

УДК 355.4:351.743:623.618

О. А. Олещенко, В. Ю. Поляков

ОСНОВНІ АСПЕКТИ СТВОРЕННЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Визначено основні підходи та проблемні питання щодо створення інформаційно-телекомунікаційної системи Національної гвардії України з урахуванням досвіду розвинутих країн світу.

Ключові слова: автоматизація, система управління, автоматизована система управління військами, інформаційно-телекомунікаційна система, інформаційно-телекомунікаційна мережа, інформаційні переваги, інформаційна війна, мережецентрична війна, Збройні Сили, Національна гвардія.

Постановка проблеми. Нові виклики і загрози безпеці України зумовлюють необхідність адаптації форм і способів застосування Збройних Сил України, Національної гвардії України та інших військових формувань до сучасних умов. Сьогодні ми вступили у нову еру стратегії непрямих дій.

У зв'язку з цим можна зрозуміти прагнення багатьох закордонних військових спеціалістів прогнозувати зміст майбутніх воєнних дій на основі аналізу концепції, так званої, “мережецентричної війни” (мережевої війни, мережецентричних дій). Головний зміст концепції “мережецентричної війни” полягає у зміні способу управління військами (силами) при інтенсивному застосуванні можливостей систем розвідки, управління і забезпечення. Саме це потребує розвитку системи управління збройних сил та інших військових формувань за рахунок упровадження нових інформаційно-комунікаційних технологій.

Принцип зосередження сил і засобів на вирішальному напрямку, який існує з давніх часів, сьогодні поширюється на засоби дальнього вогневого, радіоелектронного та інформаційного ураження [11]. Війни і збройні конфлікти ХХІ ст. показали реальну можливість технічної реалізації цих підходів порівняно з усталеними воєнними стратегіями [14]. Особливо зростає інформаційне протистояння з метою придушення здатності ймовірних противників до розвитку власних оригінальних інформаційних технологій у сфері управління, а також маніпулювання відкритою інформацією для примушення до роззброєння, зниження бойової готовності, створення невідгдних юридичних аспектів міжнародного права щодо утворення коаліцій тощо [3].

Сучасні досягнення у галузі новітніх

інформаційних технологій і бурхливий розвиток автоматизованих систем управління зумовлюють необхідність удосконалювання моделей і методів управління військами в усіх ланках і сферах діяльності військ (сил). Стан і розвиток управління військами справедливо розцінюються як найважливіші показники бойової потужності і бойової готовності Збройних Сил України та інших військових формувань, рівня їхньої організаційної і технічної досконалості [11]. Тому автоматизація процесів управління у розвинених державах світу належить до рангу національних стратегій, а інформаційні війни набули стратегічного значення.

Проте стан наявних систем автоматизації управління у військових формуваннях України, на жаль, не відповідає сучасним вимогам. Причини – застаріла елементна база засобів автоматизації (розроблення 60–80 рр.), їх значна енергоємність, низька швидкість оброблення інформації, відомі недоліки бойових алгоритмів та моделей, що використовуються у системах управління. До того ж виробнича база більшості комплексів автоматизації знаходиться у Російській Федерації, а їхній ремонт потребує значних фінансових витрат. Тому фактично немає цілісної автоматизованої системи управління військами (АСУВ), яка відповідала б сучасним вимогам за структурою, складом і змістом вирішуваних завдань [5]. Крім зазначеного є низка проблем загального характеру: недостатнє розроблення методології автоматизації управління військами (силами); застарілість державних і галузевих стандартів; відсутність методик розрахунку витрат на створення АСУВ; відсутність вихідних даних для створення АСУВ; недостатність наукових, матеріальних і фінансових ресурсів тощо. Це

© О. А. Олещенко, В. Ю. Поляков

стосується й Національної гвардії України.

Таким чином, автоматизація системи управління Національної гвардії України та приведення її до рівня сучасних вимог є актуальною проблемою, що потребує, перш за все, визначення концепції та програми розвитку систем автоматизованого управління діяльністю сил гвардії.

Виклад основного матеріалу. Побудовою інформаційних моделей та вдосконалюванням сучасної системи управління збройних сил займаються такі науковці, як: П. Стужук, П. Грицай, Ю. Вознюк [8], В. Косс [3], Р. Гумінський, Є. Рижов, О. Корольова, В. Фролов [10], Б. Нізієнко [5], В. Камінський, О. Сісков, О. Александров та ін. Проблематиці реформування системи управління Збройних Сил України та її автоматизації присвячено праці Л. Бондаренка, П. Кисиленка, С. Срібного, О. Василенка, В. Толубка [9], Ю. Плугового, С. Дружиніна, О. Климовича, О. Саєнко [1] та деяких інших науковців. Їх огляд дозволяє сформулювати таку позицію.

Аналіз збройних конфліктів останніх десятиліть, а також поглядів військових фахівців на еволюцію збройної боротьби свідчить, що однією з основних тенденцій розвитку форм і способів застосування військ (сил) є перехід від концепції “платформно-центричної війни”, у рамках якої увагу було акцентовано на кількості озброєння та військової техніки, до концепції “мережецентричної війни”, яка являє собою сталу систему поглядів на військово-технічне забезпечення та ведення бойових дій в умовах тотальної комп’ютеризації сил і засобів збройної боротьби. Головний зміст концепції “мережецентричної війни” полягає не у нових формах і видах ведення воєнних дій, а у зміні способу управління військами (силами). Мережецентрична концепція управління розглядається у працях таких фахівців, як В. Чельцов, С. Волков, А. Раскін, В. Пеляк, В. Антонов, О. Пермяков, В. Ляпін, В. Зимін, В. Барвиненко [4].

Аналіз результатів згаданих праць свідчить, що автоматизація є пріоритетним напрямом подальшого вдосконалювання системи державного, у тому числі військового управління. Проте зазначені наукові праці здебільшого присвячені або суто теоретичним і методологічним проблемам, що стосуються розвитку інформаційного суспільства, або загальним питанням державно-управлінських відносин, нормативно-правовому регулюванню телекомунікацій з боку держави. У той же час

залишається недостатньо розробленою проблематика впровадження автоматизації в управлінську діяльність з урахуванням необхідності переходу до сучасних принципів управління військами [11].

Система управління військами порівняно з іншими має низку особливостей: значна різноманітність різнорідних багатофункціональних об’єктів управління; інтенсивні потоки неоднорідної за призначенням, складом та змістом, методами кодування інформації; висока динамічність і темпи зміни обстановки; функціонування об’єктів управління у значному просторовому діапазоні у реальному масштабі часу; прийняття рішень за обмежені терміни в умовах недостатності та невизначеності інформації про обстановку, що вимагає використання інтелектуальних методів та алгоритмів управління.

Аналіз цих особливостей управління діяльністю військ визначає специфічні вимоги до автоматизованої системи управління: безперервність управління; функціонування в реальному масштабі часу; випереджаюча готовність системи управління порівняно з військами (силами); адаптованість системи (можливість її реконфігурації та нарощування) залежно від завдань, що вирішуються у мирний час та в особливий період [5]. Основним завданням АСУВ є підвищення надійності, оперативності збирання, оброблення, видачі та відображення даних обстановки на робочих місцях посадових осіб, проведення за короткі терміни оперативних розрахунків і прогнозування розвитку обстановки та результатів дій; досягнення оптимальності прийнятих рішень і планованих заходів, своєчасне та якісне доведення до військ (сил) наказів, команд бойового управління та бойових завдань і забезпечення контролю за їх виконанням; скорочення термінів оформлення, розмноження і передачі бойових і службових документів. АСУВ будуються відповідно до загальної ієрархічної структури військових формувань.

У провідних у військовому відношенні країнах світу постійно проводять роботи зі створення нових і подальшого вдосконалювання існуючих АСУВ різного призначення. Найбільш значущими серед них є ті, що проводяться за стратегічною концепцією США “Поєднання та функціональна інтеграція систем управління, зв’язку, обчислювальної техніки та розвідки”, – С4І (Command, Control, Communications, Computers and Intelligence). В основу

інформаційної інфраструктури С4І покладено сукупність інформаційних систем оперативного-стратегічного, оперативного-тактичного і тактичного рівнів управління, взаємопов'язаних як по вертикалі, так і по горизонталі.

Головними принципами створення і вдосконалення цієї інфраструктури є: висока надійність централізованого управління; можливість децентралізованого управління в окремому регіоні; високий ступінь готовності системи, що забезпечує безперервність управління; широкі можливості з оперативного збирання, оброблення і доведення необхідної інформації до органів управління; забезпечення стійкості і живучості системи управління; висока прихованість управління як під час повсякденної діяльності, так і під час ведення операцій.

З технічного боку С4І – це глобальна територіально розподілена інтегрована телекомунікаційна система інформаційно-обчислювальних центрів та автоматизованих робочих місць, розгорнутих на командних пунктах штабів і пунктах управління збройних сил, що функціонує за принципом єдиного інформаційного простору (ЄІП). У тому ж напрямку рухається Російська Федерація, яка у своїй Концепції розвитку системи управління збройних сил Російської Федерації до 2025 р. визначає однією з головних цілей гарантоване управління військами в ЄІП.

Аналіз подій, що розгортаються в інформаційному просторі, характерному для армій розвинутих країн світу, дозволяє відзначити такі тенденції: глобалізація об'єктів інформаційного впливу, розвиток відповідно до цього форм і способів ведення інформаційного протиборства; наявність майбутніх конфліктів в інформаційному просторі; боротьба з кібертероризмом; упровадження віртуальних спільнот для забезпечення маніпулювання свідомістю як світової громади, так і населення окремої країни; виділення інформаційного забезпечення у самостійний вид; формування відповідних військових структур для здійснення інформаційного протиборства та управління ними [6].

Як відомо, існуючі концепції інформаційної переваги спираються на три складники: оперативне отримання інформації, адекватне розуміння ситуації у бойовому просторі, ефективне використання кожного бойового ресурсу. Отже, для досягнення саме інформаційної переваги необхідно створити комплекс інформаційних мереж, які стануть

технічною основою системи управління і дозволять організувати горизонтальні і вертикальні зв'язки обміну інформацією між будь-якими об'єктами у зоні бойового простору в реальному часі.

Реалізація АСУВ за принципом ЄІП передбачає: володіння взаємодіючими органами управління незалежною інформацією про об'єкти взаємодії в реальному масштабі часу; незалежність загальної інформаційної основи управління від ієрархії органів управління; об'єднання етапів загального і безпосереднього планування та здійснення його в єдиному органі; формування єдиного віртуального бойового простору; розвиток глобальної телекомунікаційної інфраструктури; розвиток космічних засобів розвідки та таких, що сприяють досягненню інформаційної переваги [2].

Створення ЄІП об'єднає сучасні системи управління, зв'язку, розвідки та озброєння в єдину систему, даючи можливість доступу до них усім посадовим особам, що, своєю чергою, стає технічною основою нової мережецентричної концепції ведення бойових дій [7].

Основною ідеєю мережецентричних війн (МЦВ) є інтеграція всіх сил і засобів у ЄІП, що дозволяє багаторазово збільшити ефективність їх бойового застосування. По суті, концепція МЦВ є концепцією управління військами, яка дає змогу організувати війська за принципом “з низу до верху” чи самосинхронізації, або відчуження наміру командира. Вона може застосовуватися на всіх рівнях ведення бойових дій (операцій) і сприяє інтеграції стратегії, оперативного мистецтва та тактики.

Самосинхронізацією є здатність добре інформованих військ організувати і синхронізувати комплексні бойові дії “з низу до верху”. Організуючими принципами є об'єднання зусиль, чітко сформульовані наміри командира і певні правила застосування зброї. Самосинхронізація досягається завдяки високому рівню знання своїх власних сил, сил противника і всіх відповідних елементів операційного середовища. Вона дозволяє уникнути бойових втрат, характерних для більш традиційних доктрин командування за принципом “з верху до низу”, і переводить бій з покроковою функцією у високошвидкісний континуум [11].

Другою особливістю МЦВ є швидкість командування. Швидкість командування є процесом, за якого інформаційні переваги

перетворюються на конкурентну перевагу. Вона характеризується вирішальною зміною стартових умов, високим темпом змін обстановки і зосередженням на успіх, у той же час передбачаючи блокування альтернативних дій противника. Такий ефект ґрунтується на усвідомленні органом управління всіх елементів оперативної обстановки і досягненні потрібного результату через наслідки взаємопов'язаних між собою подій, у першу чергу, керованих.

МЦВ черпає свою силу з потужної мережевої, добре інформованої, але географічно розпорошеної сили. Ключовими елементами організації дій стають висока продуктивність інформаційної мережі, вільний доступ до всіх потрібних джерел інформації, достатній радіус дії зброї і маневрування з необхідною точністю та швидкістю реакції, досконали процеси командування і контролю, включаючи високошвидкісний автоматизований розподіл необхідних ресурсів.

Таким чином, основна перевага мережецентричної концепції ведення бойових дій проявляється у високій маневреності частин і з'єднань, здатних під час маршу оперативно планувати свої наступні дії, постійно одержуючи свіжі дані розвідки; вступати у бій, не переймаючись тиловим постачанням, що надійде у потрібний час і точно за призначенням. Отже, система управління військами потребує для цього комплексного вдосконалювання, адаптації органів і пунктів управління, систем зв'язку та автоматизації, структури військ (сил) та їх чисельності до виконання майбутніх завдань. Технічною основою вдосконалювання системи управління військами стане глобальна інформаційно-телекомунікаційна система, яка об'єднає всі сучасні засоби озброєння, розвідки та управління [11].

В основу наведеної системи має бути покладена єдина тривірнева АСУВ, у якій стратегічні, оперативні і тактичні рівні та органи управління взаємопов'язані по вертикалі і по горизонталі за стратегічним принципом єдиного інформаційного простору. Реалізація цього загального принципу передбачає: володіння взаємодіючими органами управління незалежною інформацією про об'єкти взаємодії в реальному масштабі часу; незалежність загальної інформаційної основи управління від ієрархії органів управління; формування єдиного віртуального бойового простору; розвиток глобальної

інформаційно-телекомунікаційної інфраструктури.

Тому головними вимогами до створювання і вдосконалювання потрібної інформаційно-телекомунікаційної системи є: висока надійність централізованого управління; можливість децентралізованого управління в окремому регіоні; високий ступінь готовності системи; широкі можливості з оперативного збирання, оброблення і доведення необхідної інформації; забезпечення стійкості і живучості системи управління; висока прихованість управління як під час повсякденної діяльності, так і під час ведення операцій.

Розвиток будь-якої системи автоматизованого управління військами передбачає виконання таких пріоритетних завдань: створення автоматизованих систем управління різного функціонального призначення, у першу чергу, створення АСУ оперативного (бойового) управління військами (силами); розроблення автоматизованих систем спеціального призначення; розроблення інтегрованого банку даних єдиної автоматизованої системи управління (ЄАСУ); створення системи розроблення і впровадження спеціального математичного і програмного забезпечення АСУВ відповідно до стандартів збройних сил провідних країн світу [11]. Із цих поглядів Національна гвардія України як суб'єкт забезпечення національної безпеки нашої держави також потребує створення інформаційно-телекомунікаційної системи (ІТС), яка окрім здійснення управління силами і засобами гвардії повинна бути інтегрованою у загальну інформаційно-телекомунікаційну інфраструктуру як Збройних Сил України, так і держави загалом, але в першу чергу – сил охорони правопорядку.

У зв'язку з цим на порядку денному постає проблема створення єдиного інформаційного середовища для Національної гвардії України, інтегрованого в інформаційний простір держави, яке забезпечить інтеграцію інформаційних ресурсів, необхідних для забезпечення управління наявними силами і засобами.

Основною метою створення ІТС Національної академії України є підвищення оперативності і якості управління з'єднаннями, військовими частинами та підрозділами НГ України, їх бойової і мобілізаційної готовності за рахунок забезпечення швидкого обміну інформацією між організаційно-штатними одиницями з використанням сучасних методів і засобів оброблення, зберігання, передавання та пошуку інформації.

Під такою інформаційно-телекомунікаційною системою наразі розуміють комплекс програмних і апаратних засобів, призначених для створення, передавання, обміну, оброблення, поширення, збереження даних та інформації, управління ними, пошуку і видачі інформації споживачам за їх запитом та проведення потрібних розрахунків для обґрунтування рішень, що приймаються та впроваджуються у практику НГ України. Наведена інформаційно-телекомунікаційна система складається з таких функціональних та технологічних підсистем.

1. Функціональні підсистеми, які забезпечують вирішення функціональних завдань повсякденної (адміністративно-господарської) та оперативної діяльності сил НГ України, а саме:

- збирання, аналізу, оброблення інформації – для автоматизації процесів збирання, аналізу, оброблення інформації та усвідомлення завдань;

- підтримки прийняття рішень – для автоматизації процесів генерування, оцінювання і вибору раціонального рішення з альтернативних варіантів;

- планування операцій (бойових, спеціальних дій) – для реалізації процесів моделювання, проведення відповідних розрахунків;

- оперативного (бойового) управління – для забезпечення і реалізації безпосереднього управління підпорядкованими військовими формуваннями під час виконання ними поставлених завдань;

- забезпечення операцій (бойових, спеціальних дій) – для автоматизації процесів планування, контролю, аналізу оперативного, матеріально-технічного, морально-психологічного і медичного забезпечення операцій (бойових, стабілізаційних та специфічних дій);

- організації, координації і контролю – для реалізації процесів організації управління, узгодження дій, контролю та перевірки готовності військових формувань.

2. Технологічні підсистеми:

- електронного документообігу;
- електронної пошти;
- геоінформаційна;
- довідково-інформаційна;
- візуального відображення інформації;
- відеоконференцзв'язку;
- телекомунікаційна мережа;
- комплексна система захисту інформації.

Підсистеми ІТС являють собою програмно-технічні комплекси, які містять сучасне обчислювальне і периферійне обладнання,

високоєфективні цифрові телекомунікаційні мережі, засоби захисту інформації, а також загальне і спеціальне програмне забезпечення [13]. Потрібна нам інформаційно-телекомунікаційна система забезпечуватиме доступ до загальних ресурсів і дозволить користуватися різноманітними послугами ЄАСУ та її складників АСУ різного призначення. Зрозуміло, що ІТС треба будувати так, щоб забезпечити інформаційний зв'язок між її компонентами і взаємодію елементів функціональних та технологічних підсистем АСУ.

Проте попри нагальну необхідність створення ІТС як і у Національній гвардії України, так і у Збройних Силах України, існує першочергова проблема – відсутність у країні державної телекомунікаційної мережі.

Події у Криму і на сході України за лічені дні виявили велику кількість неув'язок, у тому числі й в інформаційно-телекомунікаційній сфері, у зв'язку з якими українські війська, правоохоронні органи і суспільство загалом зазнають значних людських та матеріальних втрат. Причин виникнення такої ситуації багато. Найголовніша серед них – в Україні немає державного оператора і державної телекомунікаційної мережі. Це, своєю чергою, зумовлює відсутність інших складників, зокрема:

- надійного захищеного зв'язку між державними структурами;

- зв'язку в умовах надзвичайного чи воєнного стану;

- єдиного державного органу управління галуззю інформаційних технологій;

- державної ІТ-інфраструктури.

Органи державної влади України повністю залежні від приватних ІТ-компаній (телекомунікація, телебачення, радіомовлення, доступ до мережі Інтернет тощо). Через відсутність державної телекомунікаційної мережі управління органами державної влади забезпечується за допомогою приватних операторів зв'язку, на базі яких також функціонує система управління терористичними угрупованнями та їх координація з-за кордону.

Отже, виникає парадокс: заборонити роботу приватних операторів держава не може, оскільки таким чином сама залишиться без зв'язку. Збройні Сили України та інші військові формування в умовах ведення бойових дій змушені розгортати телекомунікаційну мережу польовими засобами. При цьому польова мережа має малу потужність і є практично не захищеною від несанкціонованого доступу [12].

Висновок

Таким чином, в умовах активного використання проти України засобів ведення мережецентричної війни створення інформаційно-телекоммуникаційної системи ЗС України, НГ України та інших військових формувань є важливим і актуальним на сьогодні завданням, для виконання якого необхідно докласти максимум зусиль.

Наразі у Головному управлінні НГ України створено управління, завданням якого і є організація розроблення та впровадження ІТС. Початкові роботи з її створення вже проводяться.

Проте є й серйозніша проблема – повернення у державну власність існуючої телекоммуникаційної мережі або створення нової, що крім значних фінансових інвестицій потребує прийняття низки важливих рішень на рівні керівництва держави.

Список використаних джерел

1. Дружинін, С. В. Сучасний стан автоматизації управління військами в Збройних силах України [Текст] / С. В. Дружинін, О. К. Климович, О. Г. Саєнко // Системи озброєння і військова техніка : зб. наук. пр. – Полтава : Військ. ін-т телекомунацій та інформатизації Нац. техн. ун-ту України “КПІ”, 2010. – № 1(21).

2. Кірсанов, С. О. Перспективи розвитку системи управління Збройних Сил України з використанням принципу єдиного інформаційного простору / С. О. Кірсанов [Текст] // Наука і техніка Повітряних Сил Збройних Сил України, 2010. – № 1(3) – С. 15–20.

3. Косс, В. А. Інформаційна модель системи управління збройними силами як сучасний різновид стратегічного озброєння [Електронний ресурс]. – Режим доступу : http://www.immsp.kiev.ua/perspages/koss_va/publ/13_statya_gpu.pdf. – Назва з екрана.

4. Ляпин, В. Р. О построении комплексов средств автоматизации в АСУ войсками (силами) для ведения сетевых действий [Текст] / В. Р. Ляпин, В. Н. Зимин, В. В. Барвиненко // Военная мысль. – 2011. – № 11. – С. 54–61.

5. Напрямки розвитку автоматизованих систем управління, що залучаються до виконання завдань протиповітряної оборони Збройних сил України [Текст] / [Б. І. Нізієнко, В. В. Камінський, О. В. Сісков, О. В. Александров] // Збірник наукових праць Харківського

університету Повітряних Сил. – 2010. – Вип. 2 (24). – С. 18–22.

6. Пермяков, О. Ю. Інформаційне протистояння: реальність і тенденції [Текст] / О. Ю. Пермяков, І. Є. Вернер // Арсенал XXI століття. – 2002. – № 2. – С. 17–20.

7. Савин, Л. В. Сетевая война. Введение в концепцию [Текст] / Л. В. Савин. – М. : Евразийское движение, 2011. – 130 с.

8. Стужук, П. І. Світові тенденції, проблеми та перспективи створення автоматизованих систем управління військами (силами) [Текст] / П. І. Стужук, П. М. Грицай, Ю. С. Вознюк // Збірник наукових праць Центру воєнно-стратегічних досліджень. – 2012. – № 1 (45). – С. 68–76.

9. Толубко, В. Б. Інформатизація управлінської діяльності як чинник інформаційної безпеки держави [Текст] : монографія / В. Б. Толубко, А. А. Рось, І. В. Замаруєва. – К. : НАОУ, 2010. – 213 с.

10. Фролов, В. С. Структурно-логічна схема Єдиної автоматизованої системи управління Збройних Сил України [Текст] / В. С. Фролов // Наука і оборона. – 2012. – № 1. – С. 15–23.

11. Клімушин, П. С. Автоматизована система управління Збройних сил України як сучасний різновид стратегічного озброєння [Електронний ресурс] / П. С. Клімушин, В. Д. Кротов. – Режим доступу : <http://www.kbuara.kharkov.ua/e-book/tpdu/2014-1/doc/1/03.pdf>. – Назва з екрана.

12. Террористы и государство на одной связи [Електронний ресурс]. – Режим доступу : http://gazeta.zn.ua/internal/terroristy-i-gosudarstvo-na-odnoy-svyazi_.html. – Назва з екрана.

13. Внедрение современных информационных технологий в вооруженных силах [Електронний ресурс]. – Режим доступу : <http://uos.ua/produktsiya/svyaz-i-asu/35-vnedrenie-sovremennih-informatsionnih-tehnologiy-v-vooruzhennih-silah>. – Назва з екрана.

14. Паршин, С. А. Концепции сетевых боевого управления ВС США, Великобритании и ОВС НАТО. Общие и различия [Текст] / С. А. Паршин // Зарубежное военное обозрение. – 2010. – № 4. – С. 7–10.

Стаття надійшла до редакції 14.05.2015 р.

Рецензент – доктор військових наук, професор О. М. Шмаков, Національна академія Національної гвардії України, Харків, Україна