УДК: 355.40. 35.074.5
Гаценко С.С.[1];
Кальницький Ю.М.[2];
Гельвейчук О.М.[2]

[1] - Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського;
[2] - Національний університет оборони України імені Івана Черняховського

Проблема розподілу інформаційних потоків в автоматизованих системах управління військами (силами) Збройних Сил України

Проблема распределения информационных потоков в автоматизированных системах управления войсками (силами) Вооруженных Сил Украины

The problem of distribution of information flows in automated control systems of tpoops (forces) of Armed Forces of Ukraine

Резюме. На основі аналізу досвіду провідних країн світу щодо впровадження концепцій мережовоцентричних війн розглядається проблема розподілу інформаційних потоків для прийняття рішень в системах управління військами силами з метою подальшого врахування виникаючих проблем при розробці автоматизованих систем управління військами (силами) Збройних Сил України.

Ключові слова: концепція мережевих (мережево-центричних) війн, інформаційні потоки, автоматизовані системи управління військами (силами).

Резюме. На основании анализа опыта ведущих стран мира по внедрению концепций сете-центрических войн рассматривается проблема распределения информационных потоков для принятия решений в системах управления войсками силами с целью дальнейшего учета возникающих проблем при разработке автоматизированных систем управления войсками (силами) Вооруженных Сил Украины.

Ключевые слова: концепция сетевых (сетецентрических) войн, информационные потоки, автоматизированные системы управления войсками (силами).

Resume. Based on the analysis of the experience of the leading countries of the world to introduce the concepts of network-centric warfare addresses the problem of the distribution of information flows for decision making in command and control systems forces to further account of emerging issues in the development of automated control systems of troops (forces) of the Armed Forces of Ukraine.

Keywords: concept network (network-centric) wars, information flowes, automated control systems of troops (forces).

Постановка проблеми. Війни і локальні конфлікти другої половини XX – початку XXI сторіччя характеризуються високою динамікою змін обстановки та асиметричним характером збройної боротьби, що внесло значні корективи у форми та методи оперативного і бойового застосування збройних сил. У сучасних умовах основним фактором досягнення переваги над противником є впровадження у війська інформаційних технологій і нанотехнологій, застосуванням космічних навігаційних, розвідувальних та ударних систем, зростанням масштабів інформаційно-психологічної та радіоелектронної боротьби в наземному та повітряному середовищах, застосуванням зброї, діючої на нових фізичних принципах, переходом до адаптивних форм воєнних дій. Ці фактори зумовили розробку концепції майбутніх війн шостого і сьомого покоління – концепції мережевих (мережецентричних) війн

(NCW, Net-Centric Warfare). В основу концепції закладено принципи створення надсистеми, що забезпечить максимальне скорочення часу реакції систем управління, зв'язку і ураження на зміну оперативної обстановки, зменшення кількості проміжних і ретранслюючих ланок у системі "розвідка – передача даних – ураження", гарантованого ураження цілі для зменшення ймовірності нанесення противником удару у відповідь.

Але поряд із перевагами нової концепції ведення бойових дій виявлено і ряд значних недоліків його реалізації, що пропонуються до розгляду в статті.

Аналіз останніх досліджень і публікацій.

Останнім часом аналіз у відкритих джерел зарубіжної преси значно зменшилася кількість публікацій з питань "мережоцентричних війн", з'являються матеріали критичного характеру. Зокрема в [1] переоцінення концепції "мережевецентричної війни" веде до ряду суттєвих помилок у прийнятті управлінських рішень. У [2, 3] висвітлені проблеми перебоїв у системах взаємодії між суб'єктами та об'єктами управління особливо при загостренні психологічної напруги та високої зміни обстановки. Але особливо гостро стоїть питання розподілу та оптимальності обсягів інформації, що надходить до споживачів, як частини загальної системи управління [4-6]. Це обумовлює актуальність проведення відповідних досліджень.

Мета статті. Аналіз найважливіших проблем реалізації концепції "мережево-центричних війн", передових країн світу та врахування їх при створенні автоматизованих систем управління військами (силами).

Викладення основного матеріалу. Хід впровадження та удосконалення концепції мережових (мережецентричних) війн (NCW, Net-Centric Warfare) у ЗС передових країн світу.

На сьогодні в ЗС передових країн світу, в рамках концепції мережоцентричних війн, продовжується створення та удосконалення єдиної глобальної мереже-центричної системи, яка об'єднає розосереджені в єдиному бойовому просторі JWS (Joint Warfighting Space) всі роди військ, і забезпечить горизонтальну і вертикальну інтеграцію сил і засобів. Мережоцентрична система є інструментом реалізації концепції мережових (мережоцентричних) війн (NCW, Net-Centric Warfare).

Процес ведення мережоцентричної війни передбачає інтегрування і забезпечення ефективного функціонування:

об'єднаної комп'ютерної мережі;

розосереджених, керованих і живучих засобів розвідки;

ефективних засобів ураження.

На основі порівняльного концептуально-прогнозтичного аналізу ефективності класичного способу ведення бойових дій порівняно з веденням війни по концепції Net-Centric Warfare, проведеного військовими експертами, було зроблено попередній висновок щодо перспективності цієї концепції та її затребуваності для методів і способів ведення війн шостого і сьомого поколінь.

У ході реалізації концепції Net-Centric Warfare провідні військові експерти визначили ключові аспекти відмінності даної концепції від традиційного способу ведення бойових дій на прикладі порівняння деяких аспектів і особливостей, в тому числі, надання повноважень посадовим особам під час ведення бойових дій на застосування сили (зброї), характеру надання, розподілу, доступу і використання розвідувальної інформації (таблиця 1).

Процес інформатизації збройних сил дозволяє поєднати в єдину систему засоби зв'язку, управління, розвідки та ураження, що забезпечуватиме командирам усіх рівнів точні і своєчасні дані про обстановку на полі бою і різко підвищити ефективність бойового застосування засобів ураження, що являється основою концепції мережоцентричної війни.

Проблемні питання реалізації концепції мережевих (мережоцентричних) війн (NCW, Net-Centric Warfare) в ЗС передових країн світу.

Деякі експерти застерігають від перетворення концепції "мережоцентричних війн" у панацею. Наприклад, заступник директора Інституту з проблем оборони А. Кауфман вважає, що технології займають занадто багато місця в американській військовій стратегії, неправомірно нав'язуючи свою логіку. Надії Пентагону на те, що інновації принесуть перемогу на полі бою так само, як вони дають прибуток у бізнесі, неспроможні, засилання технократизму у вигляді концепції "мережоцентричної] війни" веде до наступних помилок:

переоцінка здатності людини адекватно переробляти великий обсяг суперечливої інформації;

спрощене бачення противника через зведення його стратегії до асиметричних дій;

недостатній облік мінливої природи бою та невиправдана бюрократизація процесу управління;

явна або неявна посилка, що військова перемога є кінцевою метою всієї кампанії [1].

Таблиця 1

Аспекти відмінності концепції Net-Centric Warfare від традиційного способу ведення бойових дій

Об'єкт порівняння	**Традиційний спосіб ведення бойових дій**	**Ведення бойових дій по концепції Net-Centric Warfare**
Командування	Визначається наказом (директивою)	Залежить від обстановки, що склалася
Керівництво	Визначається посадовими повноваженнями	Визначається компетенцією щодо спроможності оптимального реагування на ситуацію, що склалася
Оперативне управління	Згідно наказів, постанов і директив	Емерджентний* характер оперативного управління
Прийняття рішення	Визначається наказом	Спільна участь у прийнятті рішення
Розвідувальна інформація	Накопичування	Накопичування, обробка і використання розвідувальних даних
Інформаційні потоки	Вертикальні, обумовлені порядком підлеглості органів управління	Вертикальні і горизонтальні, незалежно від підлеглості (ієрархії) органів (пунктів) управління
Характер передачі інформації по трафіках	“Активне, примусове” забезпечення регламентованим об’ємом інформації (незалежно від запиту користувача)	Забезпечення необхідною інформацією, в тому числі по запиту
Джерела розвідувальної інформації	Структури і відомства різних рівнів, структур і типів підпорядкування	Гнучкі схеми розподілу розвідувальної інформації від усіх джерел
Організаційні заходи	Послідовні, суворо регламентовані	Динамічні, паралельні
Посадові особи-учасники бойових дій, які безпосередньо застосовують силу (зброю), або віддають накази (приймають рішення) на її застосування	Алгоритми дій, інструкції	Надання більших повноважень у випадках виникнення критичних ситуацій

Емерджéнтність (англ. *emergence* — виникнення, поява нового) в теорії систем — наявність у будь-якої системи особливих властивостей, не властивих її підсистемам і блокам, а також сумі елементів, не пов'язаних системоутвірними зв'язками; неможливість зведення властивостей системи до суми властивостей її компонентів. Синонім — “системний ефект”.

Надмірна залежність від інформації

Деякі фахівці застерігають, що значення величезних інформаційних ресурсів як засобу розробки та проведення ефективних військових операцій може бути переоцінене і що процес прийняття важливих військових рішень не можна зводити тільки до розумового аналізу інформації. Вони стверджують, що дискусії про - трансформацію збройних сил були надмірно сфокусовані на перевагах, які надає інформація, і що види збройних сил, органи забезпечення національної безпеки і розвідувальне співтовариство не вивчили уважно ризики, пов'язані з військовою доктриною, в основі якої полягає інформація. Наведемо деякі проблеми, які були підняті фахівцями:

опора на сучасні інформаційні системи може призвести до самовпевненості управлінського персоналу;

кількісні зміни в інформації та її аналізі дуже часто ведуть до змін у поведінці окремих людей та організацій, що призводить до зворотних результатів. Наприклад, інформаційні технічні засоби дозволяють виявляти більшу кількість цілей, боєприпаси можуть витрачатися

швидше, що веде до більшої залежності від матеріально-технічного забезпечення;

обстановка, що характеризується великою кількістю інформації і можливостей, може змінити цінність інформації, змусити переглянути цілі військової місії і, можливо, збільшити ймовірність прийняття помилкових рішень [2].

Необхідність роботи з надмірним обсягом інформації Поширення датчиків на полі бою створило проблему "перевантаження інформацією". Величезні потоки вхідної інформації можуть приголомшити користувачів і створити загрозу для процесу прийняття рішення. Керівництво збройними силами провідних країн світу вивчає питання використання центрів "злиття інформації", в якому буде застосовуватися спеціальне програмне забезпечення, щоб фільтрувати інформацію про бойову обстановку, яка не потрібна військовослужбовцям, які ведуть бойові дії, для того щоб забезпечити контроль і захист радіочастот від перешкод противника.

Зростаюча складність бойових систем Бойові системи та програмне забезпечення стають все більш складними. Програмне забезпечення призначене для обробки інформації, визначення положення противника і своїх військ, комплексу цілей, подачі сигналу тривоги, координації та управління діями екіпажних і безпілотних бойових засобів на землі, на морі і в повітрі. Наприклад, за оцінками фахівців, для роботи перспективної бойової системи сухопутних військ буде потрібно 31 млн. рядків кодів комп'ютерних програм. Крім того, багато бойових систем, що працюють із власним обладнанням зрештою будуть об'єднані в мережеві системи. Однак у міру збільшення складності компонентів мережових систем доведеться обробляти інформацію, що отримується від систем, можливості і надійність яких не завжди відомі.

Ось що говориться про складність комп'ютерних систем військового призначення в статті, виданій Інститутом з розробки програмного забезпечення Карнегі Меллона: "Коли говорять про сучасні системи", то багато систем називають "необмеженими", тому що вони охоплюють невідому кількість учасників або, іншими словами, вимагають, щоб окремі учасники діяли або взаємодіяли в умовах відсутності необхідної інформації. Для складних "систем ", створених сьогодні і призначених для майбутнього, вже неможливо, щоб людський або автоматизований компонент володів повним знанням системи. Кожен компонент системи повинен залежати від інформації, отриманої від інших систем, можливості, цілі і надійність яких невідомі [3].

Однією з основних проблем надійності функціонування і живучості глобальної мережоцентричної системи являється забезпечення надійної інформаційної захищеності складових елементів системи. Теоретично, для виведення з ладу глобальної мережоцентричної системи достатньо зменшити швидкість передачі даних, що призведе до багатократного збільшення часу проходження інформації від засобів розвідки до пунктів обробки інформації і засобів ураження і, практично, паралізує ланку "виявлення-ідентифікація-цілевказівка-ураження". Однією з необхідних умов реалізації концепції мережоцентричних війн є необхідність досягнення високого рівня захищеності каналів передачі даних і каналів зв'язку, які, гіпотетично, можуть бути викриті противником за допомогою інформаційних і комп'ютерних технологій. Сучасний рівень розвитку програмного забезпечення підвищує ймовірність отримання противником несанкціонованого доступу до елементів управління і зв'язку мережоцентричної системи, що значно знижує ефективність концепції.

Проблемним питанням концепції Net-Centric Warfare є необхідність задіювання інформаційно-управляючого комплексу, який являтиме собою суперкомп'ютер (комп'ютер із високою продуктивністю і необхідним програмним забезпеченням), спроможний обробляти велику кількість інформації в реальному масштабі часу.

Проблемним питанням реалізації концепції мережоцентричних війн є створення надійного високоінтелектуального комунікаційного середовища для забезпечення обробки різних потоків розвідувальної інформації про ціль (об'єкт), і забезпечення можливості заміни (перепрограмування) алгоритму обробки розвідувальних даних у залежності від динаміки розвитку обстановки (зміна векторів зовнішньої і внутрішньої політики, військово-політичної обстановки тощо) [4-6].

Усунення виникаючих проблем, шляхи удосконалення концепції мережових (мережоцентричних) війн в ЗС передових країн світу та використання передового досвіду при розробці та конструюванні АСУ ЗС України.

Отже інтенсивний розвиток мережоцентричної концепції ведення бойових дій у збройних силах провідних країн світу приводить до необхідності опрацювання все

більших обсягів інформації кожним військовослужбовцем. Така тенденція постійно посилюється і з кожним роком дані подаються все в більших пропорціях, що призводить до все більших збоїв у традиційних системах взаємодії між суб'єктами проведення операцій.

Виходом із зазначеного становища є проведення операцій з використанням інтегрованого командного середовища, де кожний військовий спеціаліст представляє собою частину загальної системи. Такий підхід значно спрощує процес прийняття рішень у ході проведення операцій та підвищує їх ефективність.

Доцільно проводити роботу над тим, щоб повністю інтегрувати людину і техніку в командне середовище. При цьому постає головне завдання максимально обробити та спростити інформацію, щоб людина зрозуміла все на півслова. Таким чином, процес прийняття рішень підчас бойових дій, та ще у стресовій ситуації стане набагато простішим, а значить і ефективнішим.

Найважливішу роль у формуванні інтегрованого командного середовища відіграють інформаційні технології, які забезпечують фільтрування, відокремлення та розподіл необхідної інформації у певний момент розвитку операційної ситуації для кожного військовослужбовця, який бачить картину бою у цілому, при цьому слідкуючи за її окремим елементом. Зазначений вище підхід вимагає подальшого розвитку інформаційних технологій, основними з яких є: створення поглибленої архітектури безпеки для захисту, виявлення, своєчасного реагування та відновлення інформаційних систем під час випадкових помилок суб'єктів операцій, внутрішніх та зовнішніх шкідливих атак тощо; забезпечення інформаційної доступності, цілісності, конфіденційності, аутентифікації і безвідказності; забезпечення ефективного захисту інформаційно-психологічного впливу противника; забезпечення обміну даних у реальному часі; забезпечення інформаційної підтримки суб'єктів операцій через мережеві інфраструктури.

Необхідно вивчати питання щодо розподілу потоків інформації та можливе створення підрозділів "злиття та розподілу інформації", в яких буде застосовуватися спеціальне програмне забезпечення для фільтрування інформації про бойову обстановку [7].

Висновки. Таким чином, головне завдання щодо створення автоматизованих систем управління Збройними Силами України полягає у впровадженні сучасних інформаційних технологій в управління військами, бойовими засобами та зброєю.

Ідеологія побудови АСУ ЗС України сьогодні має враховувати як розвиток підсистеми стратегічного рівня управління, так і створення АСУ тактичної ланки, а також безумовну інформаційну інтеграцію всіх рівнів управління АСУ ЗС України.

Основну роботу та **подальші дослідження** з врахуванням досвіду передових країн світу необхідно присвятити оптимальному розподілу інформаційних потоків у підсистемі автоматизованої системи управління військами, а саме у підсистемі зв'язку та передачі даних.

СПИСОК ЛІТЕРАТУРИ

1. Thomas T.L. Chinese and American network warfare // Joint Force Qwarterly, July, 2005.
2. David Fisher and Dennis Smith, Emergent Issues in Inoperability, News@SEI,2004, [http:www.cmu.edu/news-at-sei/columns/eye-on-integration/2004/3/eye-on-integration-2004-3.htm].
3. Ільяшов О.А. Тенденції розвитку збройної боротьби у війнах четвертого – шостого поколінь України / О.А. Ільяшов // Наука і оборона. – 2009. – № 3. - С. 43-49.
4. АСУ: проблемы и решения [Електронний ресурс]. Режим доступу до ресурсу: http://www.vko.ru/DesktopModules/Articles.
5. Клиланд Д., Кинг В. Системный анализ и целевое управление. Пер. с англ. – М: Советское радио, 1974. – 280 с.
6. Чельцов В. Сетевые войны XXI века / В. Чельцов, С. Волков // Воздушно-космическая оборона. – 2008. – № 4 (41). – С. 9-16.
7. Редько В.Г. Эволюция, нейронные сети, интеллект: Модели и концепции эволюционной кибернетики. – М.: Ком Книга, 2007. – 224 с.