

НАЦІОНАЛЬНА АКАДЕМІЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Збірник тез доповідей НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

**“Службово-бойова діяльність
Національної гвардії України:
сучасний стан, проблеми
та перспективи”**

Секція 5

**Актуальні проблеми зв'язку
та інформатизації службово-бойової
діяльності Національної гвардії України**

(<http://nangu.edu.ua>)

29 березня 2018 року

м. Харків

Оргкомітет конференції

Голова оргкомітету – перший заступник начальника Національної академії з навчально-методичної та наукової роботи полковник **Морозов О.О.**

Відповідальний секретар оргкомітету:

науковий співробітник науково-організаційного відділу **Бондаренко О.В.**
(057-739-26-68, 4-68)

Члени оргкомітету:

начальник науково-дослідного центру полковник **Приходько І.І.**;

начальник навчально-методичного центру полковник **Тробюк В.І.**;

начальник факультету №1 полковник **Овчаренко В.В.**;

начальник факультету №2 полковник **Єманов В.В.**;

начальник факультету №3 полковник **Павлов С.П.**;

начальник факультету №4 полковник **Іщенко С.О.**;

заступник начальника Київського факультету з навчально-методичної та наукової роботи підполковник **Бєлай С.В.**;

начальник відділу по роботі з особовим складом полковник **Драган Ю.А.**;

начальник відділу родів військ та служб полковник **Держач О.В.**;

начальник науково-організаційного відділу підполковник **Морозов І.Є.**

Адреса оргкомітету: 61001, м. Харків, майдан Захисників України, 3, Національна академія Національної гвардії України, науково-організаційний відділ.

Контактні телефони: 057-739-26-02, 057-739-26-68.

Електронна адреса: nov_nangu@ukr.net

Доповіді відтворені безпосередньо з авторських оригіналів. За достовірність представлених результатів відповідальність несуть автори

Секція № 5

Актуальні проблеми зв'язку та інформатизації службово-бойової діяльності Національної гвардії України

Керівник секції: кандидат технічних наук, доцент полковник **Іохов О.Ю.**
Секретар секції: кандидат технічних наук полковник **Оленченко В.Т.**

Тематика секції:

- організація зв'язку;
- технічне забезпечення зв'язку та інформатизація;
- бойове застосування вузлів зв'язку пунктів управління Національної гвардії України;
- електронно-обчислювальна техніка та радіокомпонентна база зв'язку та інформатизації військ;
- телекомунікаційні та інформатизаційні мережі;
- комплексний інженерно-технічний захист об'єктів службово-бойового забезпечення Національної гвардії України.

УДК 621.396

Борисенко М.В., кандидат технічних наук, Харківський національний університет Повітряних Сил імені Івана Кожедуба; **Шапран Ю.Є.**, Державний університет інфраструктури та технологій

АВТОМАТИЗОВАНА СИСТЕМА КОНТРОЛЮ ТА ДІАГНОСТИКИ РАДІОТЕХНІЧНОЇ АПАРАТУРИ

У доповіді показано, що з ускладненням технічних об'єктів (літальних апаратів, морських суден, електростанцій різних типів, засобів передачі та приймання інформації тощо) для визначення їх технічного стану з метою недопущення аварій і поломок необхідно застосовувати автоматизовані системи контролю та діагностування (АСКД).

Наведено, що відповідно до галузей застосування АСКД можливо розділити на стаціонарні та пересувні (бортові). Розглянуті особливості стаціонарних і пересувних АСКД.

Стаціонарні АСКД призначені, як правило, для вирішення різних задач контролю технічного стану радіотехнічної апаратури складних технічних об'єктів при проведенні технічного обслуговування чи регламентних робіт. Їх пропонується розробляти на основі застосування обчислювальної техніки та набору програм для здійснення різних видів контролю параметрів радіотехнічної апаратури. При цьому ЕОМ керує процесом вимірювання параметрів, оцінює їх результати, порівнює їх з встановленими допусками, а потім у потрібному вигляді друкує ці результати на папері з вказівкою, який обсяг регулювання або ремонту потрібно виконувати. Такий тип АСКД дає можливість значно скоротити час, який потрібно витратити на перевірку технічного стану радіотехнічної апаратури складних технічних об'єктів.

Пересувні АСКД пропонується створювати за декількома напрямками.

Перший з цих напрямків пов'язаний з розробкою вбудованих (бортових комплексних АСКД) для багатогабаритних об'єктів (наприклад, важких багатомісних літаків, вантажних морських суден, засобів передачі та приймання інформації тощо) до складу персоналу яких входить інженери. Особливістю такої системи є наявність комплексів контролю силового, радіоелектронного, енергетичного, механічного та іншого обладнання, яка може працювати в двох режимах: автоматичному (з безперервним контролем і необхідним інформуванням) та вибіркового ручного контролю (або діагностичному).

Другий напрямок пов'язаний зі створенням комплексних АСКД. У подібних АСКД вимірювання параметрів, що контролюються, порівняння їх значень з допустимими границями та винесення висновку про працездатність здійснюється за допомогою спеціальних схем порівняння, які вбудовуються

безпосередньо в апаратуру підсистем, що контролюються. Граничні значення параметрів, що вимірюються, "закладаються" у вимірювальні схеми під час їх проектування та виготовлення. Роль обчислювальної техніки у подібних системах контролю зводиться до опитування у відповідній послідовності вбудованих схем контролю, що надають її результати оцінки працездатності, які отримані. За умов наявності відмови (несправності) видається на спеціальне табло світловий сигнал попередження.

Крім контролю під час функціонування бортові АСКД можуть працювати також у складі наземних систем технічного обслуговування авіаційної техніки чи морських суден. Такі АСКД в основному застосовуються на етапі проведення профілактичних робіт.

Запропонований підхід до побудови АСКД дозволяє скоротити час на визначення технічного стану радіотехнічної апаратури складних технічних об'єктів і підвищити рівень їх достовірності визначення технічного стану.

УДК 621.396

Власік С.М., кандидат технічних наук, старший науковий співробітник, Харківський національний університет Повітряних Сил імені Івана Кожедуба; **Сметана Є.А.**, Харківський національний університет Повітряних Сил імені Івана Кожедуба; **Лабунець В.О.**, Повітряне командування «Центр»

РОЗРОБКА РАДІОТЕХНІЧНИХ СИСТЕМ ДЛЯ БЛОКУВАННЯ ЗАСОБІВ РАДІОЗВ'ЯЗКУ ПРИ ПРОВЕДЕННІ СПЕЦІАЛЬНИХ ОПЕРАЦІЙ

До головних завдань на сучасному етапі боротьби з тероризмом відносять створення ефективної системи розвідки у складі антитерористичних структур. Одним з основних її складових елементів має бути система радіомоніторингу за роботою засобів радіозв'язку, яка дозволить викривати систему управління терористів і видавати інформацію, необхідну для роботи засобів радіоелектронної боротьби і дезінформації.

Результати аналізу використання можливих засобів зв'язку терористичними групами, частотно-часових характеристик їх сигналів указують на те, що радіоконтроль необхідно проводити у всій смузі частотного діапазону з різною тривалістю сигналу (посилки).

Для придушення засобів зв'язку лідерів і членів терористичних груп з метою порушення системи управління при проведенні антитерористичних операцій пропонується використовувати надширокосмугові радіотехнічні системи, основу яких складає тракт формування та випромінювання надширокосмугових сигналів, що є достатньо пропрацьованим технічним рішенням. Його

особливістю є широка смуга частот. Тому такий тракт може бути покладений в основу й при розробці та створенні конкурентно здатних засобів функціонального придушення (ураження) засобів радіозв'язку.

У доповіді показано, що під функціональним придушенням засобів радіозв'язку розуміється такий вплив на засоби та канали радіозв'язку, при якому здійснення зв'язку не можливе. Під функціональним ураженням розуміється такий вплив спеціально сформованим електромагнітним імпульсом, при якому виникає незворотній вихід зі строю окремих елементів або функціональних пристроїв, що виключає самостійне відновлення функціонування радіоелектронних систем і потребує проведення ремонтно-відновлювальних заходів.

Енергетичний потенціал поешкоди залежить від потужності поешкоди та коефіцієнта посилення антени, який визначається шириною її діаграми спрямованості. Використання всенаправлених лінійно поляризованих антен призводить до зниження енергетичного потенціалу засобів придушення. Тому доцільним є використання засобів функціонального придушення (ураження) каналів радіозв'язку з гостронаправленими антенами. Можливість секторного огляду такої антени по азимуту передбачає зменшення потужності, яка випромінюється, в напрямках, відмінних від напрямку головного максимуму діаграми спрямованості, що грає істотну роль при рішенні задачі електромагнітної сумісності засобу функціонального придушення (ураження) із застосуванням надширокосмугових сигналів із засобами зв'язку і захисту обслуговуючого персоналу від електромагнітного випромінювання.

Приводяться результати розрахунків конструкції та параметрів опромінювача надширокосмугової дзеркальної антени засобу функціонального придушення (ураження) у вигляді конічної спіралі, що дозволяє внести поешкоди у роботу засобів радіозв'язку на території приблизно одного квадратного кілометра.

Представлена розроблена методика визначення потужності ненавмисної поешкоди на вході основного каналу прийому.

УДК 681.772

Власов К.В., старший викладач кафедри управління діями підрозділів із засобами військового зв'язку Національної академії Національній гвардії України

СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ НА БАЗІ ОБЛАДНАННЯ HIKVISION ТА МОЖЛИВОСТІ ЇХ ЗАСТОСУВАННЯ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Сучасний досвід участі збройних сил провідних країн світу у збройних конфліктах останніх десятиліть та в миротворчих операціях, аналіз причин та

*Секція 5. Актуальні проблеми зв'язку та інформатизації службово-бойової діяльності
Національної гвардії України*

наслідків діяльності терористичних організацій проти військових об'єктів свідчать, що ефективність підготовки військ (сил), збереження життя особового складу, озброєння і військової техніки знаходяться в прямій залежності від якості організації охорони та оборони військових об'єктів, а також від спроможності в автоматичному режимі виявляти порушників на підступах до військових об'єктів, що охороняються, та адекватно реагувати на порушення.

Підрозділи різних силових структур зарубіжних країн широко використовують системи відеоспостереження. Вони дозволяють ефективно вести спостереження в значних районах з різним рельєфом місцевості, в будь-який час доби, при будь-якій видимості і погоді. Використання систем дозволяє істотно скоротити сили і засоби, які залучаються для вирішення перерахованих завдань. Особливо їх роль зросла в локальних конфліктах малої інтенсивності і миротворчих операціях, тому ведеться безперервне вдосконалення існуючих і розробка нових систем.

Основним напрямком розвитку технічних засобів охорони в НГУ є впровадження сучасних цифрових засобів та інтеграція систем відеоспостереження, контролю управління доступом та охоронної сигналізації в єдину мережу.

З метою можливості централізованої підготовки фахівців з налаштування, монтажу, обслуговування та ремонту технічних засобів охорони та інтеграції систем ТЗО в єдину мережу з використанням загальних ресурсів, каналів зв'язку, серверів тощо, Головним управлінням НГУ визначено, що при проектуванні та будівництві систем захисту на об'єктах військових частин використовувати системи відеоспостереження на базі обладнання HIKVISION.

Підрозділами Національної гвардії України доцільно використовувати сучасні цифрові системи відеоспостереження HIKVISION у повсякденній діяльності (спостереження за об'єктами частини, несенням служби внутрішніх нарядів і варт та т.п.) та при виконанні завдань з охорони громадського порядку (підключення та взаємодія до міської системи відеоспостереження, встановлення відеокамер для трансляції відео з місць проведення масових заходів, використання персональних відеореєстраторів та застосування доступу до систем відеоспостереження подій з пред'явленням інформації на пунктах управління).

УДК 004.023

Воробйов Є.С., ад'юнкт, Харківський національний університет Повітряних Сил імені Івана Кожедуба, капітан; **Павленко М.А.**, доктор технічних наук, доцент, начальник кафедри, Харківський національний університет Повітряних Сил імені Івана Кожедуба, полковник; **Черток О.А.**, ад'юнкт, Харківський національний університет Повітряних Сил імені Івана Кожедуба, капітан; **Гладишев М.Г.**, начальник групи, Харківський національний університет Повітряних Сил імені Івана Кожедуба, капітан

ОБҐРУНТУВАННЯ МЕТОДУ АВТОМАТИЗАЦІЇ ПРОЦЕСУ РОЗРАХУНКІВ ОПТИМАЛЬНОГО МАРШРУТУ ДЛЯ УДАРНОЇ АВІАЦІЇ ПОВІТРЯНИХ СИЛ ЗС УКРАЇНИ

В умовах стрімкого розвитку озброєння і військової техніки, та постійній автоматизації оперативно-тактичних розрахунків, постає питання з оптимізацією, оперативності та обґрунтованості по визначенню маршруту польоту ударної авіації в умовах які зміни обстановки, в реальному масштабі.

Розрахунок маршруту польоту ударної авіації складається з надійністю орієнтування і виводу на основну та запасну ціль з вигіднішим напрямком в зазначений час, необхідність забезпеченням найменших витрат палива, необхідність прихованого польоту над територією противника, з урахування рельєфу місцевості і стану погоди, та кількістю програмованих точок маршруту польоту, всі ці розрахунки і умови при виборі маршруту впливають на час, оптимальність та вірність вибору маршруту польоту повітряного об'єкту, для успішного виконання бойового завдання. В процесі цих розрахунків необхідна автоматизація процесу визначення маршруту, що надасть покращення часових характеристик та зменшить похибки у результаті неавтоматизованих розрахунків.

Розвиток автоматизації у військовій сфері, безпосередньо впливає на підвищення боєздатності військ, що тягне за собою збільшення процента успішного виконання поставлених задач покладених на Збройні Сили України. Розглядаючи завдання, які за допомогою автоматизації вирішуються на пунктах управління, можуть скоротити час на прийняття рішення та зменшити помилки в процесі розрахунків, що істотно відобразиться на результаті виконаного завдання.

Досягнення результату полягає у виборі методу рішення задачі визначення маршруту польоту ударної авіації. Одним з запропонованих методів є метод з використанням клітинного автомату (КА), в пошуку оптимального маршруту повітряного об'єкту. Клітинний автомат являє собою дискретну динамічну систему, яка складається з сукупності однакових клітин, розміщених на клітинній решітці, а кожна клітина являє собою кінцевий автомат, стан якої

визначається по стану сусідніх клітин, а також її станом. Визначальним фактором є те, що КА дозволяє імітувати живі системи, наприклад політ повітряного об'єкту у просторі, з метою виконання покладеного завдання. Але головна відмінність від інших методів, які орієнтовні на вирішення однокритеріальних задач, метод з використанням клітинного автомату дає можливість розв'язувати багатокритеріальні задачі. Відносно простий математичний апарат формалізації функціонування КА і багатий набір правил їх функціонування дозволяє описати складну модель діяльності в різноманітних умовах .

Таким чином, для автоматизації вирішення поставлених завдань, доцільно використання методу з використанням КА, який надасть збільшення процента успішного виконання поставлених задач покладених на Повітряні Сили Збройних Сил України.

УДК. 681.772

Воронін О.І., старший викладач кафедри управління діями підрозділів із засобами військового зв'язку Національної академії Національній гвардії України

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ В ЧАСТИНАХ ТА З'ЄДНАННЯХ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ СПЕЦІАЛЬНОГО ПОЛЬОВОГО ТЕЛЕКОМУНІКАЦІЙНОГО КОМПЛЕКТУ

Комплект супутникового зв'язку «TOOWAY» забезпечує потреби системи управління НГУ при виконанні службово-бойових завдань в зоні АТО та в повсякденній діяльності. Комплект з'єднав польовий компонент системи зв'язку та інформатизації НГУ з її стаціонарною цифровою мережею, забезпечуючи утворення необхідної кількості телефонних каналів зв'язку та каналів передачі даних.

Виявленні недоліки в конструкції антенної системи комплекту, недостатня кількість абонентів, що обслуговуються, та поява нового більш ефективного обладнання призвели до появи нового СПТК-2.

СПТК-2 призначений для забезпечення відкритого телефонного зв'язку та передачі даних, а також надання телекомунікаційного ресурсу мережам спеціального зв'язку та є закінченим телекомунікаційним пристроєм.

До складу комплекту СПТК-2 в залежності від варіанту поставки можуть входити:

- антена супутникового зв'язку АС-0,75;
- RT4000N передавач Consumer TRIA-1IFL;

- супутниковий модем RM4100N-016-IFL;
 - телекомунікаційний модуль у складі маршрутизатора Cisco 880; комутатора Cisco Catalyst 2960; VoIP шлюзу Grandstream; G/SHDSL Bis модему/маршрутизатора 2-проводового DYNAMIX (з 4-портовим комутатором); міні-серверу керування та конфігурування ТК, SIP-телефонії; медіаконвертеру TP-Link MC100CM;
 - модуль електроживлення PSU ТК2-4 з АКБ та інвертором 12-24В та 220В; СПТК-2 забезпечує:
 - маршрутизацію та комутацію пакетів в інформаційно-телекомунікаційних мережах з підтримкою стеку протоколів TCP/IP;
 - підтримку технології VLAN IEEE 802.1Q Ethernet;
 - динамічну маршрутизацію пакетів за протоколом BGPv4, OSPFv2, RIPv2;
 - підтримку технології підміни IP-адрес (NAT) на портах підключення каналів передачі даних до інформаційно-телекомунікаційної мережі;
 - кодування аналогових телефонних сигналів у цифрові пакети з використанням аудіокодеків G.711 (основний), G.723.1, G.729A/B, G.726 і LBC;
 - маршрутизацію телефонних викликів між підключеними телефонами та відповідним SIP-сервером за протоколом SIP;
 - організацію модемної лінії зі швидкістю до 5,6 Мбіт/сек по мідній парі;
 - організацію супутникової лінії зв'язку з L Band Input 1000 - 1500 MHz (Ka) та S Band Output 1880 - 2300 MHz (Ka).
- СПТК-2 дає змогу забезпечити зв'язок в польових умовах більшій кількості абонентів, забезпечити проведення відеоконференцій. Використання комплекту на ПУ з'єднань і частин НГУ суттєво підвищить надійність, мобільність та пропускну здатність системи управління НГУ.

УДК 621.396

Герасимов С.В., доктор технічних наук, старший науковий співробітник, провідний науковий співробітник науково-дослідного центру Харківського національного університету Повітряних Сил імені Івана Кожедуба;
Тимочко О.І., доктор технічних наук, професор, професор кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба

МЕТОДИ ТА ЗАСОБИ КОНТРОЛЮ ТЕХНІЧНОГО СТАНУ БЕЗПЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

Результати проведення антитерористичної операції на сході України та інші збройних конфліктів, що відбулися останнім часом в світі, свідчать про підвищення ролі безпілотних літальних апаратів (БПЛА) у вирішенні завдань

тактичного та оперативно-тактичного рівнів. Однак, відсутність дієвої системи контролю та діагностування технічного стану БПЛА призводили до численних „не бойових” втрат апаратів із-за несвоєчасного виявлення відмов. Отже, наукова задача синтезу вимірювальних сигналів для визначення технічного стану БПЛА з метою підвищення їх надійності та боєздатності є актуальною.

Основою контролю технічного стану БПЛА є дослідження динамічних характеристик їх складових елементів, особливо радіоелектронного обладнання (РЕО). Для цього на вхід РЕО БПЛА діють відомим вимірювальним (тестовим, випробувальним) сигналом, який формується генератором тестових сигналів (засобом вимірювальної техніки) і має певні характеристики. Під впливом вхідного вимірювального сигналу на виході РЕО БПЛА утворюється вихідний сигнал (сигнал-відгук), або реакція певної форми залежно від форми вхідного сигналу та параметрів РЕО. Вхідний вимірювальний сигнал і вихідний сигнал РЕО подаються в аналізатор (засіб вимірювальної техніки), за допомогою якого визначаються параметри контролю або параметри, що отримані після проведення контролю (апостеріорні параметри контролю), значення яких дозволяють визначити технічний стан апарату.

Обґрунтовано, що при заданому часі контролю (кількості точок відліків) параметрів РЕО БПЛА, точності засобів вимірювальної техніки (рівня перешкод), що застосовуються при контролі, визначення оптимальної для даної кількісної оцінки методики контролю полягає у знаходженні параметрів такого вхідного вимірювального сигналу (синтезу вимірювального сигналу), який забезпечує найбільше або найменше значення цієї оцінки.

Запропоновано за такі оцінки використовувати кількісні оцінки якості контролю: чутливість, точність, кількість вимірювальної інформації. Тому, при оптимізації за чутливістю вхідний сигнал повинен забезпечувати найбільше значення чутливості, при оптимізації за точністю параметри вимірювального сигналу повинні приводити до найменшого значення похибки вимірювання.

Показано, що розв'язання задачі синтезу вимірювальних сигналів дозволяє також визначити вхідний сигнал, який забезпечує при заданому значенні оцінки мінімальний час контролю, що призводить до підвищення оперативності проведення операцій визначення технічного стану РЕО БПЛА, тобто підвищує їх коефіцієнт готовності.

Таким чином, синтез оптимального вхідного вимірювального сигналу при контролі технічного стану РЕО БПЛА зводиться до вирішення варіаційної задачі знаходження найбільшого (найменшого) значення деякого функціоналу в класі вхідних сигналів. Обґрунтовані математичні моделі обмежень щодо синтезу вхідних вимірювальних сигналів.

Розроблені методики синтезу (визначення параметрів) оптимальних вимірювальних сигналів для визначення технічного стану РЕО БПЛА при інтегральних і локальних обмеженнях.

УДК. 681.772

Глущенко М.О., старший викладач кафедри управління діями підрозділів із засобами військового зв'язку Національної академії Національній гвардії України.

ОСОБЛИВОСТІ ПРОВЕДЕННЯ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ЦИФРОВИХ ЗАСОБІВ ЗВ'ЯЗКУ

Основні зусилля з розвитку техніки зв'язку спрямовуються на модернізацію системи зв'язку тактичної ланки управління, тобто сегменту системи зв'язку, який безпосередньо використовується при веденні бойових дій та при виконанні інших службово-бойових завдань підрозділами Національної гвардії України.

Незважаючи на те, що укомплектованість військових частин Національної гвардії України цифровими засобами зв'язку складає більше 50% існує розрив між науково-технічними досягненнями в сфері цифрових засобів зв'язку і практичними рекомендаціями щодо методики проведення технічного обслуговування, і в першу чергу, це пов'язано з відсутністю повної технічної документації на зарубіжні зразки техніки, а забезпечення високої боєготовності та експлуатаційної надійності засобів зв'язку командири підрозділів вирішують самостійно, відсутній практичний комплексний підхід щодо проведення технічного обслуговування цифрових засобів зв'язку.

Перелік та зміст операцій, які проводяться під час технічного обслуговування засобів зв'язку, визначаються для кожного зразка особисто. Вони залежать від складності та надійності засобу зв'язку, особливостей конструкції, потрібної боєздатності та безвідмовності функціонування, а також зовнішніх умов, під впливом яких знаходиться засіб зв'язку в процесі бойового використання.

Для більшості цифрових засобів зв'язку можна виділити наступний, найбільш характерний, перелік видів технічного обслуговування: щоденне технічне обслуговування, щотижневе технічне обслуговування, технічне обслуговування за необхідності, позапланове технічне обслуговування.

Для щоденного технічного обслуговування цифрових засобів зв'язку рекомендується проведення самотестування радіостанції (згідно вбудованих тестів), а для щотижневого – періодичний візуальний огляд і очищення без їх розкриття.

Технічне обслуговування за необхідності. Об'єкт перевірки – засоби живлення. Після взаємодії з прісною або солоною водою необхідно від'єднати акумуляторну батарею та промити її чистою прісною водою і витерти насухо м'якою тканиною для запобігання корозії. Якщо має місце корозія, то необхідно очистити контакти за допомогою нейлонового сітчастого абразивного матеріалу або аналогічним. Не намагайтесь чистити позолочені роз'єми радіостанції.

Технічне обслуговування третього рівня (при сервісному обслуговуванні або ремонті) проводиться в наступних випадках:

- користувач виконав вбудовані тести і виявив несправність радіостанції;
- під час роботи радіостанції з'явилося повідомлення про несправність;
- користувач помітив погіршення якості роботи радіостанції.

Для очищення внутрішніх компонентів радіостанції рекомендується ізопропіленовий спирт (70% або 100%), з застосуванням неметалевої коротко шерстної щітки для видалення прилиплих речовин. Для сушіння радіостанції використовується м'яка абсорбуюча не ворсиста тканина.

УДК 629.017

Горєлишев С.А., кандидат технічних наук, доцент, старший науковий співробітник науково-дослідної лабораторії забезпечення службово-бойової діяльності НГУ науково-дослідного центру Національної академії Національній гвардії України; **Баулін Д.С.**, кандидат технічних наук, старший науковий співробітник, старший науковий співробітник науково-дослідної лабораторії забезпечення службово-бойової діяльності НГУ науково-дослідного центру Національної академії Національній гвардії України; **Нікорчук А.І.**, кандидат технічних наук, заступник начальника науково-дослідного центру – начальник науково-дослідної лабораторії забезпечення службово-бойової діяльності НГУ Національної академії Національній гвардії України, полковник

ВИКОРИСТАННЯ ГЕОІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ МАНЕВРНОСТІ БЕЗПІЛОТНИХ АВТОМОБІЛІВ

За останні кілька років у промисловості виробництва безпілотних автомобілів відбувся незрівнянний прогрес. Ряд автовиробників, включаючи Tesla, Fiat, Chrysler, General Motors та інші, активно працюють над створенням нових моделей автомобілів 4 і 5 рівнів автоматизації.

Загальні принципи роботи у всіх безпілотних автомобілів приблизно однакові. До складу обладнання на безпілотному автомобілі входять набір датчиків далекомірів оптичного розпізнавання (LIDAR), системи стереозрення, системи глобального позиціонування (GPS, ГЛОНАСС), гіростабілізації, інерції.

Технології безпілотного автомобіля відносяться до класу задач штучного інтелекту. Деякі технології покладаються на інфраструктурні системи (наприклад, вбудовані в дорогу або біля неї), але більш сучасні технології дозволяють імітувати присутність людини на рівні прийняття рішень про управління машиною і швидкістю, завдяки набору камер, сенсорів, радарів,

геоінформаційних технологій і супутникової навігації.

Безпілотний автомобіль повинен знати з точністю до сантиметрів, де саме він знаходиться і що знаходиться далі на дорозі поза зоною поточної фізичної видимості. Тому використання геоінформаційних технологій, зокрема карт високої точності є фундаментальним елементом на доповнення до сенсорам і камерам для того, щоб безпілотний автомобіль міг орієнтуватися в навколишньому середовищі.

Карти повинні відображати і місце розташування автомобіля, і дозволяти йому знати, що знаходиться далі, за поворотом, чого не можуть забезпечити камери і сенсори. Тоді автомобіль зможе вибудувувати не реактивну, а проактивну стратегію водіння.

Однак рішення даної задачі досить трудомістким. Якщо для тестування безпілотних автомобілів ще можливо попередньо побудувати детальні 3D-карти на пілотних маршрутах, що враховують навіть невеликі особливості доріг, то коли потрібно створити карти для доріг протяжністю в мільйони кілометрів, дана задача виглядає складно реалізованою. Крім того, одного разу створені карти необхідно підтримувати і оновлювати, так як картина на дорогах може змінюватися дуже часто. Спростити створення точних карт для автомобілів може співробітництво з автовиробниками: їх машини, оснащені сенсорами і радарми, можуть "ділитися" одержуваною з доріг інформацією з розробниками картографічних сервісів. За рахунок цього карти могли б оновлюватися буквально в режимі реального часу.

Таким чином, одна з ключових завдань для безпілотних автомобілів – забезпечення їх можливостями високошвидкісного мережевого підключення. Мережі п'ятого покоління (5G) розглядаються як драйвер технологій автономного водіння: вони дозволять автомобілю максимально оперативно отримувати інформацію і взаємодіяти з іншими автомобілями і навколишнього його інфраструктурою. Мінімальні затримки передачі інформації, які очікуються в 5G, не перевищать 4 мс (для 4G LTE цей значення становить близько 20 мс). Для комунікації з оточуючими об'єктами також розробляються спеціальні системи, що дозволяють автомобілю обмінюватися даними з іншими об'єктами.

УДК 355.422.21: 519.172.3

Горелишев С.А., кандидат технічних наук, доцент, старший науковий співробітник науково-дослідної лабораторії забезпечення службово-бойової діяльності НГУ науково-дослідного центру Національної академії Національній гвардії України; **Баулін Д.С.**, кандидат технічних наук, старший науковий співробітник, старший науковий співробітник науково-дослідної лабораторії забезпечення службово-бойової діяльності НГУ науково-дослідного центру Національної академії Національній гвардії України; **Побережний А.А.**, старший науковий співробітник науково-дослідної лабораторії забезпечення службово-бойової діяльності НГУ науково-дослідного центру Національної академії Національній гвардії України, підполковник; **Цис О.І.**, кандидат військових наук, начальник служби планування та аналітики відділу планування Управління бойової та спеціальної підготовки Головного управління Національній гвардії України, полковник

ПРІОРИТЕТНІ НАПРЯМКИ РОЗВИТКУ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СЛУЖБОВО-БОЙОВОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Одним з пріоритетних напрямків удосконалення інформаційно-аналітичного забезпечення службово-бойової діяльності (СБД) частин та підрозділів Національної гвардії (НГ) України є впровадження інформаційно-аналітичних систем (ІАС) на всіх рівнях управління НГ України для динамічного подання й багатомірного аналізу вихідних і поточних даних, аналізу тенденцій, моделювання й прогнозування результатів різних управлінських рішень. ІАС на даний момент виступають як високоефективні інструменти підтримки прийняття рішень. Основними функціями ІАС є:

- витяг з багатьох джерел різномірних даних, представлених у різних форматах, їхнє перетворення до єдиного формату і єдиної структури й завантаження в сховище;
- організація зберігання й надання користувачам необхідної для прийняття рішень інформації;
- безпосередній аналіз і підготовка планової або регулярної оцінки стану управління СБД у вигляді паперових документів або екранних форм;
- підготовка результатів аналізу для ефективного їхнього сприйняття споживачами й прийняття адекватних рішень.

У зв'язку з великим обсягом і складністю аналіз даних має два напрямки:

- оперативний аналіз даних (OLAP-аналіз) – швидке вилучення необхідної аналітики для обґрунтування або прийняття рішення інформації;
- інтелектуальний аналіз інформації (Data Mining) призначений для

фундаментального дослідження проблем, які виникли при СБД НГ України. Вимоги по часу менше жорсткі, але використовуються більш складні методики.

ІАС є надбудовою над уже функціонуючим в НГ України програмним забезпеченням і не вимагають їх заміни, які акумулюють дані по всіх видах діяльності НГ України. ІАС верхнього рівня служать для прийняття стратегічних рішень. Вони дозволять вирішити такі завдання:

– складання консолідованої звітності та подання зведеної інформації про діяльність НГ України в цілому;

– аналіз СБД (основні показники, тенденції, проблеми), підготовка та оптимізація варіантів рішень стратегічного рівня;

– проведення комплексної оцінки діяльності частин і підрозділів НГ України, заснованої на постійному контролі найбільш істотних її аспектів.

ІАС підрозділів передбачають більшу деталізацію і більш складну аналітичну обробку. Ці системи допомагають підготувати інформацію для прийняття рішень при плануванні конкретних заходів СБД.

ІАС по режиму і темпу аналізу підрозділяються на статичні (мають заздалегідь розроблений сценарій обробки даних при досить обмежених можливостях варіацій запитів) та динамічні (забезпечують обробку нерегламентованих запитів і гнучку систему підготовки звітів). Функціонування ІАС НГ України відбувається, як правило, в умовах неповноти інформації, незнання основних закономірностей розвитку подій й постійної зміни множини зовнішніх і внутрішніх факторів. Тому процес формування управлінського рішення має відповідну невизначеність і є багатокроковим.

Данилов Ю.А., Харківський національний університет Повітряних Сил імені Івана Кожедуба; **Медведев В.К.**, Харківський національний університет Повітряних Сил імені Івана Кожедуба; **Павленко М.А.**, доктор технічних наук, доцент, начальник кафедри, Харківський національний університет Повітряних Сил імені Івана Кожедуба, полковник; **Ясинецкий В.П.**, Харківський національний університет Повітряних Сил імені Івана Кожедуба; **Могилатенко А.В.**, Харківський національний університет Повітряних Сил імені Івана Кожедуба

АЛГОРИТМЫ, ОБЕСПЕЧИВАЮЩИЕ СОПРОВОЖДЕНИЯ ТРАЕКТОРИЙ ВОЗДУШНЫХ ЦЕЛЕЙ С УЧЕТОМ ИХ ВОЗМОЖНОГО НЕРАЗРЕШЕНИЯ

Многоцелевой подход к решению задачи сопровождения траекторий воздушных объектов (ВО), предполагает выдвигание и проверку большого количества гипотез совместного и поточечного отождествления отметок.

Количество гипотез, с увеличением числа сопровождаемых траекторий ВО, лавинообразно нарастает.

При разработке и описании квазиоптимальных алгоритмов сопровождения траекторий с учетом их возможного неразрешения не были проанализированы некоторые вопросы, связанные с реализацией этих алгоритмов в реальных системах вторичной обработки РЛИ.

Практически это можно осуществить фиксацией количества тактов обновления информации, в которых не произошло подтверждение гипотезы о классе отметки. Например, если в α смежных тактах обновления информации подряд не было отдельного наблюдения ВО, породивших отметку то принимается решение о том, что она порождена одиночным ВО.

В этом случае, необходимо предусмотреть разделение ВО (размножение отметки). Самый простой способ решения этой задачи состоит в том, что разделяющиеся ВО будут захватываться на сопровождение (обнаруживаться) как одиночные. Другим способом решения задачи может быть известный и применяющийся в системах вторичной обработки метод "размножения траекторий", когда после разделения всем "отдалившимся" траекториям присваиваются значения параметров "общей" траектории с последующим отдельным сопровождением. При построении адаптивного алгоритма сопровождения траекторий ВО с учетом их возможного неразрешения многогипотезная модель траектории движения ВО использовалась в каждом такте обновления информации, независимо от количества отметок, сопровождаемых траекторий. При реализации данного алгоритма в системах вторичной обработки РЛИ, с целью экономии вычислительных ресурсов, можно и целесообразно использовать многогипотезную модель траектории движения ВО после выявления маневра. Одногопотезная модель траектории движения ВО может, в этом случае, послужить основой выявления начала и конца регулярного преднамеренного маневра. При разработке квазиоптимальных алгоритмов ограничение количества выдвигаемых и проверяемых гипотез СО достигалось путем исключения из рассмотрения заведомо ложных гипотез, исходя из потенциальных возможностей современных летательных аппаратов. Дальнейшее уменьшение количества проверяемых гипотез возможно путем введения ограничений на использование многогипотезной модели траектории движения ВО и количество классов отметок. Таким образом, информационному обеспечению траекторий воздушных объектов, обработке радиолокационной информации приводится новое решение задачи разработки эффективных в качественном отношении решающих правил и алгоритмов, составляющих математическую основу процесса сопровождения траекторий воздушных объектов в условиях их плотных потоков и возможного маневра. Задача сопровождения траекторий в

многоцелевої обстановке являється одной из актуальных задач современной радио- и гидролокации. Она имеет различные приложения: в системах управления противовоздушной обороной, воздушным движением, наблюдением за морским пространством.

УДК 004.9:623.618

Дробаха Г.А., доктор військових наук, професор, головний науковий співробітник науково-дослідного центру Національної академії Національній гвардії України; **Лісіцин В.Е.**, науковий співробітник науково-дослідної лабораторії забезпечення службово-бойової діяльності НГУ науково-дослідного центру Національної академії Національній гвардії України

СИСТЕМИ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ У ВИРІШЕННІ СЛУЖБОВО-БОЙОВИХ ЗАВДАНЬ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

У питаннях планування та підготовки військових та спеціальних операцій Національна гвардія України (НГУ) поступово переходить на рішення та стандарти Північноатлантичного альянсу (НАТО). Такі підходи спонукають до застосування сучасних інформаційних технологій отримання та аналізу інформації щодо місцевості проведення операції. В країнах НАТО застосовуються комп'ютерні програмні комплекси, засновані на технологіях імітаційного моделювання бойових дій, з метою зменшення часу на підготовку картографічного матеріалу та штабних документів. Це дозволяє автоматизувати вирішення, наприклад, наступних задач на полі бою та у штабній роботі:

- вибір цілей та високоточне наведення у системах автоматичного та автоматизованого управління вогнем;
- відстеження трас спеціальних перевезень та вирішення логістичних завдань і завдань матеріально-технічного забезпечення підрозділів;
- отримання координат розташування підрозділів на полі бою;
- побудова зон ізоляції районів хімічного забруднення та екологічних катастроф і розташування підрозділів уздовж периметрів таких зон.

В Україні вже проводяться роботи по втіленню подібних технологій у службово-бойову діяльність Збройних Сил України (ЗСУ). На Львівщині відкрито центр імітаційного моделювання бойових дій, де готуватимуться штаби рівня батальйон-бригада, та проводитимуть комп'ютерні навчання військових. Збудували його коштом міністерства оборони, а обладнання закупили партнери зі США із загальним кошторисом 22 млн. доларів. В ході планування прийняття рішення, та контролю проведення навчань, у центрі

готуватимуться штаби рівня батальйон-бригада (механізовані, танкові, високомобільні десантні війська і частини ЗСУ), проводитимуться командно-штабні комп'ютерні навчання рівня «рота-бригада», впроваджуватимуться в процес підготовки та повсякденну діяльність підрозділів сучасні інформаційні технології та системи віртуального моделювання.

Ще одним прикладом є центр імітаційного моделювання у Харківському національному університеті Повітряних Сил імені Івана Кожедуба, призначений для моделювання бойових дій військових частин (підрозділів) Повітряних Сил ЗСУ та проведення розрахунків їх бойових можливостей в ході воєнно-спеціальної гри з науково-педагогічними працівниками, тактико-спеціальних та навчальних занять, комп'ютерних тренувань з курсантами університету, офіцерів тактичної ланки управління, що проходять перенавчання і підвищення кваліфікації. Діяльність центру спрямована на вирішення спеціалізованих завдань в інтересах Повітряних Сил ЗСУ.

Більш універсальним, та близьким до завдань НГУ є центр імітаційного моделювання. Національний університет оборони України імені Івана Черняхівського. Центр є головним елементом систем моделювання Збройних Сил України, на який покладаються завдання організації, координації та методичного забезпечення заходів з впровадження технологій імітаційного моделювання в систему підготовки військових фахівців. Серед іншої інформації, що розмішена на сайті центру є система графічних символів та позначень НАТО, порядок роботи з картою за стандартами НАТО та бібліотека стандартних алгоритмів імітаційного моделювання бойових дій. У поєднанні із можливостями геоінформаційних технологій та геопросторового аналізу даних такої набір алгоритмів може стати потужним інструментом для забезпечення підрозділів НГУ.

УДК 623.765:681.513.6

Зусь П.П., кандидат технічних наук, командування Повітряних Сил Збройних Сил України; **Тімочко О.О.**, фірма “ХХІ століття”, м. Гамбург

МЕТОД ФОРМАЛІЗАЦІЇ ЗАДАЧІ СИТУАЦІЙНОГО АНАЛІЗУ У ПОВІТРЯНОМУ ПРОСТОРИ

Результати військових конфліктів у світі та проведення антитерористичної операції на сході України показали, що збільшені можливості сил і засобів повітряного нападу противника (як пілотованих, так і безпілотних засобів) приводять до необхідності своєчасного та достовірного розпізнавання повітряної ситуації черговими силами повітряного командування (ПвК) у

секторі прикриття повітряного простору.

Основною метою розпізнавання ситуацій є віднесення їх формалізованих описів до відповідних класів. Автоматизація процедур розпізнавання повітряних засобів (ПЗ) у повітряному просторі є елементом автоматизації прийняття рішень. За наслідками розпізнавання ситуацій приймаються рішення про застосування чергових сил ПвК.

У доповіді задані класи на безлічі рішень і розпізнаних ситуацій. Встановлена однозначна відповідність між класами. Для розпізнавання ситуацій у повітряному просторі пропонується побудова сукупності моделей, що відображають уявлення про повітряну обстановку в зоні відповідальності ПвК. Запропонований підхід до розпізнавання повітряної ситуації є удосконаленням відомих методів теорії розпізнавання та теорії інтелектуальних систем. Він відрізняється виявленням ступеня небезпеки ситуацій, що складаються, у повітряному просторі на основі застосування апарату нечітких множин і методу аналізу ієрархій.

Показано, що поточні дані про повітряну обстановку у межах відповідальності ПвК поступають від засобів радіолокаційного та диспетчерського контролю.

Засоби радіолокаційного контролю за наслідками кожного огляду повітряного простору формують і видають з мінімальною затримкою координатні, часові дані та приналежність по кожному з повітряних об'єктів.

Значна частина даних, що використовуються при розв'язанні поставленої задачі, недоступна у формі точних, чітко визначених чисел.

Отже, похибки методу та засобів вимірювань, суб'єктивізм особи, що приймає рішення, у контурі обробки даних тощо є основними джерелами невизначеності при рішенні поставленої задачі. Тому наявність методів прийняття та аналізу невизначеності (у тому числі суб'єктивною) є необхідною умовою рішення задачі розпізнавання.

Сформульовані особливості запропонованого методу розпізнавання ситуацій у повітряному просторі.

Завдання розпізнавання ситуацій характеризуються невизначеною класифікацією. Тому правомірно говорити лише про ступінь приналежності розпізнаваної ситуації. Це може бути враховано тільки у рамках нечіткої класифікації, що описує нечіткі межі між класами. Згідно логічному підходу, значення істинності розглядаються як ступінь приналежності розпізнаваної ситуації деякому класу. Тому запропонований підхід до введення нечіткої логіки. Вона забезпечує ефективну обробку якісної інформації нарівні з чіткими, кількісними даними при оцінці ситуацій.

Показано, що використання нечіткої логіки і логічних висновків у моделях складних систем забезпечує спілкування з користувачем на професійно-орієнтованій мові, зберігання, накопичення, обробку якісної інформації.

УДК 623.55.02

Юхов О.Ю., кандидат технічних наук, доцент, старший науковий співробітник, начальник кафедри інформатики та прикладних інформаційних технологій Національної академії Національній гвардії України, полковник; **Малюк В.Г.**, кандидат технічних наук, доцент, доцент кафедри інформатики та прикладних інформаційних технологій Національної академії Національній гвардії України

МЕТОД ОПТИМІЗАЦІЇ РОЗВІДЗАХИЩЕНОСТІ РАДІООБМІНУ В МЕРЕЖАХ ЗВ'ЯЗКУ УГРУПУВАНЬ ВІЙСЬК (СИЛ) НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Серед тенденцій розвитку сучасних засобів радіоелектронної боротьби активності набувають технічні рішення, пов'язані з використанням наземних мобільних та повітряних засобів радіорозвідки, у задачі яких входять сканування, перехоплення, оцінка, виявлення, аналіз, класифікація та моніторинг радіопередач, які характеризуються високою мобільністю, короткочасністю, сучасними видами сигналів і частими змінами їх параметрів.

Література за даною тематикою, в основному, присвячена питанням радіомаскування (РМ) окремих радіостанцій, а не систем радіозв'язку військового призначення в цілому.

Запропонований критерій достатності функціонування засобів активного та пасивного радіомаскування, який визначає правило прийняття рішення щодо можливості використання наявних засобів для здійснення радіомаскування у визначеній точці оперативного простору та визначається як сукупність вимог електромагнітної сумісності засобів постановки навмисних завад з засобами радіозв'язку угруповань військ (сил) за умов виконання завдання придушення корисного сигналу у визначених точках траєкторії пересування засобу радіорозвідки противника.

Критерій дозволяє формалізувати процес визначення достатніх умов функціонування засобів активного та пасивного радіомаскування у залежності від просторового розташування засобів радіорозвідки противника.

Розроблений метод оцінки стану радіозв'язку в умовах застосування радіомаскування, основою якого є імітаційна модель радіообміну в процесі функціонування засобів радіомаскування при зміні просторового розташування та орієнтації спрямованих антен засобів захисту. Метод дозволяє оцінити стан радіозв'язку в будь-якій точці оперативного простору, враховуючи характеристики тривимірних діаграм спрямованості додаткових антенних пристроїв, визначати оптимальну орієнтацію засобів активного радіомаскування залежно від просторового розташування радіомережі та засобів радіорозвідки противника.

Запропонований метод оптимізації параметрів елементів активного радіомаскування систем та комплексів угруповань військ (сил), який дозволяє визначити реальні зони розміщення засобів активного радіомаскування з урахуванням параметрів систем і комплексів радіозв'язку, особливостей оперативного розташування радіозасобів, характеристик наявних антенних пристроїв постановників завад маскування, а також максимізувати кількість подавлених точок траєкторії пересування засобу радіорозвідки противника для визначеного розташування елементів активного радіомаскування.

УДК. 372.862

Казіміров О.О., кандидат військових наук, доцент, доцент кафедри управління діями підрозділів із засобами військового зв'язку Національної академії Національної гвардії України; **Куртов А.І.**, кандидат технічних наук, доцент, професор кафедри загальновійськових дисциплін Національного юридичного університету імені Я.Мудрого

НАВЧАЛЬНИЙ ТЕЛЕГРАФНИЙ КЛЮЧ, СУМІСНИЙ З ПЕРСОНАЛЬНОЮ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЮ МАШИНОЮ

Підготовка фахівця слухового радіотелеграфного зв'язку включає три основні завдання: навчити приймати на слух знаки азбуки Морзе; навчити передавати телеграфним ключем знаки азбуки Морзе; навчити порядку та правилам ведення зв'язку в слуховому радіотелеграфному режимі. Достовірний прийом інформації в слуховому радіотелеграфі залежить не тільки від майстерності того, хто приймає на слух але й від якості передачі ключем того хто передає цю інформацію. Тому, завдання навчити радиста якісній передачі телеграфним ключем є не менш важливим ніж навчити радиста достовірно приймати знаки азбуки Морзе.

Для підвищення ефективності навчання спеціалістів радіотелеграфного зв'язку передачі знаків азбуки Морзе телеграфним ключем пропонується впровадження та використання навчального телеграфного ключа, сумісного з персональною електронно-обчислювальною машиною.

Пропонуємий зразок телеграфного ключа зібраний на базі телеграфного ключа з фільтром зразка 1972 року. Корпус ключа має дві частини: верхню та нижню. У верхній частині розташовані механічні елементи класичного телеграфного ключа Морзе. В нижній частині замість плати з фільтром розташована плата управління від комп'ютерного маніпулятора типу "Миша" з кабелем, що має інтерфейс типу USB.

На верхній частині ключа змонтований звуковипромінювач. Мінусовий вихід

звуківипромінювача під'єднаний до “мінусового” контакту USB-роз'єму, а плюсовий – до “плюсового” контакту USB-роз'єму через робочий контакт та пружину класичного телеграфного ключа Морзе, розташованого у верхній частині. При натисканні на головку ключа створюється замкнутий ланцюг та на звуківипромінювач подається напруга який видає коливання звукової частоти.

Живлення на USB-роз'єм може подаватися як при підключенні його до USB-порту ПЕОМ, так й при підключенні його до USB-роз'єму стандартного телефонного зарядного пристрою.

Сумісність навчального телеграфного ключа з ПЕОМ забезпечується завдяки єдиному стандартному драйверу, що входить в операційну систему Windows. При підключенні ключа проходить автоматичне його налаштування та ПЕОМ сприймає його як маніпулятор типу ”Миша”.

Змонтований на корпусі навчального телеграфного ключа звуківипромінювач дозволяє навчаємому у процесі навчання передачі телеграфним ключем знаків азбуки Морзе контролювати на слух якість своєї передачі, при цьому ключ може використовуватися як сумісно з персональною електронно-обчислювальною машиною, так й окремо при живленні від стандартного телефонного зарядного пристрою.

УДК37.013:355.23:351.746.1

Корєхов А.О., старший викладач кафедри транспортних засобів та спеціальної техніки Національної академії Державної прикордонної служби України імені Богдана Хмельницького

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В СИСТЕМІ АВТО ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ.

Розвиток та інтенсифікація навчального процесу змушує науковців постійно працювати над дослідженням, які характеризуються моніторингом існуючого стану, а також впровадженням сучасних технологій в навчальний процес. Не винятком є і ВВНЗ, актуальність яких, враховуючи ситуацію в країні, зросла.

Сучасна модель охорони включає широке застосування транспортних засобів (ТЗ), як складову мобільної, оперативно-розшукової одиниці. Тому у структурі ДПСУ використовується система авто технічного забезпечення (АТЗ). Система авто технічного забезпечення це сукупність органів управління військових частин і установ автомобільної служби (ремонтних, евакуаційних органів, органів забезпечення, навчальних та науково-випробувальних) від центру до підрозділу, які об'єднані єдиними цілями і діють на основі спільних принципів.

Секція 5. Актуальні проблеми зв'язку та інформатизації службово-бойової діяльності Національної гвардії України

В свою чергу, АТЗ - це комплекс заходів із оснащення військових частин автомобільною технікою і автомобільним майном, підтримання автомобільної техніки у стані, який забезпечує постійну готовність підрозділів до раптово виникаючих. Майбутні бакалаври автосправи повинні чітко усвідомлювати ці задачі і в процесі навчання отримувати необхідні знання, які забезпечать якісну професійну діяльність в підрозділах ДПСУ.

Враховуючи реалії сьогодення, та виклики, які стоять перед країною, постійним інформаційним тиском, яке чиниться на суспільство та масові інформаційні атаки, змушують постійно вдосконалювати систему підготовки високоякісних фахівців у будь якій сфері для забезпечення якісного та безпечного існування суспільства. Не винятком є і майбутні бакалаври автосправи, які повинні отримувати сучасні новітні знання і в подальшому вміло їх застосовувати у професійній діяльності. Тому є нагальна потреба інтенсифікувати навчальний процес інформаційно-комунікативними технологіями та забезпечити інформаційний розвиток майбутніх бакалаврів автосправи в процесі навчання професійно-орієнтованих дисциплін.

Важливо відзначити, що у кожному навчального закладу закладі існує своя специфіка використання програмного забезпечення у процесі формування професійних якостей особистості. Але для ВВНЗ дана специфіка не може в повному обсязі забезпечити ті якості які повинні мати майбутні бакалаври автотранспорту, адже в процесі підготовки повинні використовуватись спеціальне програмне забезпечення притаманне тільки для військової структури. Важливо зазначити що майбутні випускники у ВВНЗ отримують і цивільну спеціальність, а тому повинні використовувати типові ПЗ для більшості навчальних закладів які готують майбутніх бакалаврів автосправи.

Проаналізувавши кваліфікаційні характеристики, які ставляться до випускників, доцільно зауважити, що випускник повинен володіти певним логічно завершений обсяг знань, необхідний для виконання практичної роботи. Це досягається інтенсифікацією навчального процесу та включення в аудиторну роботу завдань пов'язаних з роботою в спеціалізованому програмному забезпеченні. Тому важливим є активне і широке застосування освітніх технологій у вищій професійній освіті, як засіб підвищення педагогічної майстерності викладачів та ефективної діяльності курсантів у досягненні більш високих освітніх результатів, розширення можливостей щодо вибору найефективніших способів вирішення завдань професійної освіти відповідно державним стандартам.

УДК 035

Косюк В.П., старший викладач кафедри військово-спеціальних дисциплін Київського факультету Національної академії Національної гвардії України

ЗАСТОСУВАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ КОМПЛЕКСІВ УПРАВЛІННЯ РЕСУРСАМИ В СИСТЕМАХ УПРАВЛІННЯ БОЄМ

Виконання покладених на Національну гвардію України задач та участь в проведенні антитерористичної операції на Сході країни вимагає чіткого налагодження системи зв'язку та застосування автоматизованої системи управління військами (АСУВ), оскільки військовий зв'язок є невід'ємною складовою частиною управління військовими частинами та підрозділами, його матеріальною основою

Системи управління боєм – це потужний інструмент для попереднього планування військово-польових операцій, швидкого розповсюдження розвідувальної інформації та оновлених фотопланів між учасниками, а також оперативного керівництва структурними одиницями на місцевості в режимі, що максимально наближений до реального часу.

Головна сфера застосування – покращення взаємодії при виконанні польових завдань військовими підрозділами. Велику увагу приділяється питанням безпеки, шифрування і аутентифікації користувачів, що в комплексі з автономною системою польової передачі даних робить систему незамінним інструментом в реальних бойових умовах.

Основна функціональність комплексу – це взаємне відображення користувачів на карті місцевості, використовуючи систему визначення положення, автоматична синхронізація між користувачами завданих ними об'єктів (таких як: мітки дружніх, ворожих, нейтральних і інших юнітів; області на карті, нанесені за допомогою різних геометричних фігур; поточні цілі для кожного з користувачів; маршрути руху та іншої інформації), а так само установка цілей і віддача оперативних цілевказань одних користувачів іншим користувачам, розмежування їх прав, управління одне одним, видимість об'єктів на карті на основі певної ієрархічної структури підрозділів.

Особливістю комплексу є система шарів, тригерів і скриптова мова, що дозволяють автоматизувати процес на програмному рівні, а саме дає можливість:

- заздалегідь нанести плани різних етапів заходу на різні шари, кожен з яких можна приховувати і відображати окремо в потрібний момент, а також присвоїти їм різні права видимості;
- автоматично змінювати інформацію на мапі та давати цілевказівки користувачам на основі інформації про їхнє становище в просторі та взаємодії з

об'єктами на карті за допомогою тригерів і гнучкої скриптової мови.

Для повноцінної роботи системи необхідно бездротове з'єднання між додатком і сервером. Однак додаток може працювати і автономно як звичайний офлайн навігатор без синхронізації даних між користувачами, або в режимі прямого обміну даними між клієнтськими пристроями (P2P), але з обмеженими можливостями. Бездротове з'єднання з сервером в автономному або P2P режимі необхідно тільки для первинного завантаження карти місцевості. Додаток оптимізовано для роботи на низькошвидкісних і нестабільних з'єднаннях.

Кротов В.Д., провідний науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут

ІНФОРМАЦІЙНА СИСТЕМА ОБРОБКИ ДАНИХ ЯК ОСНОВА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ СИСТЕМИ УПРАВЛІННЯ ЗВ'ЯЗКОМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

При виробленні і прийнятті рішень в системі управління зв'язком спеціального призначення (СУЗ), що відповідають обстановці зі зв'язку, основну роль грає їх обґрунтування за наявною інформацією, яка повинна задовольняти вимогам повноти, достовірності, адекватності, несуперечності. В інтересах вироблення адекватного рішення використовуються як внутрішні, так і зовнішні по відношенню до об'єкта управління інформаційні ресурси. Ці обставини змушують використовувати наявні у даний час розвинені програмно-технічні засоби і нові інформаційні технології для створення системи підтримки прийняття рішення (СППР).

Широке і ефективне застосування цих засобів на пунктах управління зв'язком різних рівнів стає необхідною складовою для прийняття обґрунтованих рішень в СУЗ.

Процес прийняття рішення зі зв'язку ускладнюється тим, що він проходить у наступних специфічних умовах:

- величезних обсягів довідкової та розпорядчої інформації;
- неповноти і суперечності інформації з різних джерел;
- різноманітності форм представлення даних;
- коротких термінів на прийняття рішення;
- унеможливлення помилки прийнятого рішення;
- високий ступінь взаємозалежності посадових осіб при обміні інформацією.

Сучасний рівень розвитку апаратних і програмних засобів дозволяє ведення баз даних оперативної інформації на всіх рівнях управління. В процесі своєї

Секція 5. Актуальні проблеми зв'язку та інформатизації службово-бойової діяльності Національної гвардії України

діяльності в інформаційних системах військового призначення склалася парадоксальна ситуація – інформація начебто є, її навіть забагато, але вона неструктурована, неузгоджена, розрізнена, не завжди достовірна, її практично неможливо знайти і отримати.

Саме на вирішення цього протиріччя – відсутність інформації при її наявності і навіть надлишку – націлена концепція “інформаційної системи обробки даних”. Ця система виконує функції попередньої підготовки і зберігання даних для СППР на основі інформації з системи управління зв'язком (чи баз даних СУЗ), а також інформації із зовнішніх джерел, які завжди є присутніми у достатній кількості впродовж тривалого часу. Дані використовуються в різних режимах для аналізу, як джерел даних для різного роду звітності і обґрунтування управлінських рішень.

У основі концепції інформаційної системи обробки даних (ІСОД) лежать такі ідеї, як інтеграція раніше роз'єднаних деталізованих даних, їх узгодження і можлива агрегація. Предметом розгляду цієї концепції є самі дані.

В результаті концепція ІСОД має такі відмітні риси:

– вона є не концепцією аналізу даних, а концепцією підготовки даних для аналізу;

– вона не зумовлює архітектуру цільової аналітичної системи, а говорить про те, які процеси повинні виконуватися в системі, не конкретизуючи, де конкретно і як ці процеси повинні виконуватися;

– вона припускає не просто єдиний логічний погляд на дані, а реалізацію єдиного інтегрованого джерела даних.

Окрім єдиного довідника метаданих, засобів вивантаження, агрегації і узгодження даних, концепція ІСОД має на увазі інтегрованість, підтримку хронології і узгодженість даних. І якщо перша властивість (інтегрованість) впливає в основному тільки на режими аналізу даних не інтегрованої бази даних, в якій використовуються спеціалізовані методи зберігання і доступу, то останні два (підтримка хронології і узгодженість), істотно звужують список аналітичних завдань, що вирішуються.

Основною вимогою аналітичної обробки даних є не стільки оперативність, скільки достовірність інформації. Але достовірність, і визначається узгодженістю.

У СУЗ проблема узгодженості даних стоїть надзвичайно гостро. Це пов'язано як з асинхронністю модифікації даних, так і відмінностями в трактуванні одних і тих же подій, понять і даних, зміною семантики даних, елементарними помилками при введенні і обробці, частковою втратою окремих фрагментів інформації і таке інше.

Тому, концепція ІСОД визначає лише найзагальніші принципи побудови аналітичної системи СУЗ і в першу чергу сконцентрована на властивостях і

вимогам до даних, а не способах організації і представлення у базах даних.

На основі вище викладеного витікає, що побудова СППР в СУЗ нині необхідно здійснювати на основі побудови інформаційної системи СУЗ, що відповідає вимогам сучасного часу і що повністю задовольняє потребам посадових осіб. При цьому до складу СППР повинен включатися певний набір програмних продуктів.

Метою переходу від традиційних реляційних БД до ІС СУЗ, є підвищення якості інформації, що надається. Для виділення властивостей, що характеризують якість, або ефективність побудови ІСОД СУЗ досить визначити, які властивості складають зміст поняття якості інформації.

У відомому підході пропонується розглядати якість інформації за трьома основними властивостями: повнота, достовірність і оперативність інформації.

Повнота інформації – властивість, що визначає можливість вибірки з бази даних необхідної для прийняття оптимального рішення кількості інформаційних елементів.

Достовірність даних – властивість, що визначає точність даних, що зберігається і обробляється у БД. Достовірність розглядається в двох аспектах: як помилка оцінювання ситуації і як достовірність результатів обробки запитів ІСОД.

Достовірність результатів обробки запитів ІСОД при абсолютно достовірних даних, що зберігаються в ІСОД, залежить від правильного формулювання запиту посадовими особами, від обмежень, що накладаються СУБД і коректності організації логічної структури ІСОД. Як вже відзначалося, в СУЗ нині і в найближчій перспективі використовуються реляційні СУБД, які не в змозі достовірно обробити довільний темпоральний запит в ІСОД. Якщо вважати, що структура ІСОД спроектована правильно і темпоральний запит сформульований коректно, то достовірність обробки запиту залежатиме від правильності роботи алгоритмів маніпулювання даними темпоральної надбудови над реляційною СУБД.

Оперативність обробки даних – властивість, що визначає здатність обробити задану кількість інформації в необхідні часові терміни.

Перелічені вище властивості ІСОД відносяться до властивостей цільового призначення. Разом з властивостями цільового призначення, ІСОД мають властивості складу і структури, технологічні і економічні властивості, а також властивості, які характеризують ресурсоємність її використання.

Таким чином, задоволення пред'явлених вище вимог при проектуванні ІСОД дасть можливість використання ІСОД для рішення завдань організації, планування і оперативного управління зв'язком.

Кротов В.Д., провідний науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут; **Станович О.В.**, начальник науково-дослідного відділу науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут

АНАЛІЗ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ IP В ПОЛЬОВИХ AD-НОС МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Технологія IP являється основний для мережі Інтернет і є набором протоколів, що називається стеком протоколів TCP/IP, а протокол управління передачею – IP-протоколом мережі Інтернет. Саме він реалізує міжмережвий обмін. Головним його достоїнством є те, що стек протоколів TCP/IP забезпечує надійний зв'язок між мережевими обладнанням різних виробників, у зв'язку з чим важливим завданням є оцінка можливості побудови польової мережі зв'язку спеціального призначення на технології IP.

Протоколи стека TCP/IP описують формат повідомлень і вказують, яким чином слід обробляти помилки, надають механізм передачі повідомлень в мережі незалежно від типу вживаного устаткування.

Розглядаючи польові Ad-Нос мережі (Ad-Нос network) необхідно сказати, що Ad-Нос мережа є мережею без інфраструктури, де кожен вузол може працювати як маршрутизатор. У технічній літературі Ad-Нос мережі описуються як безпроводні, динамічні, децентралізовані, не мають постійної структури.

Характерними особливостями Ad-Нос мереж (на відміну від існуючих стільникових і проводових мереж) є: можливість переміщення будь-якого вузла (кожен вузол є кінцевим пристроєм і маршрутизатором); динамічність і значна розмірність мережевої топології; неоднорідність елементів мережі; обмежена потужність і час передачі абонентів; децентралізоване управління та ін.

Застосування протоколу IP дозволяє реалізувати наскрізний моніторинг усієї мережі, починаючи від магістральної транспортної і закінчуючи мережами доступу.

Проте відносно військовому зв'язку слід зазначити наступне. Система зв'язку має бути комбінованою, тобто поєднувати використання мережі зв'язку загального користування і на найбільш важливих інформаційних напрямках лінії прямого зв'язку. Окрім цього, магістральні лінії зв'язку мають бути резервовані шляхом побудови запасних ліній зв'язку і використання заводо- і розвід захищеної апаратури зв'язку інших родів зв'язку, а для забезпечення необхідної стійкості (надійності) системи зв'язку слід передбачити можливість

*Секція 5. Актуальні проблеми зв'язку та інформатизації службово-бойової діяльності
Національної гвардії України*

резервування окремих ліній зв'язку шляхом застосування мобільних ретрансляторів на безпілотних літальних апаратах.

Тут доречно відмітити, що нині МО США відмовляється від технології IP в якості основної з ряду причин:

- реалізація пріоритету тільки по виду трафіку;
- низька надійність;
- недостатня достовірність зв'язку;
- нестабільна своєчасність зв'язку (затримки доставки пакетів до одиниць секунд);
- складнощі при забезпеченні безпеки даних, що передаються системою контролю і управління доступом.

У армійських корпусах США, що брали участь в конфлікті в районі Персидської затоки, для управління використовувалася автоматизована система зв'язку MSE. Вона має підвищену мобільність і будується за принципом поєднання районного зв'язку і прямих ліній зв'язку (командному зв'язку) між пунктами управління. В цілому застосування системи MSE дозволило забезпечити більше 3000 групових і індивідуальних абонентів стаціонарних і мобільних органів управління усіма видами зв'язку.

Застосування принципу командного зв'язку припускає створення мереж зв'язку на базі вузлів зв'язку пунктів управління і прямих ліній зв'язку за підлеглістю. Сильними сторонами мережі командного зв'язку є:

- суворий розподіл відповідальності за зв'язок за підлеглістю;
- спрощене управління системою зв'язку;
- скорочена тривалість розгортання і згортання мережі зв'язку.

Слабкі сторони мережі командного зв'язку:

- зосередження на вузлах зв'язку пунктів управління (ПУ) великої кількості засобів зв'язку;
- низька ефективність використання багатоканальних засобів зв'язку.

Застосування принципу районного зв'язку припускає створення мережі зв'язку загального користування із структурою типу "сітка" на базі районних вузлів зв'язку.

Найважливішими особливостями мережі районного зв'язку є:

- однотипність районних вузлів зв'язку відповідної інстанції управління і однакова кількість каналів зв'язку між ними;
- побудова мережі з комутацією каналів і повідомлень і відсутність закріплених каналів;
- наявність засобів прив'язки безпосередньо на районних вузлах зв'язку;
- робота мобільних абонентів в мережі районного зв'язку за допомогою радіостанцій УКХ діапазону;

*Секція 5. Актуальні проблеми зв'язку та інформатизації службово-бойової діяльності
Національної гвардії України*

– безпосередня наявність управління системою зв'язку в зоні відповідальності, у тому числі централізованого контролю, як однієї з функцій цього управління.

Сильні сторони мережі районного зв'язку:

- ефективніше використання багатоканальних ліній зв'язку;
- наявність великої кількості обхідних каналів зв'язку;
- можливість використання районних вузлів зв'язку усіма підлеглими військами;
- зниження можливостей радіорозвідки противника щодо розкриття бойових порядків військ;
- стійкість структури мережі зв'язку при переміщенні ПУ.

Слабкі сторони мережі районного зв'язку:

- громіздкість, що знижує ефективність проведення динамічних операцій;
- для розгортання мережі районного зв'язку потрібно абсолютне володіння територією;
- уразливість районних вузлів зв'язку від дії з боку розвідувально-диверсійних груп, незаконних збройних формувань та ін.

Мережі командного і районного зв'язку у звичайних умовах розгортаються паралельно, причому їх засоби багатоканального зв'язку повністю сумісні. В умовах обмеженого часу спочатку розгортається мережа командного зв'язку. Польова автоматизована система зв'язку загального користування MSE призначена для управління військами армійського корпусу в районі до 150 км по фронту і до 250 км в глибину.

На ефективність управління негативно впливала і висока концентрація пунктів управління, засобів зв'язку на обмеженій території, що впливало на забезпечення електромагнітної сумісності радіоелектронних засобів, розподіл каналів зв'язку, своєчасне проходження інформації.

Виходячи з вище викладеного витікає, що технологія IP не може бути застосована в якості основної. Переваги цієї технології необхідно використати для побудови IP-мереж третього пріоритету (інформації, що не здійснює безпосередній вплив на характер управлінських рішень командира). А вказані особливості Ad-Hoc мереж вимагають вирішення ряду завдань, пов'язаних з управлінням мережевими ресурсами (радіоресурсом, маршрутизацією, топологією, потоками даних, безпекою та ін.).

УДК 681. 323

Лазарев В.Д. старший викладач кафедри управління діями підрозділів із засобами військового зв'язку Національної Академії національної гвардії України.

СТВОРЕННЯ СУЧАСНОЇ МЕРЕЖІ ОБМІНУ ІНФОРМАЦІЄЮ НА ПОЛІ БОЮ ДЛЯ ЧАСТИН ТА ПІДРОЗДІЛІВ ТАКТИЧНОЇ ЛАНКИ НАЦІОНАЛЬНОЇ ГВАРДІЇ

Сучасне поле бою – це дія, що відбувається в трьох стихіях (на землі, в небі, на воді і під водою), учасниками якого є люди (штаби, польові командири і солдати) і технічні засоби (стаціонарні і мобільні), а сучасна військова доктрина фокусується не на масовості, а на ефективному додатку зусиль для досягнення мети бою. Такий підхід вимагає чіткого розуміння ситуації на полі бою, яке ґрунтується на зборі інформації з максимальної кількості різноманітних джерел в реальному режимі часу. Для реалізації цього підходу кожен учасник бою має бути укомплектований різними облаштуваннями зняття і обміну інформацією (радіоповідомленнями, телефонними дзвінками, відео і зображеннями, телеметрією), а сам обмін повинен відбуватися у безперервному режимі.

Важливість цього обміну настільки висока, що про сучасний бій можна говорити як про то, що відбувається в комунікаційному полі і переможцем з нього вийде той, хто має не лише класичні засоби ведення бою, але також і грошові кошти комунікації. Таким чином, “комунікаційне поле бою” має своїми основними цілями поліпшення управління боєм (своєчасність здійснення бойових маневрів, забезпечення точності вогневої роботи, ефективне використання резервів) на основі обізнаності про поточну ситуацію в кожному секторі і в кожному підрозділі, що бере участь у бою. Воно повинно характеризуватися високою надійністю (безперервне забезпечення зв'язком, застосовністю (вага, розмір, енергоспоживання, універсальністю (передача інформації будь-якого роду), здатністю інтегрувати і бути інтегрованим в різноманітні і різнорідні системи бойового управління.

Реалізація цієї концепції дозволить максимально ефективно використати бойові ресурси для досягнення тактичних і стратегічних завдань.

Насправді, для цього не потрібно винахід нових засобів і механізмів зв'язку. Нинішній рівень розвитку комерційних систем передачі даних дозволяє використати їх у військових цілях без збитку для функціональності, рівня надійності і захищеності, а готові рішення дозволяють переносити їх у військове середовище з мінімальними змінами.

MANET (Mobile Ad Hot Networking) - тип мережі, в якій кожна радіостанція що носить є маршрутизатором і зв'язується з кожною радіостанцією такого типу, що знаходиться в межах видимості. Таким чином формується

багатозв'язкова мережа, яка характеризується дуже високою мірою живучості, - кожен термінал пов'язаний з множиною інших і у нього майже завжди є альтернативний маршрут до будь-якого з терміналів цієї мережі. Механізми організації зв'язності дозволяють ефективно реагувати на появу, зникнення і переміщення "сусідніх" вузлів, забезпечуючи найкращий маршрут (по пропускній смузі, затримці, та ін.) між будь-якою парою вузлів в мережі або до шлюзу в Інтернет. У цій мережі немає централізованого управління (контролера) – мережа самоорганізується, тому вивести її з ладу шляхом знищення контролера неможливо зважаючи на відсутність такого.

Технологія MANET реалізована рядом виробників, у тому числі і корпорацією Harris, радіостанції якої все більше надходять на озброєння Національної гвардії України.

УДК 621.396

Майборода І.М., кандидат військових наук, доцент, завідувач кафедри управління діями підрозділів із засобами військового зв'язку Національної академії Національної гвардії України

ЗАСТОСУВАННЯ ПРИСТРОЇВ АДАПТАЦІЇ СУЧАСНИХ ЦИФРОВИХ ЗАСОБІВ ЗВ'ЯЗКУ ВІТЧИЗНЯНОГО ВИРОБНИЦТВА У СКЛАДІ АПАРАТУРИ ВНУТРІШНЬОГО ЗВ'ЯЗКУ БРОНЕОБ'ЄКТІВ

У зв'язку з широким впровадженням у війська сучасних цифрових засобів зв'язку (ЦЗЗ), вироблених на вітчизняних або іноземних заводах та підприємствах військово-промислового комплексу, гостро постало питання щодо їх пристосовності до умов експлуатації з урахуванням використання на броньованих підрозділах ЗСУ та НГУ. Для забезпечення стійкої роботи ЦЗЗ у складі апаратури внутрішнього зв'язку броньованих об'єктів пропонується використовувати пристрої адаптації вітчизняного виробництва товариства "Доля", що дозволяють застосовувати їх разом із штатними радіостанціями.

Виріб "Либідь ПП-124" – перехідний пристрій комутації цифрової радіостанції транкінгового зв'язку на базі радіостанції Motorola серії DM 4000 до телекомунікаційної мережі броньованого об'єкта. Призначений для з'єднання вхідного/вихідного інтерфейсу радіостанції Motorola серії DM4000 з переговорним пристроєм Р-124 броньованого об'єкта та підсилення сигналу звукової частоти, що надходить від ларингофонів шоломофона.

Виріб "Либідь ПК" – пристрій для дистанційного керування цифровою радіостанцією транкінгового зв'язку на базі радіостанції Motorola серії DM 4000 за допомогою польового телефонного апарату ТА-57. Призначений для

з'єднання вхідного/вихідного інтерфейсу виробу “Либідь К-1А” з телефонним апаратом ТА-57. Забезпечує дистанційне керування виробом “Либідь К-1А” за допомогою ТА-57 на відстані до 500 м.

Імпульсний перетворювач напруги Либідь ПН 24-12. Призначений для організації необхідного електроживлення радіостанції Motorola від бортової мережі 18-30 В броньованого об'єкта. Забезпечує захист від зворотної полярності, перевищення вхідної напруги, перенавантаження.

Виріб “Спеціальний кабель №1” – кабель для комутації цифрової радіостанції Motorola серії DM 4000 до телекомунікаційної мережі броньованого об'єкта. Призначений для з'єднання вхідного/вихідного інтерфейсу радіостанції Motorola серії DM4000 з виробом “Либідь ПП-124” або з переговорним пристроєм Р-124 броньованого об'єкта та підключення живлення до виробу “Либідь АК-2”.

Пристрій налаштування каналів та потужності (ПНКП). Підключається до аксесуарного роз'єму ретранслятора SLR 5500 (SLR 8000) та призначений для перемикання каналів та зміни рівня потужності.

Виріб “Либідь АК-2” – пристрій ВЧ-комутації цифрової радіостанції транкінгового зв'язку на базі радіостанції Motorola» серії DM 4000 до штатної антени броньованого об'єкта. Призначений для забезпечення почергової роботи штатних радіостанцій броньованого об'єкта та радіостанції Motorola серії DM4000 на одну штатну антену АШ-4.

Застосування пристроїв адаптації цифрових засобів зв'язку у складі апаратури внутрішнього зв'язку броньованих об'єктів дозволить використовувати їх в процесі управління підрозділами та частинами НГУ одночасно із штатними радіостанціями та виносними пристроями аналогового зв'язку.

Минько О.В., старший викладач кафедри службово-бойового застосування військових частин Національної академії Національної гвардії України;
Юхов О.Ю., начальник кафедри інформатики та прикладних інформаційних технологій, кандидат технічних наук, доцент

ДЕЯКІ ПИТАННЯ РОЗРОБКИ СТАНДАРТНИХ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ, ЯК ЕЛЕМЕНТУ ОРГАНІЗАЦІЙНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ЦИРКУЛЮЄ У ЕЛЕМЕНТАХ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Національна гвардія України на сучасному етапі розвитку перебуває на шляху реформ. У зв'язку з тим, що одним з пріоритетних напрямків реформування Національної гвардії України є удосконалення системи підготовки органів управління, а також автоматизація їх роботи.

Секція 5. Актуальні проблеми зв'язку та інформатизації службово-бойової діяльності Національної гвардії України

На всіх етапах підготовки бою (операції, службово-бойового застосування), а також в ході управління військами під час виконання поставлених завдань в середині системи управління бригади Національної гвардії України (між структурними підрозділами штабу, між штабом бригади та підлеглими штабами підрозділів бригади) та за її межами (обмін інформацією зі старшим штабом, штабами сусідів, органами управління взаємодіючих ІВФ та ПрО) буде здійснюватись обмін даними, що використовуються в практичній роботі командирів, штабів, начальників родів військ і служб, органів виховної роботи в процесі управління військами.

Разом з тим, не слід забувати про одну з головних вимог до управління військами – скритність управління. Складовими частинами скритного управління військами (силами) є забезпечення безпеки зв'язку та інформації і захист системи управління та протидія технічним засобам розвідки противника. З метою забезпечення безпеки зв'язку та інформації командирами та штабами використовуються апаратні; програмні; криптографічні; організаційні методи захисту інформації.

До організаційних методів захисту інформації можна віднести створення органом управління *профілю захищеності*.

З кожним роком рівень автоматизації управління військ значно збільшується. Все частіше у своїй діяльності органи військового управління застосовують елементи автоматизованих систем.

Автоматизована система (АС) являє собою організаційно-технічну систему, що об'єднує обчислювальну систему (ОС), фізичне середовище, персонал і оброблювану інформацію (Рис.1). Вимоги до функціонального складу комплексу засобів захисту (КЗЗ) залежать від характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми. Вимоги до гарантій визначаються насамперед характером (важливістю) оброблюваної інформації і призначенням АС.

Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.

Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються.

Метою доповіді є загострення уваги на важливості створення стандартних профілів захищеності елементів автоматизованих систем управління військами (АСУВ), що використовуються органами управління у Національній гвардії України на сучасному етапі її розвитку.

УДК 621.391

Обіход Я.Я., аспірант Українського державного університету залізничного транспорту; **Лисечко В.П.**, кандидат технічних наук, доцент, Українського державного університету залізничного транспорту

РОЗРОБКА МЕТОДУ ВИБОРУ КАНАЛІВ КОГНІТИВНОГО РАДІОПРИЙМАЧА ПРИ МНОЖИННОМУ ДОСТУПУ ПЕРВИННИХ ТА ВТОРИННИХ КОРИСТУВАЧІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ «ENERGY HARVESTING» ПІД КЕРУВАННЯМ НЕЙРОННОЇ МЕРЕЖІ

Когнітивний радіоприймач (КР) стає основою частиною телекомунікаційних систем зв'язку (ТСС-ЮЕ) у зв'язку з тим, що здатен вирішити питання дефіциту спектру та впровадження інтелектуальних функцій. Вибір каналу з множинним доступом Первинних користувачів (ПП) та Вторинних користувачів (ВП), є головною проблемою стандарту. Через конкуренцію каналів відбувається взаємний вплив пакетів ПП і ВП. Необхідно розробити метод, який передбачає спільне співіснування користувачів для виключення колізії (впливів) пакетів між ПП та ВП, а також збір даних аналізу спектру ВП для спільного співіснування. Для зменшення конкуренції каналів серед ВП, також розроблено гібридну модель передачі даних під керуванням нейронної мережі для одного ВП. Ця модель, при якій ВП може випадково не регульований чином працювати в двох режимах:

- суміщення з зайнятими каналами з використанням технології «Energy harvesting» (Е.Х.);
- перекриття.

Було розроблено метод на основі конкуренції каналів між ВП, для досягнення мінімальної кількості помилок в каналах з ПП, в мережі КР з безліччю ВП і ПП. На сьогоднішній день немає ефективного вирішення конкуренції каналів між декількома ВП і ПП. Таким чином, ґрунтуючись на методі виявлення та концепцію конкуренції каналів, для вирішення поставлених завдань, отримано можливість поліпшити точність аналізу спектра і пропускну здатність ВП. Також завдяки розробленому методу ВП зможуть «збирати» радіочастотну енергію з зайнятих каналів, використовуючи технологію «Energy harvesting».

Оленченко В.Т., кандидат технічних наук, доцент кафедри інформатики та прикладних інформаційних технологій Національної академії Національної гвардії України, полковник

ПЕРЕВАГИ ТА ВАДИ ТОЧКИ ДОСТУПУ НА БАЗІ ТЕХНОЛОГІЇ WI-FI

При побудові телекомунікаційних мереж і, зокрема, комп'ютерних завжди виникає питання щодо організації “останньої милі” – точки доступу обладнання клієнта до комутуючого обладнання мережі. Таке підключення передбачає як дротове, так і бездротове підключення.

Бездротове підключення можливо реалізувати різними способами:

- за технологією IEEE 802.16 WiMAX;
- за технологією IEEE 802.11 Wi-Fi;
- оптичним бездротовим зв'язком.

До числа переваг бездротового способу підключення можна віднести швидке розгортання мережі, мобільність та можливість підключення значної кількості кінцевих пристроїв.

До числа ж найбільш істотних вад можна віднести:

- обмежений радіус дії, особливо у Wi-Fi – до 100 метрів на штатну антену;
- необхідність враховувати роботу різноманітних електронних приладів – у тому числі побутових;
- простота виявлення роботи даних технологій та можливість отримання несанкціонованого доступу до мережі.

Частково ці проблеми можливо вирішити шляхом застосування різноманітних підсилювачів вихідного сигналу, направлених антен та шляхом грамотного розміщення комутуючого обладнання.

Дещо складніше і у той же час простіше вирішується останнє питання. По-перше, це зменшення радіусу дії технології, що ускладнює процес виявлення її роботи або/також недопущення проникнення зловмисників у зону її дії.

Недопущення несанкціонованого доступу забезпечується як технічними, так і організаційними заходами.

До числа технічних можна віднести: налаштування комутаційного обладнання на унікальні ідентифікатори зареєстрованих абонентів та застосування надійних методів шифрування обміну даним.

Серед організаційних засобів перед усім необхідно звернути увагу на використання складних паролів доступу до мережі – понад 10 символів як літер (з різним регістром написання), так і цифр. Адже, як правило, злом паролю здійснюється шляхом перебору комбінацій і починається він саме з цифрових значень.

Виконання перелічених заходів дозволить якісно використовувати бездротове підключення до мережі за допомогою технології Wi-Fi.

УДК 681.51

Павленко М.А., доктор технічних наук, доцент, начальник кафедри, Харківський національний університет Повітряних Сил імені Івана Кожедуба;
Зуев П.П., кандидат технічних наук, командування Повітряних Сил Збройних Сил України

ПРИМЕНЕНИЕ АСУ В УСЛОВИЯХ ВЕДЕНИЯ СОВРЕМЕННОЙ ВОЙНЫ

На сегодняшний день понятие информационная борьба, а тем более информационная борьба систем имеет множество толкований и интерпретаций. Рассмотрим системную информационную борьбу на примере военного

протистояння. С точки зору управління, кожна з протистояючих сторін може бути представлена в вигляд складної системи. Їх протистояння буде являтися боротьбою систем. На сьогоднішній день діяльність кожної з систем в такому протистоянні добре описує кібернетична модель управління Бойда.

Дана модель визначає цикл отримання інформації, цикл обробки інформації, цикл прийняття рішення і цикл впливу. Дана модель управління реалізована практично во всіх озброєних силах всіх армій. Використовуючи цю модель управління достатньо просто провести оцінку оперативності управління і ефективності системи в цілому.

В таких умовах достатньо просто визначаються основні напрями удосконалення такої системи. Це удосконалення систем отримання інформації, підвищення оперативності обробки інформації, скорочення часу прийняття рішень і удосконалення засобів впливу або захисту.

Тоді закономірно виникає питання, чи можна боротися з більш досконалою системою? Чи інше питання як побудувати свою систему управління, щоб вона була спроможна протидіяти більш досконалої системі?

Відповіді на ці питання не очевидні і вимагають великої дослідницької роботи по своєму рішення. Особливо актуальним дослідження в даному напрямку стає в умовах використання мережецентричних систем управління, а також відкриваються можливості при використанні таких систем. Залишаються відкритими питання структурної і функціональної стійкості і надійності. Відокремлено необхідно розглянути питання пов'язані з формуванням тимчасових (оперативних) органів і підсистем управління. А також причини виникнення умов формування таких підсистем управління, порядку формування (виділення) їх з основної системи і їх інтеграція в систему після завершення рішення завдань оперативного управління. При цьому ще більш гостро стоїть питання збереження структури системи управління і функцій управління, реалізовані даною системою.

При розгляді питань системного аналізу необхідно розглядати внутрисистемні взаємодії, взаємодії між системами, а також взаємодії типу система-зовнішня середовище і взаємодії систем через зовнішнє середовище.

Одним з підходів до рішення представленої класу завдань є використання методології загальної теорії систем, синергетичних підходів, а також теорії хаосу і катастроф. Використання сукупності даних підходів і методів дозволить знайти відповіді на нові питання в теорії і практиці функціонування систем їх життєвого циклу, їх трансформації і реалізації механізмів адаптації і зміни в різних умовах функціонування.

УДК 623.618

Побережний А.А., старший науковий співробітник науково-дослідної лабораторії забезпечення службово-бойової діяльності НГУ науково-дослідного центру Національної академії Національній гвардії України, підполковник

МЕТОД ОБҐРУНТУВАННЯ СПЕЦІАЛІЗОВАНОЇ ГЕОІНФОРМАЦІЙНОЇ СИСТЕМИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Планування службово-бойової діяльності (СБД) підрозділів та частин Національної гвардії України (НГУ) є досить складним процесом, що потребує виконання вимог значного скорочення часу підготовки, підвищення ефективності, врахування багатьох швидкозмінних факторів. Цього можна досягнути тільки шляхом автоматизації за допомогою сучасної обчислювальної техніки процесів оброблення та узагальнення інформації, моделювання дій, що плануються, та оптимізації рішень, що приймаються.

Багато завдань, які вирішуються НГУ в ході СБД, пов'язані з оперативним аналізом інформації про місцевість, включаючи повну інформацію про будинки, спорудження, їхнє призначення. Обсяг інформації, яку необхідно обробити для прийняття обґрунтованого рішення в умовах наявного ліміту часу значно перевищує можливості органів управління НГУ. Звідси виникає протиріччя між необхідністю використання отриманої інформації та методами її оброблення, що існують в інтересах планування СБД органами управління НГУ.

На сьогодні у силових відомствах розвинених країн світу вирішення даного протиріччя проводиться шляхом використання геоінформаційних систем (ГІС). Всі ці ГІС є вузько спеціалізовані під вирішення завдань окремих видів чи родів військ і не пристосовані для використання у СБД військових частин НГУ.

Слід розуміти, що ГІС НГУ на сьогодні не існує, її необхідно розробляти, і швидко її отримати неможливо. З досвіду розроблення подібних систем можна чітко сказати, що для розроблення ГІС не менше 1-го року займе тільки розроблення технічного завдання (ТЗ) на розроблення ГІС. ТЗ може розробити тільки виробник ГІС у тісній співпраці з усіма зацікавленими управліннями та службами НГУ. Тільки після того, як ТЗ буде узгоджено можна приступати до розроблення програмного забезпечення.

Це доволі коштовний і тривалий процес, тому щоб уникнути зайвих витрат в Національній академії НГУ був розроблений метод обґрунтування спеціалізованої геоінформаційної системи НГУ. Даний метод визначає тактичні і технічні вимоги, які необхідно пред'явити до спеціалізованої ГІС НГУ. В основу даного методу покладено обґрунтування переліку задач, які потрібно вирішувати з використанням спеціалізованої ГІС НГУ, він дозволяє отримати

загальну структуру та врахувати особливості побудови, сформувані вимоги до спеціалізованої ГІС НГУ та провести обґрунтування технології розроблення спеціального програмного забезпечення спеціалізованої ГІС для інформаційно-аналітичного забезпечення СБД НГУ.

При побудові ГІС необхідно виділити чотири основних рівня вирішення завдань з використанням цифрової картографічної інформації: оперативний, оперативно-тактичний, тактичний та спеціальний. На кожному рівні потрібні цифрові карти різних масштабів і змісту. ГІС повинна мати можливість розширення до глобальної загальнодержавної системи, що заснована на клієнт-серверній архітектурі з використанням комп'ютерних мереж. Технологія розроблення спеціального програмного забезпечення ГІС НГУ має будуватися на основі процесно-орієнтованого підходу і врахувати усі специфічні особливості застосування даної ГІС.

Використання запропонованого методу приведе до зменшення строків розроблення, підвищення якості даної ГІС зі збільшенням співвідношення функціональність/вартість, до рентабельності впровадження й використання спеціалізованої ГІС НГУ.

Самокіш А.В., ад'юнкт Харківського національного університету Повітряних Сил імені Івана Кожедуба; **Олизаренко С.А.**, доктор технічних наук, старший науковий співробітник, заступник начальника кафедри автоматизованих систем управління Харківського національного університету Повітряних Сил імені Івана Кожедуба; **Перепелиця О.В.**, кандидат технічних наук, старший науковий співробітник науково-дослідного центру Харківського національного університету Повітряних Сил імені Івана Кожедуба; **Шаповалов О.В.**, кандидат технічних наук, викладач автоматизованих систем управління Харківського національного університету Повітряних Сил імені Івана Кожедуба

ПРОПОЗИЦІЇ ЩОДО ФОРМАЛІЗАЦІЇ ПРОЦЕСУ ОЦІНКИ ОБСТАНОВКИ ПРИ ВИРОБЛЕННІ РЕКОМЕНДАЦІЙ ПО ВИЗНАЧЕННЮ ПАРАМЕТРІВ НАВЕДЕННЯ НА НАЗЕМНУ ЦІЛЬ НА ОСНОВІ НЕЧІТКИХ МНОЖИН ТИПУ 1

При вирішенні задачі цілевказання (наведення) штурмової авіації (ША) на наземну ціль (НЦ), на борт літака (льотчику) передовий авіанавідник (ПАН) видає команди управління. Цими командами ПАН реалізує одну із стратегій (методів) цілевказання (наведення). На вибір стратегії (методу) цілевказання (наведення) впливають зовнішні фактори та досвід ОПР. При цьому метою

ОПР є вибір оптимальної стратегії (методу) цілевказання (наведення) для нанесення максимального ураження НЦ при мінімумі ризику для засобу нанесення ураження противнику (ЗНУП), в даному випадку літака (групи літаків) ША. Тому основні зусилля ОПР зосереджені, з одного боку на підвищенні ступеню ураження НЦ, а з іншої, у недопущенні пошкодження або знищення ЗНУП. Для вибору оптимальної стратегії (методу) цілевказання (наведення) ОПР має враховувати фактори, що впливають на процес прийняття рішень, властивостей ЗНУП та НЦ. Одним із важливих факторів, які впливають на процес рішення задачі наведення є оцінка обстановки. При попередніх розрахунках ПАН має врахувати метеорологічну обстановку, час доби, місцевість та характер бойових дій. Оцінку цих факторів ПАН проводить на основі положень керівних документів та особистого досвіду успішного наведення ША на НЦ. В зв'язку з цим, при розробці систем автоматизації однією з основних проблем є перенесення знань та досвіду ПАН в базу знань відповідної системи. Це зумовлено тим, що вхідними даними є інтервальні оцінки та лінгвістичні змінні, а процес вирішення представляється у вигляді евристичних правил прийняття рішень. Перелічені вище чинники відносяться до нестохастичної невизначеності і для їх врахування в процесі формалізації знань ефективно використовувати теорію нечітких множин. В доповіді наводиться метод формалізації процесу оцінки обстановки при прийнятті рішення щодо наведення ША на НЦ з використанням ієрархічної нечіткої продукційної моделі на основі нечітких множин типу 1.

Семенко Є.Ю., старший науковий співробітник науково-дослідного центру СБД НГУ Національної академії Національної гвардії України; **Споришев К.О.**, кандидат технічних наук, доцент, інформатики та прикладних інформаційних технологій Національної академії Національній гвардії України, полковник

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМАХ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Інформаційна безпека такий стан системи, при якому вона, з одного боку, здатна протистояти дестабілізуючого впливу зовнішніх і внутрішніх інформаційних загроз, а з іншого – її функціонування не створює інформаційних загроз для елементів самої системи і зовнішнього середовища.

Забезпечення інформаційної безпеки в загальній постановці проблеми може бути досягнуто лише при взаємопов'язаних вирішенні трьох складових проблем: перша – захист знаходиться в системі інформації від дестабілізуючого впливу зовнішніх і внутрішніх загроз інформації; друга – захист елементів

системи від дестабілізуючого впливу зовнішніх і внутрішніх інформаційних загроз; третя – захист зовнішнього середовища від інформаційних загроз з боку даної системи.

В даний час комп'ютерні злочини надзвичайно різноманітні. Це несанкціонований доступ до інформації, що зберігається в комп'ютері, введення в програмне забезпечення логічних бомб, розробка і поширення комп'ютерних вірусів, розкрадання комп'ютерної інформації, недбалість у розробці, виготовленні та експлуатації програмно-обчислювальних комплексів, підробка комп'ютерної інформації.

Всі заходи протидії комп'ютерним злочинам, що безпосередньо забезпечують безпеку інформації, можна підрозділити на:

- правові;
- організаційно-адміністративні;
- інженерно-технічні.

До правових заходів варто віднести розробку норм, що встановлюють відповідальність за комп'ютерні злочини, захист авторських прав програмістів, удосконалювання кримінального і цивільного законодавства, а також судочинства. До них відносяться також питання суспільного контролю за розроблювачами комп'ютерних систем і прийняття відповідних міжнародних договорів про обмеження, якщо вони впливають або можуть вплинути на військові, економічні і соціальні аспекти країн. Тільки в останні роки з'явилися роботи з проблем правової боротьби з комп'ютерними злочинами. А зовсім недавно і вітчизняне законодавство стало на шлях боротьби з комп'ютерною злочинністю.

До організаційно-адміністративних заходів відносяться: охорона комп'ютерних систем, підбір персоналу, виключення випадків ведення особливо важливих робіт тільки однією людиною, наявність плану відновлення працездатності центру після виходу його з ладу, обслуговування обчислювального центру сторонньою організацією або особами, незацікавленими в приховуванні фактів порушення роботи центру, універсальність засобів захисту від усіх користувачів (включаючи вище керівництво), покладання відповідальності на осіб, що повинні забезпечити безпеку центру, вибір місця розташування центру і т.п.

До інженерно-технічних заходів можна віднести захист від несанкціонованого доступу до комп'ютерної системи, резервування важливих комп'ютерних систем, забезпечення захисту від розкрадань і диверсій, резервне електроживлення, розробку і реалізацію спеціальних програмних і апаратних комплексів безпеки тощо.

Фізичні засоби містять у собі різні інженерні засоби, що перешкоджають фізичному проникненню злоумисників на об'єкти захисту і захищаючий персонал, особисті засоби безпеки, матеріальні засоби і фінанси, інформацію від протиправних дій.

До апаратних засобів відносяться прилади, пристрої, пристосування та інші технічні рішення, які використовуються в інтересах забезпечення безпеки. У практиці діяльності будь-якої організації знаходить широке застосування різна апаратура: від телефонного апарату до розроблених автоматизованих інформаційних систем, що забезпечують її виробничу діяльність. Основна задача апаратних засобів - стійка безпека діяльності.

Інформація в системах управління Національної гвардії України має обмежений доступ. Її особливістю є важливість, оперативність. Втрата інформації або її перекручення може привести не тільки до матеріальних втрат але і до втрат особового складу. Все це приводить до необхідності забезпечення безпеки інформації в системах управління Національної гвардії України.

УДК 681.518.3

Сербин В.В., провідний фахівець Державного підприємства «КБ «Південне»»

ПРИНЦИПИ ПОБУДОВИ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ВІЙСЬКОВИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Питання управління військовими підрозділами висувуються на одне з перших місць серед проблем наукових досліджень у питаннях розроблення озброєння, військової та спеціальної техніки. На сьогодні особливої гостроти набуває ряд завдань, які пов'язані із розробленням теоретичних положень щодо організації управління підрозділами Національної гвардії України. Важливість ефективного управління значно зростає при підготовці та проведенні спеціальних операцій, вторгненні збройних угруповань та злочинних організацій на територію України, а також заходів, пов'язаних з припиненням терористичної діяльності.

При цьому в умовах зміни характеру і змісту збройного протистояння способи ведення бойових дій та методи управління військовими формуваннями постійно розвиваються і наповнюються новим змістом. Тому їх вивчення і своєчасна реалізація в практиці - закономірний процес.

Еволюція способів ведення бойових дій та методів управління військовими підрозділами є наслідком безперервного розвитку засобів збройного протистояння, зміни характеру і змісту бойових дій, а також цілей і завдань застосування в них військових формувань.

Найбільш гострим питанням управління військовими підрозділами є підвищення динамічності управління і ефективності виконання службово-бойових завдань, забезпечення можливості обробки великого об'єму інформації в військових підрозділах.

УДК 358:007.35

Скопінцев О.О., Харківський національний університет Повітряних Сил імені Івана Кожедуба

ЗАДАЧА ВИБОРУ ВРАЖАЮЧОЇ КОМБІНАЦІЇ ПРИ ПЛАНУВАННІ УДАРІВ ПО МАЛОРОЗМІРНИМ ЗАХИЩЕНИМ ОБ'ЄКТАМ

Поява високоточної зброї дозволило говорити про виборчий спосіб ураження елементів об'єкта. Іншими словами – для досягнення мети операції цілком достатньо вражати не весь об'єкт як такий, а певні його елементи. Вводиться поняття «вражаємо комбінація», коли у складі групового об'єкта досить знищити одну або кілька елементарних цілей, втрата яких призводить до втрати боєздатності об'єкта у цілому.

Попередньо розглянемо процес ураження одиночного малорозмірного захищеного об'єкта однієї фугасною бойовою частиною (ФБЧ).

З достатньою точністю для проведення оцінки застосування ФБЧ по малорозмірним об'єктам у цьому процесі будемо розглядати тільки сам об'єкт і ФБЧ, абстрагуючись від ряду факторів, наприклад, таких як погодні умови (стан атмосфери, швидкість вітру і т.д.).

Модель об'єкта ураження повинна відображати його міцність і геометричні розміри. Характеристики міцності об'єкта визначаються матеріалами його конструкції. Так при прямому влученні ФБЧ в об'єкт збиток оцінюється залежно від характеристик захисної споруди. Пропонується розглядати такі ступені руйнування:

- 1) сильне – настає при наскрізь пробитті захисної споруди;
- 2) середнє – настає при пробитті не менше 0,5 товщини захисної споруди;
- 3) слабке – настає при пробитті не більше 0,5 товщини захисної споруди.

Матеріал бокових стінок споруди опосередковано характеризується надлишковим тиском, що призводить до сильного, середнього та слабого руйнування об'єкта. Крім того, утворюється надлишковий тиск при промаху ФБЧ по захисному спорудженню.

При проведенні оцінки результатів застосування ФБЧ на перше місце виходить її бойова сила. Бойова сила насамперед залежить від ваги бойової частини і точності самого удару. Вага бойової частини виражається через вагу в тротиловому еквіваленті.

На точність удару впливають дві групи помилок: однакові для всіх пострілів (пусків) помилки цілевказівки і помилки індивідуального розсіювання.

Групові помилки підкоряються нормальному закону та характеризуються ймовірними відхиленнями (при нульових математичних очікуваннях).

Індивідуальні помилки також підкоряються нормальному закону та мають ймовірні відхилення від точки прицілювання.

Процес отримання об'єктом певної міри руйнування за своєю суттю є випадковим, так як в його основі лежить вибух ФБЧ, координати якого, виходячи зі сказаного вище, випадкові.

Таким чином, події отримання об'єктом сильної, середньої, слабкої ступеня руйнування випадкові та характеризуються відповідними можливостями їх настання. Дані ймовірності можуть служити оцінкою ефективності застосування ФБЧ при ураженні малорозмірних захищених об'єктів.

Отримання аналітичних залежностей ймовірностей отримання об'єктом відповідних ступенів руйнування при впливі ФБЧ важко через впливу багатьох важко прогнозованих факторів.

Імітаційний підхід дає можливість з достатньою достовірністю оцінити ці ймовірності. Для цього вводиться у розгляд три лічильника підрахунку отримання об'єктом ураження в кожній реалізації імітаційної моделі відповідного ступеня руйнування.

Станович О.В., начальник науково-дослідного відділу науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут; **Кротов В.Д.**, провідний науковий співробітник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут

ПРИНЦИПИ ОРГАНІЗАЦІЇ І ПОБУДОВИ ЄДИНОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

В сучасних умовах, що характеризуються багатоваріантністю загроз і завдань, що вирішуються структурами Воєнної організації держави, а також високою динамічністю зміни обстановки, для прийняття та реалізації своєчасних ефективних рішень і забезпечення узгодженості дій потрібен перегляд принципів і підходів побудови і застосування телекомунікаційної компоненти системи управління. Комплексність сучасних загроз ускладнює вирішення проблем старими методами. У зв'язку з цим все більш актуальним і пріоритетним напрямком реформування військово-силових структур стає всебічна інтеграція бойових формувань і підвищення рівня їх взаємодії на основі створеного єдиного інформаційного простору для всіх ланок управління за рахунок реалізації мережецентричного управління (МЦУ) та інтеграції систем зв'язку, засобів ураження, розвідки та всебічного забезпечення.

Проблеми створення єдиного простору

Розуміння нового підходу до ведення протиборства в єдиному інформаційному просторі тільки формується. Окремі фрагменти представляють

розрізненість бачення проблем, як у напрямку розвитку електроніки, так і в інших напрямках, в тому числі в управлінні, топологіях і телекомунікаціях.

На сьогодні є ряд проблемних питань щодо телекомунікацій, які “лежать на поверхні” при реалізації принципів МЦУ. Це, перш за все, реалізація простору з численними взаємопов'язаними засобами мережо- і каналоутворення, тобто необхідна широкопasmова високошвидкісна транспортна основа (транспортна мережа) автоматизованих систем зв'язку спеціального призначення, яка не тільки побудована за принципами вертикальної ієрархії, а й з сильно розвиненими горизонтальними зв'язками (перш за все міжвидовими), що дозволить здійснити як вертикальну так і горизонтальну інтеграцію всіх компонентів об'єднаних сил угруповання. При цьому широкопasmова пов'язаність простору повинна доходити до мобільного високошвидкісного об'єкта в умовах дії агресивного зовнішнього середовища в різних фізичних умовах: атмосфера, космос, вода. Основними вимогами при формуванні такої “горизонтальної” інтеграції є: забезпечення необхідної пропускну здатності каналів передачі даних; організація взаємодії на будь-якому рівні управління та інше. А головним принципом такої структури стає забезпечення постійного зв'язку між будь-якими двома споживачами в будь-який час і в будь-якому місці.

Фактично, швидкість і пропускну здатність з точки зору зв'язку винна бути забезпечена за схемою “кожен з кожним”. А без наявності в мережах взаємодії достатньої кількості каналів з широкопasmовим доступом, забезпечення простору МЦУ важко. Отримання сьогодні високих показників по надійним і широкопasmовим каналам зв'язку до кожного окремого підрозділу досить важко, оскільки їх технічне переоснащення поки ще не завершено.

Швидкості і навантаження це далеко не всі “вузькі” місця в сучасних мережах зв'язку. Проблеми виникають в управлінні цими розподіленими багаторівневими технічно складними системами. Тому, основним напрямком удосконалення системи управління є створення інтегрованих систем управління мережевої архітектури, що забезпечить реалізацію єдиної інформаційної структури і єдиного інформаційного простору всіх учасників бойових дій. Конфігурувати сучасні мережі вручну практично неможливо, тому, настав час для змін в управлінні архітектурою мереж і розрахунків в них.

Це далеко не повний перелік проблем і особливостей, які необхідно врахувати фахівцям і промисловості для формування принципів створення і забезпечення нормального функціонування телекомунікаційного середовища спеціального призначення.

Принципи формування телекомунікаційного середовища

Аналіз показує, що проблеми інтеграції та конвергенції різних видів зв'язку, включаючи інформаційний, системний і мережевий аспекти, протягом останніх

*Секція 5. Актуальні проблеми зв'язку та інформатизації службово-бойової діяльності
Національної гвардії України*

років залишаються найбільш актуальними в телекомунікаціях. Складність вирішення зазначених проблем пов'язана з двома особливостями телекомунікаційних систем як інформаційно-технічних систем з ресурсами колективного використання: географічної розпорошеністю мережевих ресурсів, джерел та одержувачів інформації, а також пульсуючим характером трафіку.

Перша особливість визначає високу вартість мережевих ресурсів і висуває вимогу їх ефективного використання. Тому система управління повинна забезпечувати колективний доступ до ресурсів мережі в режимі поділу часу, при якому ресурси надаються великому числу користувачів, кожен з яких пред'являє відносно невеликі вимоги, але які визначають загальний профіль навантаження (трафіка), що забезпечує рівномірне і ефективне їх використання. Таким чином, друга особливість призвела до необхідності застосування методу комутації з проміжним накопиченням (пакетна комутація).

Звідси випливає загальна задача проектування телекомунікаційної системи спеціального призначення – досягнення ефективного колективного використання ресурсів безлічі несумісних пристроїв географічно розподіленої системи, в якій доступ до ресурсів виникає від асинхронних процесів в істотно нерівні проміжки часу. Із загальної задачі випливає третя особливість телекомунікаційних систем – різномірність обладнання та застосовуваних мережевих технологій. Однак проблема сумісності різних пристроїв, долається в рамках еталонної моделі взаємодії відкритих систем і регламентується протоколами на всіх рівнях її організації. Виходячи з вищевикладеного та на основі досліджень, сформулюємо основні принципи організації та побудови телекомунікаційної мережі спеціального призначення (ТКМ) в системному аспекті.

ТКМ повинна: мати максимальну інформаційну ємність; мати максимальну зв'язаність; бути ізотропною; забезпечувати мінімальні втрати цільової інформації; використовувати мінімальний обсяг буферної пам'яті, який достатній для оптимального узгодження параметрів трафіку з параметрами каналів зв'язку; бути гнучкою і швидко реагувати на зміну стану її елементів і зовнішнього середовища.

Таким чином, сформульовані загальні принципи організації і побудови телекомунікаційної мережі спеціального призначення в системному аспекті розглядають мережі зв'язку з загальних позицій, що не залежать від існуючих технологій. Використання регулярних структур у поєднанні з принципом ізотропності дозволяє отримати аналітичне рішення більшості завдань оптимізації мережевих ресурсів, що полегшує інтерпретацію результатів рішення. Точне дозування обсягу буферної пам'яті вузлів комутації дозволяє здійснити оптимізацію трафіка з метою узгодження його статистичних характеристик з параметрами мережі та при необхідності, реалізацію процесів обміну з дотриманням основних якісних показників. Використання даних принципів вимагає глибокого аналізу властивостей потоку даних.

УДК 681.51

Тимочко А.І., Харківський національний університет Повітряних Сил імені Івана Кожедуба; **Павленко М.А.**, Харківський національний університет Повітряних Сил імені Івана Кожедуба; **Касьяненко М.В.**, Харківський національний університет Повітряних Сил імені Івана Кожедуба; **Литвиненко М.І.**, Харківський національний університет Повітряних Сил імені Івана Кожедуба; **Полонский Ю.І.**, Харківський національний університет Повітряних Сил імені Івана Кожедуба

ОБЕСПЕЧЕНИЕ РАДИОЛОКАЦИОННОЙ ИНФОРМАЦИЕЙ В ПРОЦЕССЕ УПРАВЛЕНИЯ ВОЗДУШНЫМ ДВИЖЕНИЕМ В РЕГИОНАЛЬНЫХ ЦЕНТРАХ УПРАВЛЕНИЯ ВОЗДУШНЫМ ДВИЖЕНИЕМ

Необходимым условием решения задач управления на центрах управления воздушным движением (ЦУВД) является наличие радиолокационной информации (РЛИ) о воздушных объектах (ВО). Обеспечение радиолокационной информацией центров управления воздушным движением является одной из функций АСУ центров управления воздушным движением и представляет собой совокупность взаимосвязанных мероприятий по выявлению, сбору, обработке, анализу и выдаче данных о воздушных объектах от источников радиолокационной информации на центры управления воздушным движением. Можно выделить ряд топологических особенностей подсистемы обеспечения радиолокационной информацией ЦУВД:

Подсистема обеспечения радиолокационной информацией регионального центра управления воздушным движением имеет сложную структуру и информация о ВО от источников радиолокационной информации может поступать на региональный центр управления воздушным движением через несколько звеньев управления. Основными направлениями выдачи радиолокационной информации являются направления по вертикали управления, т.е. между подчиненными и вышестоящими ЦУВД. Наличие территориально разнесенных источников и потребителей радиолокационной информации в АСУ регионального ЦУВД обуславливает необходимость использования протяженных каналов передачи данных. Такие каналы передачи данных представляют собой сложные и дорогостоящие сооружения, что определяет актуальность задачи эффективного их использования.

Перечисленные особенности подсистемы обеспечения радиолокационной информацией регионального ЦУВД определяют порядок решения задач этой подсистемой. К таким задачам относятся: радиолокационное наблюдение за воздушным пространством, сбор, обработка и анализ радиолокационной

інформації, формування і видача повідомлень о ВО потребителям. Проведемо аналіз цих завдань.

Радиолокаційне спостереження в районі відповідальності ЦУВД і на підступах к нему ґрунтується на визначеному порядку розміщення радиолокаційних засобів для створення сплошного радиолокаційного поля з метою своєчасного виявлення, ідентифікації, розпізнавання і неперервного супроводження ВО.

Особливу увагу при зборі РЛІ приділяють перевантаженням в ланках управління АСУ. Перевантаження представляють собою ситуації, коли вхідний потік РЛІ не може бути повністю оброблений на ЦУВД і виданий потребителям з встановленою дискретністю, т.е. встановленим інтервалом часу між сусідніми повідомленнями про одне ВО. Це може бути викликане обмеженою продуктивністю АСУ і недостатньою пропускною здатністю каналів передачі даних з причин їх радіоелектронного придушення, а також збільшення густоти потоку повідомлень о ВО.

Таким чином, причини перевантажень в ланках збору РЛІ можуть призвести до перевищення продуктивності джерел РЛІ над пропускною здатністю каналів передачі даних. При такому розгладженні між продуктивністю джерел і пропускною здатністю каналів передачі даних забезпечувані ЦУВД будуть отримувати РЛІ не в повному об'ємі, що впливає на якість рішення завдань обробки і аналізу РЛІ на цих ЦУВД.

УДК 621.391

Ткаченко К.М., ад'юнкту Національної академії Національної гвардії України, старший лейтенант

ОБґРУНТУВАННЯ АКТУАЛЬНОСТІ ЗАСТОСУВАННЯ ДОДАТКОВИХ ТЕХНІЧНИХ ЗАХОДІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРИХОВАНОВОГО РАДІООБМІНУ МІЖ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ У ХОДІ ВИКОНАННЯ СЛУЖБОВО-БОЙОВИХ ЗАВДАНЬ

На сьогодні, зважаючи на особливості ведення воєнних дій, невід'ємною складовою системи управління силами НГУ, при виконанні службово-бойових завдань, в більшості випадків, є радіозв'язок. Одним із головних показників якості роботи системи радіозв'язку є безпека зв'язку, яка характеризується здатністю забезпечувати розвідзахищеність та імітостійкість. На озброєнні розвинених у воєнному відношенні країн світу стоять сучасні мобільні засоби

радіорозвідки, які спроможні з високою ефективністю виконувати сканування, перехоплення, аналіз, класифікацію та моніторинг радіопередач, це робить актуальною задачу зниження ефективності впливу цих засобів.

Аналіз застосування системи радіозв'язку Національної гвардії України (НГУ) під час проведення АТО виявив недоліки у забезпеченні захисту радіообміну в умовах дії сучасних засобів радіорозвідки противника, звідки постає задача створення альтернативних організаційно-технічних заходів з підвищення показників розвідвахищеності системи радіозв'язку НГУ. Проведений аналіз підтверджує, що способи пасивного радіомаскування, засновані на екрануванні, регламентації робіт на випромінювання лише частково вирішують проблеми приховування радіомереж та окремих засобів радіозв'язку від радіоелектронної розвідки, тому для забезпечення розвідвахищеності необхідно додатково використовувати засоби активного радіомаскування (ЗРМ). Такі засоби створюють спеціальні поля перешкод, що ускладнюють несанкціонований прийом сигналу засобами радіотехнічної розвідки і виділення повідомлень засобами радіорозвідки. Результатом дії активних шумових перешкод є маскування корисних сигналів в деякому тілесному куті і певному інтервалі відстаней. Внаслідок цього істотно погіршуються характеристики виявлення засобів радіозв'язку, їх роздільна здатність і точність визначення координат.

Аналіз існуючих робіт показав, що моделі, описані в них, мають певні недоліки та потребують доопрацювань. На відміну від вже існуючих, запропонована модель має можливість оцінювати вплив кількох ЗРМ на розвідвахищеність радіозасобів підрозділів НГУ від декількох засобів радіорозвідки противника (ЗРЕРп). Введення до характеристик ЗРМ такої величин, як кут місця цілі, дозволило вдосконалити існуючу модель, надавши можливість використовувати її проти повітряних засобів радіоелектронної розвідки. Також, однією з переваг запропонованої моделі є врахування того, що траєкторія руху БПЛА являє собою не одну, а множину точок, які потрібно придушувати одночасно.

У результаті дослідження отримано удосконалену модель захисту інформаційного обміну в каналах радіозв'язку НГУ за рахунок урахування властивостей діаграми направленості направлених антенних пристроїв, при зміні азимуту та кута місця у напрямку на повітряні засоби радіорозвідки, що дозволить дослідити ступінь захищеності радіообміну від просторових координат можливої траєкторії повітряних ЗРЕРп та комплексу ЗРМ. Програмна реалізація моделі дозволяє обчислити оптимальну орієнтацію ЗРМ.

УДК 351.862.4

Устименко О.В., кандидат наук з державного управління, старший науковий співробітник, старший науковий співробітник Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, полковник запасу

СИТУАЦІЙНІ ЦЕНТРИ ДЕРЖАВНИХ ОРГАНІВ ЯК СКЛАДОВІ СИСТЕМИ ДЕРЖАВНОГО КРИЗОВОГО РЕАГУВАННЯ У СФЕРІ ОБОРОНИ

В Стратегії національної безпеки України зазначається, що необхідно забезпечити “удосконалення державної системи стратегічного планування, створення єдиної системи моніторингу, аналізу, прогнозування та прийняття рішень у сфері національної безпеки і оборони, забезпечення ефективної координації та функціонування єдиної системи ситуаційних центрів профільних органів державної влади сектору безпеки і оборони”. Стратегічним оборонним бюлетенем України передбачається, що до кінця 2020 року буде “створено систему ситуаційних центрів для сектору оборони на базі захищених інформаційно-телекомунікаційних систем”.

Ситуаційний центр це організаційно-технічна система, яка забезпечує збір, накопичення, обробку і аналіз інформації (моніторинг), необхідної для прогнозування, планування та прийняття рішень у сфері національної безпеки і оборони. Планується, що результати моніторингу будуть подаватися до Апарату Ради національної безпеки і оборони (РНБО) України щоквартально. Водночас, у разі виявлення під час моніторингу раптових змін індикаторів, які свідчать про кризу - різке погіршення стану національної безпеки України, орган державної влади зобов'язаний невідкладно надати результати моніторингу до Апарату РНБО України.

Доцільно передбачити можливість, щоб у разі критичного рівня національної безпеки України відповідні сигнали з ситуаційних центрів надходили не лише до Апарату РНБО України та керівництва держави, а й до частин і підрозділів сил оборони, активізуючи механізми приведення у вищі ступені бойової готовності.

За досвідом ЗС СРСР частини і підрозділи ЗС України (сил оборони) приводяться у вищі ступені бойової готовності бойовими розпорядженнями, які закладені в відповідних пакетах. Сигнали на їх розпечатування доводяться з пунктів управління ГШ ЗС України.

Втім, як свідчить досвід, під час захоплення Російською Федерацією Криму та міста Севастополь у 2014 році система стратегічного керівництва обороною знаходилася в колапсі, а механізми приведення у вищі ступені бойової готовності частин і підрозділів ЗС України виявилися недієздатними. В частини

і підрозділи сил оборони не надходили адекватні ситуації вказівки і розпорядження, сигнали на приведення у вищі ступені бойової готовності, коли розпочалося блокування російськими військовими без розпізнавальних знаків (“зеленими чоловічками”) українських військових частин на півострові, кораблів на базах, відбувалося захоплення Сімферопольського аеропорту, об'єктів критичної інфраструктури тощо. Отже механізми приведення у вищі ступені бойової готовності частин і підрозділів складових сил оборони необхідно удосконалити. При цьому необхідно врахувати можливість: деструктивного впливу на систему військового управління, що може призвести до порушень роботи штатної системи приведення у вищі ступені бойової готовності частин і підрозділів сил оборони; політичної кризи, що може спричинити колапс системи державного управління в цілому.

Отже вже у процесі створення системи ситуаційних центрів складових сектору безпеки і оборони доцільно передбачити можливість їх використання як резервної системи приведення у вищі ступені бойової готовності частин і підрозділів сил оборони.

УДК 681.5: 62-5: 004.5

Федотов Д.О., кандидат технічних наук, доцент, провідний науковий співробітник, Харківський національний університет Повітряних Сил імені Івана Кожедуба; **Кураш Л.С.**, старший науковий співробітник, Харківський національний університет Повітряних Сил імені Івана Кожедуба, підполковник

БАГАТОКАСКАДНЕ ПІДСИЛЕННЯ В РАДІОКОМПОНЕНТНІЙ БАЗІ ЗВ'ЯЗКУ ТА ІНФОРМАЦІЙНИХ МЕРЕЖАХ

Основу радіокомпонентної бази зв'язку та інформаційних мереж, що актуально для військової техніки, складають активні схеми підсилення, функціонального перетворення чи формування інформаційних сигналів для пристроїв електроніки із заданим коефіцієнтом, які передбачають взаємодію каналу прямої передачі з суттєвим в ньому коефіцієнтом підсилення та каналу зворотного зв'язку, чим задають необхідну функцію, але створюють при цьому методичну похибку перетворення [Бобровников Л.З. Радотехника и электроника: учеб. для вузов. – 4-е изд., М.: Недра, 1990.– 374 С. ISBN 5-247-01313-1, – С.97-103]. Через наявну похибку перетворення не рекомендується застосовувати підсилення в одному каскаді більше, ніж $K_U > 1000$, навіть, сучасними операційними підсилювачами (ОП) з власним коефіцієнтом $K_{OP} = 10^6$. За цієї причини загальний коефіцієнт K_U підсилення встановлюють добутком каскадних K_{U_i} за принципом конвеєра напруги в багатокаскадному

підсилювачі [Гусев В.Г., Гусев Ю.М. Электроника. М.: Высшая школа, 1991. – 622 С., глава 5, – С.331-350].

Наразі, не існує наукового обґрунтування алгоритму обрання, як кількості m -каскадів, так і співвідношення їх каскадного підсилення K_{Ui} . Це, у підсумку, призводить до обмеження частоти перетворення, суттєвої похибки підсилення та неоптимального фазовому зсуву, що є причиною неналежного вибору і зумовлює указані недоліки.

Метою пропозиції в роботі є підвищення точності встановлення коефіцієнту підсилення напруги інформаційного сигналу за рахунок визначення оптимальної кількості необхідних m -каскадів, забезпечення якісного підсилення, а саме, максимально можливої частоти підсилення, мінімальних фазового зсуву та похибок перетворення.

Указана технічна задача вирішується таким чином [Патент України на винахід №107617, МПК H03F 3/213, H03F 3/217, H01H 11/00, номер заявки а 201308297 від 01.07.2013, публ. Бюл. №1 від 26.01.2015, власник Харківський національний університет радіоелектроніки, автори Сліпченко М.І., Федотов П.Д., Федотов Д.О., Крук О.Я.].

Кількість m -каскадів конвеєра напруги визначають, як натуральний логарифм заданого загального коефіцієнта K_U підсилення. Встановлюють каскадні коефіцієнти підсилення K_{Ui} , рівними $e = 2,718$ – основи натурального логарифма та за необхідності додатковим $m+1$ каскадом компенсують підсилення до заданого загального коефіцієнта K_U .

Як визначають теоретичні дослідження [Сліпченко Н.И., Исследование точности процесса преобразования при многокаскадном усилении / Н.И. Слипченко, П.Д. Федотов, Д.А. Федотов, О.Я. Крук // Системи обробки інформації: Зб. наукових праць. Випуск 3(101), Том 1, Харків, 2012. – С.50-55], отримані залежності коефіцієнта похибки, оптимального коефіцієнта похибки при рівнопідсилювальному режимі з урахуванням заданих параметрах схеми загального коефіцієнта K_U підсилення, та власного коефіцієнта підсилення $K_{оп}$ операційного підсилювача указують на реальну можливість суттєвого розширення полоси частот, обмеженої частотою зрізу АЧХ на рівні -3дБ, зменшеною фазочастотною залежністю в процесі підсилення інформаційного сигналу, чим підтверджується можливість досягнення поставленої мети.

Проведені авторами експериментальні дослідження дозволили встановити, що оптимальне виконання, з точки зору експоненціальної складової каскадних коефіцієнтів, у порівнянні з однокаскадним підсилювачем може у десятки разів розширити частотний діапазон, що еквівалентно зменшенню фазового зсуву при суттєвому зниженні відносної похибки сигналу перетворення.

Автори виходять з того, що процес затухання сигналів у довгих лініях, які можна розглядати, як багатокаскадне з'єднання елементарних ланцюгів,

відбувається за експоненціальним законом, тому, природньо, можна стверджувати, що процес підсилення необхідно здійснювати за цим же законом. Параметри точності каскаду з K_{Ui} , рівному $e = 2,718$ є оптимальними з точки зору похибки перетворення, частотного діапазону та фазового зсуву, при цьому, якщо загальний коефіцієнт визначається добутком каскадних коефіцієнтів, то фазовий зсув забезпечується тільки сумою мінімальних складових, чим забезпечується розширення робочої полоси частот.

Запропоновані теоретичні та експериментальні дослідження, наведені в цій роботі та наведених джерелах, розширюють практичні можливості радіокомпонентної бази зв'язку та інформаційних мереж, актуальних при створенні нових зразків електронних пристроїв для військової техніки.

УДК 621.396:654.19

Флорін О.П., кандидат технічних наук, доцент, доцент кафедри управління діями підрозділів із засобами військового зв'язку Національної академії Національної гвардії України

АНАЛІЗ МОЖЛИВОСТЕЙ ІНФОРМАЦІЙНИХ ОБЛІКОВИХ СИСТЕМ ДЛЯ ПОБУДОВИ АВТОМАТИЗОВАНОЇ СИСТЕМИ ОБЛІКУ МАЙНА ЗВ'ЯЗКУ В ЧАСТИНАХ ТА ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Облік майна зв'язку частин та підрозділів Національної гвардії України (НГУ) є однією з складових комплексу заходів технічного забезпечення зв'язку, що має надавати командирам своєчасну, повну і достовірну інформацію про його стан та наявність для прийняття обґрунтованих рішень при виконанні службово-бойових завдань та у повсякденній діяльності.

Облік майна зв'язку, що знаходиться на озброєнні НГУ організовано згідно вимог керівних документів, однак при його організації у службах зв'язку територіальних управлінь (військових частин) та підрозділах існують певні обмеження щодо оперативності отримання та достовірності інформації (особливо з віддалених підрозділів), не враховується необхідність автоматизації облікових процесів, інтеграції та взаємозв'язку системи обліку з іншими складовими перспективних систем автоматизації.

Аналіз інформаційних систем вітчизняного та закордонного виробництва, що мають підсистеми обліку матеріальних засобів проведений з метою визначення можливості їх адаптації до потреб служб зв'язку частин і підрозділів НГУ дозволив зробити такі висновки:

– сучасний стан обліку майна зв'язку в НГУ не відповідає вимогам стосовно оперативності отримання та достовірності інформації. Вирішення проблеми

полягає в впровадженні автоматизованих інформаційних систем;

– сучасні інформаційні системи дозволяють здійснювати облік матеріальних засобів, однак частина з них розроблені російськими компаніями і не можуть бути використані в Україні, а вітчизняні системи не враховують специфіку обліку матеріальних засобів у військових формуваннях;

– автоматизовані системи з функціями обліку матеріальних засобів вітчизняного та іноземного виробництва мають суттєві недоліки, що не дають можливості їх застосовування для потреб служб зв'язку НГУ;

– визначена специфіка обліку майна зв'язку надасть можливість формулювання уточнених вимог до майбутньої автоматизованої системи обліку.

Сформульовано положення про доцільність розробки автоматизованої системи обліку майна зв'язку як підсистеми єдиної інформаційно-аналітичної системи НГУ з можливістю інтеграції та взаємозв'язку її з іншими складовими систем автоматизації, що буде спиратись на положення Стратегічного оборонного бюлетеня України.

Подальші дослідження доцільно спрямувати на обґрунтування вимог і розробку структури, функцій та алгоритмів функціонування автоматизованої системи обліку майна зв'язку. Отримані результати можна використовувати при побудові автоматизованої системи обліку майна зв'язку.

Борисенко М.В., Шапран Ю.Є., АВТОМАТИЗОВАНА СИСТЕМА КОНТРОЛЮ ТА ДІАГНОСТИКИ РАДІОТЕХНІЧНОЇ АПАРАТУРИ..	4
Власік С.М., Сметана Є.А., Лабунець В.О., РОЗРОБКА РАДІОТЕХНІЧНИХ СИСТЕМ ДЛЯ БЛОКУВАННЯ ЗАСОБІВ РАДІОЗВ'ЯЗКУ ПРИ ПРОВЕДЕННІ СПЕЦІАЛЬНИХ ОПЕРАЦІЙ.....	5
Власов К.В. СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ НА БАЗІ ОБЛАДНАННЯ НІК VISION ТА МОЖЛИВОСТІ ЇХ ЗАСТОСУВАННЯ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ.....	6
Воробйов Є.С., Павленко М.А., Черток О.А., Гладишев М.Г. ОБҐРУНТУВАННЯ МЕТОДУ АВТОМАТИЗАЦІЇ ПРОЦЕСУ РОЗРАХУНКІВ ОПТИМАЛЬНОГО МАРШРУТУ ДЛЯ УДАРНОЇ АВІАЦІЇ ПОВІТРЯНИХ СИЛ ЗС УКРАЇНИ.....	8
Воронін О.І. ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ В ЧАСТИНАХ ТА З'ЄДНАННЯХ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ СПЕЦІАЛЬНОГО ПОЛЬОВОГО ТЕЛЕКОМУНІКАЦІЙНОГО КОМПЛЕКТУ.....	9
Герасимов С.В., Тимочко О.І. МЕТОДИ ТА ЗАСОБИ КОНТРОЛЮ ТЕХНІЧНОГО СТАНУ БЕЗПЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ.....	10
Глушенко М.О. ОСОБЛИВОСТІ ПРОВЕДЕННЯ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ЦИФРОВИХ ЗАСОБІВ ЗВ'ЯЗКУ.....	12
Горєлишев С.А., Баулін Д.С., Нікорчук А.І. ВИКОРИСТАННЯ ГЕОІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ПІДВИЩЕННЯ МАНЕВРНОСТІ БЕЗПЛОТНИХ АВТОМОБІЛІВ.....	13
Горєлишев С.А., Баулін Д.С., Побережний А.А., Цис О.І. ПРІОРИТЕТНІ НАПРЯМКИ РОЗВИТКУ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ СЛУЖБОВО-БОЙОВОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ.....	15
Данилов Ю.А., Медведєв В.К., Павленко М.А., Ясинецький В.П., Могилатенко А.В., АЛГОРИТМИ, ОБЕСПЕЧИВАЮЩІЕ СОПРОВОЖДЕНИЯ ТРАЕКТОРИЙ ВОЗДУШНЫХ ЦЕЛЕЙ С УЧЕТОМ ИХ ВОЗМОЖНОГО НЕРАЗРЕШЕНИЯ.....	16
Дробаха Г.А., Лісіцин В.Е. СИСТЕМИ ІМІТАЦІЙНОГО МОДЕЛЮВАННЯ У ВИРІШЕННІ СЛУЖБОВО-БОЙОВИХ ЗАВДАНЬ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ.....	18
Зуєв П.П., Тимочко О.О. МЕТОД ФОРМАЛІЗАЦІЇ ЗАДАЧІ СИТУАЦІЙНОГО АНАЛІЗУ У ПОВІТРЯНОМУ ПРОСТОРІ.....	19
Іохов О.Ю., Малюк В.Г. МЕТОД ОПТИМІЗАЦІЇ РОЗВІДЗАХИЩЕНОСТІ РАДІООБМІНУ В МЕРЕЖАХ ЗВ'ЯЗКУ УГРУПУВАНЬ ВІЙСЬК (СИЛ) НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ..	21

Казіміров О.О., Куртов А.І. НАВЧАЛЬНИЙ ТЕЛЕГРАФНИЙ КЛЮЧ, СУМІСНИЙ З ПЕРСОНАЛЬНОЮ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНОЮ МАШИНОЮ.....	22
Корєхов А.О. ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ В СИСТЕМІ АВТО ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ ДЕРЖАВНОЇ ПРИКОРДОННОЇ СЛУЖБИ УКРАЇНИ.....	23
Косюк В.П. ЗАСТОСУВАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ КОМПЛЕКСІВ УПРАВЛІННЯ РЕСУРСАМИ В СИСТЕМАХ УПРАВЛІННЯ БОЄМ.....	25
Кротов В.Д. ІНФОРМАЦІЙНА СИСТЕМА ОБРОБКИ ДАНИХ ЯК ОСНОВА СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕННЯ СИСТЕМИ УПРАВЛІННЯ ЗВ'ЯЗКОМ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ.....	26
Кротов В.Д., Станович О.В. АНАЛІЗ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ІР В ПОЛЬОВИХ АД-НОС МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ.....	29
Лазарев В.Д. СТВОРЕННЯ СУЧАСНОЇ МЕРЕЖІ ОБМІНУ ІНФОРМАЦІЄЮ НА ПОЛІ БОЮ ДЛЯ ЧАСТИН ТА ПІДРОЗДІЛІВ ТАКТИЧНОЇ ЛАНКИ НАЦІОНАЛЬНОЇ ГВАРДІЇ.....	32
Майборода І.М. ЗАСТОСУВАННЯ ПРИСТРОЇВ АДАПТАЦІЇ СУЧАСНИХ ЦИФРОВИХ ЗАСОБІВ ЗВ'ЯЗКУ ВІТЧИЗНЯНОГО ВИРОБНИЦТВА У СКЛАДІ АПАРАТУРИ ВНУТРІШНЬОГО ЗВ'ЯЗКУ БРОНЕОБ'ЄКТІВ.....	33
Минько О.В., Іохов О.Ю., ДЕЯКІ ПИТАННЯ РОЗРОБКИ СТАНДАРТНИХ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАХИЩЕНОСТІ, ЯК ЕЛЕМЕНТУ ОРГАНІЗАЦІЙНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ЦИРКУЛЮЄ У ЕЛЕМЕНТАХ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ.....	34
Обіход Я.Я., Лисечко В.П. РОЗРОБКА МЕТОДУ ВИБОРУ КАНАЛІВ КОГНІТИВНОГО РАДІОПРИЙМАЧА ПРИ МНОЖИННОМУ ДОСТУПУ ПЕРВИННИХ ТА ВТОРИННИХ КОРИСТУВАЧІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ «ENERGY HARVESTING» ПІД КЕРУВАННЯМ НЕЙРОННОЇ МЕРЕЖІ.....	36
Оленченко В.Т. ПЕРЕВАГИ ТА ВАДИ ТОЧКИ ДОСТУПУ НА БАЗІ ТЕХНОЛОГІЇ WI-FI.....	36
Павленко М.А., Зуев П.П. ПРИМЕНЕНИЕ АСУ В УСЛОВИЯХ ВЕДЕНИЯ СОВРЕМЕННОЙ ВОЙНЫ.....	37
Побережний А.А. МЕТОД ОБҐРУНТУВАННЯ СПЕЦІАЛІЗОВАНОЇ ГЕОІНФОРМАЦІЙНОЇ СИСТЕМИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ.	39

Самокіш А.В., Перепелиця О.В., Шаповалов О.В. ПРОПОЗИЦІЇ ЩОДО ФОРМАЛІЗАЦІЇ ПРОЦЕСУ ОЦІНКИ ОБСТАНОВКИ ПРИ ВИРОБЛЕННІ РЕКОМЕНДАЦІЙ ПО ВИЗНАЧЕННЮ ПАРАМЕТРІВ НАВЕДЕННЯ НА НАЗЕМНУ ЦІЛЬ НА ОСНОВІ НЕЧІТКИХ МНОЖИН ТИПУ 1.....	40
Семенко Є.Ю., Споришев К.О. ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В СИСТЕМАХ УПРАВЛІННЯ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ.....	41
Сербин В.В., ПРИНЦИПИ ПОБУДОВИ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ ВІЙСЬКОВИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ.....	43
Скопінцев О.О. ЗАДАЧА ВИБОРУ ВРАЖАЮЧОЇ КОМБІНАЦІЇ ПРИ ПЛАНУВАННІ УДАРІВ ПО МАЛОРОЗМІРНИМ ЗАХИЩЕНИМ ОБ'ЄКТАМ.....	44
Станович О.В., Кротов В.Д. ПРИНЦИПИ ОРГАНІЗАЦІЇ І ПОБУДОВИ ЄДИНОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ.....	45
Тимочко А.И., Павленко М.А., Касьяненко М.В., Литвиненко М.И., Полонский Ю.И. ОБЕСПЕЧЕНИЕ РАДИОЛОКАЦИОННОЙ ИНФОРМАЦИЕЙ В ПРОЦЕССЕ УПРАВЛЕНИЯ ВОЗДУШНЫМ ДВИЖЕНИЕМ В РЕГИОНАЛЬНЫХ ЦЕНТРАХ УПРАВЛЕНИЯ ВОЗДУШНЫМ ДВИЖЕНИЕМ.....	48
Ткаченко К. М. ОБГРУНТУВАННЯ АКТУАЛЬНОСТІ ЗАСТОСУВАННЯ ДОДАТКОВИХ ТЕХНІЧНИХ ЗАХОДІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ПРИХОВАНОГО РАДІООБМІНУ МІЖ ПІДРОЗДІЛАМИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ У ХОДІ ВИКОНАННЯ СЛУЖБОВО-БОЙОВИХ ЗАВДАНЬ.....	49
Устименко О.В. СИТУАЦІЙНІ ЦЕНТРИ ДЕРЖАВНИХ ОРГАНІВ ЯК СКЛАДОВІ СИСТЕМИ ДЕРЖАВНОГО КРИЗОВОГО РЕАГУВАННЯ У СФЕРІ ОБОРОНИ.....	51
Федотов Д.О., Кураш Л.С. БАГАТОКАСКАДНЕ ПІДСИЛЕННЯ В РАДІОКОМПОНЕНТНІЙ БАЗІ ЗВ'ЯЗКУ ТА ІНФОРМАЦІЙНИХ МЕРЕЖАХ.....	52
Флорін О.П. АНАЛІЗ МОЖЛИВОСТЕЙ ІНФОРМАЦІЙНИХ ОБЛІКОВИХ СИСТЕМ ДЛЯ ПОБУДОВИ АВТОМАТИЗОВАНОЇ СИСТЕМИ ОБЛІКУ МАЙНА ЗВ'ЯЗКУ В ЧАСТИНАХ ТА ПІДРОЗДІЛАХ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ.....	54

Для нотаток

НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ

**“Службово-бойова діяльність
Національної гвардії України:
сучасний стан, проблеми та перспективи”**

Секція 5

Збірник тез доповідей

Відповідальний за випуск: *І.Є. Морозов*

Комп'ютерне складання і верстання: *С.О. Воробйов;
О.В.Ніконенко*

Формат 60x84¹/₁₆. Ум. друк. арк. 3,49.
Тираж 50 прим. Зам. № 149

Видавець і виготовлювач Національної академії Національної гвардії України
майдан Захисників України, 3, м. Харків-1, 61001.
Свідоцтво суб'єкта видавничої справи ДК № 4794 від 24.11.2014 р.