УДК 355/359.07 DOI: https://doi.org/10.33099/2304-2745/2021-2-72/40-50

Сніцаренко П. М., д-р техн. наук, ст. наук. співроб. (0000-0002-6525-7064)
Саричев Ю. А., канд. техн. наук, ст. наук. співроб. (0000-0003-1380-4959)
Ткаченко В. А., канд. військ. наук (0000-0002-9625-2434)
Зубков В. П. (0000-0003-1616-2795)

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Досвід збройних сил провідних країн світу в інтересах удосконалення інформаційного забезпечення Збройних Сил України

Резюме. У статті аналізується досвід упровадження інформаційних систем для управління збройними силами провідних країн, особливості їх організації та здійснення в арміях держав – членів НАТО. За результатами цього аналізу пропонуються підходи до визначення шляхів удосконалення інформаційного забезпечення систем управління Збройних Сил України.

Ключові слова: інформаційні системи; системи управління; мережецентрична війна.

Постановка проблеми. Сучасні збройні конфлікти характеризуються посиленням ролі політичних, економічних, екологічних та особливо інформаційних засобів під час підготовки і воєнного протистояння, перетворенням сухопутного, повітряного, космічного, морського та інформаційного просторів у єдиний театр воєнних дій. До того ж постерігається швидкоплинність воєнних дій, які можуть поширюватися на всю територію держав-суперниць. Набирає обертів тенденція до "безконтактних" та асиметричних бойових дій, зосередження зусиль на виведенні з ладу "критичних центрів" противника, насамперед, органів політичного та військового керівництва, об'єктів, які мають стратегічне значення для економіки та безпеки держави.

Усе це створило передумови докорінного перегляду характеру майбутніх операцій (бойових дій), які все більше набувають інформаційно-технологічного характеру в усіх сферах воєнних дій та змусило керівництво провідних держав світу переглянути теорію і практику військового будівництва. Саме тому, із врахуванням змін характеру війн і воєнних конфліктів, продовжується масштабне реформування збройних сил провідних країн світу, спрямоване, зокрема, на структурні та функціональні зміни в системах їх управління, що тісно пов'язане з удосконаленням процесів інформаційного забезпечення.

Аналіз публікацій показує, що на сьогодні активно досліджується проблематика формування майбутнього обрису Збройних Сил України (ЗС України) за досвідом держав – членів Альянсу. Зміст концепцій і планів будівництва та розвитку збройних сил країн світу показує, що удосконалення системи управління військами (силами) відноситься до пріоритетних напрямів [1, 2]. Водночас, досвід участі збройних сил провідних країн світу в операціях кінця XX – початку XXI століття визначив основною тенденцією розвитку теорії і практики управління військами – розроблення та впровадження концепції мережецентричних війн (Net-Centric Warfare – NCW) [3–9]. У цих публікаціях стверджується, що мережецентрична війна – війна, у якій досягнення успіху забезпечується на основі інформаційної переваги над противником за допомогою об'єднання військових об'єктів у *єдину інформаційну мережу* [10].

У наведених виданнях досліджуються в основному принципові завдання побудови автоматизованих систем управління для реалізації концепції мережецентричних війн [9]. Водночас, у них не достатньо уваги приділяється саме інформаційному забезпеченню таких систем. Без актуальної інформації будь-яка автоматизована система не спроможна виконати функціональні завдання за призначенням. До того ж інформаційна перевага може бути досягнута своєчасним інформаційним забезпеченням процесу прийняття рішень та дій на всіх рівнях системи управління військами (силами). Отже питання інформаційного забезпечення сучасних систем управління у воєнній сфері набуває найважливішого значення.

Метою статті є обґрунтування підходів до визначення напрямів (шляхів) удосконалення інформаційного забезпечення

системи управління ЗС України на підставі досвіду побудови та використання інформаційних систем для управління збройними силами провідних країн світу. У статті позначені лише основні контури розвитку систем в умовах підготовки до ведення принципово нових війн XXI століття.

Виклад основного матеріалу. Наприкінці XX століття американськими військовими аналітиками було проведено дослідження характеру воєн і воєнних конфліктів у світі, починаючи з XVI століття. Війна майбутнього видається не тільки як високотехнологічна війна, а, насамперед, як "мережева" війна, що потребує об'єднання всіх учасників бойових дій, надання точних і своєчасних даних про обстановку на полі бою в реальному масштабі часу для забезпечення упереджувального ураження об'єктів противника [11].

Водночас, однією з найбільш поширених помилок є думка про те, що механічне об'єднання органів управління військових формувань усіх рівнів інформаційною мережею дасть змогу вирішити проблеми стійкості та надійності керівництва військами (силами). Такі мережі, як і всі комп'ютерні системи, працюють за принципом "сміття на вході – сміття на виході", тобто це принцип програмування, відповідно до якого невірні вхідні дані не можуть привести до правильного кінцевого результату. Отже, без точних об'єктивних даних актуальної інформації, якими наповнюють мережі, самі собою ці мережі залишаються не більше ніж високошвидкісними цифровими трактами обміну інформацією між об'єктами.

Саме для мережевого принципу забезпечення військ (сил) точною та своєчасною інформацією і проводиться реформування збройних сил провідних країн світу, а також реалізуються нові принципи управління і ведення бойових дій, передбачені перспективними "мережецентричними" концепціями.

На сьогодні поняття інформації має багато визначень. Для воєнної сфери доцільно вважати, що узагальнено під *інформацією* розуміються оброблені та осмислені дані (відомості), тобто їх змістовність, значення (сутність), знання або висновки, отримані на їх основі незалежно від форми подання [12]. При цьому цінність інформації визначається корисністю та її здатністю забезпечити певного суб'єкта необхідними умовами для досягнення ним поставленої мети.

Слід зауважити, що за законами кібернетики [13] будь-яка функція управління в системах реалізується виключно інформаційним шляхом, а тому зрозуміло, що процес всякого управління, а у воєнній сфері особливо, потребує реалізації низки інформаційних процесів, що мають вплив на усі елементи механізму управління. Сукупність цих інформаційних процесів власне і об'єднується поняттям *інформаційного забезпечення*, яке пронизує замкнений контур управління, а його сутність полягає, з одного боку, у формування завдань та їх донесення від органу управління до суб'єктів системи, а з іншого – у можливості отримання органом управління зворотної інформації для контролю процесу управління та коригування інформаційного впливу. Зазначене узагальнюється доречними визначеннями, наведеними у Військовому стандарті [12].

Інформаційне забезпечення (у воєнній сфері) – сукупність заходів органів військового управління усіх рівнів, дій військ (сил) та інших суб'єктів інформаційної діяльності з метою створення (формування) і використання в інформаційному просторі воєнної сфери необхідних інформаційних ресурсів для реалізації процесів управління в інтересах оборони держави.

Інформаційний простір воєнної сфери – частина інформаційного простору держави: середовище, у якому відбуваються інформаційні процеси та інформаційні відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації (інформаційних продуктів, інформаційних ресурсів) воєнного характеру.

Невід'ємними складовими інформаційного середовища є інформаційні ресурси, інформаційна інфраструктура та інформаційні технології, що становлять сутність національного інформаційного потенціалу.

Інформаційний ресурс – дані та знання, відмінною і невід'ємною характеристикою яких є їхня прагматична цінність, що визначається практичними потребами в інтересах вирішення певних завдань.

Інформаційна інфраструктура – сукупність різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікацій і управління інформаційними потоками, а також організаційно-технічних структур,

механізмів, що забезпечують їх функціонування.

Нині саме рівень інформаційного потенціалу, в основі якого лежить інформаційний ресурс, що продукується елементами інформаційної інфраструктури, та можливість його ефективного, зокрема автоматизованого, використання, все більшою мірою зумовлює високу оперативність та якість прийняття рішень, необхідні структуру і характеристики органів управління, зразків озброєнь, оцінку рівня їх достатності, у цілому з великою ймовірністю визначає результат збройного протистояння.

Принципи ведення воєнних дій, будівництва збройних сил і управління бойовими формуваннями в XX столітті, в епоху "індустріальної ери", серед військових фахівців отримали найменування "платформоцентричні" (Platform-Centric Warfare). Тим часом успіх операцій (боїв) залежав, здебільшого, від індивідуальних можливостей бойових засобів, а об'єднання мережами, хоча і передбачалося, але не давало змоги домогтися ефекту, який дають нові інформаційні технології [9].

У сучасну епоху "інформаційної ери" (*Information Age, Digital Age, Computer Age*) на перше місце виходять нові інформаційні технології. Їх впровадження у військову сферу також спрямовано на підвищення бойових можливостей формувань, але вже не тільки через підвищення розвідувальних, вогневих, маневрених та інших характеристик індивідуальних зразків (платформ), але, насамперед, завдяки наявності кращого інформаційного забезпечення та можливості скорочення циклу бойового управління в операції (бою) [14].

Об'єднання мережею охоплює не тільки системи бойового управління, зв'язку, обчислювальної техніки, розвідки і спостереження, а й бойові платформи, і насамперед такі, як носії засобів вогневого ураження. Це і визначає формування нової системи поглядів на форми і способи ведення збройної боротьби. Тому найімовірніше, що у 2020-х збройні сили провідних країн світу повністю перейдуть від "платформоцентричних" до "мережецентричних" операцій, що передбачають отримання нових можливостей формувань від об'єднання різноманітних платформ в єдиний бойовий інформаційно-комунікаційний простір.

Поняття "мережецентрична війна", або "ведення бойових дій в єдиному інформаційно-комунікаційному просторі", розглядає елементи збройних сил як пристрої, підключені до мережі. Залежно від вибору мережевої архітектури і її типу засобами мережі можуть бути військові частини та підрозділи, кораблі, літаки, засоби ураження, органи управління, зв'язку, розвідки, а також комбінація і тих, і інших. Можливості таких бойових одиниць визначаються не стільки індивідуальними характеристиками, скільки можливостями всієї групи підключених до мережі засобів, як єдиного цілого.

За розрахунками спеціалістів, автоматизація процесів збору, оброблення, узагальнення, передавання (приймання), використання інформації може сприяти підвищенню бойових можливостей військ (сил) на 15–20 % і водночас на 50 % скоротити час, який витрачають органи військового управління всіх рівнів на прийняття рішень і доведення завдань до підлеглих [15].

Забезпечення всебічної інтеграції, підвищення рівня взаємодії завдяки реалізації принципів нових мережецентричних концепцій та інтеграції систем управління, зв'язку, розвідки і ураження стає все більш актуальним і пріоритетним напрямом реформування збройних сил більшості країн світу.

Загалом, заходи з питань упровадження мережецентричних концепцій в основному здійснюються в трьох ключових напрямах:

розроблення систем отримання, обробки, аналізу і розподілу інформації, що використовують уніфіковані інструментарії її обробки і формати передання;

розгортання сучасних систем зв'язку і передання даних;

оптимізації організаційних структур органів управління, обробки та аналізу інформації, підготовка особового складу та перегляд доктринальних документів.

Відомо, що у ***НАТО*** реалізується концепція "Комплексні мережеві можливості" (NATO Network Enabled Capabilities – NNEC), яка призначена для організації взаємодії високотехнологічних формувань національних збройних сил у збройних конфліктах [9, 16, 17]. Її реалізація дасть змогу здійснювати ефективне інформаційне забезпечення операцій всього можливого спектру, починаючи від миротворчих операцій зі встановлення миру до великомасштабних бойових дій високої інтенсивності. Водночас, військові фахівці НАТО підкреслюють, що NNEC – це не тільки інтеграція систем управління і зв'язку, а й можливість підвищити рівень інформаційної взаємодії всіх учасників операції (бойових дій), зокрема

і засобів ураження, органів і пунктів матеріально-технічного забезпечення.

У ***США*** сутність поняття "мережецентрична війна", "ведення бойових дій у єдиному інформаційно-комунікаційному просторі", зважаючи на досвід застосування військ (сил) у сучасних конфліктах, набула найбільшого практичного наповнення у єдиній системі розвідувально-інформаційного забезпечення і бойового управління ЗС США – "Мережецентрична війна" (Network Centric Warfare – NCW) [9, 16].

Тим часом у ***Великобританії*** формується власна інформаційна інфраструктура (Network Enabled Capability), що являє собою єдину інформаційно-керуючу мережу, зі спеціалізованими системами забезпечення безпеки і єдиним сімейством програмного інструментарію. У майбутньому можливості інформаційної інфраструктури планується розширити для організації взаємодії та забезпечення доступу до інформаційних ресурсів збройних сил союзників: США, Канади, Австралії та Нової Зеландії [9, 16, 17].

У ***Франції*** такі заходи реалізуються також у межах мережецентричної концепції (Інформаційно-центрична війна (Guerre Infocentre), яка, здебільшого, акцентує увагу на інформаційних потоках, а не самих мережах, як прийнято у США [16]. Розгорнуті командно-інформаційні системи рівня С2: у сухопутних військах – для дивізій, полків, артилерії, протиповітряної оборони, ВПС – для управління повітряними операціями, у ВМС тактичні системи встановлені на авіаносцях та фрегатах [9, 17].

У ***ФРН*** також працюють над створенням перспективної системи "Піхотник майбутнього" (Infanterist der Zukunft), для реалізації нових принципів інформаційного забезпечення та зв'язку між бойовими формуваннями і вищими органами управління. Заходи включають розроблення перспективних засобів розвідки, комп'ютерних систем, військових систем управління та зв'язку типу "тактичний інтернет", що дасть змогу організувати взаємодію між аналоговими засобами зв'язку та цифровими системами передавання даних [9, 17, 18].

Крім того, вперше в світовій історії дві держави, ФРН і Нідерланди, домовилися щодо об'єднання в єдине ціле своїх оборонних інформаційних мереж. Нова єдина система стане називатися "Tactical Edge Networking" (TEN). Вона буде пробною версією для об'єднання в подальшому оборонних інформаційних мереж інших держав Північноатлантичного Альянсу [19].

Ізраїль також розглядає впровадження інформаційних технологій як невід'ємний і обов'язковий атрибут сучасних і майбутніх операцій [16].

Китай серйозно ставиться до мережецентричної концепції інформаційного забезпечення управління і ведення бойових дій. У документах Національно-визвольної армії Китаю (НВАК) зустрічається термін "інтегрована мережева і електронна війна" (Integrated Network-Electronic Warfare- INEW) [9, 20].

В ***Австралії*** в межах концепції "Мережецентрична війна" (Network Centric Warfare) розробляються нові засоби добування інформації, впроваджуються перспективні інформаційні технології, проводяться випробування безпілотних і роботизованих комплексів і систем для того, щоб зробити свої нечисленні збройні сили більш ефективними. Проводиться тестування перспективних мережевих засобів зв'язку і передавання даних, які повинні дати змогу одному оператору здійснювати управління угрупованням робототехнічних засобів, здатних також виходити з мережі і діяти самостійно в цілях збору розвідувальної інформації або нанесення ударів по виявлених об'єктах і цілях [16].

Керівництво збройних сил ***Російської Федерації*** розробляє практичні заходи переходу до управління військами за "мережецентричним" принципом, розглядаючи міжвидове (об'єднане) угруповання військ (сил) як набір елементів мережі, а її застосування, залежно від обраного варіанта дій, як багатоваріантна комбінація дій елементів мережі (бойових формувань). Вважається, що можливості таких бойових формувань визначатимуться не стільки індивідуальними характеристиками, скільки можливостями всієї групи підключених до мережі засобів як єдиного цілого, а успіх у таких умовах залежатиме від ступеня об'єднання всіх учасників операції (бойових дій) у єдиний інформаційно-комунікаційний простір [9, 21].

Очевидно, що головними принципами реалізації заходів щодо широкого впровадження інформаційних складових у воєнну сферу в межах концепції мережецентричних операцій є:

забезпечення реальної інформаційної об'єднаності угруповань;

застосування відкритої архітектури і модульної побудови сучасних систем і комплексів збройної боротьби;

здійснення вертикальної і горизонтальної інформаційної інтеграції та взаємодії всіх учасників операції (бойових дій).

Аналітиками стверджується [9], що війни наступного покоління – це, насамперед, війни розвідок, де володіння необхідною інформацією про противника є ключем до досягнення успіху в таких війнах. В сучасних умовах у провідних країнах світу проглядається стійка тенденція щодо акцентування уваги на здобуванні та інтеграції різноманітної інформації про стан політичних, економічних, соціальних, воєнних, наукових, науково-технічних, інформаційних, правових, організаційних, інших відносин між державами, групами держав та й у світі в цілому.

Отже, такий вид інформаційного забезпечення як моніторинг противника, в основі якої процес всебічної розвідки, є домінуючим у загальній системі інформаційного забезпечення військ (сил). До того ж, будь-яку мережецентричну систему неможливо використовувати за призначенням без актуальної інформації у реальному масштабі часу. Залежно від рівня мережецентрична система за наявністю повної, достовірної, своєчасної, потрібної розвідувальної інформації спроможна наочно відображати обстановку, оцінювати місцевість, стан противника і своїх військ (сил), моделювати розвиток бойових дій, виробляти рекомендації, варіанти рішень, проєкти бойових документів, доводити завдання до підлеглих пунктів управління.

З цією метою військові експерти США [9, 22] вважають за доцільне мати розгалужену структуру збору та постачання розвідувальної інформації для ефективного функціонування мережецентричної системи. Саме тому найбільш розвинута система добування розвідувальної інформації була створена у Сполучених Штатах Америки. Розвідувальне співтовариство Сполучених Штатів включає в себе 16 суб'єктів, серед яких, зокрема, військові структури:

розвідувальне управління міністерства оборони (РУМО) – головний орган, який здійснює свою діяльність в інтересах інформаційного забезпечення прийняття рішень військово-політичним керівництвом країни, а також надає розвідувальну інформацію міністру оборони, комітету начальників штабів (КНШ), об'єднаним командуванням, командуванням видів збройних сил;

агентство національної безпеки – організовує, координує та безпосередньо веде радіо- і радіотехнічну розвідку в глобальному масштабі, а також забезпечує безпеку своїх систем управління та зв'язку;

національне управління геопросторової розвідки – надає своєчасні і точні дані видової розвідки, метеорологічної, океанографічної та іншої інформації, керує силами і засобами видової розвідки національного рівня;

національне управління повітряно-космічної розвідки – здійснює розроблення та управління розвідувальними системами космічного базування, збір і обробку видобутої такими системами розвідувальної інформації;

органи розвідки Сухопутних військ (Army), ВПС (Air Force), ВМС (Navy) – у межах компетенції здійснюють розвідувальне забезпечення бойових дій, управління силами і засобами розвідки, участь у розробленні, оснащення підлеглих структур розвідувальної технікою, навчання особового складу.

Невійськові члени співтовариства: центральне розвідувальне управління, управління розвідки і досліджень державного департаменту, федеральне бюро розслідувань, управління аналізу інформації та захисту інфраструктури міністерстві внутрішньої безпеки, органи розвідки Берегової охорони, відділ розвідки і інформаційно-аналітичної діяльності міністерства фінансів, розвідувальний відділ міністерства енергетики здійснюють за своїми напрямами добування інформації, аналіз та формування висновків для керівництва держави, інших державних органів.

Така потужна структура розвідувальних органів США дає змогу вирішувати весь спектр стратегічних, оперативних і тактичних завдань з розвідки, забезпечувати надання своєчасної і достовірної інформації з політичних, військових, технічних, економічних та інших питань не тільки керівництву держави, міністерству оборони та військовим формуванням, але й іншим державним органам країни.

Зауважимо, що поряд із перевагами мережецентричної концепції ведення бойових дій виявлено і низку проблем щодо її реалізації. Зокрема, гостро постає питання раціонального розподілу та обробки великих обсягів інформації, що надходять до споживачів.

Для ліпшого розуміння цієї проблеми вважаємо за доцільне зупинитися на розподілі класів мережецентричних систем залежно від ступенів автоматизації керованих процесів і потоків інформації, яка в них циркулює.

Досвід розроблення, впровадження та експлуатації мережецентричних систем у США свідчить [9, 23], що сучасні автоматизовані системи управління, які за своєю сутністю є інформаційними, поділяються на декілька класів відповідно від функцій, що виконуються системами – командування, управління, зв'язок, комп'ютери (інформатизація), загальна розвідка, спостереження, розвідка в режимі реального часу (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance).

До того ж, системи різняться за ступенем автоматизації керованих процесів відповідно до цієї класифікації. Кожна система відноситься до конкретного класу відповідно до рівня *автоматизації управлінських функцій.*

Так, якщо система управління в автоматизованому режимі має лише дві функції, наприклад, командування і управління (Command and Control), то відповідатиме класу "СС" (С2).

Якщо в системі автоматизовані чотири функції – командування, управління, зв'язок, інформатизація (Command, Control, Communications, Computers), то таку систему відносять до класу "СССС"(С4).

До того ж, функції, починаючи з буквами "С" використовуються як базові, а інші – додаткові.

З погляду автоматизованих управлінських функцій (завдань), система управління, яка містить у своїй абревіатурі більше букв "С", є більш досконалою. Так, система класу C2SR (Command, Control, Surveillance, Reconnaissance) буде поступатися системі класу С4 за спектром завдань, які використовуються в автоматизованому режимі.

Системи, у яких автоматизовані функції Command and Control (С2), вирішують такі завдання:

відображення та передання бойових завдань підлеглим органам управління (об'єктам управління) у формалізованому текстовому та графічному форматі з використанням єдиної мережі;

визначення положень власних об'єктів управління та оповіщення своїх органів управління і сусідів про їх місцезнаходження з відображенням на електронних картах;

відображення на електронних картах і обмін даними про виявлені об'єкти противника, елементи інфраструктури на полі бою;

відбір і розрахунки маршрутів руху за відомими даними про дорожню мережу та відображення пройденого шляху.

Система С2 дає змогу командиру лише швидко довести прийняте рішення до підлеглих і контролювати хід його виконання. До того ж функції оцінювання обстановки і прийняття рішення повною мірою покладається саме на людину.

Деякі системи, що відносяться до класу С2, можуть виконувати взаємне розпізнавання об'єктів, які знаходяться в системі, за принципом "свій-чужий", а також виконувати ідентифікацію цілей та надавати в автоматичному режимі цілевказівки засобам вогневого ураження, що входять до системи.

Системи управління, у яких автоматизовані такі функції, мають додаткові літери "SR" (Surveillance, Reconnaissance) і позначаються як C2SR (або С2+).

До того ж комп'ютери, які використовуються в системах класу С2, розглядаються тільки як засоби первинної обробки та відображення інформації. Хоча системи С2 і містить у своєму складі ПЕОМ, але слово "Computers" і відповідну літеру в абревіатурі свого класу не мають.

Загалом, система класу С2 лише допомагає командирам доводити до підлеглих завдання, збирати та відображати поточну інформацію про противника та стан своїх об'єктів управління. При цьому, про інтелектуальну підтримку прийняття рішень та про вироблення варіантів рішень на бій і їх моделювання поки ще не йдеться.

Такі завдання, як автоматична організація зв'язку та локальних обчислювальних мереж – це вже відмінність системи, яка має у назві свого класу абревіатуру слова Communications (С3).

Наявність в абревіатурі класу системи четвертої літери "С" (Computers), а також літери "I" (Intelligence) означає, по-перше, повну автоматичну обробку даних, отриманих під час реалізації перших двох "С" – Command and Control, по-друге, вироблення на підставі обробки первинних даних варіанта ситуаційного рішення командира та його представлення у найзручнішій для людини формі, відповідно.

Системи класу С4 (крім виконання функцій, реалізованих в системах класу С2 і С3), мають бути здатні вирішувати такі завдання:

повна автоматизація збору і обробки інформації;

інформаційна підтримка вироблення командиром варіантів рішення (наявність програм типу "Sketch in the decision" – замисел рішення);

моделювання бойових дій за обраними варіантами виконання бойових завдань з графічним відображенням їх ходу і результатів на електронних картах, зокрема з використанням засобів тривимірного відображення поля бою;

інформаційна підтримка розроблення плануючих документів (програма "Sketch in the plan" (начерк до плану), що здійснює перетворення графічних і аудіоматеріалів у плануючі документи;

інформаційна підтримка прийняття рішень під час виконання бойового завдання (оновлення оцінок і висновків на підставі інформації, отриманої під час бою).

Принципова відмінність систем класу С4І від класу С2 полягає в більш високому ступені автоматизації інформаційних та управлінських завдань.

У збройних силах навіть розвинених технологічно країн системи класу С4І і С4SR за рівнем управління відносяться до систем *оперативної або оперативно-стратегічної ланки.*

Наявні на озброєнні іноземних держав системи тактичної ланки відносяться до класу С2 або С2+ і розрізняються між собою лише невеликим розширенням спектру розв'язуваних завдань. До того ж, усі системи тактичного призначення принципово не досягають навіть класу С3.

На думку військових експертів [22], основними перешкодами на шляху розвитку систем тактичної ланки з класу С2 до класу С3 і С4 є:

відсутність математично коректних алгоритмів оцінки дій військ на тактичному рівні, зважаючи на величезну різноманітність застосовуваних ними способів і прийомів виконання бойових завдань;

складність створення автоматизованої системи збору та оцінки даних тактичної обстановки, з огляду на велику різноманітність її параметрів і швидкоплинність змін (порівняно з оперативною ланкою управління);

необхідність обробки великої кількості даних в одиницю часу, які за своїми обсягами на сьогодні перевищують можливості машинного забезпечення, що використовується в тактичної ланці управління;

складність створення мереж зв'язку і надійних локальних мереж (систем передачі даних) між великою кількістю високомобільних об'єктів управління.

На теперішній час вагомий розвиток систем класу С+ в інтересах реалізації концепції мережецентричних операцій здійснено фахівцями США.

Найбільш відомою з усіх існуючих систем тактичної ланки є американська система класу "C2SR" FBCB2 – Force XXI Battle Command Brigade and Below ("Система управління бригадою та підпорядкованими підрозділами в бою (битві) двадцять першого століття") – один з основних компонентів автоматизованої системи управління сухопутних військ США ABCS (Army Battle Command System), яка зіграла ключову роль в операціях в Іраку і Афганістані [23].

Слід зауважити, що на цьому етапі розвитку ЗС України стан автоматизації управлінських процесів неможливо назвати задовільним. Відповідно до [24] автоматизація діяльності органів військового управління становить лише 10-30 % від потреб, наявні засоби не складають цілісних систем, існуючі інформаційно-розрахункові ресурси відповідають потребам органів управління лише на 12-15 %. До того ж рівень інформатизації систем управління суб'єктів оборони держави порівняно зі збройними силами провідних країн світу становить 2-2,5 %. Водночас слід зауважити, що наявність на пункті управління великих екранів зі значками різних кольорів на електронній топографічній карті не є ознакою високого рівня автоматизації системи управління військами. За роки незалежності в ЗС України, незважаючи на низку спроб, не було створено жодної завершеної інформаційної системи як управління військами (силами), так і оборонними ресурсами [25]. Виявилося, що таке завдання постало надто складним.

Тим часом у цьому контексті вищим військовим керівництвом України визначено бачення щодо розвитку системи управління військами (силами): "… Необхідно побудувати у Збройних Силах України надійну систему зв'язку, автоматизації, розвідки та спостереження (С4ISR), стійку до зовнішнього впливу, захищену від засобів

РЕБ, яка буде мати альтернативні канали зв'язку. Засоби зв'язку повинні бути поєднані із засобами зв'язку країн – партнерів. Необхідно створити інформаційну мережу в інтересах сектору безпеки і оборони держави, яка забезпечуватиме набуття інформаційних спроможностей для отримання, опрацювання, зберігання, передавання, контролю та надання інформації на вимогу командувачів (командирів) та штабів (тактичного, оперативного, стратегічного рівнів) об'єднаних сил" [26].

На нашу думку, робити спробу на створення одразу системи C4ISR – це завдання, яке не відповідає ресурсним можливостям держави. Як приклад, для оптимізації проведених заходів реалізації концепції НАТО "Комплексні мережеві можливості" (NATO Network Enabled Capabilities – NNEC) сформовано спеціальний консорціум NCOIC (96 компаній з 32 країн, 26 з яких є членами НАТО), призначений забезпечити єдність протоколів обробки інформації та координацію зусиль промисловості у виконанні вимог щодо досягнення необхідного рівня взаємодії і інтеграції перспективних систем стосовно забезпечення реалізації мережецентричних принципів управління військовими формуваннями.

Так, за висновками американських аналітиків, жоден з європейських союзників у найближчому майбутньому, швидше за все, не зможе створити повністю мережеву армію. Найбільшим обмеженням для європейських інвестицій у C4ISR є загальні обмеження оборонних бюджетів, а не відсутність адекватної технології [17].

Може бути запозичений також і досвід Китаю, де військові фахівці усвідомлюють, що створити мережецентричну систему, адекватну американській, незважаючи на наявність значного воєнного бюджету, в найближчому майбутньому їм не вдасться. Тому ставка робиться на створення сил, систем і засобів, що забезпечують асиметричну дію на противника – вогнева і електронна поразка елементів інформаційних структур (командних пунктів, вузлів зв'язку, орбітального угруповання супутників розвідки та управління і т. ін.) [27].

З огляду на зазначене, в Україні розроблення С-подібної системи доцільно починати з рівня С2+, з подальшим еволюційним нарощуванням до С3 і вище, зважаючи на результати випробувань, досвіду експлуатації та ресурсних можливостей. Однак слід пам'ятати, що інформаційне забезпечення органів управління є пріоритетним завданням – без інформації будь-яка система управління працює неефективно. Лише за наявністю актуальної інформації система спроможна виконати функціональні завдання за призначенням.

На наш погляд, рівень інформаційного забезпечення військ (сил) в інтересах ситуаційної обізнаності має забезпечувати:

для *тактичного рівня (взвод, рота, батальйон, бригада)* – за допомогою системи типу С2+, з вирішенням таких завдань:

обмін інформацією про положення, виявлені об'єкти противника та його дії в автоматизованому режимі у реальному масштабі часу з відображенням на електронних картах зверху вниз і знизу вгору;

передання бойових завдань підлеглим у формалізованому текстовому та графічному форматі та контроль їх виконання;

визначення положень власних об'єктів управління та оповіщення своїх органів управління і сусідів про їх місцезнаходження з відображенням на електронних картах;

взаємне розпізнавання об'єктів, що знаходяться в системі, за принципом "свій-чужий";

ідентифікація цілей та надання в автоматизованому режимі цілевказівки засобам вогневого ураження;

для *оперативного та стратегічного рівнів* – за допомогою системи типу С3 (надалі – С4 з додатками), яка має бути здатною вирішувати такі завдання:

повна автоматизація збору і оброблення інформації у реальному (близькому до реального) масштабі часу про противника, положення та стан своїх військ (сил);

інформаційна підтримка вироблення варіантів рішень на застосування Збройних Сил, військ (сил), з'єднань та військових частин;

моделювання операцій (бойових дій) за обраними варіантами з графічним відображенням їх ходу і результатів на електронних картах, у тому числі, з використанням засобів тривимірного відображення;

інформаційна підтримка розроблення плануючих документів, перетворення графічних і аудіо матеріалів в плануючі документи;

інформаційна підтримка уточнення рішень у ході операцій (бойових дій).

Отже, досвід провідних країн світу переконливо свідчить, що під час

впровадження мережецентричної концепції для систем управління ЗС України головна увага має бути зосереджена на питаннях збору, обробки, аналізу, ототожнення та безпеки інформації для підтримки прийняття рішень керівниками усіх рівнів. До того ж, надання своєчасної актуальної достовірної (релевантної) інформації для систем управління військового призначення постає головним завданням в загальному процесі інформаційного забезпечення ЗС України.

Висновки

1. Діяльність щодо побудови та використання інформаційних систем для управління збройними силами провідних країн світу, насамперед, досвід держав – членів НАТО, викликає нагальну потребу для подальшого пошуку підходів до удосконалення *інформаційного забезпечення* систем управління ЗС України. Мережеву війну можна виграти тільки мережевими засобами, адаптувавши до власних умов і цілій ефективні технології.

2. Концепція мережецентричних війн являє собою систему поглядів на ведення бойових дій та військово-технічне забезпечення в умовах повної комп'ютеризації сил і засобів збройної боротьби. При цьому функціональна сумісність автоматизованих систем розвідки, управління військами та зброєю, а також забезпечення стійкої взаємодії між ними розглядаються як ключові компоненти, необхідні для досягнення *інформаційної переваги* і, як наслідок, переваги у виробленні та прийнятті рішення з метою рішучого упередження противника за всім циклом бойового управління (за принципом "першим побачив – першим вистрілив").

3. Інформаційне забезпечення мережевих структур стає головною і необхідною умовою ефективного функціонування систем управління. Для створення такої структури та єдиного інформаційного простору для користувачів у реальному (близькому до реального) масштабі часу необхідно об'єднання автоматизованими системами всіх сил і засобів добування та генерування інформації.

4. Належне та своєчасне інформаційне забезпечення систем управління військового призначення, як необхідна умова втілення мережецентричних принципів ведення бойових дій, може бути реалізоване в ЗС України впровадженням С-подібної системи автоматизованого управління шляхом її еволюційного розвитку, починаючи з побудови системи класу С2+. У цьому разі, враховуючи великий досвід, набутий збройними силами США щодо розвитку інформатизації воєнної сфери, впровадження у практику теорії мережецентричних операцій, а також той факт, що Україна знаходиться у стані війни, вважаємо за доцільне:

узяти за приклад для впровадження у ЗС України існуючу американську автоматизовану систему управління тактичної ланки класу C2SR – Force XXI Battle Command Brigade and Below (FBCB2) або іншу перспективну автоматизовану систему управління іноземного виробництва;

на першому етапі, як невідкладний захід, розглянути питання щодо закупівлі бригадного комплекту автоматизованої системи управління тактичної ланки для проведення випробувань для визначення доцільності щодо подальшого впровадження у ЗС України;

у разі отримання позитивних результатів порушити питання щодо поетапного оснащення військових частин та підрозділів Сухопутних військ ЗС України перспективними автоматизованими системами управління тактичної ланки іноземного виробництва;

одночасно набутий досвід спрямувати на розроблення вітчизняних (з урахуванням можливостей науки і промисловості України) С-подібних перспективних адаптивних систем управління різних рівнів, сумісних з автоматизованими системами управління збройних сил країн – членів НАТО.

Подальші дослідження доцільно спрямувати на розвиток інформаційного забезпечення ЗС України за допомогою більш чіткого визначення складу, структури та обсягів потоків інформації, які циркулюють у системах управління, обґрунтуванні функціональних складових інформаційного процесу в таких системах, що дасть змогу оптимізувати перелік завдань, які мають виконуватися на кожному етапі циклу управління.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Пащетник О. Д. Аналіз світових тенденцій розвитку автоматизованих систем управління військами і зброєю. *Наука і техніка Повітряних Сил Збройних Сил України*. Харків, 2015. № 2 (19). С. 64–68.
2. Короленко В. А., Синявский В. К., Верещагин С. И. Автоматизация системы управления войсками: на пути от идеи к решению. URL: https://docplayer.ru/56089435-Avtomatizaciya-sistemy-upravleniya-voyskami-na-

puti-ot-idei-k-resheniyu.html. (дата звернення: 28.06.2021).
3. Ільяшов О. А. Тенденції розвитку збройної боротьби у війнах четвертого – шостого поколінь. *Наука і оборона*. 2009. № 3. С.43–48.
4. Савин Л. В. Сетецентричная и сетевая война. Введение в концепцию. Москва : Евразийское движение, 2011. 130 с. URL: https://www.geopolitica.ru/sites/default/ files/ncw.pdf. (дата звернення: 28.06.2021).
5. Гаврилов А. Автоматизированная система сбора, обработки и распределения разведывательной информации СВ США DCGS-A. *Зарубежное военное обозрение*. 2010. № 7. С. 32–40. URL: http://pentagonus.ru/publ/ 122-1-0-1596 (дата звернення: 25.06.2021).
6. Кондратьев А. Реализация концепции “Сетецентрическая война” в ВВС США. *Зарубежное военное обозрение*. 2009. №5. С. 44–49. URL: http://pentagonus.ru/publ/24-1-0-1159 (дата звернення: 25.06.2021).
7. Баулин В., Кондратьев А. Реализация концепции “Сетецентрическая война” в ВМС США. *Зарубежное военное обозрение*. 2009. № 6. С. 61–67. URL: http://pentagonus.ru/publ/26-1-0-811 (дата звернення: 27.06.2021).
8. Кондратьев А. Е. Борьба за информацию на основе информации. *Независимое военное обозрение*. 2008. № 10. URL: https://nvo.ng.ru/concepts/ 2008-10-24/1_info.html. (дата звернення: 27.06.2021).
9. Теоретичні основи управління угрупованням військ (сил) у сучасних умовах збройної боротьби : монографія / О. М. Загорка, А. К. Павліковський, А. А. Корецький, С. О .Кириченко, І. О. Загорка ; за заг. ред. І. С. Руснака. Київ : НУОУ ім. Івана Черняховського, 2020. 248 с.
10. Воєнна доктрина США “Joint Vision 2020”. URL: http://pentagonus.ru/doc/JV2020.pdf. (дата звернення: 28.06.2021).
11. Балахонцев Я., Кондратьев А. Влияние концепции “сетецентрическая война” на эффективность разведывательного обеспечения Вооружённых сил США. *Зарубежное военное обозрение*. 2011. № 2. С. 14–20.
12. Військовий стандарт ВСТ 01.004.004 – 2014 (01) “Інформаційна безпека держави у воєнній сфері. Терміни та визначення” [затверджено наказом начальника Центрального управління метрології і стандартизації Збройних Сил України Озброєння Збройних Сил України – головного метролога Збройних Сил України від 27.02.2014 р. № 1].
13. Винер Н. Кибернетика или управление и связь в животном и машине. Москва : Сов. Радио, 1968. 328 с.
14. Кондратьев А. Е. Общая характеристика сетевых архитектур, применяемых при реализации перспективных сетецентрических концепций ведущих зарубежных стран. *Военная мысль*. 2008. № 12. С. 63–73.
15. Фролов В. С. Структурно-логічна схема Єдиної автоматизованої системи управління Збройних Сил України. *Наука і оборона*. 2012. № 1. С. 15.
16. Молитвин А.О реализации концепции единого информационного пространства НАТО. *Зарубежное военное обозрение*. 2008. № 1. С. 23–27.
17. Adams G., Ben-Ari G., Logsdon J., Williamson R. (2004). European C4ISR Capabilities and Transatlantic Interoperability. The George Washington University.
18. Корчагин С. Автоматизированные системы управления Сухопутных войск Бундесвера. *Зарубежное военное обозрение*. 2013. № 7. С. 47–53. URL: http://factmil.com/publ/strana/germanija/ 41-1-0-266 (дата звернення: 28.06.2021).
19. MILITARYEXP.COM. URL: https:// militaryexp.com/v-evrosoyuze-vpervye-v-istorii-dogovorilis-o-sozdanii-voennoy-vsemirnoy-pautiny (дата звернення: 25.06.2021).
20. Thomas T. L. (2005). Chinese and American network warfare // Joint Force Quarterly, July, 2005.
21. Долгополов А. И еще раз о сетецентрических войнах. *Армейский сборник*. Февраль 2015. № 2. URL: https://sc.mil.ru/files/morf/military/archive/ ac_5_02_2015.pdf. (дата звернення: 25.06.2021).
22. Разведывательное сообщество США // ВПК. 2009. № 22. URL: vpk-news.ru/sites/default/ files/pdf/issue_288.pdf. (дата звернення: 27.06.2021).
23. Американська АСУ військами FBCB2. URL: http://dragon-first-ru.livejournal.com/33339.html; http://defense-update.com/; http: // pentagonus.ru / (дата звернення: 25.06.2021).
24. Гаценко С. С. Аналіз вимог до систем управління військами та шляхи їх удосконалення. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2015. № 2. С. 85–90.
25. Галаган В. І., Полішко С. В., Бондарчук С. В. Пропозиції щодо удосконалення процесу впровадження інформаційних систем іноземного виробництва в діяльність Збройних Сил України. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського*. Київ, 2019. № 2. С. 62–68.
26. Візія Генерального штабу ЗС України щодо розвитку Збройних Сил України на найближчі 10 років. URL: https://www.mil.gov.ua/news/ 2020/01/11/viziya-generalnogo-shtabu-zs-ukraini-shhodo-rozvitku-zbrojnih-sil-ukraini-na-najblizhchi - 10-rokiv/ (дата звернення: 28.06.2021).
27. Буренок В. А., Кравченко А. Ю., Смирнов С. С. Сетецентричные войны “Воздушно-космическая оборона”. URL: https://www. Мережецентричні війни\ВКО-03-06-11.mht. (дата звернення: 26.06.2021).

Стаття надійшла до редакційної колегії 30.07.2021

The experience of the armed forces of the world's leading countries in the interests of improving the information support of the Armed Forces of Ukraine

Annotation

The experience of the armed forces of the world's leading countries in the operations of the late twentieth and early twenty-first centuries identified the main trend in the development of the theory and practice of troop management - the introduction of the concept of network-centric wars.

The purpose of the article is to substantiate the approaches to determining the directions (ways) of improving the information support of the control systems of the Armed Forces of Ukraine on the basis of the experience of using information systems to manage the armed forces of leading countries.

It is estimated that automation of the processes of collecting, processing, summarizing, transmitting (receiving) information can increase the combat capabilities of troops (forces) by 15-20% and reduce by 50% the time spent on decision-making and bringing tasks to subordinates.

Modern automated control systems, which are essentially informational, are focused on "network-centric actions". The article presents key areas for the implementation of network-centric concepts, the distribution of classes of network-centric systems depending on the degree of automation of controlled processes and the flow of information circulating in them.

The level of automation of military administration at this stage of development of the Armed Forces of Ukraine is only 10-30% of the needs. During the years of independence, the Armed Forces of Ukraine has not created any complete information system for both the management of troops (forces) and defense resources.

The article offers recommendations for the implementation of a network-centric concept (for example C-control system by Armed Forces of USA with an evolution since S2 to S4ISR) for control systems of the Armed Forces of Ukraine. From the experience of the world's leading countries in implementing a network-centric concept for the control systems of the Armed Forces of Ukraine, the main focus should be on the collection, processing, analysis, identification and security of information to support decision-making by managers at all levels. Providing timely up-to-date reliable (relevant) information for military management systems is the main task in the overall process of information support of the Armed Forces of Ukraine.

Keywords: information systems; control systems; network-centric war.