

УДК 621.396

Л.І. Поліщук**О.К. Климович**, к.т.н., с.н.с.**С.М. Богуцький**, к.т.н., с.н.с.*Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, м. Львів, Україна*

ОСОБЛИВОСТІ СТВОРЕННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ВІЙСЬКАМИ ЗБРОЙНИХ СИЛ УКРАЇНИ З УРАХУВАННЯМ ДОСВІДУ КРАЇН НАТО

Системи управління військами і зброєю при веденні бойових дій в сучасних умовах за останні десятиліття зазнали значних змін завдяки їх всебічній автоматизації. Одним із найбільш перспективних шляхів покращення якості і ефективності системи управління військами і зброєю є комплексна автоматизація процесів, які в ній здійснюються, і оснащення її структурних елементів сучасними засобами зв'язку, передачі даних, автоматизації і захисту інформації. В статті проводиться аналіз досвіду розробки автоматизованих систем управління військами (силами) у збройних силах країн НАТО. На підставі проведеного аналізу надаються рекомендації щодо створення автоматизованих систем управління військами (силами) у Збройних Силах України.

Ключові слова: телекомунікаційна мережа спеціального призначення, автоматизовані системи управління, Збройні Сили України.

Вступ

В останні роки в економічно і технічно розвинених державах світу і перш за все у США особлива увага приділяється активному розвитку теорії і практики ведення мережецентричних дій, які кардинально змінюють погляди на підготовку і застосування Збройних сил у сучасних війнах і конфліктах.

Матеріальною основою мережецентричних дій є мережецентричні системи управління. Перевага над противником під час ведення мережецентричних дій досягається, в першу чергу, за рахунок суттєвого підвищення якості управління військами і зброєю, повноти і глибини єдиного розуміння оцінки і прогнозування командування усіх рівнів динаміки розвитку обстановки, оперативності реагування на її зміни, прийняття своєчасних і обґрунтованих рішень, швидкого доведення завдань до різних угруповань військ.

Події на Сході України показали нагальну необхідність вирішення питань переведення системи управління на цифрові засоби зв'язку з подальшим створенням інформаційно-телекомунікаційних мереж, які дадуть можливість створення і автоматизації системи управління військами і засобами ураження.

Мета статті

З оголошенням Президентом України рішення про підготовку до вступу до НАТО, виникло питання переходу Збройних Сил України (ЗСУ) і інших силових структур на стандарти НАТО, що означає проведення оборонної реформи з перебудови ЗСУ, в тому числі і системи управління військами (силами) і зброєю у відповідність до цих стандартів. 6 червня 2016 року Президентом України було схвалено рішення Ради національної безпеки і оборони України «Про стратегічний оборонний бюлетень України», в якому визначені мета, стратегічні та оперативні цілі оборонної реформи до кінця 2020 року.

Метою статті є аналіз шляхів створення автоматизованої системи управління військами ЗСУ з урахуванням досвіду провідних країн світу для досягнення нинішніх стандартів НАТО, за рахунок чого і як це планується здійснити в ЗСУ, а також розгляд проблемних питань, які при цьому виникають.

Виклад основного матеріалу

Особливостями протиборотства в ХХІ столітті є те, що в останні роки військово-політичне керівництво ряду країн світу, в тому числі і Російської федерації, все більш активно розвивають і випробовують концепції війн нового покоління, відомих як «гібридні війни», «проксі війни» і війни «по довіреності».

В гібридній війні, яку розв'язала Російська федерація на території України найбільш уразливими виявилися системи управління і зв'язку, побудовані за класичними принципами і схемами, що негативно відобразилось на ефективності системи оперативного (бойового) управління, зв'язку, розвідки, неспроможності оперативно реагувати на зростаючу кількість і потужність кібератак і протистояти кіберзлочинності.

Одним із сучасних підходів до ведення війни є мережецентричні війни. В основу концепції «мережецентричної війни» покладені стандартизація, уніфікації і комплексне впровадження новітніх інформаційних технологій, що дозволяє створити єдиний інформаційний простір – об'єднання в єдину інформаційно-телекомунікаційну мережу засобів і органів управління, розвідки, зв'язку і автоматизації, а також їх взаємодії з мережами ураження і всебічного забезпечення [1].

В умовах розвитку інформаційно-телекомунікаційного простору виникає необхідність створення автоматизованих систем управління (АСУ) військами (силами) та засобами ураження, які будуть використовувати сучасні високотехнологічні досягнення в цій області. Основним призначенням таких АСУ є підвищення основних оперативно-тактичних показників системи – стійкості, мобільності, пропускнуої спроможності і безпеки, що приводить до значного покращення ефективності і якості управління військами і зброєю під час підготовки і ведення бойових дій.

Одним із головних напрямків широкомасштабної автоматизації управління військами і зброєю у збройних сил країн НАТО є створення органів управління і засобів, що дозволяють формувати єдину картину «поля бою» на основі інформації від територіально рознесених різних джерел інформації, доводити її до відповідних органів управління у зручному для прийняття рішення вигляді, планування ведення бойових дій і доведення їх до виконавців у близькому до реального масштабі часу [2].

Аналізуючи реальний стан автоматизації і управління у збройних сил країн НАТО і Російської федерації, можна зазначити, що всі вони взяли курс на розвиток вітчизняних збройних сил шляхом оснащення бойових підрозділів сучасними системами зв'язку та автоматизації. Прикладом таких систем є: глобальна система управління та спостереження Збройних сил США GCCS (Global Command and Control System-Army) (рис. 1) [3], інформаційно-телекомунікаційна система і Збройних сил Туреччини TASMUS (Taktik Sana Muhabere Sistemi) (рис. 2) [4], АСУ тактичної ланки Збройних сил Російської федерації «Созвездие» (рис. 3) [5].

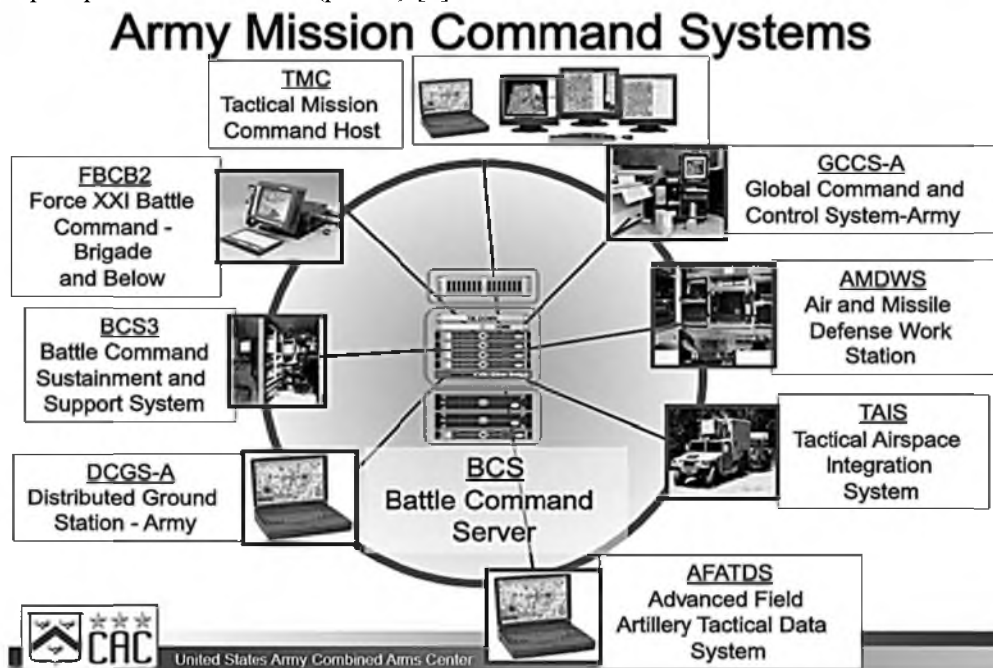


Рис. 1. Системи управління бойовими діями Збройних сил США

Для створення подібної системи задіяні сотні телекомунікаційних систем і мереж, які базуються на військових і комерційних системах зв'язку і використовуються різними військовими відомствами.

Перша система – забезпечує командування і штаби первинною інформацією, яка надходить від джерел, що діють на всьому просторі ведення бойових дій. Вона узагальнює ці дані для того, щоб представити органам управління на всіх рівнях єдину інформаційну картину про стан сил і засобів ураження противника і своїх сил, навколишнє середовище (район ведення бойових дій, метеорологічні умови, умови розповсюдження електромагнітних хвиль).

Друга система – для збору, обробки та аналізу первинних даних, а також для їх зберігання і передачі по запитам користувачам. На відміну від первинної, ця інформація отримується в результаті класифікації цілей, розподілу засобів ураження по них та розробки даних наведення. Таким чином, ця система насичує тривимірний інформаційний простір поля бою даними для планування бойових дій, управління ними та ураження з метою досягнення переваги над противником.

Третя система – це засоби, що забезпечують застосування зброї і ураження об'єктів високоточними боеприпасами, що дозволяє досягти цієї переваги.

Кінцева мета системи, що створюється – збір, обробка, аналіз і розподіл інформації, що забезпечує застосування засобів ураження з великим ступенем своєчасності і надійності, випереджаючи противника у цьому.

Якщо розглядати у цьому напрямку НАТО, то досвід розвитку систем і засобів зв'язку, без яких неможливо створити сучасні АСУ, у збройних сил держав, які входять до блоку, показує, що там визначені загальні (єдині) шляхи їх розвитку з перспективою забезпечення повної інтеграції військових та цивільних систем і засобів зв'язку. Так, наприклад, об'єднана система зв'язку NICS (NATO Integrated Communications System), що забезпечує процес функціонування органів і пунктів управління вищої ланки управління збройних сил блоку НАТО, включає каналотворюючі системи супутникового, тропосферного, радіорелейного, проводового і радіозв'язку НАТО, а також лінії зв'язку, які орендовані у цивільних відомств країн – учасників блоку. Система NICS сполучена з національними військовими системами зв'язку стратегічної та оперативно-тактичної ланок управління збройних сил країн НАТО.

Для сумісності в роботі і розвитку телекомунікаційних мереж спеціального призначення (ТКМ СП) країн НАТО впроваджені стандарти TACOMS POST – 2000, які розглядаються, як методологія інтелектуальних телекомунікацій, які забезпечують для НАТО можливість ведення коаліційних мережецентричних операцій. Ці стандарти також використовуються для реалізації концепції приналежності бойових систем, як інтеграції мереж сенсорних засобів в мережах вузлів управління засобами ураження. Вони базуються на SDR (Software Defined Radio) - системах, головна перевага технологій яких на даному етапі – можливість добитись сумісності різнотипних пристроїв, що дозволяє не тільки забезпечити надійність функціонування пристрою, але й спростити проблеми сумісності на міжнаціональному рівні, особливо при багатонаціональних розробках. При цьому, при роботі на перспективу, SDR пристрої повинні мати ще й додаткові можливості по пропускній спроможності, завадозахищеності, криптологічній стійкості та ін..

Тактична система комутації MIDS (Multifunctional Information Distribution System) – призначена для поєднання різних типів платформ у загальну тактичну мережу передачі даних. Одним із цифрових сервісів MIDS, відповідно до угоди про стандартизацію STANAG- 5516, є протокол LINK-16. Відповідні термінали використовуються на літаках F-18, Tomado, ЗПК SAMP/T, фрегаті Horizon та інших бойових засобах ураження.

Характерною рисою розвитку сучасних ТКМ СП є впровадження мереж нового покоління NGN (Next Generation System) – технологій мультисервісного абонентського доступу, пакетної комутації, які вимагають якісно нового технологічного розвитку транспортної мережі. Найпростішим напрямком розвитку ТКМ СП є використання технологій багатопроTOCOLьної комутації міток MPLS (Multiprotocol Label Switching). Головною особливістю цієї технології є відокремлення процесу комутації пакета від аналізу IP-адреси в його заголовку, що дозволяє здійснити комутацію пакетів значно швидше. MPLS VPN (Virtual Private Network) забезпечує можливість використання таких сервісів, як відеотелефонія, відеоконференцз'язок, віддалене відеоспостереження, а додавання нових вузлів віртуальної мережі не

ускладнює масштабування. Таким чином MPLS забезпечує можливість раціонального поєднання централізованого і децентралізованого використання інформації на всіх рівнях управління.

Проведена в рамках комплексного огляду сектору безпеки і оборони оцінка стану воєнної безпеки держави, а також набутий досвід участі ЗСУ у Антитерористичній операції виявили низку проблем функціонування сил оборони в умовах існуючих та потенційних загроз, в тому числі, і управління ними. Виникла необхідність проведення оборонної реформи в Україні, яка має відповідати актуальним проблемам оборони України, сприяти зміцненню спроможності сил оборони, підвищенню їх готовності до виконання завдань за призначенням та участі у проведенні спільних бойових дій (операцій) з підрозділами НАТО [6].

Єдиною всеосяжною метою оборонної реформи є розвиток, відповідно до євроатлантичних норм та критеріїв членства в НАТО, спроможностей ЗСУ та інших складових сил оборони, які необхідні для адекватного реагування на загрози національній безпеці у воєнній сфері, захисту України, її суверенітету, територіальної цілісності та непорушності кордонів, підтримки міжнародного миру та безпеки.

Відповідно до положень Стратегічного оборонного бюлетеня України, який визначає основні напрямки реалізації воєнної доктрини України та розвитку сил оборони до кінця 2020 року, в розділі «Оперативна ціль 1.2» шляхів досягнення стратегічних цілей «Удосконалення системи управління силами оборони», визначений очікуваний результат: «створено відповідно до євроатлантичних стандартів ефективну систему управління, що дає змогу проявляти ініціативу і надає більшу самостійність керівникам органів управління сил оборони усіх рівнів у прийнятті управлінських рішень, удосконалено координацію між складовими сил оборони та впроваджено механізм, що забезпечує їх консолідований розвиток, досягнуто необхідні оперативні спроможності для забезпечення оборони держави».

В розділі – Оперативна ціль 1.4 «Створення ефективної системи оперативного (бойового) управління і зв'язку, розвідки та спостереження (C4ISR)» (рис. 4) [7], очікуваним результатом повинно бути: «створено національну телекомунікаційну мережу, модернізовано та переведено на сучасні цифрові технології систему спеціального зв'язку, відомчі інформаційно-телекомунікаційні мережі та системи зв'язку пунктів управління органів державної влади, а також створено автоматизовану систему управління C4ISR складових оборони, яка відповідає стандартам і рекомендаціям НАТО, забезпечено її інтеграцію в систему управління оборонними ресурсами». Також повинно бути створено у Міністерстві оборони України, інших складових сектору оборони підрозділи кіберзахисту, протидії технічним розвідкам, впровадження заходів із захисту інформації відповідно до вимог нормативно-правових актів України та з урахуванням стандартів НАТО і ISO/IEC.

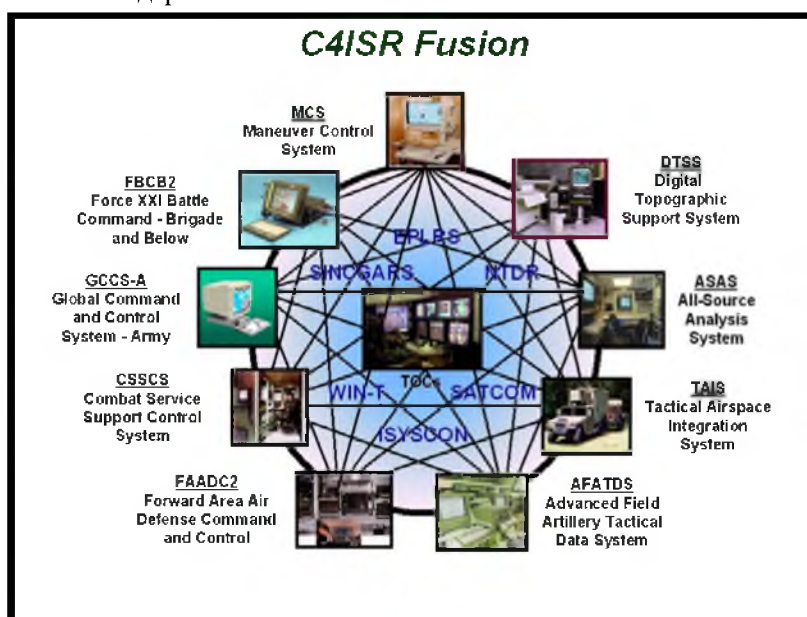


Рис. 4. Система оперативного (бойового) управління і зв'язку, розвідки та спостереження (C4ISR)

Якщо проаналізувати розвиток ТКМ СП і створення АСУ провідних країн світу, то можна визначити такі етапи [8]:

60-ті – початок 90-х років минулого сторіччя – впровадження систем автоматизації опрацювання даних, тобто створення безлічі слабоінтегрованих систем, що автоматизують окремі процеси, функції, види постачання;

з 90-х до 2000-х років – інтеграція роз'єднаних АСУ та автоматизованих інформаційних систем на основі принципів систем відкритої та сервісорієнтованої архітектури на базі веб-технологій і стандартизації обміну даними;

з 2000-х років до теперішнього часу – відмова від інтеграції спеціалізованих автоматизованих інформаційних систем і перехід на комерційні системи при спрямуванні на створення єдиного інформаційного віртуального середовища різних видів бойового забезпечення.

В Україні про створення єдиної АСУ ЗСУ і її складових розмови ведуться з 90-х років минулого сторіччя, але створено практично за цей час було з різних причин дуже мало.

Наприклад, усі національні виробники, яким було видане технічне завдання на розробку необхідних засобів радіозв'язку за 3 роки не вийшли на рівень, який би дав право на виробництво необхідних засобів. Не створено навіть зразків.

З початком проведення Антитерористичної операції на початку 2014 року було прийнято рішення на рівні Генерального штабу ЗСУ про оснащення ЗСУ засобами зв'язку, виходячи з ситуації, що складається – одночасним використанням різних засобів зв'язку. Результатом цього на теперішній час стало:

1. Радіозв'язок в УКХ діапазоні – бойові частини ЗСУ забезпечені обладнанням компанії Motorola приблизно на 70%, решта частин – на 30%. Для повного оснащення ЗСУ потрібно близько 100 тисяч радіостанцій різного типу. Розміри технічної допомоги в рамках програми західної підтримки дорівнює обсягам оснащення засобами зв'язку двох батальйонів на рік.

Переможцем у порівняльних випробуваннях, які проводились у ЗСУ, стала Турецька компанія Aselsan. Турецькі засоби радіозв'язку УКХ діапазону розроблені і виготовлені з врахуванням вимог і стандартів НАТО. По своїх технічних можливостях, а також по критерію «ефективність – ціна», радіостанція серії 9661 стала кращою, як по дальності встановлення зв'язку, так і по здатності працювати під впливом потужних засобів радіоелектронної боротьби.

Компанія Aselsan зобов'язалась:

передати ключові технології українській стороні на виготовлення радіостанцій;

для ремонту засобів радіозв'язку створити і обладнати сервісний центр;

реалізувати сумісний з українською стороною науково-технічний проект по створенню власного програмного забезпечення;

досягнута домовленість про можливість заміни турецького алгоритму шифрування на національний;

підготовка військовослужбовців ЗСУ буде проводитись у Військовому інституті телекомунікацій і інформатизації імені Героїв Крут, включаючи розробку навчальних посібників.

Мережі тактичного радіозв'язку Aselsan можуть бути інтегровані в будь-які види оперативно-тактичних і стратегічних мереж зв'язку для одночасної передачі голосової інформації і IP-даних.

Партером компанії Aselsan в роботі на ринку України є компанія «Everest Limited», яка входить в групу компаній Everest.

2. Радіозв'язок в КХ діапазоні – прийнято рішення озброювати ЗСУ, Прикордонні війська і Національну гвардію радіостанціями американської компанії Harris, що забезпечує сумісність комунікаційних систем різних відомств і потреба в таких радіостанціях значно менша.

Оснащення такими радіостанціями УКХ, КХ діапазонів дає можливість створення і обладнання командно-штабних машин і пунктів управління на рухомій базі, що покращить умови для створення АСУ в тактичній ланці управління.

3. Радіорелейний зв'язок – використовуються послуги «Укртелекому», комерційної компанії, за що потрібно платити. З прийняттям на озброєння цифрових радіорелейних станцій Р-414МУ та Р-425 С3, які розроблені вітчизняними підприємствами у 2016 році розпочалось будівництво власної опорної мережі радіорелейними засобами, що особливо важливо для зони Антитерористичної операції, а також зменшує залежність від «Укртелекому».

4. Тропосферний зв'язок – практично не використовується тому, що енергозатратний і вимагає багато коштів для утримання і він знаходиться в резерві. Планується розгорнути сучасну систему зв'язку, яка за своїми характеристиками буде значно перевищувати існуючі системи.

5. По супутниковому зв'язку лідером на ринку телекомунікаційних послуг в цьому сегменті є оператор зв'язку «Датагруп». Мобільні комплекти супутникового зв'язку ЗТК-1С, МКС3-V1-РОЕ, які вони постачають для силових структур в Україні призначені для забезпечення абонентів послугами відкритого телефонного зв'язку, використовуючи які, разом із супутником іноземної держави, являються посередником між іноземною компанією і Генеральним штабом ЗСУ.

6. Постачання ноутбуків і планшетів, сервісного і мережевого обладнання, систем електроживлення до них, систем візуалізації (різних дисплеїв в захищеному вигляді) для ЗСУ займається компанія Roda Computer GmbH (Німеччина) в Україні. Таке ж обладнання використовується в арміях країн членів НАТО і повністю відповідає їх стандартам, що можна віднести до позитиву. Але компанія не може постачати програмне забезпечення і відповідні засоби зв'язку.

7. Лідером у забезпеченні принтерами і проєкторами, без яких уже не можна собі уявити роботу об'єктів управління та пунктів управління, є компанія Epson. Проєктори цієї компанії можуть встановлюватись як у стаціонарному, так і в мобільному варіантах. За своїми можливостями інтерактивний комплекс Epson дозволяє організувати відеоконференції, у яких можна приймати участь з мобільних пристроїв.

Давно відомо, що однією із моделей перспективного розвитку і удосконалення системи зв'язку і автоматизації є створення інформаційно-телекомунікаційних систем за відповідними стандартами, умовами і принципами. Для забезпечення роботи таких систем необхідно створити єдиний інформаційний простір для всіх учасників ведення бойових дій.

Дотримуючись таких правил Сухопутні війська США і НАТО пройшли шлях створення нинішньої автоматизації управління веденням бойових дій починаючи з 60-х років минулого сторіччя. У ЗСУ подібний шлях по створенню АСУ С4ISR, яка повинна відповідати стандартам НАТО необхідно пройти за 4 роки, один з яких уже пройшов. При цьому:

1. Не завершено створення в державі відповідної нормативно-правової бази для повноцінної підготовки с управління силами оборони в особливий період, що підтверджують випадки неоперативної видачі телекомунікаційного ресурсу з боку існуючих операторів телекомунікаційних послуг за запитом системи управління збройних сил.

2. На сьогоднішній день для отримання телекомунікаційного ресурсу підрозділами збройних сил та інших силових структур (Прикордонні війська, Національна гвардія та ін.) практично використовуються телекомунікаційні системи і мережі різних операторів телекомунікаційних послуг, які створювались за різними стандартами і принципами. Це стало наслідком відсутності своєї окремої, як стаціонарної, так і рухомої телекомунікаційних мереж зв'язку і автоматизації, які свого часу були знищені або продані теперішнім їх власникам.

3. Відсутній супутниковий зв'язок і платформи для повітряних ретрансляторів, які є обов'язковими в нинішніх умовах, для підвищення надійності, стійкості, скритності і безперервності управління військами і засобами ураження.

4. Рішення, які прийняті, на комплектування ЗСУ засобами зв'язку і IT-обладнанням, які створені в різних державах, часто за різними стандартами, без гарантій оснащення програмним забезпеченням та засобами і методами шифрування, приведе до залежності від держав постачальників в забезпеченні, обслуговуванні, ремонті, навчанні обслуговуючого персоналу, а головне – в сумісності роботи при створенні єдиної телекомунікаційної системи для створення і роботи АСУ С4ISR.

5. Відсутня єдина уніфікована організаційно-штатна структура штабів усіх ланок управління ЗСУ, які спроможні готувати і здійснювати прийняття рішень на підготовку і ведення бойових дій, а також повсякденного забезпечення життєдіяльності військ за стандартами НАТО.

6. Склад пунктів управління всіх ланок управління ЗСУ до цього часу є громіздким із-за повільного зменшення кількості техніки на них за рахунок створення сучасних уніфікованих цифрових засобів зв'язку і автоматизації на відповідній колісній і гусеничній базі, що значно підвищує розвідвахищеність і маршеві можливості таких пунктів управління.

Для створення АСУ С4ISR (розвідка, спостереження, рекогносцировка) необхідні органи і засоби для організації і управління космічною, наземною, повітряною і іншими розвідками, перша з яких відсутня, друга – використовується з використанням старого парку розвідзасобів, третя – майже відсутня. Крім цього, повинні бути створені відповідні бази знань і даних за вірогідного противника, свої війська і території, на яких можуть вестись бойові дії.

Таким чином, стоїть завдання за короткий час інтегрувати розвідку, радіоелектронну боротьбу, геоінформаційні системи, системи автоматизації і зв'язку у єдину систему у відповідності до стандартів і структур НАТО. На сьогоднішній день ці елементи розвиваються окремо, а повинні працювати під єдиним командуванням в єдиній структурі.

Висновки

1. В найкоротший час створити повну нормативно-правову основу, яка буде базою для створення АСУ С4ISR в усіх ланках управління ЗСУ і інших структур сил оборони.

2. Прикласти максимум зусиль для розгортання окремої військової стаціонарної телекомунікаційної мережі, яка б була незалежною від комерційних структур і включала в себе сучасні лінії радіорелейного, тропосферного, супутникового, радіо, по можливості проводового зв'язку.

3. Добиватись від держав-постачальників засобів зв'язку та ІТ-обладнання передачі ключових технологій українській стороні та їх виготовлення. При цьому, мати можливість виготовлення і застосування власного програмного забезпечення і заміни іноземного алгоритму шифрування на національний.

4. Привести організаційно-штатні структури штабів усіх ланок управління ЗСУ до структур НАТО і стандартів їх роботи.

5. Відповідно до змін у забезпеченні і оснащенні пунктів управління усіх ланок управління сучасними засобами зв'язку і автоматизації, удосконалюючи їх структуру, добитись максимального скорочення кількості техніки у їх складі.

6. Для створення АСУ С4ISR необхідно створити єдину систему розвідки, радіоелектронної боротьби, геоінформаційних систем, зв'язку і автоматизації.

7. Відмовитись від посередників постачання засобів зв'язку і інформаційно-телекомунікаційного обладнання та перейти на прямі відносини Міністерства оборони України з виробниками цих засобів і обладнання.

Список використаних джерел

1. Зотова І.Г. *Стан і перспективи розвитку автоматизованих систем управління військами (зброєю) передових країн світу* / І.Г. Зотова, М.Ю. Голобородько, О.В. Поривай // *Збірник наукових праць центру воєнно-стратегічних досліджень Національного університету оборони України*. – 2013. – №2(48). – С. 36.

2. Бондаренко Л.О. *Аналіз міжнародного досвіду з розвитку системи зв'язку збройних сил провідних країн* / Л.О. Бондаренко, Зінченко М.О., Скидан І.В., Мальцева І.Р. // *Междисциплинарные исследования в науке и образовании*. – 2013. – №2Кд. – С. 5-7.

3. <http://slideplayer.com/slide/4880213>.

4. <https://teknoformat.com/tasmus-taktik-saha-muhabere-sistemi-11195>.

5. <http://bastion-opk.ru/asuv-tz>.

6. Указ Президента України №240/2016 „Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року „Про Стратегічний оборонний бюлетень України” від 6 червня 2016 р. [Електронний ресурс] / Офіційне інтернет-представництво Президента України. – Режим доступу: <http://www.president.gov.ua/documents/2402016-20137>.

7. <http://archive.defense.gov/DODCMSShare/briefingslide/214/010517-D-6570D-006.jpg>.

8. Кондратьев А.Е. Сетецентрический фронт. Боевые действия в едином информационном пространстве / А.Е. Кондратьев // Национальная оборона. – 2011. – №2. – С. 26– 30.

Рецензент: А.М. Зубков, д.т.н., с.н.с., Національна академія сухопутних військ імені гетьмана Петра Сагайдачного, м. Львів

ОСОБЕННОСТИ СОЗДАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ВОЙСКАМИ ВООРУЖЕННЫХ СИЛ УКРАИНЫ С УЧЕТОМ ОПЫТА СТРАН НАТО

Л.И. Полищук, О.К. Климович, С.Н. Богуцкий

Системы управления войсками и вооружением при ведении боевых действий в современных условиях за последнее десятилетие существенно изменились благодаря всесторонней автоматизации. Одним из наиболее перспективных путей улучшения качества и эффективности системы управления войсками и вооружением является комплексная автоматизация процессов, которые осуществляются, и оснащение её структурных элементов современными средствами связи, передачи данных, автоматизации и защиты информации. В статье проводится анализ опыта разработки автоматизированных систем управления войсками (силами) в вооружённых силах стран НАТО. На основании проведенного анализа представляются рекомендации по созданию автоматизированных систем управления войсками (силами) в Вооружённых Силах Украины.

Ключевые слова: телекоммуникационная сеть специального назначения, автоматизированные системы управления, Вооружённые Силы Украины.

FEATURES OF CREATION OF THE AUTOMATED CONTROL SYSTEM BY THE TROOPS OF THE ARMED FORCES OF UKRAINE TAKING INTO ACCOUNT EXPERIENCE OF COUNTRIES NATO

L. Polishchuk, O. Klimovich, S. Bogutskiy

The systems of command and control of troops and armaments in the conduct of hostilities in modern conditions over the last decade have changed significantly due to comprehensive automation. One of the most promising ways to improve the quality and effectiveness of the system of command and control of troops and weapons is the integrated automation of the processes that are carried out and the equipping of its structural elements with modern means of communication, data transmission, automation and information protection. The article analyzes the experience of developing automated control systems for troops (forces) in the armed forces of NATO countries. On the basis of the analysis, recommendations are presented on the creation of automated control systems for troops (forces) in the Armed Forces of Ukraine.

Keywords: special purpose telecommunications network, automated control systems, the Armed Forces of Ukraine.