для активних дій військ хмарної дощової погоди, в яку значно знижуються можливості противника з використання засобів розвідки та високоточної зброї; бойові зіткнення здійснювати рішуче, розвиваючи успіх з урахуванням розімкнутого бойового порядку противника, його можливості швидко перегруповуватися і оперативно отримувати вогневу підтримку; нав'язування противнику тактики ближнього бою, яка вимушує його задля зменшення ймовірності "дружнього вогню" зменшувати обсяг вогневої підтримки з боку авіації та ВМС.

Організація захисту своїх військ, який повинен здійснюватися у двох напрямках: маневрування та маскування.

Заходи щодо маневрування: мобільним комплексам ЗРВ і військ ППО СВ здійснювати потайливе маневрування з позиції на позицію; перегрупування військ здійснювати виключно вночі, краще в хмарну погоду; виключити одночасне маневрування з'єднаннями та частинами, маневрування здійснювати підрозділами з використанням кількох основних маршрутів руху та кількох хибних, за якими рухаються автомобілі з включеними гучномовцями для імітації руху колон; хибні колони повинні пересуватися щоночі в різних напрямках для присипання пильності противника.

Заходи щодо маскування: маскування військової техніки та озброєння під цивільні об'єкти; використання для укриття особового складу та техніки лісосмуг з щільним листяним покровом, який перешкоджає проходженню сигналу навігації GPS і заважає точному наведенню зброї з використанням даної системи; використання аерозольного маскування як окремих зразків ОВТ, так і цілих підрозділів на великих ділянках або штучне запилення (в тих районах де це можливо) з метою перешкоджання застосуванню противником бомб з лазерним наведенням та інфрачервоним наведенням, які потребують підсвічування цілі на весь час їх падіння, інакше вони "гублять захоплення" і далі падають як звичайні "залізні бомби"; використання тепловідбиваючих покриттів для зниження помітності теплоконтрастних об'єктів; використання форми з вшитими на рівні плечей фрагментами тканини, яка вночі відбиває ІЧ опромінення і дозволяє вночі ідентифікувати противнику наших військовослужбовців як своїх; застосування нахильних масок-екранів (радіорозсіюючих і радіопоглинаючих інженерних маскувальних комплектів), використання радіолокаційних куточкових відбивачів з метою викривлення конфігурації об'єктів і рельєфу місцевості при протидії засобам радіолокаційної розвідки; імітація ураження крупних площадних об'єктів за допомогою імітаційних маскуючих покриттів – плівки, яка імітує проломи в дахах будівель, вибиті віконні та дверні пройми тощо, а також піротехнічними засобами імітації пожеж для введення в оману противника при використанні ним засобів оптичної розвідки.

Ефективність будь-якого маскування можуть забезпечити висока швидкість створення маскувального ефекту, комплексне використання різноманітних засобів і видів маскування (у тому числі імітації, приховання об'єктів, застосування нових технологій зниження їхньої помітності), а також засобів радіотехнічної протидії різним системам високоточних засобів ураження противника.

Організація управління та розвідки: при організації оборони об'єктів і військ повинний бути налагоджений надійний зв'язок не тільки з КП бригад (полків), а й безпосередньо між підрозділами на випадок знищення КП; забезпечення додаткових каналів прямого зв'язку для передачі розвідувальної та бойової інформації від розвідувальних підрозділів безпосередньо на вогневі в усіх видах і родах військ; переважне використання станцій пасивної радіотехнічної розвідки "Кольчуга", засоби яких постійно змінюють позиції з забезпеченням їх прикриття засобами ППО (Стрела-10, ПЗРК); використання для організації запасного мережевого зв'язку між підрозділами автомобілів МВС, таксі та швидкої допомоги обладнаних засобами радіозв'язку; використання даних оперативної агентурної розвідки про зліт літаків з аеродромів противника, їх кількість, тип і напрямок їх польоту.

Програмний вплив на інформатизовані системи та засоби противника: проведення хакерських атак на державні сайти противника, з цією метою здійснення підключення з використанням мережі Інтернет до комп'ютерних мереж противника та перевантаження їх потоками запитів і трафіків, внаслідок чого забезпечити збої в роботі системи управління й ускладнити функцій передачі або прийому даних між її елементами; здійснення семантичних атак, у ході яких інформаційна система противника продовжує функціонувати, причому зовні її робота не викликає ніякої підозри, однак вхідна інформація виявляється не адекватною реальності; зараження бойових інформаційних мереж противника вірусами, які знищують або пошкоджують програмне забезпечення.

З урахуванням наведених можливостей збройних сил побудованих за мережецентричною концепцією та запропонованих засобів протидії йому сформулюємо *пропозиції щодо напрямків розвитку в Україні засобів боротьби з високотехнологічним противником*. Вони можуть бути такими:

1. Оскільки основну роль у фізичному втіленні циклів управління мережецентричної системи відіграє електроніка, то саме вона повинна представляти першочергову мішень для бойових засобів функціонального ураження. Розробка таких засобів може бути виконана у формі наземних генераторів електромагнітного випромінювання, а також у формі вибухомагнітних генераторів (ВМГ), які доставляються до цілі ракетами носіями [13]. В якості носіїв можуть бути використані ракети ЗРК С-200В або інших комплексів ЗРВ, а також ракети "повітря – повітря", оснащені бойовою частиною у вигляді ВМГ.

2. Використовувати існуючі та перспективні засоби протиповітряної оборони не в "штатній" однорідній структурі, а в певній комбінації (наприклад,

С-300ПС + "Оса-АКМ" + ЗУ-23-2;

"Бук-М1" + "Тунгуска"),

тобто створити на їх основі комбіновані розвідувально-вогневі бойові модулі, орієнтовані на високоефективне вирішення конкретних завдань в умовах активного застосування противником БЛА, протирадіолокаційних ракет та іншої ВТЗ.

3. Робота складних систем озброєння КП, АСУ, будь-яких радіоелектронних засобів, крупних об'єктів воєнної інфраструктури супроводжується випромінюванням електромагнітних полів, які створюються не тільки активними засобами але також і джерелами побічного і ненавмисного випромінювання, обчислювальними засобами, елементами фідерних трактів, гетеродинними приймачами та ін., тому одним із напрямків повинно стати створення та удосконалення точнісних характеристик ракет з головками самонаведення на високоенергетичні об'єкти.

4. Модифікація бортових РЛС винищувачів Су-27 і розробка ракет "повітря – повітря" з дальністю пуску 120 км і більше для успішної боротьби з авіацією противника.

5. Розробка засобів маскування в інфрачервоному діапазоні, які б складалися з ІЧ-камер колового огляду та активних тепловипромінюючих панелей, які "малюють" теплову картину навколишньої місцевості [22]. Подібні засоби вночі не тільки спроможні скрити, наприклад, бронетехніку на місцевості, а й імітувати різні об'єкти для введення противника в оману.

6. Розробка та виробництво засобів РЕБ для постановки завад системам космічної навігації для боротьби з БЛА противника, які дозволять порушувати режим їх роботи або перехоплювати їх подібно операції проведеної іранською стороною відносно американського апарату RQ-170 "Sentinel" у 2011 році [22].

7. Розробка та виробництво великої кількості передавачів РЕБ, які закидаються снарядами РСЗВ, артснарядами, оперативно-тактичними ракетами.

8. Виробництво або закупівля БЛА для потреб розвідки, а також розробка та виробництво малих літальних апаратів типу дельтапланів та радіоуправляємих авіамоделей для боротьби з "мікро" та "міні" БЛА противника.

9. Розвиток засобів інформаційної боротьби, створення кіберпідрозділів здатних вести боротьбу в глобальних, регіональних і локальних інформаційних мережах.

10. Закупівля мобільних модульних шпиталів [16] та ін.

Висновки

Вивчення особливостей побудови та досвіду бойового застосування збройних сил з мережецентричною організацією дозволяє організувати ефективну асиметричну протидію подібним збройним силам у ході воєнного конфлікту.

Заходи щодо компенсування технічних переваг противника тактичними прийомами варто спеціально планувати при веденні як оборони, так і наступу.

Кількісна перевага менш передової техніки над більш передовою технікою, що бере участь у бою на боці противника, сама по собі не може забезпечити успіх, якщо вона не поєднана з тактикою, що компенсує технічний розрив.

Список літератури

1. Буренок В.М. О некоторых аспектах информационных войн / В.М. Буренок // Вооружение и экономика, 2011. – № 3(15). – С. 5-16.

2. Великий тлумачний словник сучасної української мови (з дод. і допов.) / Уклад. і голов. ред. Бусел В.Т. – К.: Ірпінь: ВТФ "Перун", 2005. – 1728 с.

3. Вікіпедія. Електронна енциклопедія. – [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/.

4. Военное искусство в локальных войнах и вооруженных конфликтах: военно-исторический труд. – М.: Воениздат, 2009. – 764 с.

5. Военный энциклопедический словарь. – М.: Эксмо, 2007. – 1024 с.

6. Воробьев И.Н. От современной тактики к тактике сетецентрических действий / И.Н. Воробьев, В. А. Киселев // Военная мысль. – М.: МО РФ, 2011. – № 8. – С. 19-27.

7. Воройский Ф.С. Інформатика. Энциклопедический словарь – справочник: введение в современные информационные и телекоммуникационные технологи в терминах и фактах / Ф.С. Воройский. – М.: ФИЗМАТЛИТ, 2006. – 768 с.

8. Горбачев Ю.Е. Сетецентрическая война: миф или реальность? / Ю.Е. Горбачев // Военная мысль. – М.: МО РФ, 2006. – № 1. – С. 66-76.

9. Дульнев П.А. Асимметричное противодействие в сетецентрической войне / П.А. Дульнев, В.Г. Ковалев, Л.Н. Ильин // Военная мысль. – М.: МО РФ, 2011. – № 10. – С. 3-8.

10. Ильин Л.Н. Ориентиры для создания вооружения и военной техники Сухопутных войск / Л.Н. Ильин, В.Г. Ковалев, А.С. Муратханов // Военная мысль. – М.: МО РФ, 2011. – № 4. – С. 31-37.

11. Аксіоматичні основи теорії взаємодії службово-бойових систем / І.О. Кириченко, Ю.В. Аллеров, В.І. Тробюк, Ю.Ф. Урсакій // Честь і закон. – Х.: Військ. ін-т ВВ МВС України, 2006. – № 1. – С. 9-17.

12. Кириченко І.О. Визначення поняття "інформаційно-бойовий простір", змісту та ролі його складових елементів для досягнення перемоги в воєнних конфліктах XXI століття / І.О. Кириченко, С.П. Ярош // Системи озброєння і військова техніка. – Х.: ХУПС, 2011. – № 3 (27). – С. 102-108.

13. Лузан А.Г. Без надежной ПВО перевооружение войск бессмысленно и бесполезно // Независимое военное обозрение. – № 1 от 20.01.2012. – С. 10-11.

14. Максимов В. Военная политика Европейского союза // Зарубежное военное обозрение. – М.: Красная звезда, 2005. – № 9. – С. 2-8.

15. Мейгз М. Епоха стратегической асимметричности // Независимая газета. – Вып. 223 (2777) от 18.10.2002. – С. 6.

16. Мобильні шпиталі фірми ZEPPELIN MOBILE SYSTEME. [Електронний ресурс]. – Режим доступу: http://www.zeppelin-systeme.de/ starte.htm.

17. Паулюс А. Асимметричная война и понятие вооруженного конфликта – попытка разработать концептуальную модель / А. Паулюс, М. Вашакмадзе. – [Электронный ресурс]. – Режим доступа: http://www.icrc.org/rus/assets/files/ other/paulus.pdf.

18. Стратегия духа: Основы воспитания войск по взглядам А.В. Суворова и М.И. Драгомирова. – М.: Русский путь, 2000. – 184 с.

19. Храмчишин А. Армія ЕС угрожает Америке // Частный кореспондент. – 2 февраля 2009 года. – [Електронний ресурс]. – Режим доступу: http://www.chaskor.ru/article/armiya_es_ugrozhaet_amerike_3086.

20. Ярош С.П. Аналіз ведення бойових дій, тактики застосування ЗПН і використання нових інформаційних технологій у ході воєнного конфлікту в Лівії в 2011 році / С.П. Ярош // Наука і техніка Повітряних Сил Збройних Сил України. – Х.: ХУПС, 2011. – № 2 (6). – С. 19-25.

21. Cordesman A.H. Gulf military forces in an era of asymmetric wars. Volume 1 // A.H. Cordesman, K.R. Al-Rodhan. – Washington, D.C.: Center for Strategic and International Studies, 2007. – 600 p.

22. R&D. Cnews. Наука и разработки. – [Електронний ресурс]. – Режим доступу: http://www.rnd.cnews.ru/army/.

Надійшла до редколегії 12.01.2012

Рецензент: д-р військ. наук, проф. В.І. Ткаченко, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

СПОСОБЫ АСИММЕТРИЧНОГО ПРОТИВОДЕЙСТВИЯ ВООРУЖЕННЫМ СИЛАМ, ПОСТРОЕННЫМ ДЛЯ ВЕДЕНИЯ СЕТЕЦЕНТРИЧЕСКОЙ ВОЙНЫ

С.П. Ярош

В статье определены понятия "асимметричное противоборство" и "асимметричное противодействие", проанализированы основные элементы, которые обеспечивают вооруженным силам построенным в соответствии с сетецентрической концепцией преимущество в современной войне, предложены традиционные и асимметричные способы противодействия подобному противнику, сформулированы предложения относительно направлений развития средств борьбы с высокотехнологическим противником в Украине.

Ключевые слова: *противник, конфликт, асимметричное противодействие, способ, сетецентрическая концепция.*

WAYS OF ASYMMETRIC COUNTERACTION TO THE ARMED FORCES CONSTRUCTED FOR CONDUCTING OF NETWORK-CENTRIC WAR

S.P. Yarosh

In article concepts "an asymmetric antagonism" and "asymmetric counteraction" are defined, basic elements which provide to armed forces constructed according to network-centric concept advantage in modern war are analyzed, traditional and asymmetric ways of counteraction are offered the similar opponent, offers concerning directions of development of means of struggle against the highly technological opponent in Ukraine are formulated.

Keywords: *the opponent, the conflict, asymmetric counteraction, a way, the network-centric concept.*