

**НАЦІОНАЛЬНА АКАДЕМІЯ
НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ
КОМАНДНО-ШТАБНИЙ ФАКУЛЬТЕТ
КАФЕДРА ВІЙСЬКОВОГО ЗВ'ЯЗКУ**

Збірник тез науково-практичної конференції

**ПЕРСПЕКТИВИ РОЗВИТКУ ТА
ЗАСТОСУВАННЯ СУЧАСНИХ СИСТЕМ І
ЗАСОБІВ ЗВ'ЯЗКУ В ІНТЕРЕСАХ
УПРАВЛІННЯ ВІЙСЬКАМИ**

26 лютого 2019 року

Харків-2019

Перспективи розвитку та застосування сучасних систем і засобів зв'язку в інтересах управління військами: Збірник тез науково-практичної конференції (Україна, м. Харків, 26 лютого 2019 року). – Х.: Національна академія Національної гвардії України, 2019. – 20 с.

Оргкомітет науково-практичної конференції :

Голова оргкомітету – І.М. Майборода, завідувач кафедри військового зв'язку командно-штабного факультету Національної академії Національної гвардії України, кандидат військових наук, доцент.

Відповідальний секретар оргкомітету – О.О. Казіміров, доцент кафедри військового зв'язку командно-штабного факультету Національної академії Національної гвардії України, кандидат військових наук, доцент.

У збірнику представлено наукові доповіді та повідомлення, в яких визначено проблемні питання щодо перспектив розвитку та застосування сучасних систем і засобів зв'язку в інтересах управління військами та службово-бойової діяльності Національної гвардії України; результати наукових досліджень щодо удосконалення сучасних систем і засобів зв'язку.

Матеріали проведення науково-практичної конференції будуть корисними науковцям, викладачам вищих навчальних закладів, керівникам і працівникам силових структур.

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

УДК 623.1.7

Лазарев В.Д., старший викладач кафедри військового зв'язку Національної академії Національної гвардії України;

Овчаренко В.В., кандидат військових наук, доцент, начальник командно-штабного факультету Національної академії Національної гвардії України, полковник.

ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМИ ЗВ'ЯЗКУ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ НА ОСНОВІ ВИКОРИСТАННЯ СУЧАСНИХ ЦИФРОВИХ ТЕХНОЛОГІЙ

Розглянуті питання перспектив побудови та розвитку системи зв'язку Національної гвардії України на основі сучасних досягнень цифрових технологій.

Військовий зв'язок пройшов складний історичний шлях від простих звукових і зорових засобів для передачі сигналів і команд управління боєм до широко розгалужених багатоканальних автоматизованих систем, що забезпечують зв'язок практично на необмежену дальність із стаціонарними і рухомими об'єктами в режимі реального часу.

Сьогодні бойові дії вимагають ефективного управління військами і зброєю, застосування сучасних засобів і комплексів озброєння, військової і спеціальної техніки.

Одне з першочергових завдань будівництва в області військового зв'язку - створення і розгортання об'єднаної автоматизованої цифрової системи зв'язку.

При цьому ключову роль в підвищенні ефективності застосування військ і максимального розкриття бойового потенціалу озброєння грає система зв'язку Національної гвардії України, яка будується на основі останніх досягнень науки і техніки в області інформаційних і телекомунікаційних технологій.

Аналіз війн і військових конфліктів сучасності переконує, що протиборчі сторони широко і без зволікання застосовують перспективні розробки в області озброєння. У сучасній війні роль інформаційних, телекомунікаційних і автоматизованих систем зростає, постійно удосконалюються форми і способи їх використання для досягнення перемоги. Це посилює вимоги до управління військами і, як наслідок, до системи зв'язку.

За оцінками провідних українських і зарубіжних фахівців, вклад системи зв'язку в підвищення ефективності застосування військ (сил) і зброї порівняний зі значним збільшенням кількості бойових засобів або підвищенням їх бойових можливостей. Тому подальший розвиток системи і військ зв'язку – один з пріоритетних напрямків підвищення бойового потенціалу і можливостей Національної гвардії України.

Одним з першочергових завдань будівництва в області військового зв'язку доцільно вважати створення і розгортання об'єднаної автоматизованої цифрової системи зв'язку (ОАЦСЗ) НГУ на основі застосування останніх вітчизняних і зарубіжних розробок в області сучасних цифрових засобів супутникового, радіо-, радіорелейного зв'язку, а також цифрових систем передачі інформації із застосуванням волоконно-оптичних технологій. Серйозна увага повинна приділятися визначенню єдиних принципів функціонування ОАЦСЗ НГУ, її захищеності і безпеки.

УДК 621.396

Горелишев С.А., старший науковий співробітник Науково-дослідної лабораторії Науково-дослідного центра Національної академії Національній гвардії України, кандидат технічних наук, доцент;

Дробаха Г.А., головний науковий співробітник Науково-дослідного центра Національної академії Національній гвардії України, доктор військових наук, професор;

Баулін Д.С., старший науковий співробітник Науково-дослідної лабораторії Науково-дослідного центра Національної академії Національній гвардії України, кандидат технічних наук, доцент.

МОДЕЛЬ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ВІЙСЬКАМИ (СИЛАМИ) НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Розглянуто основні підходи до розроблення моделі автоматизованої системи управління військами (силами) Національної гвардії України. Визначені основні завдання моделі управління та принципи розроблення моделі управління НГ України. Запропоновано склад моделі управління підрозділами.

Модель управління включає основні положення щодо оптимізації автоматизованого управління підрозділів в умовах мінімізації складу бойової обслуги і досягненню максимального рівня автоматизації управлінських функцій.

Основними завданнями моделі управління є: визначення основних напрямків розробки з урахуванням існуючих підходів до організації управління військовими підрозділами в Україні та в провідних країнах світу; розробка основних форм і методів управління підрозділами НГ України; визначення принципів і технічних рішень щодо структури і складу системи управління (СУ) НГ України; розробка технічних рішень з централізованого і децентралізованого управління підрозділами НГ України; розробка технічних рішень по централізованому і децентралізованому, ієрархічному і мережецентричному способам управління; розробка технічних рішень по функціонуванню органів управління підрозділів НГ України; розробка технічних рішень по управлінню підрозділами на різних етапах (планування операцій та управління застосуванням); розробка технічних рішень щодо взаємодії автоматизованої СУ НГ України з іншими СУ.

Принципи розроблення моделі управління НГ України: в основу побудови АСУ НГ України повинна бути покладена відкрита архітектура СУ; розробка технічних рішень по організації АСУ НГ України високого рівня живучості; реалізацію структури автоматизованої СУ НГ України, яка за рахунок утворення інформаційно-комутаційної мережі, об'єднує джерела інформації, органи управління та засоби ураження, що дозволяє забезпечити органи управління достовірною та повною інформацією про обстановку в режимі реального часу; розробка технічних рішень зі стійкої взаємодії СУ НГ України при виконанні бойових (службово-бойових) завдань; забезпечення високого рівня автоматизації управління технічними засобами; використання стандартів НАТО з символіки та військових повідомлень.

Склад моделі управління підрозділами НГ України: загальні положення (суть управління, вимоги до управління, особливості автоматизованого управління підрозділами НГ України, огляд і аналіз принципів управління підрозділами внутрішніх сил та арміях різних країн світу); опис СУ підрозділами НГ України (органи управління, пункти управління підрозділами, основні функції органів управління в ході підготовки і ведення бойових дій та інш.); опис принципів планування службово-бойової діяльності; постановка бойових завдань (порядок, способи, форми постановки завдань підрозділам в ході підготовки і ведення бойових дій); порядок управління озброєнням (зміст, організація застосування озброєння, схеми управління, функції посадових осіб і груп управління, послідовність вирішення основних розрахункових завдань, перелік, призначення і зміст основних команд на підготовку і застосування озброєння); опис та перелік військових повідомлень за стандартами НАТО.

УДК 623.618.2

Сербин В.В., провідний фахівець Державного підприємства «Конструкторське бюро «Південне» ім. М.К. Янгеля»;

Уварова А.О., провідний інженер Державного підприємства «Конструкторське бюро «Південне» ім. М.К. Янгеля».

ОРГАНІЗАЦІЯ СИСТЕМИ ЗВ'ЯЗКУ В УМОВАХ ВИРІШЕННЯ ВНУТРІШНІХ ЗБРОЙНИХ КОНФЛІКТІВ І ЗАБЕЗПЕЧЕННЯ ГРОМАДСЬКОЇ БЕЗПЕКИ

У доповіді розглянуті пропозиції щодо побудови системи зв'язку військових підрозділів Національної гвардії України в умовах адаптивності до умов обстановки, забезпечення вирішення питань підготовки та координації бойових дій різновідомчих сил і засобів, що залучаються до операції.

Жорсткість вимог, що пред'являються до системі зв'язку в сучасних умовах ведення збройних конфліктів та забезпечення громадської безпеки, обумовлені збільшеними потребами органів управління в широкому спектрі послуг зв'язку, що забезпечують безперервне, стійке і ефективне управління при службово-бойовому застосуванні та реалізації всього потенціалу підрозділів Національної гвардії України.

Зв'язок у внутрішньому збройному конфлікті повинен забезпечити:

- управління діями з'єднань, військових частин і підрозділів при локалізації та блокуванні району конфлікту;
- підготовку і проведення спеціальних операцій і бойових дій, що проводяться з метою блокування, роззброєння, знищення незаконних збройних формувань;
- управління діями з охорони й оборони населених пунктів, важливих державних об'єктів, припинення збройних зіткнень і роз'єднання протидіючих сторін, вилученню зброї і вибухових речовин, що незаконно зберігаються;
- супровід і охорону автомобільних колон (комунікацій залізничного і водного транспорту), а також при виконанні інших задач, що виникають.

Досвід бойових дій показує, що для забезпечення управління підрозділами Національної гвардії України у ході активної фази збройного конфлікту, коли динаміка подій вимагає частоти зміни місця розташування пунктів управління, необхідно розгортати рухливі і опорні вузли зв'язку, а також використовувати стаціонарну опорну мережу - як зони відповідальності НГУ, так і взаємодіючих силових структур.

Основа системи зв'язку угруповання військових підрозділів в зоні збройного конфлікту, як правило, складають вузли зв'язку, які розгорнуті в базових районах, і лінії прямого зв'язку, які утворені різними засобами зв'язку. Вузли зв'язку повинні забезпечити обмін інформацією не тільки в інтересах свого пункту управління, але і в інтересах пунктів управління взаємодіючих органів. Концентрація каналного ресурсу на таких вузлах зв'язку повинна дозволити оперативно вирішувати питання по організації зв'язку між угрупованнями військ (сил) різних силових відомств, а також покращує якість заходів з охорони й оборони даних вузлів зв'язку.

У доповіді розглянуті пропозиції щодо організації системи зв'язку шляхом побудови вузлів зв'язку військових підрозділів Національної гвардії України на основі досвіду ДП «КБ «Південне» зі створення автоматизованих систем управління військами.

УДК 621.396

Кащишин О.Л., ад'юнкт науково – організаційного відділу Харківського національного університету Повітряних Сил ім. І. Кожедуба;

Васюта К.С., заступник начальника Харківського національного університету Повітряних Сил ім. І. Кожедуба з навчальної роботи, доктор технічних наук, професор, заслужений діяч науки і техніки;

Сокол О.О., старший викладач кафедри авіаційних радіотехнічних систем навігації та посадки факультету АСУ та наземного забезпечення польотів авіації Харківського національного університету Повітряних Сил ім. І. Кожедуба.

СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ СУЧАСНИХ ЗАСОБІВ ЗВ'ЯЗКУ ТА РАДІОТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ В ЗБРОЙНИХ СИЛАХ УКРАЇНИ

Розглядається сучасний стан та перспективи розвитку системи зв'язку та радіотехнічного забезпечення Збройних сил України.

На даний час розвиток системи зв'язку і автоматизації управління Збройних Сил України має стійку тенденцію до всебічного розвитку та модернізації, переоснащення військ зв'язку новітніми високотехнологічними засобами зв'язку і переходу на сучасні цифрові технології. Тобто питання застосування сучасних технологій та засобів зв'язку у ЗС України є актуальним.

Сьогодні у Збройних Силах України величезна увага приділяється розвитку та вдосконаленню стаціонарної і польової компонент системи зв'язку та автоматизації процесу управління на всіх ланках в частині їх повного переоснащення новітніми засобами, переходу на цифрові системи передачі та обробки інформації.

Як показує практика, станом на кінець 2018 року в Збройних Силах України активно використовуються засоби зв'язку іноземного, але, як правило, цивільного виробництва: транкінгове обладнання Motorola, супутникові термінали Tooway, станції широкосмугового доступу фірм Ubiquiti, Mikrotik, комутатори і маршрутизатори фірм Cisco, Mikrotik, обладнання мережі «Укртелекому» тощо, а також радіозасоби військового призначення фірм Harris, Aselsan. Це дозволило опанувати цифрові технології та об'єднати в короткі терміни достатньо велику кількість вузлів різного рангу в єдину мережу. Однак пошук оптимальних варіантів побудови системи зв'язку ще триває.

Сьогодні, в Збройних Силах України майже не залишилось пунктів управління підрозділів та військових частин, вузли зв'язку, в яких використовують застарілі аналогові технології. В якості первинної (транспортної) мережі передачі даних на даний час використовуються цифрові канали, утворені за допомогою технології Ethernet з використанням проводових, волоконно-оптичних, супутникових ліній зв'язку. Провайдерами надання телекомунікаційних послуг є ПрАТ «Укртелеком» (виділення ресурсу телекомунікаційної мережі загального призначення, послуга MPLS), ПрАТ «Датагруп» (послуга MPLS, надання супутникових каналів) та ін. У польових умовах для прив'язки вузлів зв'язку пунктів управління до транспортної мережі передачі даних використовуються комплексні апаратні зв'язку, обладнані радіорелейними станціями Р-450 (військовий зразок) та станціями широкосмугового доступу Mikrotik, Ubiquiti (цивільні зразки).

Застосування новітнього високотехнологічного обладнання зв'язку дало змогу відмовитись від застарілих та слабоефективних принципів організації і забезпечення зв'язку і радіотехнічного забезпечення польотів та перейти до організації надання в інтересах пунктів управління якісних інформаційно-телекомунікаційних сервісів: IP-телефонія, відео та аудіо конференція, швидкісна передача даних, криптографічний захист інформації, обмін електронними повідомленнями, тощо.

УДК 621.396

Симоненко О.В., старший викладач кафедри радіотехнічних систем навігації та посадки факультету АСУ та НЗПА Харківського національного університету Повітряних Сил ім. І.Кожедуба, кандидат технічних наук;

Черкасов А.В., курсант факультету АСУ та НЗПА Харківського національного університету Повітряних Сил ім. І. Кожедуба;

Оленич А.В. курсант факультету АСУ та НЗПА Харківського національного університету Повітряних Сил ім. І. Кожедуба.

ДОСВІД ЗАСТОСУВАННЯ ВІЙСЬК ЗВ'ЯЗКУ ТА ІНФОРМАЦІЙНИХ СИСТЕМ ПОВІТРЯНИХ СИЛ ПІД ЧАС ПРОВЕДЕННЯ АНТИТЕРОРИСТИЧНОЇ ОПЕРАЦІЇ

Наводиться досвід військ зв'язку повітряних сил під час проведення антитерористичної операції.

В ході проведення Антитерористичної операції (АТО) під час організації зв'язку з підрозділами, які висувалися у райони виконання завдань, перевага віддавалася мобільним та зручним у користуванні терміналам супутникового та транкінгового зв'язку з організацією IP-телефонії та передачі даних. Традиційні штатні засоби радіо та радіорелейного зв'язку, як правило, залишалися в якості резервних.

Зміни в системі зв'язку характеризувалися швидким переходом від використання каналів тональної частоти, систем гучномовного зв'язку до IP-телефонії із застосуванням засобів криптографічного захисту інформації, побудованих з використанням сучасних цифрових технологій. При цьому враховувалась необхідність закриття інформації в тактичній ланці управління, де наявність засобів криптографічного захисту була не передбачена відповідними штатами.

З метою приховування роботи короткохвильові постійно діючі радіолінії Повітряних Сил Збройних Сил України було переведено на режим роботи з використанням 10% потужності передавачів. В умовах застосування противником засобів радіоелектронної боротьби, під час роботи у наземних короткохвильових радіолініях Повітряних Сил, була організована робота в закріплених радіотелефонних радіомережах та радіо напрямках в режимі слуховий телеграф (АТ).

До початку АТО за основу при організації повітряного радіозв'язку управління державною авіацією (ЗС, ДПС, МВС, ДСНС, авіабудівні та авіаремонтні заводи) в країнах-учасниках СНД використовувались вихідні дані, які розроблялись Російською Федерацією (єдині повітряні радіомережі, радіомережі взаємодії, єдині паролльні числа, позивні по типам транспортних повітряних суден тощо).

Аналіз застосування авіації в умовах активної роботи радіорозвідки та радіоелектронної боротьби противника свідчить про необхідність їх самостійної розробки та доведення до підпорядкованих військ (сил), інших видів ЗС України та силових структур держави.

Для забезпечення надійного управління літаками в повітрі у повітряних радіомережах було змінено позивні льотного складу бойової авіації Збройних Сил України, силових Міністерств (відомств) України та здійснено перехід на Єдині паролльні сигнали України, що раніше не практикувалося та стало вирішальним при забезпеченні скритого управління бойовою авіацією. Після виконання зазначеного майже кожен екіпаж винищувальної авіації при передачі управління повітряним судном запитував пароль у ПУ, якому передавався під управління.

Відпрацьовано та доведено бойовий варіант повітряних радіоданих, який включав в себе окремі радіочастоти основного, запасного та прихованого каналів управління повітряними суднами у кожному з трьох діапазонів: МХ-1, МХ-2 та ДМХ.

При організації повітряного радіозв'язку управління авіацією з використанням літака-ретранслятора було визначено порядок організації повітряного радіозв'язку через ретрансляційні радіостанції бортових вузлів зв'язку літаків-ретрансляторів.

З метою підвищення достовірності доведення інформації до екіпажів повітряних суден, які залучалися до операцій в ході АТО було організовано роботу з наземних пунктів управління авіацією одночасно на каналах метрового та дециметрового діапазонів. Екіпаж (пілот) при виявленні завади на основних, запасних та прихованих метрових каналах управління без додаткової команди здійснював перехід на відповідний дециметровий канал.

Аналіз функціонування системи зв'язку Повітряних Сил на початку проведення АТО, переконливо свідчить про низький рівень її технічного оснащення сучасними засобами, що впливало на пропускну спроможність, завадо захищеність та функціональну сумісність з телекомунікаційними мережами інших міністерств та відомств України. Реалізація вище зазначених заходів дозволило та дасть можливість в подальшому здійснювати ефективне централізоване та децентралізоване управління військами (силами), як в особливий період так і в мирний час.

УДК 621.396

Белокурсський Ю.П., асистент кафедри Харківського національного університету радіоелектроніки;

Щербина О.О., кандидат технічних наук, доцент, доцент кафедри Харківського національного університету радіоелектроніки.

ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМИ РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ ПІДРОЗДІЛІВ ТАКТИЧНОЇ ЛАНКИ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Проведений аналіз можливостей та визначені особливості побудови системи радіоелектронної боротьби підрозділів тактичної ланки НГУ.

Аналіз змісту вітчизняних і зарубіжних військових статутів та настанов щодо забезпечення заходів радіоелектронної боротьби (РЕБ) в різних умовах застосування дає змогу визначити склад основних розроблених документів: карта оцінки електромагнітної обстановки (ЕМО); перелік радіоелектронних засобів (РЕЗ); каталог норм частотно-територіального розносу РЕЗ; базова модель радіопридушення радіоелектронних пристроїв; план комплексного технічного контролю; план роботи служби РЕБ; посібник з організації захисту РЕЗ і засобів радіозв'язку; базові та часткові моделі застосування сил і засобів розвідки і РЕБ противника; типові моделі перспективної електронної обстановки тощо.

На відміну від збройних сил забезпечення заходів РЕБ підрозділами тактичної ланки Національної гвардії України (НГУ) мають своє специфіку, пов'язану з розмірами позиційного району і особливостями динаміки застосування підрозділів за призначенням. Для прийняття рішення на виконання заходів РЕБ із перелічених вище документів доцільним є розроблення топографічної або електронної карти оцінки ЕМО, що містить характеристики ЕМО, позначення місць розгортання РЕЗ, відбиває питання забезпечення електромагнітної сумісності (ЕМС) РЕЗ.

Забезпечення ЕМС потребує наявності даних про розміщення сил і можливості засобів радіопридушення противника, величини напруженості електромагнітного поля (ЕМП) в зонах покриття службового і мобільного зв'язку, перелік постійно заборонених і робочих частот.

Довідковий документ з питань забезпечення ЕМС має містити перелік (каталог) РЕЗ, які функціонують в позиційному районі, координати розташування, належність, позивний, тип, а також основні тактико-технічні характеристики, що впливають на сумісність: діапазон робочих частот, потужність радіопередавальних пристроїв, ширина спектра випромінюваного сигналу, чутливість приймачів і ширина смуги пропускання, тип антенно-фідерного пристрою, його діаграма спрямованості та коефіцієнт підсилення.

Наявність перелічених вихідних даних, а також даних радіорозвідки та моніторингу електромагнітної обстановки в позиційному районі дають змогу визначити, зокрема, способи і засоби пасивного і активного маскування і побудувати ефективну систему захисту зв'язку і РЕБ підрозділу НГУ.

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ ЗАСОБІВ РАДІООБМІНУ ТА АДАПТАЦІЯ СИСТЕМИ РАДІОЗВ'ЯЗКУ ДО УМОВ ВПЛИВУ НАВМИСНИХ ЗАВАД

Доповідь присвячена розв'язанню актуальної наукової проблеми, яка полягає у забезпеченні завадозахищеності засобів радіообміну в умовах зміни заводової обстановки та дії радіотехнічної розвідки за рахунок розробки та використання імпровізованих (нестандартних) спрямованих антен та ФАР як елементів захисту радіозасобів, оптимізації їх параметрів і просторового розміщення.

За результатами аналізу стану проблеми, особливо при проведенні Антитерористичної операції (Операції об'єднаних сил) на Сході України, виявлено низку вад у системі радіозв'язку військ (сил). Визначені напрямки щодо підвищення завадозахищеності засобів радіообміну. Розв'язання наукової проблеми пропонується шляхом оптимізації параметрів засобів радіообміну та адаптації системи радіозв'язку до умов впливу навмисних завад. Оптимізацію здійснено на основі єдиного комплексного підходу чисельних методів розрахунку зон завадостійкого радіообміну та зон розташування засобів активного радіомаскування з використанням відповідних імітаційних моделей радіообміну, які враховують характеристики діаграм спрямованості антенних пристроїв.

Наукова новизна отриманих результатів полягає в розвитку теоретичних положень з оптимізації параметрів засобів радіообміну та адаптації системи радіозв'язку до умов впливу навмисних завад для підвищення їх завадозахищеності в умовах зміни заводової обстановки.

Обґрунтовано вибір конструкції антен дециметрового діапазону як базових елементів у комплексі зі штатними засобами військового призначення для побудови локальної, а також просторово-розподіленої систем радіоелектронного захисту за агрегатно-модульним принципом. Такі системи можуть бути виготовлені в польових умовах, в умовах майстерень, вбудовані в техніку та обладнання з метою усунення демаскуючих ознак. Отримані дані використані при організації зв'язку в зоні проведення ООС

Запропоновано використання конформних ФАР з можливістю фокусування послідовностей БЧ ПЧС в заданій точці простору та отримано оцінки просторово-часових характеристик БЧ ПЧС. Отримані дані можна використовувати для створення принципово нових систем мобільного радіозв'язку, побудованих на принципах структури MESH з використанням WiMAX-сумісних систем, стандарту IEEE802.16m.

Отримані у ході дослідження наукові та практичні результати в сукупності вирішують важливу наукову проблему шляхом розробки на основі єдиного теоретичного підходу методів адаптації систем радіозв'язку та оптимізації параметрів засобів радіообміну в умовах реальної заводової обстановки та дії засобів радіоелектронної розвідки. Це має велике значення як для розвитку окремого напрямку теорії захисту від навмисних завад і радіоелектронної розвідки, так і для рішення прикладних питань, пов'язаних з забезпеченням заданої завадостійкості та розвідзахищеності засобів радіообміну.

УДК. 623.612

Власов К.В., старший викладач кафедри військового зв'язку Національної академії Національній гвардії України;

Гончар Р. О., кандидат військових наук, старший науковий співробітник науково-дослідної лабораторії службово-бойового застосування Національної гвардії України науково-дослідного центру, підполковник.

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ РАДІОМЕРЕЖ ІЗ САМООРГАНІЗАЦІЄЮ У ВІЙСЬКОВИХ СИСТЕМАХ ЗВ'ЯЗКУ

Розглядається характеристика радіомереж із самоорганізацією та перспективи їх застосування у військових системах зв'язку.

Головною тенденцією розвитку майбутніх систем зв'язку є мобільність. В проєкті IST WSI, а також в „Книзі нових концепцій” Міжнародного форуму по дослідженню безпроводних технологій (WWRF) представлена нова концепція мобільного зв'язку, який, з точки зору користувача, можна представити у вигляді декількох сферичних рівнів.

У розглянутій концепції величезна роль належить радіомережам із самоорганізацією (РМС). РМС припускають можливість організації безпроводової мережі без участі людини або з її мінімальною участю. Дана архітектура мережі отримала назву ad-hoc (по-латині), що в даному випадку означає „випадкова, спонтанна” або „спеціально створена для певних цілей”.

Основою для створення таких мереж є високий рівень „інтелектуальності” сучасних радіотерміналів, що містять крім приймально-передавальних блоків досить продуктивні обчислювальні засоби - процесор, пам'ять великої ємності, що дозволяє реалізовувати складні алгоритми.

В даний час йдуть дослідження зі створення інтелектуальних радіозасобів і мереж у цілому, які можуть адаптувати свої режими і алгоритми роботи на основі рішень, що приймаються системами управління в яких використовуються бази даних і знань.

Більшість розвинених країн світу розглядають застосування військових РМС як перспективу розвитку систем зв'язку тактичного і оперативно-тактичного рівня. Мобільна компонента (сукупність мереж, що мають здатність до самоорганізації, переміщення, згортання і розгортання вузлів) покликана забезпечити інформаційний обмін в інтересах всіх військ, які є в тактичній зоні незалежно від їх підпорядкування і завдань, які вони виконують. Передбачається, що її архітектура неоднорідна, ієрархічна і складатиметься з наступних основних рівнів: 0-й рівень, який можуть утворювати сенсорні мережі (мережі телеметрії); 1-й рівень - мобільні радіомережі низової ланки управління - бойові радіомережі; 2-й рівень - мережі мобільних базових станцій (МБС), що утворюють опорну мережу; 3-й рівень - повітряна (космічна) мережа, яка може бути реалізована на безпілотних літальних апаратах (супутниках).

Система зв'язку тактичної ланки розвивається в напрямку застосування відкритої архітектури, впровадження новітніх телекомунікаційних технологій, які застосовуються у комерційних системах зв'язку.

Існуючі цивільні технології (фізичного та каналного рівнів) безпроводних мереж зв'язку являють собою основу для створення мобільних радіомереж тактичного рівня.

Розглянута архітектура мобільної компоненти систем військового зв'язку - 3-х рівнева ієрархія неоднорідних мобільних радіомереж (мобільних абонентів - мобільних базових станцій - безпілотних літальних апаратів) типу MANET. Реалізація кожного її рівня дозволить значно покращити якість функціонування системи зв'язку та параметри інформаційного обміну.

Однак для її впровадження поки необхідно вирішення низки проблем наукового (розробка математичного та програмного забезпечення інтелектуальної децентралізованої системи управління тощо) та технологічного плану (наявність програмуємих багатофункціональних багатодіапазонних радіозасобів).

ОСОБЛИВОСТІ РОЗГОРТАННЯ ТА ЗГОРТАННЯ ВУЗЛА ЗВ'ЯЗКУ ДПУ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Визначені особливості розгортання та згортання вузла зв'язку ДПУ НГУ при вирішенні завдань в інтересах управління військами.

ДПУ (допоміжний пункт управління) – це спеціально обладнані, оснащені необхідними технічними засобами зв'язку і автоматизованого управління військами комплекти на рухомій (транспортній) базі спеціальних апаратних пунктів управління (СА ПУ), з яких командувач НГУ особисто, через штаб та інші органи управління здійснює управління військами.

Вузол зв'язку ДПУ (ВЗ ДПУ) є організаційно-технічне об'єднання сил та засобів зв'язку і автоматизованого управління, призначених для обміну усіма видами інформації та ведення переговорів у процесі управління військами (силами). ВЗ ДПУ призначений для зв'язку з угрупованнями військ, які діють на ізольованому або віддаленому оперативному напрямку чи районі, завжди повинен бути готовим при виході зі строю або при переміщенні КП прийняти на себе функції основного вузла в системі зв'язку та забезпечити управління в повному обсязі. ВЗ ДПУ є постійно діючим і виконує свої задачі у ході всієї операції.

Розгортання ДПУ проводиться в районах, вказаних старшим начальником, якому підпорядковується ДПУ. По прибуттю в район розгортання, спеціальні автомобілі (СА), апаратні зв'язку (АЗ), комплексні апаратні зв'язку (КАЗ) розміщуються розосереджено, в укриттях (якщо район визначено заздалегідь та виділена необхідна кількість інженерної техніки для відривання укриття), проводиться ретельне маскуванню, приховування від усіх видів розвідки, організовується надійна охорона та оборона, встановлюється суворий порядок переміщення транспорту й особового складу. У районі розташування ДПУ забороняється робити демаскувальні позначення і написи.

Розміщення ВЗ ДПУ на місцевості, його інженерне обладнання повинно забезпечувати:

- захист засобів, і ВЗ в цілому, від засобів ураження противника;
- своєчасне встановлення всіх видів зв'язку і надання їх посадовим особам;
- зручність користування засобами зв'язку посадовим особам;
- можливість швидкої евакуації засобів зв'язку в разі необхідності;
- можливість оперативного управління ВЗ і зручність його охорони та оборони.

В залежності від характеру місцевості елементи ВЗ повинні розміщатися як на пункті управління, так і поза його межами. З метою захисту ДПУ від високоточної зброї (ВТЗ) противника необхідно розміщувати ВЗ від СА ПУ на відстані від 2 до 3 км.

В цілях захисту ВЗ від ВТЗ противника необхідно:

техніку розміщати групами по 2-3 машини на відстані 100-200 метрів між групами і 30-50 метрів між технікою;

максимально використовувати маскувальні властивості місцевості (ліс, високі кущі, зворотні схили пагорбів, яри), підручні засоби (гілки, колоди, дерен);

застосовувати табельні індивідуальні маскувальні засоби і спеціальні радіопоглинаючі покриття;

екранувати вихлопні устрої і двигуни транспортних засобів азбестом, та іншими теплоізоляційними матеріалами, виносити бензоелектричні та дизельні агрегати на максимально можливі відстані, закопувати їх з метою поглинання шуму;

застосовувати кутові відбивачі і теплові пастки.

При виборі місця розгортання радіорелейної станції необхідно враховувати рельєф місцевості (відсутність перешкод на трасі), можливість під'їзду станції до місця розгортання, а також можливість укриття і маскуванню.

Після розгортання автономної мережі або підключення до промислової мережі живлення розгортається система зв'язку (прокладаються кабелі зв'язку від ВЗ ПУ до СА ПУ; утворюються канали засобами прямого зв'язку, проводиться їх настройка вимірювання (при необхідності) і розподіл; приймаються канали від опорної мережі зв'язку, проводиться їх вимірювання, розподіл та комутація (транзит); розгортається робота шифроргану; встановлюються заплановані зв'язки і забезпечується їх постійна готовність до передачі (прийому) інформації; забезпечується обмін всіма видами інформації у встановлені нормативами терміни; організовується внутрішній оперативний та телефонний зв'язок на ПУ, розгортається робота частотно-диспетчерської служби; проводиться завчасна підготовка на важливих інформаційних напрямках декількох видів зв'язку, а також резервування засобів зв'язку і каналів, розробляється порядок нарощування системи зв'язку та маневрування засобами, каналами і видами зв'язку). Лінії внутрішнього зв'язку в районі розміщення ДПУ повинні бути закопані в ґрунт або замасковані.

Після розгортання ДПУ з особовим складом проводиться тренування по зв'язку під час здійснення охорони та оборони з використанням сигналів оповіщення, прихованого управління. До особового складу доводиться порядок та час зміни паролів в районі розміщення ДПУ, проводиться ТСЗ щодо порядку дій особового складу по тривозі, проводиться збір особового складу в районі збору, доводиться порядок та шляхи виходу по тривозі.

Для забезпечення швидкого згорання ВЗ проводяться підготовчі заходи: звільняються від кріплення кабельні лінії; готуються котушки для зняття з'єднувальних ліній; згортаються найменш важливі лінії внутрішнього і дальнього зв'язку, резервні антени КШМ; КШМ готуються для забезпечення зв'язку під час руху. Посадові особи ДПУ, перед згоранням ВЗ, переходять для роботи в КШМ. Порядок і час згорання ВЗ доводиться до особового складу завчасно, а робота по згоранню починається по команді (сигналу) відповідного начальника.

Згорання проводиться в наступній послідовності:

проводиться демаскування СА ПУ, апаратних зв'язку, наметів;

одночасно проводиться згорання системи зв'язку (кабелів зв'язку від ВЗ ПУ до СА ПУ), промислової мережі живлення, завантаження виносного обладнання, згорання наметів та завантаження їх на транспорт, згорання робочих місць, апаратури зв'язку;

знищуються всі сліди перебування в районі військової техніки та особового складу.

УДК 629.735

Чечуй О.В., доцент кафедри радіоелектронних систем пунктів управління Повітряних Сил Харківського національного університету Повітряних Сил, кандидат технічних наук, доцент;

Комін Д.С., старший викладач кафедри радіоелектронних систем пунктів управління Повітряних Сил Харківського національного університету Повітряних Сил, кандидат технічних наук;

Панхохін О.С., курсант Харківського національного університету Повітряних Сил;

Павловський В.А., курсант Харківського національного університету Повітряних Сил.

ФОРМАЛІЗОВАНА МОДЕЛЬ ОЦІНКИ ГАРАНТІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Розглянуті особливості проведення оцінювання гарантій інформаційної безпеки для комплексної системи захисту інформації. Запропоновано застосування формалізованої моделі процесу оцінювання вимог гарантій інформаційної безпеки суб'єктів експертизи із застосуванням аксіоматичних конструкцій.

Невід'ємною частиною будь-якої інформаційно-телекомунікаційної системи (ІТС) військового призначення, особливо там, де здійснюється обробка інформації з обмеженим доступом (ІзОД), є комплекс заходів, пов'язаний із забезпеченням збереження, цілісності інформації та належного порядку доступу до неї. Для цього розробляється та впроваджується в ІТС комплексна

система захисту інформації (КСЗІ). Для оцінки якості та відповідності КСЗІ проводиться експертиза із залученням відповідних організацій та компетентних експертів, які мають оцінити рівень гарантій інформаційної безпеки (ІБ). Існує цілий ряд методів оцінки гарантій ІБ за вимогами міжнародних стандартів. Однією з основних проблем які виникають у сфері оцінки гарантій ІБ, є те, що для більшої частини вимог гарантій застосовуються лише кількісні значення.

Пропонується застосування формалізованого підходу для побудови моделі оцінки гарантій ІБ КСЗІ. Оскільки оцінка гарантій ІБ є діяльністю, яка включає процеси взаємодії суб'єктів експертизи і процеси виконання дій з оцінки в ході експертизи, то до оцінки гарантій доцільно підходити з позицій процесного підходу.

При розробці моделі процесу оцінки гарантій ІБ були враховані наступні аспекти:

- функціональний, який точно визначає, що здійснюється елементами процесу;
- інформаційний, який відображає інформаційну сутність, яка формується, виробляється або використовується процесом;
- організаційний, який описує хто і коли виконує конкретні дії, роботи, операції процесу із включенням фізичних механізмів передачі і зберігання об'єктів;
- каузальний, який відноситься до координації і залежності дій, суб'єктів цих дій.

Дана модель може розглядатись як базова та може застосовуватись для подальших досліджень процесу оцінювання гарантій ІБ, а саме для визначення вимог до результатів експертизи, щодо неупередженості, об'єктивності, повторюваності, відтворюваності і порівнянності.

УДК 355.404

Воронін О.І., старший викладач кафедри військового зв'язку Національної академії Національної гвардії України;

Вахненко О.О., начальник відділу зв'язку штабу - начальник зв'язку Східного територіального управління Національної гвардії України, полковник.

ОСОБЛИВОСТІ БОЙОВОГО ЗАСТОСУВАННЯ ЦИФРОВИХ РАДІОРЕЛЕЙНИХ СТАНЦІЙ Р-402 У СИСТЕМІ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ

Розглянуті можливі варіанти застосування радіорелейних станцій Р-402 при виконанні завдань зі зв'язку частинами і підрозділами зв'язку НГУ.

Надходження на озброєння у частини і підрозділи зв'язку НГУ цифрових радіорелейних станцій Р-402 вимагає здійснювати пошуки ефективного використання їх можливостей при виконанні НГУ бойових та службово-бойових завдань.

Радіорелейна станція Р-402 дозволяє створювати радіоканали дальньої дії з пропускнуою здатністю до 300 Мбіт/с та дальністю до 35 кілометрів для одного інтервалу у діапазоні частот 4800-6100 ГГц. Комплект антен може забезпечити роботу станції у варіантах «точка-точка» або «точка-багатоточка» для утворення радіомережі з географічно-широкою зоною покриття.

Варіантами бойового застосування Р-402 можуть бути:

1. Прив'язка вузлів зв'язку ПУ НГУ мобільної компоненти до вузлів зв'язку операторів зв'язку. Забезпечується доступ посадових осіб рухомих ПУ до цифрової телекомунікаційної мережі НГУ. Підвищується надійність, розвідзахищеність та завадозахищеність зв'язку без зниження його якості та зменшення пропускнуої здатності.

2. Прив'язка вузлів зв'язку ПУ НГУ мобільної компоненти до стаціонарних вузлів зв'язку військових частин НГУ. Може використовуватись при проведенні комплексних навчальних занять, навчань, бойового злагодження в межах навчальних центрів, районів зосередження військових частин. Забезпечується доступ керівних посадових осіб навчань, злагодження до цифрової телекомунікаційної мережі НГУ.

3. Забезпечення обміну інформацією між ПУ НГУ вищої ланки системи управління з декількома ПУ нижньої ланки («точка-багатоточка»).

4. Забезпечення зв'язку взаємодії між ПУ частин та з'єднань НГУ при виконання бойових та службово-бойових завдань.

5. Прив'язка вузлів зв'язку ПУ НГУ мобільної компоненти до опорних вузлів зв'язку ЗСУ. Забезпечується доступ посадових осіб рухомих ПУ до цифрової телекомунікаційної мережі НГУ та забезпечення взаємодії з оперативним складом ПУ ЗСУ.

6. Забезпечення дистанційного управління радіостанціями середньої потужності короткохвильового діапазону та станцій супутникового зв'язку при винесенні їх за межі ПУ. Підвищується надійність, розвідзахищеність та завадозахищеність зв'язку без зниження його якості та зменшення пропускну здатності.

На відміну від аналогових радіорелейних станцій Р-409, Р-402 забезпечує більшу якість каналів зв'язку, більшу пропускну здатність радіорелейних ліній, більшу їх, надійність, розвідзахищеність та завадозахищеність. Крім того, Р-402 має набагато меншу масу і розміри ніж Р-409, не потребує особистої транспортної бази для переміщення, тобто може перевозитись будь-яким транспортом, що дає суттєві переваги за мобільністю.

Розглянуті варіанти бойового застосування радіорелейних станцій Р-402 суттєво підвищують ефективність радіорелейного зв'язку.

УДК 621.396

Майборода І.М., завідувач кафедри військового зв'язку Національної академії Національної гвардії України, кандидат військових наук, доцент.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ NVIS ТЕХНОЛОГІЇ ПРИ ОРГАНІЗАЦІЇ КХ РАДІОЗВ'ЯЗКУ

Розглянуті особливості використання NVIS технології та визначені її переваги при організації КХ радіозв'язку в інтересах управління військами.

NVIS (Near Vertikal Incidence Skywave) технологія передбачає використання іоносферних хвиль, що забезпечують дальність зв'язку до 500 км за рахунок реалізації методу просторового поширення сигналу, наближеного до вертикального.

По перше, ця технологія надає можливість не враховувати рельєф місцевості та інші перешкоди на шляху поширення радіохвиль при організації КХ радіозв'язку. Крім того, при NVIS поширенні практично відсутні замирання сигналу (fading) та майже відсутня зона «мовчання» (Skip zone), а змінюючи кут випромінювання антени можливо забезпечувати тривалий час надійний зв'язок на короткі та середні відстані.

По друге, правильно сформований сигнал NVIS має максимальну величину випромінювання у вертикальному напрямку та мінімальний рівень поверхневої хвилі, що ускладнює виявлення противником місцезнаходження радіостанції. Також технологія NVIS дозволяє значно знизити рівень шуму і перешкод, що сприяє підвищенню рівня сигнал/шум (SNR) та у поєднанні з низьким рівнем втрат надає можливість використовувати сучасні цифрові радіостанції військового призначення з малим (20-30 Вт) рівнем потужності передавача, які мають дуже високу надійність та невеликі ваго-габаритні показники, що робить їх дуже сприятливими для організації радіозв'язку в тактичній ланці управління та при проведенні спеціальних операцій.

В третє, антени, оптимізовані для NVIS, зазвичай, низько розташовані, та можуть бути добре замасковані, при цьому оптимальне значення кута випромінювання для NVIS досягається при висоті точки живлення антени від 0,25 до 0,1 довжини хвилі над землею. На практиці, в залежності від значень провідності ґрунту, цілком задовільно працюють навіть антени з висотою від 1,5 до 3 метрів над землею. антени в режимі NVIS не мають вираженої направленості в горизонтальній площині і не потребують азимутальної орієнтації.

Для успішної цілодобової роботи NVIS необхідно принаймні три різні смуги частот і тому бажано використовувати багато- або широкосмугові антени. Прості диполі також дуже добре

працюють та можуть бути легко встановлені в польових умовах. Диполь може успішно використовуватися як базисний варіант при створенні різноманітних конфігурацій антен зенітного випромінювання (АЗВ), наприклад: «Перевернуте V»; «Нахилена V»; «Вертикальний напівромб»; «Довгий провід LW»; «Перевернуте L»; «L- подібна».

Основною вимогою до АЗВ є формування діаграми направленості (ДН) в якій основне випромінювання відбувається під високими кутами від 50° до 90° до горизонту. Цей механізм NVIS іоносферного поширення дозволяє покриття значної території (радіусом до 750км) без зони «мовчання», подібно до того, як вода, що витікає з направленою вертикально вгору шлангу створює ефект «парасольки».

Необхідно відзначити, що, наприклад, у випадках інсталяції КХ-радіостанцій виробництва Harris на командно- штабних машинах Р-142 та радіостанціях Р-161 можливе використання штатних антен АЗВ, які є готовим рішенням для режиму NVIS. Для цього необхідна лише незначна модернізація блоків узгодження цих антен.

УДК 621.396.24

Глущенко М.О., старший викладач кафедри військового зв'язку Національної академії Національної гвардії України.

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ПРОГРАМИ HARRIS VOACAP ДЛЯ ПРОГНОЗУВАННЯ ПОШИРЕННЯ РАДІОХВИЛЬ КХ ДІАПАЗОНУ

Розглянуті особливості використання програми Harris VOACAP для прогнозування поширення радіохвиль на КХ іоносферних радіолініях зв'язку.

Надійність і стійкість КХ іоносферних радіоліній визначаються часом доби, порою року, активністю сонця та рівнем космічного випромінювання. Особливо це становиться актуальним для груп розвідки, які діють за межами прямої дальності зв'язку, тому звичайні системи тактичного радіозв'язку не відповідають вимогам передачі інформації підрозділами розвідки, де точна і своєчасна передача отриманих відомостей є найбільш важливим аспектом їх бойових завдань.

Групи розвідки повинні оснащуватися і працювати на системах зв'язку із збільшеною дальністю дії. Короткохвильова радіостанція, наприклад радіостанція Harris RF-7800H-MP, є надійним засобом зв'язку з дальністю дії до 800 км. Для кожного сеансу зв'язку повинна бути обрана необхідна частота, а для кожної передачі повинна бути правильно обрана антена.

Якість, безперервність, стійкість та таємність зв'язку залежить від вміння оператора у практичній роботі максимально врахувати фактори, які впливають на поширення радіохвиль у КХ-діапазоні, особливо іоносферною хвилею. Для цього необхідно знати, які чинники впливають сильніше, як їх враховувати, де брати необхідні дані для розрахунків та своєчасно реагувати на їх зміну.

Основними умовами успішного КХ-зв'язку іоносферною хвилею є:

- відбиття (переломлювання) радіохвиль від іоносфери;
- напруженість поля корисного сигналу повинна перевищувати рівень перешкод (радіохвилі не повинні суттєво послаблюватись шарами іоносфери).

Головним чином ці фактори впливають на вибір частот і конфігурацію антен. В залежності від частоти радіохвилі мають різні властивості - енергетику, проникаючу здатність тощо, а від конфігурації антени залежить те, під яким кутом до горизонту буде здійснено випромінювання, та рівень напруженості електромагнітного поля.

У програмне забезпечення Harris Communications Planning Application (CPA) вбудовано відомий програмний продукт HF Propagation, який базується на алгоритмах VOACAP. Цей програмний продукт дозволяє дізнатися про оптимальні робочі частоти для визначеного регіону або радіотраси впродовж доби. Щоб скористатися цим продуктом треба знати координати розташування передавача та приймача.

За наявності підключення до мережі Інтернет програма автоматично отримає необхідні

данні про стан сонця з сайту Центру прогнозування космічної погоди (SPACE WEATHER PREDICTION CENTER) Національного управління океану та атмосфери Сполучених Штатів Америки. Також оператор отримує розрахункові значення відстані та напрямку на кореспондента, що допоможе зорієнтувати антени.

Оператору необхідно повторити процес прогнозування VOACAP кілька разів, намагаючись розібрати різні варіанти антен або різні потужності, щоб побачити, який маємо ефект та прогнозовану надійність.

Для дальнього зв'язку вдень доцільно використовувати частоти від 10 МГц і вище, вночі - від 9 МГц і нижче. Для покриття зони до 500 км від радіопередавача є сенс використовувати технологію NVIS (частоти 3,5-5 МГц і відповідні антени). В окремих випадках, для компенсації втрат в шарі D, необхідно збільшувати вихідну потужність радіопередавача та застосовувати антени з більшим коефіцієнтом підсилення.

УДК. 372.862

Казіміров О.О., доцент кафедри військового зв'язку Національної академії Національній гвардії України, кандидат військових наук, доцент;

Куртов А. І., професор кафедри загальновійськових дисциплін військово-юридичного факультету Національного юридичного університету ім. Ярослава Мудрого, кандидат технічних наук, доцент;

Потіхенський А.І., викладач кафедри підготовки офіцерів запасу військово-юридичного факультету Національного юридичного університету ім. Ярослава Мудрого

ОСОБЛИВОСТІ СТВОРЕННЯ ФАЙЛУ ПРОШИВКИ ДЛЯ ЦИФРОВИХ РАДІОСТАНЦІЙ СИСТЕМИ “МОТОТРВО” ВИРОБНИЦТВА “MOTOROLA”

Розглядаються особливості програмування радіостанцій “Motorola” системи “Mototrbo” прошивкою 2017 року.

У 2016 році введена в дію інструкція про порядок програмування цифрових радіостанцій в Національній гвардії України. Ця інструкція визначає: вимоги до програмування засобів цифрового радіозв'язку; обов'язки посадових осіб щодо програмування цифрових радіостанцій; особливості програмування цифрових радіостанцій Motorola та порядок заміни ключів шифрування на радіостанціях “Motorola”.

Програмування цифрових радіостанцій проводиться на персональних електронно-обчислювальних машинах з використанням спеціального програмного забезпечення, інтерфейсного кабелю для програмування та підготовлених файлів з відповідними параметрами конфігурації. Файли для прошивки радіостанцій підготовлюються для кожного типу радіостанцій на основі єдиних файлів конфігурації, розроблених управлінням зв'язку та інформатизації штабу Головного управління Національної гвардії України. Файли прошивки радіостанцій відрізняються ім'ям радіостанції, ID-номером радіостанції, паролем на включення радіостанції та паролем блоку параметрів.

У файлі прошивки 2017 року створено 9 зон, які призначені для організації радіозв'язку в різних умовах несення служби. За кожною зоною закріплені відповідні ключі шифрування – по два на кожну. При цьому непарні ключі шифрування закріплені за локальними каналами, а парні – за каналами ретрансляторів. Заміну ключі шифрування дозволяється проводити у військових частинах лише у зоні, яка закріплена за частиною.

Для зв'язку між абонентами обов'язковим являється їх робота на одних каналах в одних та тих же зонах. На випадок компрометації ключів шифрування у файлі конфігурації передбачені запасна зона та резервні канали.

Застосування визначеного порядку програмування радіостанцій з єдиним файлом конфігурації виключить втрату зв'язку між частинами та підрозділами Національної гвардії

України, а також зв'язку взаємодії з частинами та підрозділами Збройних сил України при виконанні службово-бойових завдань.

УДК 621.396

Красноручський А.О., начальник кафедри авіаційних радіоелектронних комплексів інженерно-авіаційного факультету Харківського національного університету Повітряних Сил, кандидат технічних наук, старший науковий співробітник;

Олексін О.О., старший викладач кафедри авіаційних радіоелектронних комплексів інженерно-авіаційного факультету Харківського національного університету Повітряних Сил.

БОРОТЬБА З БПЛА ПРОТИВНИКА ТА ТЕНДЕНЦІ ПРОТИДІЇ БПЛА РАДІОЕЛЕКТРОННА РУШНИЦЯ ДЛЯ БОРОТЬБИ З БПЛА

Розглянуті основні тенденції протидії БпЛА. Надається інформація щодо використання радіоелектронних рушниць для боротьби з БпЛА зарубіжних та вітчизняних виробників.

В умовах сучасного ведення війни інформаційна складова має вирішальне значення для обох сторін конфлікту. Саме найпростіші дешеві безпілотні літальні апарати різних типів найбільш масово застосовуються в сучасних локальних і гібридних війнах. Десятки ворожих апаратів збирають інформацію про місце дислокації українських військових. Чи не єдиним способом для нашої армії знешкодити такі пристрої є знищення їх за допомогою стрілецької зброї чи зенітних установок. Для знешкодження невеликого безпілотника такі методи неефективні та потребують значних ресурсів. Тому проти міні-БпЛА доцільно використовувати засоби радіоелектронної боротьби (РЕБ). І цілком природно, що виник світовий тренд розробки мобільних, і простих в експлуатації засобів боротьби для їх придушення.

Важливою вразливою ланкою в управлінні БпЛА є необхідність ведення постійного обміну інформацією з наземними пунктами управління. Великий обсяг переданих даних вимагає наявності досить активних каналів радіозв'язку, для яких дуже складно (практично неможливо в сучасних умовах) забезпечити необхідні скритність роботи і високий рівень надійності. Розвідавши частоти роботи каналів зв'язку БпЛА з наземними пунктами управління, наявними постановниками перешкод («глушилками»), цілком можливо ці працюючі канали зв'язку забити перешкодами.

Створення купола радіоелектронних перешкод для систем навігації, управління польотом, каналів зв'язку та радіоліній прийому-передачі над полем бою здатне привести до значного зниження ефективності бойового застосування або до повної нейтралізації БпЛА. Щорічно розробники з усього світу представляють нові системи знешкодження БпЛА.

Компанія Battelle у 2015 році розробила унікальну антидронову гвинтівку. Пристрій створює радіоперешкоди, після чого БпЛА зазвичай застосовує протокол безпеки та виконує одну із запрограмованих дій: зависає в повітрі, робить посадку чи повертається назад. Drone Defender від компанії Battelle (США) може впевнено знешкоджувати безпілотники на відстані до 400 метрів.

Турецькою Компанією Aselsan була розроблена антидронна система HASAVAR. Вона являє собою комплект з портативного рюкзака й антидронного глушника-рушниць. Рушниця повністю «відрізає» безпілотник від оператора. Пристрій усуває необхідність відстеження сенсорних систем та дозволяє одразу знешкодити БпЛА».

Концерн «Калашников» розробив рушницю REX 1. Пристрій пригнічує канали управління БпЛА, глушить GPS, ГЛОНАСС і WI-FI-сигнали, а також мобільний зв'язок. Рушниця REX-1 важить 4,2 кілограма і може працювати без заряджання до трьох годин.

Фахівцями компанії «Укрспецтехніка» розроблено першу вітчизняну портативну зброю для протидії БпЛА. Принцип дії – постановка перешкод навігаційним каналам.

УДК 621.391

Чечуй О.В., доцент кафедри радіоелектронних систем пунктів управління Повітряних Сил Харківського національного університету Повітряних Сил, кандидат технічних наук, доцент;

Женжера С.В., старший викладач кафедри радіоелектронних систем пунктів управління Повітряних Сил Харківського національного університету Повітряних Сил, кандидат технічних наук;

Зливко А.О., курсант Харківського національного університету Повітряних Сил.

МЕТОДИ ПОБУДОВИ АНТЕННО-ФІДЕРНИХ СИСТЕМ В МЕРЕЖАХ ТРАНКІНГОВОГО ЗВ'ЯЗКУ ДЛЯ БОРОТЬБИ З НАПРАВЛЕНИМИ ЗАВАДАМИ

Розглянуті методи побудови вібраторних синфазних антенних решіток для антенно-фідерних систем ретрансляторів транкінгового зв'язку в умовах застосування противником направлених завад з метою підвищення якості зв'язку.

Досвід ведення бойових дій при проведенні ООС свідчить про широке застосування супротивником засобів РЕБ у всіх ланках управління військами, при чому ці засоби є сучасними і застосовуються у широкому діапазоні частот. Особливої актуальності набуває вирішення питання забезпечення якісного зв'язку в мережах транкінгового зв'язку тактичної ланки управління військами при створенні супротивником складної завадової обстановки.

Аналіз існуючих антенно-фідерних систем (АФС) транкінгового зв'язку показує, що їхні характеристики відповідають вимогам, які пред'являються до цивільних систем зв'язку (забезпечення максимальної зони покриття), а для АФС військового призначення постає необхідність побудови антен, які повинні мати додаткові, більш жорсткіші вимоги до розвід захищеності, формуванню зон покриття, електромагнітної сумісності радіоелектронних засобів, які працюють на пунктах управління.

Для вирішення такої задачі пропонується застосування вібраторних антени, які виконані у вигляді двох симетричних вібраторів над циліндричною поверхнею із застосуванням діаграмно-створюючої схеми, що дозволяє реалізувати необхідний амплітудно-фазовий розподіл струмів в симетричних вібраторах і тим самим отримати заданий розподіл поля випромінювання в азимутальному просторі.

За результатами розрахунків проведено моделювання АФС за допомогою програми MMANA та здійснено аналіз отриманих результатів.

Запропонований антенний пристрій з секторальною діаграмою спрямованості в порівнянні з антенами не напрямленого типу дозволяє підняти енергетичний потенціал транкінгової мережі радіозв'язку, а отже підвищити якість зв'язку при застосуванні супротивником засобів РЕБ.

УДК 621.317.3

О. П. Флорін, доцент кафедри військового зв'язку Національної академії Національної гвардії України, кандидат технічних наук, доцент.

ВІРТУАЛЬНИЙ РЕКОНФІГУРОВАННИЙ ВИМІРЮВАЧ ПАРАМЕТРІВ І ХАРАКТЕРИСТИК ВІЙСЬКОВОЇ ТЕХНІКИ ЗВ'ЯЗКУ

Розглянуто результати розробки архітектури віртуального реконфігурованого вимірювача параметрів і характеристик військової техніки зв'язку. Обґрунтована доцільність побудови віртуального вимірювача з використанням програмованих логічних інтегральних схем. На основі запропонованої архітектури створений один з можливих варіантів реалізації вимірювача.

При випробуваннях та експлуатації зразків військової техніки зв'язку (ВТЗ) виникає необхідність у вимірюваннях великої кількості їх параметрів і характеристик. Для вирішення цього завдання застосовують відповідну кількість засобів виміральної техніки (ЗВТ) або

одного складеного. Використання одного складеного віртуального вимірювача (ВВ), що виконує функції декількох вимірювальних приладів, дозволяє комплексно аналізувати значення параметрів і характеристик ВТЗ.

Розглянуто можливості використання програмованих логічних інтегральних схем для побудови віртуальних реконфігурованих вимірювачів. Розглядаються результати розробки архітектури віртуального реконфігурованого вимірювача параметрів та характеристик озброєння і військової техніки, що включає апаратне та програмне забезпечення. Апаратне забезпечення включає комп'ютер, засоби вводу-виводу, що складаються з датчиків, вторинного перетворювача з використанням програмованих логічних інтегральних схем і вузлів сполучення інтерфейсів та програматор. Програмне забезпечення (ПЗ) складається з системного, інструментального та прикладного ПЗ. В якості системного ПЗ використовувалася операційна система Windows. Інструментальна складова ПЗ представлена системою автоматизованого проектування (САПР) LabVIEW. Інструментальне програмне забезпечення передбачає використання САПР Quartus.

На основі запропонованої архітектури створений один з можливих варіантів реалізації вимірювача. Вимірювач дозволяє змінювати свою конфігурацію (номенклатуру параметрів, їх кількість та метод вимірювання) безпосередньо в процесі проведення вимірювань за командою оператора або автоматично за заданими критеріями.

Показані особливості архітектури і побудованого на її основі вимірювача, а також переваги використання віртуального вимірювача при проведенні технічного обслуговування ВТЗ.

УДК 621.396.96

Кондратенко О.П., професор кафедри автобронетанкової техніки Національної академії Національної гвардії України, доктор технічних наук, професор;

Волков П.Ю., ад'юнкту докторантури та ад'юнктури Національної академії Національної гвардії України, майор.

КОНЦЕПЦІЯ МОНІТОРИНГУ РУХОМИХ ОБ'ЄКТІВ В ЗОНІ ОХОРОНИ ВАЖЛИВИХ ДЕРЖАВНИХ ОБ'ЄКТІВ ТЕХНІЧНИМИ ЗАСОБАМИ ОХОРОНИ

Розглянуто рекомендації для ефективного захисту особливо важливих державних об'єктів в умовах виникнення терористичних загроз.

Забезпечення безпеки на важливих державних об'єктах на даний час здобуває особливу актуальність. Концепція розвитку сектора безпеки і оборони України, вимоги до поетапного розвитку НГУ передбачають оснащення підрозділів охорони сучасними технічними засобами охорони, які забезпечать адекватність сучасним загрозам національній безпеці держави. Разом з тим стрімкий розвиток технічних засобів охорони у світі, поява нових загроз і небезпек у сфері охорони державних об'єктів, нових видів рухомих об'єктів, виявили низку невідповідностей зіставлення сучасного стану техніки загрозам і небезпекам, щодо яких можна здійснювати моніторинг і яким можна протидіяти в сфері охорони державних об'єктів із застосуванням таких технічних засобів. Це потребує переосмислення, удосконалення, узагальнення класифікації технічних засобів, які можуть застосовуватись для охорони та захисту охороняємих державних об'єктів.

Саме коректна класифікація як технічних засобів, так і загроз національній безпеці дозволить здійснити адекватний вибір нових технічних рішень і засобів для виявлення і протидії загрозам і небезпекам у сфері охорони державних об'єктів.

Сучасне забезпечення моніторингу охороняємих ділянок місцевості визначається в основному міжнародною технічною допомогою у вигляді тепловізійних комплексів і систем оптико-електронного спостереження. У 2017 році прийнято до експлуатації підрозділами НГУ засіб наземної розвідки РЛС "Лис-2М". Крім зазначених нових засобів охорони у підрозділах

НГУ використовуються РЛС типів СБР-3, ПСНР-5 та їх модифікації. При цьому факторами, що принципово обмежують використання таких технічних засобів охорони, є лісистість місцевості, її пересіченість, а також вплив гідрометеорологічних факторів. Ці фактори ослаблюють потужність радіолокаційного сигналу, отже, зменшують дальність виявлення РЛС.

Для складання обрисів перспективної РЛС необхідно визначитися з простим питанням, а саме – рух яких об'єктів повинен бути зафіксований. Додатково до людини та автотранспорту останнім часом з'явилися такі об'єкти-порушники, як безпілотні літальні апарати (БПЛА) та малі пілотовані літальні апарати, а також підземні об'єкти (трубопроводи, тунелі). Отже, вертикальна шкала виявлення об'єктів має обмежуватися 1–2 км над поверхнею землі і виявлення повинно відбуватись автоматично.

Загальні вимоги та підходи до організації охорони особливо важливих державних об'єктів.

Актуальність розробки рекомендацій для ефективного захисту особливо важливих об'єктів досить висока і визначається станом сил і технічних засобів охорони на об'єктах, що захищаються, реальностями виникнення терористичних загроз. Не виключено, що об'єктами терористичних актів можуть стати важливі і особливо важливі об'єкти, а також об'єкти підвищеної небезпеки і життєзабезпечення.

При виборі технічних засобів охорони особливе значення має правильне застосування технічних засобів захисту, їх тактично правильне розташування в зонах безпеки і узгодженість в роботі. При виборі засобів захисту необхідно звернути увагу на:

- сумісність;
- умови експлуатації;
- стійкість;
- електроживлення;
- термін служби;
- функції управління.

При формуванні вимог до системи безпеки для захисту середніх і великих об'єктів, для периметра території об'єкта доцільно використовувати такі засоби захисту:

- різні огорожі і паркани;
- перешкоди, які повинні ускладнити пересування порушника по території об'єкта і підвищити ймовірність його виявлення системою сигналізації;
- спеціально обладнані в'їзди і проходи на територію, де знаходяться перші пости охорони, які контролюють доступ відвідувачів і проїзди автомашин до будівель. Останнім часом набули поширення пристрої, що швидко висувуються (за сигналом тривоги) — з полотна в'їзної дороги залізобетонні перешкоди-пандуси;
- система охоронної сигналізації для захисту всього периметра об'єкта або особливо вразливих його частин;
- система охоронного відеоспостереження для візуального спостереження за периметром території об'єкта, за проходами і в'їздами на територію, а також за найбільш важливими ділянками території, такими як склади, стоянки автомашин тощо;
- система чергового і тривожного освітлення території об'єкта: чергове освітлення вмикається постійно в нічний час, а тривожне освітлення тільки після спрацьовування сигналізації, для освітлення найбільш важливих зон території і підходів до будівель.

Таким чином, рекомендації та пропозиції вироблені на основі результатів наукових досліджень, закладаються в методологічну основу для розробки більш ефективних засобів фізичного захисту особливо важливих об'єктів.

Національна гвардія не відстає від часу, і на багатьох об'єктах часові замінені відеокамерами, датчиками руху і багатьма іншими сучасними охоронними системами. При спрацьовуванні будь-якого датчика на об'єкті, що охороняється, на це місце негайно висувається добре озброєна тривожна група на бронемашинах.

ЗМІСТ

Лазарев В.Д., Овчаренко В.В. Особливості побудови системи зв'язку Національної гвардії України на основі використання сучасних цифрових технологій.....	3
Горєлишев С.А, Дробаха Г.А., Баулін Д.С. Модель автоматизованої системи управління військами (силами) Національної гвардії України.....	4
Сербин В.В., Уварова А.О. Організація системи зв'язку в умовах вирішення внутрішніх збройних конфліктів і забезпечення громадської безпеки.....	5
Кашишин О.Л., Васюта К.С., Сокол О.О. Сучасний стан та перспективи застосування сучасних засобів зв'язку та радіотехнічного забезпечення в Збройних силах України.....	6
Симоненко О.В., Черкасов А.В., Оленич А.В. Досвід застосування військ зв'язку та інформаційних систем повітряних сил під час проведення антитерористичної операції.....	7
Белокурский Ю.П., Щербина О.О. Особливості побудови системи радіоелектронної боротьби підрозділів тактичної ланки Національної гвардії України.....	8
Іохов О.Ю. Оптимізація параметрів засобів радіообміну та адаптація системи радіозв'язку до умов впливу навмисних завад.....	9
Власов К.В. , Гончар Р.О. Перспективи застосування радіомереж із самоорганізацією у військових системах зв'язку.....	10
Горбатюк П.М., Мехов С.Д. Особливості розгортання та згортання вузла зв'язку ДПУ Національної гвардії України.....	11
Чечуй О.В., Комін Д.С., Панхохін О.С., Павловський В.А. Формалізована модель оцінки гарантій інформаційної безпеки комплексної системи захисту інформації	12
Воронін О.І., Вахненко О.О. Особливості бойового застосування цифрових радіорелейних станцій Р-402 у системі зв'язку та інформатизації Національної гвардії України.....	13
Майборода І.М. Особливості використання NVIS технології при організації КХ радіозв'язку.....	14
Глущенко М.О. Особливості використання програми Harris VOACAP для прогнозування поширення радіохвиль КХ діапазон.....	15
Казіміров О.О. Куртов А. І., Потіхенький А.І., Особливості створення файлу прошивки для цифрових радіостанцій системи “MOTOTRBO” виробництва “MOTOROLA”.....	16
Красноруцький А.О., Олексін О. О. Боротьба з БПЛА противника та тенденції протидії БПЛА. Радіоелектронна рушниця для боротьби з БПЛА.....	17
Чечуй О.В Женжера С.В., Зливко А.О. Методи побудови антенно-фідерних систем в мережах транкінгового зв'язку для боротьби з направленими завадами	18
Флорін О.П. Віртуальний реконфігурований виміррювач параметрів і характеристик військової техніки зв'язку.....	18
Кондратенко О.П., Волков П.Ю. Концепція моніторингу рухомих об'єктів в зоні охорони важливих державних об'єктів технічними засобами охорони.....	19

НАУКОВЕ ВИДАННЯ

ПЕРСПЕКТИВИ РОЗВИТКУ ТА
ЗАСТОСУВАННЯ СУЧАСНИХ СИСТЕМ І
ЗАСОБІВ ЗВ'ЯЗКУ В ІНТЕРЕСАХ
УПРАВЛІННЯ ВІЙСЬКАМИ

Збірник тез науково-практичної конференції

(українською мовою)

Друкується в авторській редакції

Кафедра військового зв'язку командно-штабного факультету
Національної академії Національної гвардії України
61001, м. Харків, пл. захисників України, 3