Центральний науково-дослідний інститут
Збройних Сил України
Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.06

Концептуальний підхід до удосконалення інформаційного забезпечення перспективних Збройних Сил України

Олександр ПЕРЕДРІЙ
кандидат військових наук, старший дослідник,
начальник науково-дослідного управління Центру воєнно-стратегічних досліджень
Національного університету оборони України,
03049, пр-т Повітряних Сил, 28, Київ, Україна, e-mail: pomichnik2@gmail.com
ORCID:0000-0003-2877-4959

Петро СНІЦАРЕНКО
доктор технічних наук, старший науковий співробітник, провідний науковий співробітник
Центру воєнно-стратегічних досліджень Національного університету оборони України,
03049, пр-т Повітряних Сил, 28, Київ, Україна, e-mail: snits1954@gmail.com
ORCID:0000-0002-6525-7064

Юрій САРИЧЕВ
кандидат технічних наук, старший науковий співробітник, провідний науковий
співробітник Центру воєнно-стратегічних досліджень Національного університету оборони
України, 03049, пр-т Повітряних Сил, 28, м. Київ, Україна, e-mail: y.sarych@gmail.com
ORCID: 0000-0003-1380-4959

Віктор ЗУБКОВ
старший науковий співробітник Центру воєнно-стратегічних досліджень
Національного університету оборони України, 03049, пр-т Повітряних Сил, 28,
м. Київ, Україна, e-mail: zubkov870@gmail.com
ORCID: 0009-0008-5755-2339

Анотація. Актуальність даної статті обумовлена тим, що сучасні збройні конфлікти призводять до зміни характеру воєнних дій, які все більше набувають інформаційно-технологічного характеру. Це змушує керівництво провідних держав світу переглянути теорію і практику військового будівництва для реалізації концепції “мережецентричної війни”. Такий підхід передбачає розгляд органів управління, підрозділів, літаків, кораблів, зв’язку, розвідки збройних сил як об’єктів, що підключені до єдиної інформаційно-комунікаційної мережі. Можливості такої мережецентричної системи ведення воєнних дій визначаються спроможностями всієї групи об’єктів, підключених до мережі (синергетичний ефект). У реалізації цієї концепції ключова роль належить інформаційному забезпеченню об’єктів єдиної мережі, яке має ряд складових, котрі потребують реалізації в мережецентричній системі ведення воєнних дій. Вимога високої оперативності інформаційного забезпечення спричиняє необхідність широкого впровадження в ній автоматизованих систем управління (АСУ). При цьому інформаційне забезпечення об’єктів єдиної мережі є головним призначенням АСУ. Її засоби в автоматичному режимі дозволяють оперативно відображати обстановку, оцінювати місцевість, стан противника, своїх військ (сил), моделювати розвиток бойових дій, розробляти варіанти рішень, проєкти бойових документів, доводити завдання до підлеглих, здійснювати контроль їх виконання.

У статті аналізується досвід впровадження інформаційних систем для управління збройними силами провідних країн, особливості їх організації та здійснення в арміях держав-

членів НАТО. За результатами цього аналізу пропонуються концептуальні підходи до визначення шляхів удосконалення інформаційного забезпечення систем управління Збройних Сил (ЗС) України. Одним з головних завдань ЗС України (Сил оборони) на шляху до членства у НАТО є створення системи військового управління за мережецентричним принципом. Ця система повинна бути оснащена АСУ та сумісною з системами військового управління Альянсу. Між тим, за даними іноземних публікацій, рівень автоматизації систем управління сил оборони України сьогодні становить 2-2,5% порівняно зі збройними силами провідних країн світу, у яких АСУ забезпечує рівень автоматизації управлінських функцій C4ISR (командування, управління, зв'язок, інформатизація, розвідка тощо). З цієї причини на даний час стан інформаційного забезпечення управлінських процесів ЗС України (сил оборони) неможливо назвати задовільним. Тому необхідною умовою втілення надійного і достатнього для реалізації мережецентричних принципів ведення операцій (бойових дій) в перспективній структурі ЗС України є впровадження С-подібної АСУ (з урахуванням досвіду російсько-української війни).

Таким чином, впровадження такого концептуального підходу до реалізації інформаційного забезпечення (за його основними видами) в С-подібній АСУ буде сприяти підвищенню бойових можливостей військ (сил) ЗС України (Сил оборони) в сучасних умовах ведення воєнних дій.

Матеріали статті можуть бути корисними для вищого командного складу ЗС України (Сил оборони), а також науковцям і дослідникам в галузі інформаційного забезпечення та розвитку оборонної сфери держави.

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

Вступ (Introduction)

Аналіз публікацій показує, що на сьогодні активно досліджується проблематика формування майбутнього обрису Збройних Сил України (ЗС України) з урахуванням досвіду провідних країн світу. Зміст концепцій будівництва та розвитку збройних сил країн світу переконливо свідчить, що до пріоритетних напрямів відноситься удосконалення саме системи управління військами (силами) [1 – 3]. Водночас, досвід участі збройних сил провідних країн світу в операціях кінця XX – початку XXI століття визначив основну тенденцією розвитку теорії і практики управління військами – розроблення та впровадження концепції мережецентричних війн (*Net-Centric Warfare - NCW*) [4 – 10]. 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 [11 – 13].

У наведених публікаціях в основному досліджуються принципові завдання побудови автоматизованих систем управління для реалізації концепції мережецентричних війн. Разом з тим, в них недостатньо уваги приділяється саме інформаційному забезпеченню таких систем. Без актуальної інформації будь-яка автоматизована система не спроможна виконати функціональні завдання за призначенням. При цьому інформаційна перевага може бути досягнута своєчасним інформаційним забезпеченням процесу прийняття рішень та дій на всіх рівнях системи управління військами (силами). Тому питання інформаційного забезпечення сучасних систем управління у воєнній сфері набуває найважливішого значення.

Метою статті є обґрунтування концептуальних 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 цій статті позначені лише основні контури розвитку систем управління в умовах принципово нових війн XXI століття.

Виклад основного матеріалу. Війна майбутнього – це не тільки високотехнологічна війна, а, в першу чергу, “мережева” війна. Вона вимагає 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 [7 – 9].

Реформування збройних сил провідних країн світу проводиться, в першу чергу, шляхом впровадження нових підходів до управління і ведення бойових дій. В їх основі лежить мережевий принцип забезпечення військ (сил) точною та своєчасною інформацією, передбачений перспективною “мережецентричною” концепцією [14].

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 [15]. 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 [16] будь-яка функція управління в системах реалізується виключно інформаційним шляхом. Це означає, 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. Його сутність полягає, з однієї сторони, у формування завдань та їх донесення від органу управління до суб’єктів системи, а з іншої – в можливості отримання органом управління зворотної інформації для контролю процесу управління та коригування інформаційного впливу. Зазначене узагальнюється наступними доречними визначеннями, наведеними у Військовому стандарті [15].

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, в 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 і 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.

Сьогодні 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. Крім того, він обумовлює також необхідну структуру і характеристики органів управління, зразків озброєнь, оцінку рівня їх достатності, загалом – з великою ймовірністю визначає результат збройного протистояння.

На підставі наукових досліджень [17, 18] сформовано повний перелік інформаційних функцій, які здійснюють реалізацію складових інформаційного забезпечення системи управління у воєнній сфері. До таких складових принаймні слід включити наступні основні види:

Моніторинг стану – комплекс заходів, що реалізує безперервний процес отримання інформації воєнного характеру на основі даних усіх видів воєнної розвідки, з метою оцінки та прогнозування розвитку оперативно-тактичної обстановки, а також висвітлення загрозливих дій в космічному, повітряному, наземному, надводному, підводному та інформаційному просторах.

Інформаційно-аналітичне забезпечення – комплекс заходів, що реалізує процеси створення інформаційних продуктів на основі використання інформаційних ресурсів, проведення розрахунків, моделювання ситуацій, аналізу даних та інформації з метою підтримки прийняття рішень органами військового управління.

Організаційно-управлінське забезпечення – комплекс організаційно-розпорядчих заходів, які реалізуються органами військового управління, командирами (начальниками) шляхом документообігу з метою підготовки і прийняття обґрунтованих рішень, доведення завдань до підлеглих, організації виконання та контролю.

Захист інформаційних ресурсів – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації (інформаційних ресурсів) та належний порядок доступу до неї (них).

Морально-психологічне забезпечення – сукупність заходів, які здійснюються з метою формування, підтримання та поновлення у особового складу військових формувань морально-бойових і психологічних якостей, морально-психологічного стану військ (сил) на рівні, необхідному для успішного виконання завдань за призначенням.

Іміджеве забезпечення – комплекс заходів, що здійснюється для висвітлення діяльності Сил оборони, з метою формування позитивної громадської думки в суспільстві та на міжнародному рівні, а також сприяння зростанню престижу військової служби у вітчизняному соціумі та за його межами.

Дезінформаційне забезпечення – комплекс заходів щодо введення противника в оману шляхом відволікаючих демонстративних дій, імітації, скритності своїх основних дій та розповсюдження хибної інформації.

Інформаційно-психологічний вплив – цілеспрямоване інформаційне втручання у свідомість (підсвідомість) керівного та особового складу військ противника з метою внесення змін у поведінку та (або) світогляд, які підривають їх морально-психологічний стан.

Інформаційно-технічний вплив – комплекс акцій та атак, якими реалізується цілеспрямоване деструктивне електронне втручання в процес функціонування об’єктів інформаційної інфраструктури противника.

Радіоелектронний захист – комплекс заходів щодо гарантування стійкості роботи радіоелектронних складових інформаційних засобів, інформаційних систем та інших носіїв інформаційних ресурсів в умовах радіопротидії з боку противника та взаємного електромагнітного впливу.

Навігаційне забезпечення – комплекс заходів з метою постійного та об’єктивного отримання в масштабі реального часу військовими об’єктами інформації про власне місцезнаходження для ефективного ведення операцій (бойових дій) і застосування озброєння та військової техніки.

Топогеодезичне (*геоінформаційне*) *забезпечення* – комплекс заходів щодо підготовки та доведення до органів військового управління всіх рівнів топографічних та спеціальних карт (у тому числі електронних), фотодокументів місцевості, а також астрономо-геодезичних

та гравіметричних даних для здійснення просторової синхронізації при управлінні військами (силами) та зброєю в ході виконання ними поставлених задач.

Гідрометеорологічне забезпечення – комплекс заходів щодо збору, аналізу та доведення до військ (сил) інформації про гідрологічну та метеорологічну обстановку.

Зазначені види становлять базовий перелік складових повного процесу інформаційного забезпечення системи управління у воєнній сфері, яка здійснює реалізацію функцій управління за цільовим призначенням.

В 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. Проте вже не тільки за рахунок підвищення розвідувальних, вогневих, маневрених та інших характеристик індивідуальних зразків (платформ), а, в першу чергу, завдяки наявності кращого інформаційного забезпечення та можливості скорочення циклу бойового управління в операції (бою) [19].

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, передачі (прийому), 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 [20].

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

Заходи з питань впровадження мережецентричних концепцій, в основному, здійснюються в трьох ключових напрямах [21]:

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

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

розгортання сучасних систем зв'язку і передачі даних.

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, 22, 23]. Її реалізація дозволить здійснювати ефективне інформаційне забезпечення операцій всього можливого спектру, починаючи від миротворчих операцій зі встановлення миру до великомасштабних бойових дій високої інтенсивності. Разом з тим, 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), в тому числі і засобів ураження, органів і пунктів матеріально-технічного забезпечення.

У США сутність поняття "мережецентрична війна", "ведення бойових дій в єдиному інформаційно-комунікаційному просторі", виходячи з досвіду 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, 22 – 24].

Аналогічні системи мають Велика Британія *(Network Enabled Capability),* Франція *(Guerre Infocentre),* ФРН *(Infanterist der Zukunft)* та спільно з Нідерландами *(“Tactical Edge Networking”)* [23], Австралія *(Network Centric Warfare)* [23], Китай *(Integrated Network-Electronic Warfare - INEW)* [24], а також Ізраїль розглядає впровадження інформаційних технологій як невід’ємний і обов’язковий атрибут сучасних і майбутніх операцій [23].

Очевидно, що головними принципами реалізації заходів щодо широкого впровадження інформаційних складових у воєнну сферу в рамках 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).

Аналітики стверджують [9], що війни наступного покоління – це, перш за все, війни розвідок, де володіння необхідною інформацією про противника є ключем до досягнення успіху в таких війнах. В сучасних умовах в 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 якого лежить процес всебічної розвідки, є домінуючим в загальної системі інформаційного забезпечення військ (сил). При цьому, будь-яку мережецентричну систему неможливо використовувати за призначенням без актуальної інформації у реальному масштабі часу. Залежно від рівня мережецентрична система за наявністю корисної, достовірної, повної, своєчасної розвідувальної інформації спроможна наочно відображати обстановку, оцінювати місцевість, стан противника і своїх військ (сил), моделювати розвиток бойових дій. Поряд з тим, система здатна виробляти рекомендації, варіанти рішень, проєкти бойових документів, доводити завдання до підлеглих пунктів управління і можливість контролю усіх інформаційних процесів.

Достовірність – це властивість інформації відображати реально існуючі об’єкти (процеси, явища) з необхідною точністю в межах певного рівня ймовірності випадку, що відображається.

Достатність (повнота) – мінімальний, але достатній для прийняття рішення склад інформаційного продукту.

Своєчасність інформації означає, що вона є саме тією, яка потрібна на даний момент, суттєвою, важливою на цей час.

Потрібність (корисність) інформації визначається з огляду на ті завдання, які можна вирішити за її допомогою.

Поряд із перевагами мережецентричної концепції ведення бойових дій виявлено і ряд проблем щодо її реалізації. Зокрема, гостро постає питання раціонального розподілу та обробки великих обсягів інформації, що надходять до споживачів. Для кращого розуміння цієї проблеми вважаємо за доцільне зупинитися на розподілі класів мережецентричних систем у залежності від ступенів автоматизації керованих процесів та потоків інформації, яка в них циркулює.

Досвід розроблення, впровадження та експлуатації мережецентричних систем у США свідчить [9, 25], що сучасні автоматизовані системи управління, які за своєю сутністю є інформаційними, поділяються на декілька класів. Відповідно від функцій, що виконуються

системами, розрізняють – командування, управління, зв'язок, комп'ютери (інформатизація), загальну розвідку, спостереження, розвідку в режимі реального часу *(Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance)*.

При цьому, системи різняться за ступенем автоматизації керованих процесів у відповідності з цією класифікацією. 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 буде відповідати класу "СС" (С2). Якщо в системі автоматизовані чотири функції – командування, управління, зв'язок, комунікація *(Command, Control, Communications, Computers)*, то таку систему відносять до класу "СССС" (С4). При цьому, функції, що починаються з букви "С", використовуються як базові, а інші - додаткові.

З точки зору автоматизованих управлінських функцій (завдань) система управління, яка містить у своїй абревіатурі більше букв "С", є більш досконалою. Так, система класу С2SR *(Command, Control, Surveillance, Reconnaissance)* буде поступатися системі класу С4 за спектром завдань, які використовуються в автоматизованому режимі.

Системи, в яких автоматизовані функції *Command and Control* (С2), вирішують наступні завдання:

відображення та передача 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 дозволяє командиру лише швидко довести прийняте рішення до підлеглих і контролювати хід його виконання. При цьому функції оцінки обстановки і прийняття рішення повною мірою покладається саме на людину. Деякі системи, що відносяться до класу С2, можуть виконувати взаємне розпізнавання об'єктів, що знаходяться в системі, за принципом "свій-чужий". Крім цього, вони можуть також виконувати ідентифікацію цілей та надавати в автоматичному режимі цілевказівки засобам вогневого ураження, що входять до системи. Системи управління, в яких автоматизовані такі функції, мають додаткові літери "SR" *(Surveillance, Reconnaissance)* і позначаються як С2SR (або С2+). При цьому комп'ютери, які використовуються в системах класу С2, розглядаються тільки в якості засобів первинної обробки та відображення інформації. Хоча системи С2 і містять 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 мова не йде.

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). Наявні на озброєнні іноземних держав системи тактичної ланки відносяться до класу С2 або С2+ і розрізняються між собою лише невеликим розширенням спектра розв'язуваних завдань. При цьому, всі системи тактичного призначення принципово не досягають навіть класу С3.

Наявність в абревіатурі класу системи четвертої літери "С" *(Computers)*, а також літери "І" *(Intelligence)* означає, по-перше, повну автоматичну обробку даних, отриманих у ході

реалізації перших двох “С” - *Command and Control*, по-друге, вироблення на підставі обробки первинних даних варіанту 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), повинні 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, у тому числі, з використанням засобів тривимірного відображення поля бою;

інформаційна підтримка розроблення плануючих документів (програма “Sketch in the plan” (начерк до плана), що здійснює перетворення графічних і аудіо- матеріалів в плануючі документи;

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

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

У збройних силах навіть розвинених в технологічному відношенні країн системи класу С4І і С4SR за рівнем управління відносяться до систем оперативної або оперативно-стратегічної ланки. На думку військових експертів [23], 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 (у порівнянні з оперативною ланкою управління);

необхідність обробки великої кількості даних в одиницю часу, які за своїми обсягами на даний час 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 отримало у США.

Найбільш відомою з усіх існуючих систем тактичної ланки є американська система класу “С2SR” 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 [25].

Військово-політичне керівництво України протягом останніх 30 років, розуміючи необхідність розвитку систем управління військового призначення, приділяло увагу процесу створення автоматизованих систем військового управління різного рівня. Так, для вирішення задач управління ЗС України в цілому була розроблена концепція функціонування та розвитку таких систем, починаючи від Єдиної автоматизованої системи управління Збройними Силами України (ЄАСУ ЗС України), яка повинна була спрягатися з іншими державними АСУ. В межах створення ЄАСУ ЗС України передбачалася розробка видових та інших АСУ різного рівня органів військового управління (тактичного, оперативного,

оперативно-стратегічного): АСУ ПД “Дніпро”, “Карпати”, “Ореанда”, “Ніка”, “Борсук”, “Простір” та ін. При цьому, особливий акцент при створенні ЄАСУ ЗС України робився на впровадженні сучасних інформаційних технологій в управління військами, бойовими засобами та зброєю.

За цей час за тематикою ЄАСУ ЗС України було виконано понад 100 науково-дослідних робіт (НДР) і понад 40 дослідно-конструкторських робіт (ДКР). Досвід проведення таких робіт засвідчив їхню низьку ефективність. Так, лише близько 20% робіт дійшли до стадії виготовлення дослідних зразків, дослідної експлуатації та держвипробувань. А близько 80% з них не знайшли свого впровадження, тому були призупинені на різних етапах виконання роботи: ескізного та технічного проектування (40%), розробки конструкторської документації (40%) [26]. За словами експертів, на недосконаліть дослідних робіт вплинуло багато проблем загального характеру. Одна з головних – відсутність у більшості організацій-розробників України належного досвіду з розробки складних, багаторозгалужених автоматизованих систем військового призначення.

Тим не менш, на сьогодні головна ідея створення ЄАСУ ЗС України – автоматизація необхідних видів діяльності органів військового управління, – в цілому вже реалізована. За цей час розроблені окремі складові АСУ різного рівня (інформаційно-аналітичні системи підтримки управління організаційно-штатною структурою й особовим складом; моніторингу і планування оборонних ресурсів; моделювання перспективних військових формувань та організаційних заходів щодо реалізації директив; створення і розвитку озброєння та військової техніки), і вони реально функціонують у захищеному режимі на об’єктах ЗС України.

Однак слід зауважити, що на даному етапі розвитку ЗС України стан автоматизації управлінських процесів неможливо назвати задовільним. Відповідно до [14] 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%. При цьому рівень інформатизації систем управління суб’єктів оборони держави порівняно зі збройними силами провідних країн світу становить 2-2,5 %. Водночас, наявність на пункті управління великих екранів зі значками різних кольорів на електронній топографічній карті не є ознакою високого рівня автоматизації системи управління військами. До того ж, до початку збройної агресії, незважаючи на ряд спроб, в ЗС України у повному обсязі не була завершена побудова автоматизованої системи бойового управління військами (силами, зброєю) [27]. Виявилося, що таке завдання постало надто складним.

В той же час, у цьому контексті вищим військовим керівництвом України було визначено бачення щодо розвитку системи управління військами (силами) [28]: “… Необхідно побудувати у Збройних Силах України надійну систему зв’язку, автоматизації, розвідки та спостереження (C4ISR), 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 та оборони держави, яка буде забезпечувати набуття інформаційних спроможностей для отримання, опрацювання, зберігання, передачі, контролю та надання інформації на вимогу командувачів (командирів) та штабів (тактичного, оперативного, стратегічного рівнів) об’єднаних сил”.

керівництвом України питанню розвитку АСУ військами (силами, зброєю) приділялася особлива увага. Результатом цього вже після повномасштабного вторгнення збройних сил РФ в Україну є прийняття на озброєння ЗС України у 2022 році АСУ “Дзвін-АС” – високоінтегрованої автоматизованої системи бойового управління військами (силами)

стратегічного, оперативного та частково тактичного рівня. Вважається, що вона дає змогу [29]:

у напівавтоматичному та автоматичному режимах генерувати документи бойового управління;

одержувати наявні розвіддані про війська противника, їх поточне та перспективне забезпечення;

створювати та відстежувати картографічну інформацію;

одержувати вичерпні дані про власні війська;

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

Крім цього, з початком ведення бойових дій у 2014 році на Сході України у стислі строки успішно запрацювала система бойового управління тактичної ланки "Кропива". Це випробувана в боях система, яка призначена для автоматизації окремих завдань управління на рівні батальйон - рота - взвод - окрема одиниця техніки (гармата). Наразі АСУ "Кропива" може використовуватись різними підрозділами сухопутних військ: артилерійськими, піхотними, танковими підрозділами, загальновійськовою розвідкою, підрозділами ППО СВ, саперними підрозділами тощо. Одночасно, для органів військового управління ЗС України впроваджено захищену інформаційну систему ситуаційної обізнаності Delta. Вона дозволяє в реальному масштабі часу здійснювати збір, обробку та відображення обстановки, що склалася, а також забезпечує підтримку прийняття рішень командиром (командувачем).

На нашу думку, робити спробу 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). Він 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.

При цьому, за висновками американських аналітиків, жоден із європейських союзників у найближчому майбутньому, швидше за все, не зможе створити повністю мережеву армію. Найбільшою проблемою для європейських інвестицій у C4ISR є загальні обмеження оборонних бюджетів, а не відсутність адекватної технології [23].

У цьому питанні доцільно запозичити також і досвід Китаю. Його 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. Під нею розуміється вогнева і електронна поразка елементів інформаційних структур (командних пунктів, вузлів зв'язку, орбітального угруповання супутників розвідки і управління і т.п.) [24].

Зважаючи на зазначене, в Україні розроблення С-подібної системи доцільно починати з рівня С2+, з подальшим її еволюційним нарощуванням до С3 і вище, виходячи з результатів випробувань, досвіду експлуатації та ресурсних можливостей. При цьому 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 надійного оперативного управління повинен 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;

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

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

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 (в подальшому – С4 з додатками), яка повинна бути здатною вирішувати такі завдання:

for operational and strategic levels - using a system of the C3 type (in the future - C4 with applications), which must be able to solve the following tasks:

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).

Результати (Results)

Таким чином, досвід провідних країн світу переконливо свідчить, що при впровадження мережецентричної концепції для систем управління ЗС України головна увага повинна бути зосереджена на питаннях збору, обробки, аналізу, ототожнення та безпеки інформації для підтримки прийняття рішень керівниками усіх рівнів. При цьому, надання своєчасної актуальної достовірної (релевантної) інформації для систем управління військового призначення постає головним завданням в загальному процесі інформаційного забезпечення ЗС України.

Проведений аналіз показує, що діяльність щодо побудови та використання інформаційних систем для управління збройними силами провідних країн світу, насамперед, досвід держав-членів НАТО, викликає нагальну потребу 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.

Висновок (Conclusion)

1. 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. Вони 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”).

2. Інформаційне забезпечення мережевих структур стає головною і необхідною умовою ефективного функціонування систем управління. З метою 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.

3. Належне та своєчасне інформаційне забезпечення систем управління військового призначення є необхідною умовою втілення мережецентричних принципів ведення бойових дій. Воно може бути реалізоване в ЗС України впровадженням С-подібної системи автоматизованого управління шляхом її еволюційного розвитку, починаючи з побудови системи класу С2+. У цьому випадку, 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:

взяти 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 аналогічну перспективну автоматизовану систему управління іноземного виробництва;

на першому етапі, як невідкладний захід, розглянути питання щодо отримання (закупівлі) бригадного комплекту автоматизованої системи управління тактичної ланки для проведення випробувань в умовах ведення реальних бойових дій 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.

Рекомендації (Recommendations)

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

Матеріали статті можуть бути корисними для вищого командного складу ЗС України (Сил оборони), а також науковцям і дослідникам в галузі інформаційного забезпечення та розвитку оборонної сфери держави.

Використані джерела

1. Ільяшов О.А. Тенденції розвитку збройної боротьби у війнах четвертого – шостого поколінь / О.А. Ільяшов // Наука і оборона. – 2009. – № 3. – С.43–48.
2. Пащетник О.Д. Аналіз світових тенденцій розвитку автоматизованих систем управління військами і зброєю. / О.Д. Пащетник // Наука і техніка Повітряних Сил Збройних Сил України. – 2015. – № 2 (19). – С.64–68.
3. Особливості та принципи побудови мережецентричної системи управління угруповання військ(сил) / О.М. Загорка, В.В. Коваль, В.В. Тюрін, В.Г. Малюга, І.О. Загорка // Збірник наукових праць Харківського університету Повітряних Сил. – 2016. – Вип. 3 (48). – С.7–11.

4. Савин Л.В. Сетецентричная и сетевая война. Введение в концепцию / Л.В. Савин. – М.: Евразийское движение, 2011. – 130 с. – [Електронний ресурс]. – Режим доступу: https://www.geopolitica.ru/sites/default/files/ncw.pdf.
5. Кондратьев А. Реализация концепции “Сетецентрическая война” в ВВС США / А.Кондратьев // Зарубежное военное обозрение. – 2009. – №5. – С.44–49. – [Електронний ресурс]. – Режим доступу: http://pentagonus.ru/publ/24-1-0-1159.
6. Баулин В., Кондратьев А. Реализация концепции “Сетецентрическая война” в ВМС США / В. Баулин, А. Кондратьев // Зарубежное военное обозрение. – 2009. – № 6. – С.61-67. – [Електронний ресурс]. – Режим доступу: http://pentagonus.ru/publ/26-1-0-811.
7. Макаренко С.И., Иванов М.С. Сетецентрическая война – принципы, технологии, примеры и перспективы / С.И. Макаренко, М.С. Иванов. – Санкт-Петербург: Наукоемкие технологии, 2018. – 898 с.
8. Опрощенко Ю.О. Мережецентрична війна: основні риси, особливості та принципи ведення / Ю.О. Опрощенко // Соціально-політичні студії. Науковий альманах. Праці молодих науковців. – 2018. - № 2. –С.7-11.
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. – К.: НУОУ ім. Івана Черняховського, 2020 – 248 с.
10. Нор П.І., Борохвостов І.В., Соломицький О.І. Основні тенденції розвитку форм і способів ведення збройної боротьби / П.І. Нор, І.В. Борохвостов, О.І. Соломицький // Наука і оборона. – 2023. – № 1. – С. 20-27.
11. Воєнна доктрина США “Joint Vision 2020”. – [Електронний ресурс]. – Режим доступу: http://pentagonus.ru/doc/JV2020.pdf.
12. Гаврилов А. Автоматизированная система сбора, обработки и распределения разведывательной информации СВ США DCGS-A / А. Гаврилов // Зарубежное военное обозрение. – 2010. – № 7. – С.32–40. – [Електронний ресурс]. – Режим доступу: http://pentagonus.ru/publ/122-1-0-1596.
13. Балахонцев Я., Кондратьев А. Влияние концепции “сетецентрическая война” на эффективность разведывательного обеспечения Вооружённых сил США / Я. Балахонцев, А. Кондратьев // Зарубежное военное обозрение. – 2011. – № 2. – С.14–20.
14. Гаценко С.С. Аналіз вимог до систем управління військами та шляхи їх удосконалення / С.С. Гаценко // Збірник наукових праць ЦВСД НУОУ. – 2015. – № 2. – С.85–90.
15. 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].
16. Винер Н. Кибернетика или управление и связь в животном и машине / Н.Винер. – М.: Сов. Радио, 1968. – 328 с.
17. Саричев Ю.О. Аналіз підходів щодо визначення сучасної ролі та місця інформаційного забезпечення в системі державного управління / Ю.О.Саричев // Вісник НАДУ при Президентові України [за заг. ред. Ю.В.Ковбасюка]. – 2016. – Вип. 3 (82). – С.138–143.
18. Саричев Ю.О. Теоретичний підхід до інформаційного забезпечення в системі державного управління у воєнній сфері / Ю.О.Саричев // Вісник НАДУ при Президентові України (Серія “Державне управління”) [за заг. ред. Ю.В. Ковбасюка]. – 2016. – Вип. 4 (83). – С.153–160.
19. Кондратьев А.Е. Общая характеристика сетевых архитектур, применяемых при реализации перспективных сетецентрических концепций ведущих зарубежных стран / А.Е.Кондратьев // Военная мысль. – 2008. – № 12. – С.63–73.
20. Фролов В.С. Структурно-логічна схема Єдиної автоматизованої системи управління Збройних Сил України / В.С. Фролов // Наука і оборона. – 2012. – № 1. – С.15.

21. Досвід збройних сил провідних країни світу в інтересах удосконалення інформаційного забезпечення ЗС України / П.М. Сніцаренко, Ю.О. Саричев, В.А. Ткаченко, В.П. Зубков // Збірник наукових праць ЦВСД НУОУ ім. І. Черняховського. – 2021. – № 2 (72). – С.40-50.
22. Молитвин А. О реализации концепции единого информационного пространства НАТО / А. Молитвин // Зарубежное военное обозрение. – 2008. – № 1. – С.23–27. – [Електронний ресурс]. – Режим доступу: http://pentagonus.ru/publ/3-1-0-565.
23. Adams G., Ben-Ari G., Logsdon J., Williamson R. (2004). European C4ISR Capabilities and Transatlantic Interoperability. The George Washington University.
24. Thomas T.L. (2005). Chinese and American network warfare // Joint Force Quarterly, July, 2005.
25. Американська АСУ військами FBCB2. – [Електронний ресурс]. – Режим доступу: http://dragon-first-ru.livejournal.com/33339.html; http://defense-update.com.
26. Пастухов А. АСУ ЗС України. Технології. – [Електронний ресурс]. – Режим доступу: https://mil.in.ua/uk/d0-b0-d1-81-d1-83-d0-b7-d0-b1-d1-80-d0-be-d0-b9-d0-bd-d0-b8-d1-85-d1-81-d0-b8-d0-bb/#google_vignette.
27. Галаган В.І., Полішко С.В., Бондарчук С.В. Пропозиції щодо удосконалення процесу впровадження інформаційних систем іноземного виробництва в діяльність Збройних Сил України / В.І. Галаган, С.В. Полішко, С.В. Бондарчук // Збірник наукових праць ЦВСД НУОУ ім. І. Черняховського. – 2019. – № 2. – С.62–68.
28. Візія Генерального штабу ЗС України щодо розвитку Збройних Сил України на найближчі 10 років. – [Електронний ресурс]. – Режим доступу: https://www.mil.gov.ua/news/ 2020/01/11/viziya-generalnogo-shtabu-zs-ukraini-shhodo-rozvitku-zbrojnih-sil-ukraini-na-najblizhchi - 10-rokiv.
29. Система управління “Дзвін-АС” стала на озброєння України. – [Електронний ресурс]. – Режим доступу: https://mil.in.ua/uk/news/systema-upravlinnya-dzvin-as-stala-na-ozbroyennya-ukrayiny.

References

1. Ilyashov O.A. Trends in the development of armed struggle in the wars of the fourth - sixth generations / O.A. Ilyashov // Science and defense. – 2009. – No. 3. – P.43–48.
2. Pashchetnyk O.D. Analysis of global trends in the development of automated systems for the management of troops and weapons. / O.D. Pachetnyk // Science and technology of the Air Force of the Armed Forces of Ukraine. – 2015. – No. 2 (19). – P.64–68.
3. Peculiarities and principles of building a network-centric management system of a group of troops (forces) / O.M. Zagorka, V.V. Koval, V.V. Tyurin, V.G. Malyuga, I.O. Zagorka // Collection of Scientific Papers of Kharkiv Air Force University. – 2016. – Issue 3(48).– P.7–11.
4. Savin L.V. Network-centric and network warfare. Introduction to the concept / L.V. Savin. – M.: Eurasian Movement, 2011. – 130 p. – [Electronic resource]. – Access mode: https://www.geopolitica.ru/sites/default/files/ncw.pdf.
5. Kondratiev A. Implementation of the concept of “Network-centric warfare” in the US Air Force / A. Kondratiev // Foreign Military Review. – 2009. – No. 5. – P.44–49. – [Electronic resource]. – Access mode: http://pentagonus.ru/publ/24-1-0-1159.
6. Baulin V., Kondratiev A. Implementation of the concept of “Network-centric warfare” in the US Navy / V. Baulin, A. Kondratiev // Foreign Military Review. – 2009. – No. 6. – P.61-67. – [Electronic resource]. – Access mode: http://pentagonus.ru/publ/26-1-0-811.
7. Makarenko S.I., Ivanov M.S. Network-centric warfare - principles, technologies, examples and prospects / S.I. Makarenko, M.S. Ivanov. – St. Petersburg: High technology, 2018. – 898 p.
8. Oproschenko Yu.O. Network-centric war: main features, peculiarities and principles of conduct / Yu.O. Oproschenko // Social and political studies. Scientific almanac. Works of young scientists. – 2018. - No. 2. – P.7-11.

9. Theoretical foundations of managing a group of troops (forces) in modern conditions of armed struggle: monograph / [O.M. Zagorka, A.K. Pavlikovsky, A.A. Koretskyi, S.O. Kyrychenko, I.O. Zagorka]; in general ed. I.S. Russian - K.: NUOU named after Ivan Chernyakhovsky, 2020 - 248 p.
10. Nor P.I., Borokhvostov I.V., Solomytskyi O.I. The main trends in the development of forms and methods of armed struggle / P.I. Nor, I.V. Borokhvostov, O.I. Solomytsky // Science and defense. – 2023. – No. 1. – P. 20-27.
11. US military doctrine "Joint Vision 2020". - [Electronic resource]. – Access mode: http://pentagonus.ru/doc/JV2020.pdf.
12. Gavrilov A. Automated system for collecting, processing and distributing intelligence information of the US Army DCGS-A / A. Gavrilov // Foreign Military Review. – 2010. – No. 7. – P.32–40. – [Electronic resource]. – Access mode: http://pentagonus.ru/publ/122-1-0-1596.
13. Balakhontsev Y., Kondratyev A. The influence of the “network-centric war” concept on the effectiveness of intelligence support for the US Armed Forces / Y. Balakhontsev, A. Kondratyev // Foreign Military Review. – 2011. – No. 2. – P.14–20.
14. Gatsenko S.S. Analysis could be used for military management systems and their improvements / S.S. Gatsenko // Collection of scientific works of the CVSD NUOU. – 2015. – No. 2. – P.85–90.
15. Military standard VST 01.004.004 – 2014 (01) “Information security of the state in the military sphere. Terms and meaning” [confirmed by the order of the head of the Central Department of Metrology and Standardization of the Armed Forces of Ukraine of the Armed Forces of Ukraine - the chief metrologist of the Armed Forces of Ukraine dated 02/27/2014. No. 1].
16. Wiener N. Cybernetics or control and communication in animals and machines / N. Wiener. – M.: Sov. Radio, 1968. – 328 p.
17. Sarychev Yu.O. Analysis of approaches to determining the modern role and place of information support in the state administration system / Yu.O. Sarychev // Bulletin of the NADU under the President of Ukraine [in general ed. Yu.V. Kovbasyuk]. – 2016. – Issue 3 (82). – P.138–143.
18. Sarychev Yu.O. Theoretical approach to information support in the system of state administration in the military sphere / Yu.O. Sarychev // Bulletin of the NADU under the President of Ukraine (Series "State Administration") [in general ed. Yu.V. Sausage]. – 2016. – Issue 4 (83). – P.153–160.
19. Kondratyev A.E. General characteristics of network architectures used in the implementation of promising network-centric concepts of leading foreign countries / A.E. Kondratyev // Military Thought. – 2008. – No. 12. – P.63–73.
20. Frolov V.S. Structural and logical scheme of the Unified automated control system of the Armed Forces of Ukraine / V.S. Frolov // Science and defense. – 2012. – No. 1. – P.15.
21. The experience of the armed forces of the leading countries of the world in the interests of improving the information support of the Armed Forces of Ukraine / P.M. Snitsarenko, Yu.O. Sarychev, V.A. Tkachenko, V.P. Zubkov // Collection of Scientific Papers of the TsVSD NUOU named after I. Chernyakhovskyi. – 2021. – No. 2 (72). - P.40-50.
22. Molitvin A. On the implementation of the concept of a single NATO information space / A. Molitvin // Foreign Military Review. – 2008. – No. 1. – P.23–27. – [Electronic resource]. – Access mode: http://pentagonus.ru/publ/3-1-0-565.
23. Adams G., Ben-Ari G., Logsdon J., Williamson R. (2004). European C4ISR Capabilities and Transatlantic Interoperability. The George Washington University.
24. Thomas T.L. (2005). Chinese and American network warfare // Joint Force Quarterly, July, 2005.
25. American ACS troops FBCB2. - [Electronic resource]. – Access mode: http://dragon-first-ru.livejournal.com/33339.html; http://defense-update.com.

26. Pastukhov A. ACS of the Armed Forces of Ukraine. Technologies. - [Electronic resource]. – Access mode: https://mil.in.ua/uk/d0-b0-d1-81-d1-83-d0-b7-d0-b1-d1-80-d0-be-d0-b9-d0-bd-d0-b8-d1-85-d1-81-d0-b8-d0-bb/#google_vignette.
27. Galagan V.I., Polishko S.V., Bondarchuk S.V. Proposals for improving the process of introducing information systems of foreign production into the activities of the Armed Forces of Ukraine / V.I. Galagan, S.V. Polishko, S.V. Bondarchuk // Collection of Scientific Papers of the TsVSD NUOU named after I. Chernyakhovskyi. – 2019. – No. 2. – P.62–68.
28. The Vision of the General Staff of the Armed Forces of Ukraine regarding the development of the Armed Forces of Ukraine for the next 10 years. - [Electronic resource]. – Access mode: https://www.mil.gov.ua/news/ 2020/01/11/viziya-generalnogo-shtabu-zs-ukraini-shhodo-rozvitku-zbrojnih-sil-ukraini-na-najblizhchi – 10 - rokiv.
29. The "Dzvin-AS" management system has been adopted by Ukraine. - [Electronic resource]. – Access mode: https://mil.in.ua/uk/news/systema-upravlinnya-dzvin-as-stala-na-ozbroyennya-ukrayiny.

Abstract. The relevance of this article is due to the fact that modern armed conflicts lead to a change in the nature of military operations, which increasingly acquire an informational and technological nature, which forces the leadership of the leading countries of the world to review the theory and practice of the military construction in order to implement the concept of "network-centric war". This approach involves considering the control bodies, units, planes, ships, communications, and intelligence of the armed forces as objects connected to a single information and communication network. The capabilities of such a network-centric system of conducting military operations are determined by the capabilities of the entire group of objects connected to the network (synergistic effect). In the implementation of this concept, a key role belongs to the information support of objects of a single network, which has a number of components that need to be implemented in a network-centric system of conducting military operations. The requirement for high operational efficiency of information support necessitates the widespread introduction of automated control systems (ACS) in such a system. At the same time, the information support of the objects of the unified network is the main purpose of the ACS, the means of which in automatic mode allow you to quickly display the situation, assess the terrain, the state of the enemy, your troops (forces), model the development of combat operations, develop options for solutions, draft combat documents, prove tasks to subordinates, control their execution.

The article analyzes the experience of implementing information systems for managing the armed forces of leading countries, the peculiarities of their organization and implementation in the armies of NATO member states. Based on the results of this analysis, approaches to determining ways to improve the information support of the control systems of the Armed Forces of Ukraine are proposed. One of the main tasks of the Armed Forces of Ukraine (Defence Forces) on the way to NATO membership is the creation of a network-centric military control system, which should be equipped with ACS and compatible with the Alliance's military control systems. Meanwhile, according to foreign publications, the level of automation of the control systems of the defense forces of Ukraine today is 2-2.5% compared to the armed forces of the leading countries in the world, in which ACS ensure the level of automation of C4ISR management functions (command, control, communication, informatization, intelligence, etc.). For this reason, at present, the state of information support for the management processes of the Armed Forces of Ukraine (Defense Forces) cannot be called satisfactory. Therefore, the implementation of C-shaped ACS (taking into account the experience of the Russian-Ukrainian war) is a necessary condition for the implementation of reliable and sufficient for the implementation of network-centric principles of conducting operations (combat operations) in the prospective structure of the Armed Forces of Ukraine.

Thus, the realization of such a conceptual approach to the implementation of information support (by its main types) in the C-shaped ACS will contribute to increasing the combat capabilities of the troops (forces) of the Armed Forces of Ukraine (Defense Forces) in the modern conditions of conducting military operations.

The materials of the article can be useful for the higher command staff of the Armed Forces of Ukraine (Defence Forces), as well as scientists and researchers in the field of information support and development of the defense sphere of the state.

Keywords: Information Systems; Control Systems; ACS, Network-Centric Warfare.