

УДК 623.618.5

Ю.І. Галушко¹, О.Д. Флоров²¹ Командування Повітряних Сил Збройних Сил України, Вінниця² Харківський університет Повітряних Сил ім. І. Кожедуба, Харків

ЗАСТОСУВАННЯ ПРИНЦИПУ ЄДИНОГО ІНФОРМАЦІЙНОГО ПРОСТОРУ ПРИ ОРГАНІЗАЦІЇ ЗЕНІТНОГО РАКЕТНОГО ПРИКРИТТЯ ВАЖЛИВИХ ОБ'ЄКТІВ ДЕРЖАВИ

У статті на основі аналізу досвіду іноземних держав щодо впровадження «мережецентричної» концепції ведення бойових дій зроблений висновок щодо необхідності розробки методики застосування принципу єдиного інформаційного простору при організації зенітного ракетного прикриття важливих об'єктів.

Ключові слова: інформаційний простір, мережецентричні війни, мережецентричні сили.

Вступ

Постановка проблеми і аналіз літератури.

Термін «Єдиний інформаційний простір» застосовується вже давно в різних галузях знань, сталою (загальноприйнятою) розуміння цього терміну не існує. У теорії будівництва Збройних Сил цей термін почав з'являтися в середині 90-х років минулого сторіччя як один з основоположних принципів концепції мережецентричної війни.

У широкому розумінні під концепцією "мережецентричної війни" (Network Centric Warfare, NCW) розуміють таку, що склалася в останні 5–7 років в США систему поглядів на військово-технічне забезпечення ведення бойових дій в умовах тотальної комп'ютеризації сил і засобів збройної боротьби [1]. Ця теорія була розроблена Офісом Реформування ЗС Секретаря Оборони (Office of Force Transformation) США під управлінням віце-адмірала Артура К. Цибровські (Sebrowski) (разом з професором Гартська в 1998 р. вони вперше висунули і обґрунтували стратегічну концепцію мережецентричних війн). 15 серпня 2001 р. президент США Буш запропонував міністру оборони Дональду Рамсфелду підготувати стратегічне уявлення про те, як американська армія "повинна виглядати сьогодні і як вона повинна виглядати завтра". А в жовтні 2001 р. в статті "За рамками війни з терором" Рамсфелдом були позначені контури цієї стратегії [2].

Вперше елементи цієї стратегії були апробовані в Югославії і сьогодні активно впроваджуються в практику ведення бойових дій США в Іраку і Афганістані, тестуються під час проведення навчань [1].

У військових діях в Іраку (2003 р.) сили НАТО були розподілені не тільки на Близькосхідному театрі воєнних дій, але і практично по всьому світу, різноманітні і різновидові, навіть такі, що навіть належать збройним силам різних держав. Сили і засоби повітряного нападу всіх видів базування по єдиному задуму і плану, узгоджено по цілях, завданням, місцю і часу завдавали скоординованих ударів за най-

важливішими пунктами управління і об'єктам інфраструктури Іраку.

Послідовно вирішуючи завдання, динамічно змінювався склад, структура і характеристики сил і засобів, що залучаються до завдання ударів, адекватно обстановці варіювалися об'єкти поразки і потужність ударів. Повним ходом йшло відпрацювання нових технологій війни і ведення воєнних дій.

Накопичений як позитивний, так і негативний досвід знайшов своє відображення в новій "Національній військовій стратегії США", прийнятій в квітні 2004 р. У ній було відображено новий напрям розвитку збройних сил країни на найближчу і середньострокову перспективу, описані способи застосування ЗС залежно від військово-стратегічної обстановки, сили і засоби, які необхідні для досягнення переваги над противником у військових операціях XXI сторіччя.

У зв'язку з цим визнано необхідним перетворити ЗС США в єдині мережецентричні і розподілені сили, забезпечивши якісне вдосконалення системи збору, обробки і розподілу інформації. З того часу Пентагон приступив до розгортання глобальної інформаційної мережі і практичного відпрацювання технологій нового вигляду війн – "мережецентричної" війни.

На думку американських військових фахівців, здійснення заходів, передбачених перспективною «мережецентричною» концепцією ведення бойових дій в умовах формування єдиного інформаційно-комунікаційного простору, повинно звільнити учасників бойових дій від необхідності думати про забезпечення взаємодії і обробки інформації. Вони повинні мати вільний доступ до вже обробленої інформації, а не до величезної кількості різноманітних даних [3].

Мета статті: аналіз досвіду іноземних держав щодо впровадження «мережецентричної» концепції ведення бойових дій та вироблення пропозицій по розвитку і впровадженню принципу єдиного інформаційного простору для організації зенітного ракетного прикриття важливих об'єктів держави.

Основна частина

Для досягнення мети статті розглянемо поняття мережецентричної війни. Мережецентрична війна – це війна, орієнтована на досягнення інформаційної переваги. Це концепція ведення військових дій, яка передбачає збільшення бойової потужності угруповання сил за рахунок створення інформаційно-комунікаційної мережі, що зв'язує джерела інформації (розвідки), органи управління і засоби поразення (придушення), яка забезпечує доведення до учасників операцій достовірної і повної інформації про обстановку практично в реальному масштабі часу [1].

"Мережа" в такому широкому розумінні включає одночасно різні складові. Ними можуть бути: бойові одиниці, система зв'язку, інформаційне забезпечення операції і таке інше.

За рахунок цього досягається прискорення процесу управління силами і засобами, підвищення темпу операцій, ефективності поразення сил противника, живучості своїх військ і рівня самосинхронізації бойових дій. Самі ж "мережецентричні сили" (у військовому сенсі) – це війська і зброя, здатні реалізувати концепцію мережецентричної війни.

На можливих театрах військових дій створюються і розгортаються розгалужені автоматизовані електронні (комп'ютеризовані) мережі розвідки, інформації і управління від тактичного до стратегічного рівня.

Вони сполучаються і зв'язуються в єдиний інформаційно-управляючий комплекс, який забезпечує безперервне оперативне керівництво силами по вертикалі і горизонталі. В сукупності всі ці засоби (джерела інформації, засоби і пункти управління, засоби знищення і придушення) створюють єдине інформаційно-управляюче поле, що охоплює весь простір війни.

Можна виявити три найбільш відмінних особливості "мережевої війни" в порівнянні з традиційною війною в нинішньому її розумінні [1, 2].

1. Широка можливість використання географічно розподіленої сили. Причому разом з інтеграцією ударних сил і засобів повітряного нападу при виконанні бойових завдань, це стосується і засобів забезпечення. Раніше із-за різного роду обмежень було необхідно, щоб підрозділи і елементи тилового забезпечення розташовувалися в одному районі в безпосередній близькості до противника або до об'єкту, що оборонявся. Нова концепція знімає ці обмеження, і це було практично підтверджено в Югославії і Іраку.

2. Відмінність "мережевої" війни полягає в тому, що сили, що беруть участь в ній високоінтелектуальні. Користуючись знаннями, отриманими від всеосяжного спостереження за бойовим простором і розширеного розуміння намірів командування, ці сили будуть здібні до самосинхронізації діяльності, стануть ефективнішими при автономних діях.

3. Наявність ефективних комунікацій між об'єктами в бойовому просторі. Це дає можливість геог-

рафічно розподіленим об'єктам проводити сумісні дії, а також динамічно розподіляти відповідальність і весь об'єм роботи, щоб пристосуватися до ситуації.

Крім того, "мережецентричні" принципи – це і зміна способів розвідувальної діяльності, спрощення процедур узгодження і координації при організації об'єднаного вогневого поразення, а також деяка нівеляція розмежування засобів по ланках управління, що дозволяє застосовувати стратегічні засоби розвідки і вогняного поразення для розвідувального і вогневого забезпечення дій тактичних формувань, як і було в Афганістані і Іраку [5].

Вперше концепція мережецентричних війн була розроблена в США, причому практична реалізація закладених в ній принципів торкнулася перш за все сухопутних військ (Army Battle Command System, Force XXI Battle Command, Brigade and Below), ВМФ (FORCEnet) і ВПС (C2 Constellation) [7].

Почата розробка аналогічних концепції для НАТО (NATO Network Enabled Capability) [6]. Перший крок до розробки подібних концепцій зроблений в Російській Федерації і Китаї [5]. Відомостей про опрацювання концепцій «єдиного інформаційного простору» для військ протиповітряної оборони в матеріалах відкритого друку немає [1]. Однак, прообрази реалізації подібних концепцій були створені у Військах ППО ще в 1970-х рр. Змішані зенітні ракетні угруповання, що складаються з 12 – 20 ЗРК, розподілені в просторі на площі більше 70 тис. кв. км. і які одержували інформацію попередження від засобів радіолокації з площі, що як мінімум удвічі перевищує вказану, під керівництвом одного достатньо інтелектуально озброєного КП з АСУ типу "Вектор", "Сенеж", а потім і "Байкал", ефективно виконували завдання поразення ЗПН у всьому діапазоні висот, причому у взаємодії з винищувальною авіацією.

При цьому для поразення повітряних цілей вибиралися різні ЗРК або літаки-винищувачі, що мають саме в даний момент часу (адаптивний до ситуації) якнайкращі можливості щодо поразення призначених цілей.

Надалі цей досвід був узагальнений і для сумісних дій частин винищувальної авіації і ЗРВ у межах корпусів і дивізій ППО, а потім і окремих армій ППО в межах, практично сумірних з театром війни.

Проте створена система мала істотні недоліки, до яких перш за все необхідно віднести:

– наявність тільки одного або слабо розвинутого інтелектуального центру (функції основного КП могли узяти на себе лише 1 – 2 КП цього ж рівня управління або навіть нижчого);

– вартісна сумісність засобів нападу і засобів поразення, а деколи і навіть підвищені витрати на поразення цілі;

– масштабна неадекватність відображення обстановки на КП різних рівнів управління.

Проте основним недоліком цих систем був обхват автоматизацією лише бойових функцій управління.

На жаль, в Україні інформація про подібні опрацювання не зустрічається. У зв'язку з цим представляє інтерес виділити часткові завдання, вирішення яких доцільно здійснити в першу чергу.

До таких завдань перш за все необхідно віднести:

- виділення підсистем, які повинні входити в систему; у якості таких підсистем повинні виступати (рис. 1): система розвідки повітряного противника; система управління засобами вогневого поразення; система засобів вогневого поразення; система технічного забезпечення; система радіоелектронної боротьби;

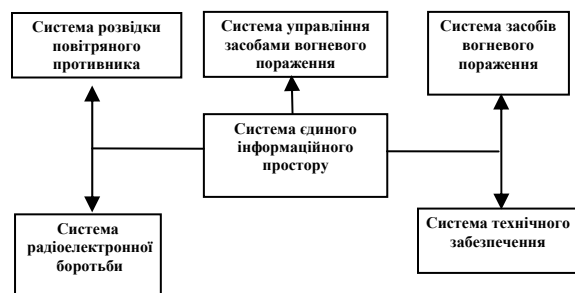


Рис. 1. Системи єдиного інформаційного простору

- аналіз інформації яка циркулює в цих підсистемах;
- приведення інформації до «єдиного протоколу»;
- пред'явлення вимог до пропускної спроможності інформаційних мереж (вертикальних і горизонтальних);
- розробка структури інформаційних мереж;
- пред'явлення вимог до продуктивності обчислювальних засобів.

Все вищенаведене свідчить про недостатнє використання "мережецентричних" принципів для військ протиповітряної оборони України.

Тому необхідна розробка методики застосування принципу єдиного інформаційного простору при організації зенітного ракетного прикриття важливих об'єктів держави.

Висновки

Застосування принципу єдиного інформаційного простору для організації зенітного ракетного прикриття важливих об'єктів держави безумовно підвищить його ефективність.

ПРИМЕНЕНИЕ ПРИНЦИПА ЕДИНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА ПРИ ОРГАНИЗАЦИИ ЗЕНИТНОГО РАКЕТНОГО ПРИКРЫТИЯ ВАЖНЫХ ГОСУДАРСТВЕННЫХ ОБЪЕКТОВ

Ю.И. Галушко, А.Д. Флоров

В статье на основе анализа опыта иностранных государств относительно внедрения «сетевцентричной» концепции ведения боевых действий сделан вывод относительно необходимости разработки методики применения принципа единого информационного пространства при организации зенитного ракетного прикрытия важных объектов.

Ключевые слова: информационное пространство, сетевцентричные войны, сетевцентричные силы.

APPLICATION OF PRINCIPLE OF SINGLE INFORMATIVE SPACE DURING ORGANIZATION OF ZENITHAL ROCKET PROTECTION OF IMPORTANT STATE OBJECTS

Yu.I. Galushko, O.D. Florov

In the article on the basis of analysis of experience of the foreign states in relation to introduction of «network-centric» conception of conduct of battle actions a conclusion is done in relation to the necessity of development of method of application of principle of single informative space during organization of zenithal rocket protection of important objects.

Keywords: informative space, network-centric wars, network-centric forces.

Для визначення кількісних показників приросту ефективності необхідно проводити подальші дослідження основних складових єдиного інформаційного простору з врахуванням:

- вимог до пропускної спроможності інформаційних мереж;
- вимог до продуктивності обчислювальних засобів;
- вимог до ТТХ перспективних ЗРК для організації зенітного ракетного прикриття в умовах єдиного інформаційного простору;
- вимог до складу і структури єдиної бази даних;
- вимог програмного забезпечення обчислювальних засобів.

Напрямок подальших досліджень – розробка методики дослідження основних складових єдиного інформаційного простору та визначення показників ефективності зенітного ракетного прикриття важливих об'єктів держави.

Список літератури

1. Чельцов Б. Сетевые войны XXI века / Б.Чельцов, С.Волков // Воздушно-космическая оборона. – 2005. – № 2.
2. Гриняев С.Н. "Сетевая война" по-американски / С.Н. Гриняев. – М.: Наука, 2006. – 224 с.
3. Кондратьев А. Реализация концепции "Сетецентрическая война" в ВВС США / А. Кондратьев // Зарубежное военное обозрение. – 2009. – №5. – С. 44-49.
4. Азов В. О реализации в США концепции ведения военных действий в едином информационном пространстве / В. Азов // ЗВО. – 2004. – №6. – С. 10-17.
5. Кондратьев А. Нужна ли информационная революция в армии? / А. Кондратьев // Военно-промышленный курьер. – 2006. - № 3.
6. Молитвин А. О реализации концепции единого информационного пространства НАТО / А. Молитвин // Зарубежное военное обозрение. – 2008. – №1. – С. 23-27.
7. Баулин В. Реализация концепции "сетевцентрическая война" в ВМС США / В. Баулин, А. Кондратьев // Зарубежное военное обозрение. – 2009. – №6. – С. 61-67.
8. Попов И. «Сетецентрическая война». Готова ли к ней Россия? [Электронный ресурс] / И. Попов // Режим доступа до ресурсу: http://www.za-nauku.ru/index.php?option=com_content &task=view&id=2469&Itemid=39.

Надійшла до редколегії 5.05.2010

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