

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

**Збірник тез науково-практичної конференції**

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

**23 лютого 2021 року**



**Харків-2021**

Перспективи розвитку та застосування сучасних систем і засобів зв'язку в інтересах управління військами: Збірник тез науково-практичної конференції (Україна, м. Харків, 23 лютого 2021 року). – Х.: Національна академія Національної гвардії України, 2021. – 50 с.

**Оргкомітет науково-практичної конференції :**

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

**Відповідальний секретар оргкомітету – О.О. Казіміров**, доцент кафедри військового зв'язку та інформатизації 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, а також результати наукових досліджень щодо удосконалення сучасних систем і засобів зв'язку.

Матеріали проведення науково-практичної конференції можуть бути корисними для науково-педагогічних працівників вищих навчальних закладів, а також офіцерів частин та підрозділів силових структур.

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

**УДК 654.01**

**Власов К.В.**, старший викладач кафедри Національної академії Національній гвардії України  
**Фик О.І.**, доцент кафедри Національної академії Національній гвардії України, доктор технічних наук, доцент

**ОСНОВНІ ТЕРМІНИ ТА ПРИНЦИПИ ЗВ'ЯЗКУ ТА ІНФОРМАЦІЙНИХ СИСТЕМ НА СУЧАСНОМУ ЕТАПІ ЗА СТАНДАРТАМИ НАТО**

Основою управління військами є рішення командира, що розробляється на основі інформації, яка отримується від різних джерел в єдиному інформаційному просторі, у т.ч. з використанням взаємосумісних систем / мереж зв'язку та інформаційних систем. У свою чергу, поняття “мережа” в сучасних війнах охоплює різні складові, які раніше розглядалися лише окремо, та між якими постійно повинен здійснюватися інформаційний обмін, наприклад: бойові одиниці (бойові машини, озброєння, підрозділи тощо), системи зв'язку, інформаційне забезпечення операцій, різноманітні джерела розвідки, логістичні та медичні інформаційні системи тощо. Тобто для ведення сучасних війн та отримання переваги над противником збройними силами повинен використовуватися єдиний інформаційний простір, побудований на взаємосумісних мережах / системах зв'язку, які забезпечують захищений обмін інформацією між ними, для підвищення загальної ситуаційної обізнаності та управління військами (силами).

На сучасному етапі в ЗСУ проведено значний обсяг роботи щодо впровадження єдиних термінів та принципів зв'язку та інформаційних систем. Станом на 02.11.2020 прийнято та впроваджується 15 стандартів та доктрина ЗСУ “Зв'язок та інформаційні системи”.

Доктрина ЗСУ “Зв'язок та інформаційні системи” (ВКП 6-00(01).01, червень 2020 року) визначає можливості зв'язку та інформаційних систем у ЗС України та інших складових сил оборони і представляє стратегічні основні принципи зв'язку та інформаційних систем, що узгоджені із Стратегією національної безпеки України, враховують вимоги Основної об'єднаної оперативної концепції “Сили оборони – 2030” та дозволяють забезпечити готовність сил оборони до всеохоплюючої (тотальної) оборони шляхом проведення об'єднаних (міжвидових, міжвідомчих, багатонаціональних) операцій з використанням єдиного інформаційного простору.

Підходи, викладені у цій Доктрині, спрямовані в першу чергу на відхід від використання радянського терміну “зв'язок і автоматизоване управління військами” в системі управління до запровадження термінів “єдиний інформаційний простір”, “комунікаційна система (система зв'язку)”, “інформаційна система” та “сервіс”, та, започаткування процесів побудови в ЗС України та інших складових сил оборони єдиного інформаційного простору, як складової системи управління, відповідно до положень концепцій, розроблених в США (ведення бойових дій з використанням єдиного інформаційного середовища (*en: Network Centric Warfare, NCW*)) та НАТО (концепція єдиного інформаційного середовища НАТО (*en: NATO Network Enabled Capability, NNEC*)).

УДК 621.396.96

**Горєлишев С.А.**, старший науковий співробітник науково-дослідної лабораторії Національної академії Національної гвардії України, кандидат технічних наук, доцент

**Волков П.Ю.**, ад'юнкт Національної академії Національної гвардії України

**Баулін Д.С.**, старший науковий співробітник науково-дослідної лабораторії Національної академії Національної гвардії України, кандидат технічних наук, старший науковий співробітник.

## ГЕОМЕТРИЧНІ ТА ЕНЕРГЕТИЧНІ ХАРАКТЕРИСТИКИ СИСТЕМИ СПОСТЕРЕЖЕННЯ У БІСТАТИЧНОЇ РАДІОЛОКАЦІЇ ПРИ ЗОВНІШНЬОМУ ПІДСВЕЧУВАННІ

Розвиток техніки радіолокації і технології дозволив у багато разів збільшити як кількість, так і підвищити якість отримуваної інформації, а також використати радіолокаційні станції для спостереження за приземними та наземними об'єктами, у тому числі і біологічними.

Проведені раніше дослідження показують, що використання передавачів цифрового телебачення формату Т2 для створення прихованої бістатичної системи спостереження цілком можливо – по крайній мере, в геометричному трактуванні. Широка мережа телевізійних передавачів дозволяє вибрати з них необхідні для створення зони попередження щодо вторгнення на територію об'єкту, що охороняється.

Разом з тим відома класична формула радіолокації вимагає уточнення в рамках зміни значення бістатичного кута залежно від можливого розташування об'єкта в геометричному полі системи. Залежно від типу джерела випромінювання геометрія системи істотно розрізняється.

Приймаючи ефективну площу розсіювання (ЕПР) рівної 0,5...1 м<sup>2</sup>, для потужності корисного сигналу одержимо -136,9 дБ/Вт. Переводячи дане значення в чутливість приймача одержуємо  $1,1 \times 10^{-14}$  Вт, що є граничною чутливістю. Такий рівень сигналу може бути отриманий у межах всієї зони підсвічування, без врахування росту ЕПР об'єкта в бістатичній області. Відзначимо, що порівняння потужності прямого та відбитого сигналів визначає вимоги до динамічного діапазону приймача - не менш 51 дБ, тобто сигнали один від одного відрізняються більше чим в 120000 разів.

ЕПР є найважливішою характеристикою виявлення об'єкта. Для однопозиційної станції ЕПР є здатність об'єкта розсіювати електромагнітну енергію в напрямку, протилежному напрямку опромінення. Для бістатичної радіолокаційної системи при описі відбиваючої здатності об'єкта необхідно враховувати можливі різні напрямки від об'єкта на передавальну (передавальна станція формату Т2) і на приймальну (наземний приймач) позицію. Такою характеристикою є бістатична ЕПР об'єкта, значення якої залежить від величини бістатичного кута від об'єкта на передавальну й на приймальну позиції.

Особливий інтерес при визначенні енергетичних характеристик бістатичної системи представляє ефект так званої “просвітної” локації, що проявляється при бістатичних кутах  $\geq 130^\circ$  та характерно для даної постановки задачі. Відповідно до теорії електромагнітного поля, з появою на шляху поширення електромагнітної хвилі абсолютно “чорного” тіла більших у порівнянні з довжиною хвилі розмірів позаду тіла з'явиться “тіньове” поле розсіювання. “Тіньове” поле зосереджене у вузькому тілесному куті поблизу бістатичного кута в  $180^\circ$ , так що його, по американській термінології, можна називати полем “розсіювання вперед”, а реальний об'єкт можна вважати абсолютно “чорним” тілом, що створює тільки “тіньове” поле розсіювання. Звідси випливає, що в наближенні фізичної оптики “тіньове” поле об'єкта не залежить від форми об'єкта і повністю визначається його “тіньовим” контуром. Крім того, на “тіньове” поле не впливає й матеріал поверхні об'єкта, що суттєво послабляє поле розсіювання цього об'єкту. Це дуже важливо для завдання виявлення малопомітних цілей, до яких можливо віднести і біологічні об'єкти. Однак при роботі РЛС у метровому та дециметровому діапазоні багато об'єктів зондування мають вже резонансне розміри, тобто порівнянні з довжиною хвилі.

У цьому випадку варто приділити особливу увагу уточненню значення бістатичної відбиваючої ефективною поверхні об'єктів зондування, як металевих, так і діелектричних при різних величинах бістатичного кута.

Наступної важливої характеристикою бістатичної РЛС, безпосередньо пов'язаної з потужністю сигналу, що розсіяне об'єктом, є зона дії бістатичної ланки, під якої будемо розуміти область простору, у якому повинен перебувати об'єкт, щоб потужність корисного сигналу на вході приймача була не гірше граничного рівня. Завдання полягає у визначенні бістатичного кута при різних азимутах й відстанях об'єкта від приймальної позиції.

Для подальших розрахунків виберемо конкретний регіон розташування передавача підсвічування та місце розташування приймальної станції. Для прикладу виберемо Харківську область, тоді для реалізації режиму “просвітної” локації, як передавач, візьмемо радіотелевізійну передавальну станцію Белгорода. Відстань Харків-Белгород становить близько 40 км, а висота підвісу антени відповідно 221 м. На цьому прикладі північної границі Харківської області й використанням підсвічування телепередавачами Білгородського регіону показана можливість спостереження об'єктів у зоні відповідальності.

Аналіз результатів проведених досліджень та розрахунків показав що:

- при використанні підсвічування сучасним сигналом телевізійної станції формується досить більша робоча зона, величину якої необхідно буде скоротити на етапі вторинної обробки прийнятої інформації;

- повний кут спостереження представляє близько  $60^0$ , що відповідним чином впливає на організацію огляду простору;

- залежно від енергетичного потенціалу бістатичної системи необхідно організувати скоординований огляд доступного кута спостереження: послідовний, паралельний, змішаний;

- для змішаного принципу огляду простору необхідно формування як мінімум 10 парціальних діаграм спрямованості приймальної антени із шириною кожної 8 градусів для виключення напрямків, що не переглядаються;

- для забезпечення контролю всієї передньої півсфери потрібно мати три таких станції з перенацілюванням бісектриси кута на відповідну передавальну станцію.

При наявності достатньої енергетики у якості приймальної антени можна використати, наприклад, уже існуючу антену типу ChannelMaster 4228, діаграми спрямованості якої будуть незначно змінюватися залежно від частоти трансляції.

Одна така антена здатна приймати сигнали в секторі приблизно  $60^0$ , що забезпечить контроль території розміром 1,5...5 км залежно від величини бази. Для повного охоплення фронтальної зони (передньої півсфери) буде потрібно не менш трьох таких антен з відповідними приймачами або з одним приймачем, що перемикається по входу при наявності запасу в часі.

Проведені дослідження підтвердили можливість ухвалення обґрунтованого рішення щодо доцільності проведення подальших досліджень у напрямку використання сигналів радіопередавальних телевізійних станцій формату Т2 для виявлення порушників зони охорони важливих державних об'єктів на тлі природних перешкод. Крім того, становлено що необхідно провести аналіз характеристик бістатичних систем, які використовують інші джерела підсвічування – наприклад, станції стільникового зв'язку, для порівняння отриманих результатів.

**УДК. 355.404**

**Воронін О.І.**, старший викладач кафедри Національної академії Національної гвардії України  
**Сальніков О.М.**, професор кафедри Національної академії Національної гвардії України

## **ВАРІАНТИ ЗАСТОСУВАННЯ ЦИФРОВИХ РАДІОРЕЛЕЙНИХ СТАНЦІЙ Р-425С3 У СИСТЕМІ ЗВ'ЯЗКУ ТА ІНФОРМАТИЗАЦІЇ НГУ**

При забезпеченні радіорелейного зв'язку в НГУ переважно використовуються цифрові радіорелейні станції Р-402. На озброєнні частин зв'язку ЗСУ перебувають цифрові радіорелейні станції Р-425С3 вітчизняного виробництва. За своїми технічними характеристиками станції не можуть працювати разом, тому є потреба розглянути варіанти застосування станцій Р-425С3 у частинах зв'язку НГУ.

Радіорелейна станція Р-425С3 дозволяє будувати цифрові лінії зв'язку в протяжність до 20 інтервалів зі швидкістю передавання інформації не менше 155 Мбіт/с у діапазоні частот 6,43-7,10 ГГц. На відміну від Р-402, станція представляє собою сукупність радіорелейного і телекомунікаційного обладнання, яке розміщене в пристрої ВО-6С і контейнері ТК-6С. Крім того, склад обладнання станції є уніфікованим, що дозволяє її використовувати як кінцеву так і як проміжну (вузлову). При забезпеченні ретрансляції станція може здійснювати шлейфи по радіочастоті, по проміжній і низькій частоті. Обладнання станції дозволяє дистанційне юстирування антени як за азимутом так і за кутом місця, чого критично не вистачає у Р-402. Ще однією перевагою Р-425С3 є наявність джерела безперебійного живлення. Воно працює від змінного струму напругою 220 В, але при вимкненні (зникненні) її, джерело живлення автоматично переходить у режим роботи від акумуляторних батарей. Наявність у складі Р-425С3 телекомунікаційного обладнання дозволяє безпосередньо від станції оперативно надавати користувачам необхідні цифрові канали.

Таким чином, радіорелейні станції Р-425С3 мають суттєві переваги перед станціями Р-402, що дозволяє пропонувати в перспективі прийняти на озброєння частин зв'язку НГУ.

Варіантами бойового застосування Р- Р-425С3 можуть бути:

1. Побудова багатоінтервальних радіорелейних ліній в'язку між ПУ НГУ на заміну супутникових або їх дублювання. Це дасть змогу підвищити надійність, розвідзахищеність та завадо захищеність зв'язку без зниження його якості та зменшення пропускну 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 зв'язку взаємодії між ПУ частин та з'єднань НГУ при виконанні бойових та службово-бойових завдань.

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

5. 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 завадо захищеність зв'язку без зниження його якості та зменшення пропускну здатності.

Розглянуті варіанти бойового застосування радіорелейних станцій Р-425С3 суттєво підвищують ефективність системи зв'язку НГУ.

**УДК 623.4.017**

**Новикова О.О.**, доцент кафедри Національної академії Національної гвардії України, кандидат технічних наук

**Глущенко М.О.**, старший викладач кафедри Національної академії Національної гвардії України.

## **СПЕЦІАЛЬНА ПІДГОТОВКА ОСОБОВОГО СКЛАДУ ІЗ ТЕХНІЧНОГО ЗАБЕЗПЕЧЕННЯ**

Висока боєготовність і боєздатність підрозділів істотно залежать від рівня підготовленості особового складу, правильної експлуатації техніки в складних умовах сучасного загальновійськового бою, вміння максимально використовувати бойові можливості, закладені в конструкцію техніки, а успішне вирішення завдань з відновлення техніки – від рівня підготовленості особового складу підрозділів і частин технічного забезпечення.

У сучасних умовах роль і значення спеціальної підготовки особового складу незмірно зростають. Це обумовлено тим, що підрозділи і частини оснащені високоефективними і складними засобами зв'язку, при створенні яких широко використовуються останні досягнення науково-технічного прогресу.

Спеціальна підготовка полягає в навчанні особового складу підрозділів технічного забезпечення прийомам і способам відновлення та правилам виконання робіт з технічного обслуговування техніки.

Для більшості засобів зв'язку за величиною відносних витрат часу на різні складові ремонту близько 50% часу займає пошук несправностей, до 30% – заміна несправного елемента (вузла), до 5% – доставка необхідного для ремонту елемента, до 15% – перевірка і налаштування комплексу техніки.

Результати спостережень показують, що при знаходженні несправностей характерними для багатьох фахівців є такі помилки:

- великий проміжок часу на постановку діагнозу причини відмови і невпевненість в поставленому діагнозі;
- виконання зайвих вимірювань, хоча в більшості випадків інформація, що отримується за допомогою сигналізації, перевірки параметрів і режимів роботи, цілком достатня для пошуку елемента, що відмовив;
- прагнення фахівців усунути несправність, використовуючи тільки зовнішні ознаки, що приводить, як правило, до вибору нераціонального алгоритму пошуку, збільшення витраченого на це часу, до невиправданих заміन деталей і до появи додаткових відмов;
- перевірка фахівцями в першу чергу більш доступних вузлів, що часто призводить до подовження процесу пошуку несправності.

Зазначені недоліки можна усунути, якщо навчити фахівців методиці пошуку несправностей на апаратурі.

Важливими напрямками вирішення проблеми скорочення термінів пошуку відмов може бути впровадження вбудованого контролю технічного стану, розробка спеціальних інструкцій і методик послідовності пошуку відмов елементів (вузлів), в яких були б викладені методи вибору оптимальної послідовності пошуку на основі глибокого вивчення структури системи, що обслуговується, а також укомплектованість ЗПП і чіткою організацією доставки необхідних деталей.

УДК 621.396.7

**Женжера С.В.**, старший викладач кафедри Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук

**Бровко А.А.**, курсант Харківського національного університету Повітряних Сил імені Івана Кожедуба

## ШЛЯХИ ЗБІЛЬШЕННЯ НАДІЙНОСТІ ОХОРОНИ ВІЙСЬКОВИХ ОБ'ЄКТІВ ПРИ ПРОТИДІІ ТАКТИЧНИМ БПЛА ШЛЯХОМ ЗАСТОСУВАННЯ ЗАСОБІВ РЕП

На даному етапі актуальним є створення таких постановників завад, які б були ефективними для протидії надлегким БПЛА при охороні військових об'єктів. Аналіз ведення бойових дій в зоні проведення ООС показав, що противник має досить значну кількість безпілотних літальних апаратів, що зумовлює необхідність створення новітніх спеціалізованих генераторів завад, які могли б протистояти цим БПЛА.

Перш за все, в зоні проведення ООС, для повітряного нападу НЗФ використовують малорозмірні та малошумні літальні апарати, з яких застосовуються запальні/фугасні боєприпаси. Вони невеликі за розміром і тому НЗФ використовують їх на багатьох ділянках – в деяких випадках до десятка апаратів вночі. Причому цілями для бойових дій, як правило, вибираються невідомі до подібного сценарію об'єкти на другій та третій лінії оборони (до 20 км) – перш за все це склади боєприпасів. Актуальність даної проблеми підтверджується випадком, який відбувся у Харківській області на складах зберігання боєприпасів в м. Балакліє.

На основі аналізу принципів та методів побудови генератора завад було запропоновано та обґрунтовано схему генератора завад, що забезпечить подавлення каналу управління БПЛА на частоті 2,4 ГГц і забезпечить більш високу надійність військових об'єктів (рис. 1).

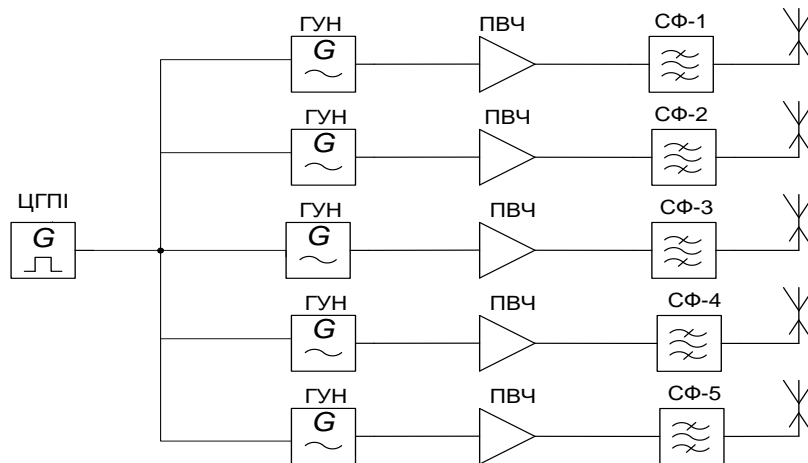


Рисунок 1 – Функціональна схема генератора завад:

ЦГПІ – цифровий генератор псевдовипадкових імпульсів; ГУН – генератори, що управляються напругою; ПВЧ – підсилювачі високої частоти; СФ – смугові фільтри

У результаті розрахунків при відстані до оператора пульта управління БПЛА 50...200 метрів дійшли до висновку, що зона подавлення відповідає нормам по охороні об'єктів складів РАО, тому доцільно використовувати запропонований пристрій при охороні об'єктів. Застосування запропонованого пристрою дозволить покращити надійність охорони об'єктів та захисту складів на приблизно 8...10%.



**УДК 372.862**

**Казіміров О.О.**, доцент кафедри Національної академії Національної гвардії України, кандидат військових наук, доцент

**Малюк В.Г.**, професор кафедри Національної академії Національної гвардії України, кандидат технічних наук, доцент

**Потіхеньський А.І.**, старший викладач кафедри Військово-юридичного інституту Національного юридичного університету ім. Я.Мудрого

## **СУЧАСНЕ ТЕЛЕКОМУНІКАЦІЙНЕ ОБЛАДНАННЯ, ЩО ЗАСТОСОВУЄТЬСЯ ПІДРОЗДІЛАМИ ЗВ'ЯЗКУ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ**

Оснащення сучасними системами військового зв'язку - один із напрямів реалізації Концепції розвитку Національної гвардії України. На озброєнні підрозділів зв'язку Національної гвардії вже надійшли та активно застосовуються для організації управління сучасні телекомунікаційні комплекти, IP-АТС, IP-телефонні апарати, шлюзи голосового зв'язку, цифрові реєстратори аудіо інформації та інше обладнання.

Телекомунікаційні комплекти ТК-1, ТК-2, ТК-3 та ТК-4 розроблені з урахуванням новітніх технологічних тенденцій та мають наступні основні можливості: маршрутизація та комутація пакетів в інформаційно-телекомунікаційних мережах з підтримкою стеку протоколів TCP/IP; підтримка технології VLAN IEEE 802.1q Ethernet; підтримка протоколів дистанційного управління телекомунікаційним обладнанням SSH, HTTPS; фільтрація мережевих пакетів відповідно до визначених правил фільтрації; динамічна маршрутизація пакетів за протоколом BGPv4, OSPFv2, RIPv2; підтримка технології підміни IP-адрес (NAT); кодування аналогових телефонних сигналів у цифрові пакети; маршрутизація телефонних викликів між підключеними телефонами та відповідним SIP-сервером за протоколом SIP; автоматизоване конфігурування за допомогою вбудованого програмного забезпечення; маскуванню передачі відкритої інформації, голосового трафіку, службової інформації та ключів. Сумарна пропускна спроможність каналів з маскуванням ТК-1, ТК-2 та ТК-3 – не менше 2, 4 та 58 МБіт/с відповідно.

IP-АТС Grandstream UCM6108 - потужна апаратна IP-АТС, що дозволяє швидко розгорнути систему офісної IP-телефонії в установах з чисельністю співробітників від 30 до 200 чоловік. Модель обладнана 8-ю портами FXO для підключення зовнішніх міських телефонних ліній і двома портами FXS для використання звичайних телефонних апаратів або факсів. При необхідності, кількість портів може бути збільшено за допомогою VoIP-шлюзів. Grandstream UCM6108 підтримує роботу з більшістю сучасних моделей завдяки тому, що працює по популярним VoIP-протоколам SIP і IAX2. Окрім голосових портів, IP-АТС обладнана високошвидкісним Ethernet-портом 10/100/1000 Мбіт/с і роз'ємами для установки SD-карти для зберігання повідомлень голосової пошти і записаних телефонних розмов. Потужний процесор підтримує ведення до 60 одночасних розмов

IP-телефон Grandstream GXP1625 - це стандартний IP-телефон, який підходить для установки на робочі місця звичайних співробітників малих і середніх організацій. Модель підтримує дві телефонні лінії, технологію HD Audio, як при розмові по телефонній трубці, так і в режимі гучного зв'язку, а також функцію живлення по мережі (PoE). Телефон оснащений якісним дисплеєм з підсвічуванням, трьома клавішами що програмуються, підтримкою для гарнітур Plantronics. Телефон може забезпечувати тристоронній конференц-зв'язок, який дозволяє швидко організовувати невеликі телефонні наради.

VoIP/SIP шлюз Cisco SPA8000 дозволяє застосувати всі можливості VoIP - телефонії, використовуючи широкопasmовий доступ в глобальну мережу. Cisco SPA8000 - це VoIP/SIP/голосовий/телефонний/ аналоговий шлюз (адаптер). Має 8 портів для підключення аналогових телефонних апаратів.

Сучасне телекомунікаційне обладнання, дозволить організувати стійкий та якісний зв'язок в інтересах управління частинами та підрозділами Національної гвардії, а також забезпечити взаємодію з іншими силовими відомствами України.

**УДК 621.391**

**Василишин В.І.**, начальник кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, доктор технічних наук, професор

**Коваль О.В.**, ад'юнкт Харківського національного університету Повітряних Сил імені Івана Кожедуба

## **АНАЛІЗ ЕФЕКТИВНОСТІ ПОДАВЛЕННЯ ШУМУ В МОВНИХ СИГНАЛАХ МЕТОДОМ СПЕКТРАЛЬНОГО ВІДНІМАННЯ**

Досвід останніх локальних війн та збройних конфліктів, проведення АТО та ООС показав необхідність вдосконалення системи зв'язку та інформаційних систем Збройних Сил України. Для забезпечення високої ефективності управління військами в умовах ведення бойових дій використовується телекомунікаційне обладнання для обробки різномірної інформації, у тому числі аудіо та відео інформації. Доволі актуальним при цьому є завдання очищення мовних сигналів від адитивних шумів. Це дозволяє підвищити розбірливість мови, що визначає розуміння поставленого завдання і т.д.

Більшість існуючих систем шумоподавлення працюють в частотній області, використовуючи варіації методу спектрального віднімання. Увага дослідників в технічній літературі до даного методу зумовлена простотою його реалізації, що зумовлено використанням перетворення Фур'є з віконною обробкою (STFT- short time Fourier Transformation). В методі робиться припущення, що спектр потужності зашумленого мовного сигналу дорівнює сумі спектра чистого сигналу та спектра некорельованого шуму. Оцінка характеристик шуму (зазвичай оцінка спектра потужності шуму здійснюється на основі використання сегментів, в яких мова відсутня) дозволяє здійснити віднімання спектру шуму, що і визначило назву даного методу. Схожі підходи щодо оцінки характеристик шуму спостереження використовуються в радіолокації і т.д.

Аналіз ефективності методу спектрального віднімання виконувався за допомогою пакета Matlab. Візуально ефект очищення від шуму аналізувався за допомогою спектрограм для випадку зашумленого мовного сигналу та очищеного від шуму.

Недоліком методу спектрального віднімання є “музичний шум”. Він з'являється так як коефіцієнти STFT шумових сигналів статистично випадкові. Це призводить до нерівномірного подавлення шумових сигналів. Тому очищений сигнал містить короткочасні та обмежені за частотою сплески енергії. На слух такі артефакти сприймаються, наприклад, як “вода, що ллється”

Таким чином доцільним є пошук підходів щодо подавлення такого артефакту (наприклад, методів усереднення і т.д). Крім того, до напрямків подальших досліджень слід віднести порівняльний аналіз методу спектрального віднімання з іншими методами подавлення шуму в мовному сигналі (на зображенні), комбінування таких методів з метою підвищення їх ефективності.

## УДК 621.371.32

**Костенко І.Л.**, начальник науково-дослідного управління наукового центру Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат військових наук, старший науковий співробітник

**Блащук С.М.**, провідний науковий співробітник наукового центру Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук

**Поздняк В.П.**, науковий співробітник наукового центру Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба

### ПРОПОЗИЦІЇ ЩОДО АВТОМАТИЗОВАНОГО РОЗРАХУНКУ РАДІОЛІНІЇ ПРИ ЗВ'ЯЗКУ ЗЕМНОЮ ХВИЛЕЮ ДЛЯ ВИЗНАЧЕННЯ ГРАНИЧНОЇ ДАЛЬНОСТІ ЗАБЕЗПЕЧЕННЯ РАДІОЗВ'ЯЗКУ

На практиці часто потрібно оцінити граничну дальність забезпечення радіозв'язку земною хвилею з заданою якістю. Гранична дальність радіозв'язку досягається тоді, коли реальне послаблення, яке визначається поглинанням на трасі поширення, дорівнює гранично допустимому послабленню, яке залежить від заводової обстановки в точці прийому, необхідної якості прийому і технічних характеристик передавального і приймального пристрою.

Прирівнявши допустиме послаблення фактичному, отримаємо граничну дальність зв'язку  $W_{доп}$ , представлену фрагментом Mathcad документа:

$$\text{Given}$$

$$W_{доп} = \begin{cases} \left[ \frac{\lambda}{4 \cdot \pi \cdot r} \cdot \left[ \frac{(2 + 0.3 \cdot x(r))}{(2 + x(r) + 0.6 \cdot x(r)^2)} - \sqrt{\frac{x(r)}{2}} \cdot e^{\frac{-5 \cdot x(r)}{8}} \cdot \frac{\varepsilon}{\sqrt{\varepsilon^2 + (60 \cdot \lambda \cdot \sigma)^2}} \right] \right] & \text{if } r < 20 \cdot \sqrt[3]{\lambda} \cdot 10^3 \\ \left[ \frac{\lambda}{4 \cdot \pi \cdot r} \cdot \left( 2 \cdot \sqrt{\pi \cdot y(r)} \cdot \left| \frac{e^{i \cdot y(r) \cdot t_1}}{t_1 + q^2} \right| \right) \right] & \text{if } r \geq 20 \cdot \sqrt[3]{\lambda} \cdot 10^3 \end{cases}$$

$$\text{Find}(r) = 7.593 \times 10^4 \quad \text{м}$$

Тобто гранична дальність забезпечення радіозв'язку з заданою якістю при вологому ґрунті дорівнює приблизно 76 км.

Розроблена методика автоматизованого розрахунку радіолінії при зв'язку земною хвилею для визначення граничної дальності забезпечення радіозв'язку з заданою якістю базується на використанні аналітичних залежностей та автоматизована за допомогою прикладного математичного пакету Mathcad.

Необхідно зазначити, що запропонована методика розроблена в припущенні, що напруженість поля земної хвилі в точці прийому є постійною величиною, яка залежить від випромінюваної потужності, робочої частоти і усереднених електричних параметрів підстилаючої поверхні.

Розглянута методика може бути застосована у тих випадках, коли потрібні багаторазово повторювані розрахунки радіоліній з різними вихідними даними, зокрема, при обґрунтуванні основних технічних параметрів засобів радіозв'язку на етапі їх проектування (модернізації, закупівлі).

**УДК 621.396**

**Шмаков В.В.**, начальник кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук

**Красноручський А.О.**, викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук

**Олексін О.О.**, старший викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба

**Федоровський О.В.**, викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба

## **ТЕНДЕНЦІЇ РОЗВИТКУ ТА ІСНУЮЧІ МОЖЛИВОСТІ АВІАЦІЙНОГО РАДІОЗВ'ЯЗКУ ВЕРТОЛЬОТІВ СИЛОВИХ СТРУКТУР**

В сучасних умовах модернізації повітряних суден, вертольоти силових структур України переобладнуються або дообладнуються новими засобами бортового радіозв'язку.

Загальні вимоги підходу до модернізації є реалізація зв'язку для забезпечення безпеки та регулярності польотів, що включає зв'язок для обслуговування повітряного руху та оперативний зв'язок, пов'язаний з контролюванням початку польоту, відхиленням від маршруту, або припинення польоту для забезпечення безпеки повітряного судна, а також відповідність до стандарту MIL-STD-704F (Aircraft Electric Power Characteristics), STANAG 3456 (Aircraft Electrical System Characteristics). Важливою складовою тут є існуючий парк вертольотів на яких встановлені бортові засоби радіозв'язку ультракороткохвильового (УКХ) діапазону. Для здійснення авіаційного радіозв'язку в УКХ діапазоні, згідно до вимог ІКАО, використовують наступний діапазон: 118 - 137 МГц. Дискретність сітки частот складає 8,33 кГц. Смуга пропускання на рівні 6 дБ повинна складати від 300 до 2500Гц.

До складу авіоніки вертольотів силових структур України відносять бортові радіостанції УКХ діапазону: Баклан-5, Баклан-20 та Р- 863, які працюють у визначеному діапазоні радіохвиль, але мають дискретність сітки частот на рівні 25кГц. Радіостанція Р - 863 (після модернізації синтезатора) має дискретність сітки частот на рівні 8,33 кГц, але тільки в діапазоні 118 - 137 МГц.

Модернізований вертоліт Ми-2МСБ оснащений радіостанцією УКХ діапазону Бриз має радіочастотний діапазон 118 - 137 МГц, але дискретність сітки частот залишилась на рівні 25кГц. Бортова радіостанція Backer RT6201/RCU6201, що встановлюється на вертоліт Ми-8МСБ має крок сітки частот 8,33/25 кГц, що дозволяє збільшити загальну кількість каналів з 760 до 2280. Проводяться роботи щодо встановлення перспективних бортових програмованих радіостанцій HARRIS FALCON III RF-7850A-MR та ASEL SAN 9681 V/UHF Airborne Radio, що відповідають стандарту STANAG 5511 (Tactical data exchange).

Важливим напрямком робіт в області техніки авіаційного радіозв'язку є створення антенно-фідерних пристроїв повітряних суден, оскільки, будучи елементами конструкції планера, вони вносять істотний внесок в забезпечення надійного зв'язку літаків і вертольотів між собою і з наземними пунктами управління. Подальшим розвитком цього напрямку є об'єднання функцій антен різного призначення (за рахунок впровадження високочастотних мультиплексорів), що в перспективі, дозволить забезпечити підвищення енергопотенціалу радіоліній на 3-10 дБ.

**УДК. 621.396.969.3**

**Таршин В.А.**, начальник кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба

**Танцюра О.Б.**, науковий співробітник Наукового центру Повітряних сил Харківського національного університету Повітряних Сил ім. І. Кожедуба

**Куравський М.В.**, ад'юнкт Харківського національного університету Повітряних Сил імені Івана Кожедуба

## **ПІДВИЩЕННЯ ІМОВІРНОСТІ ВИЯВЛЕННЯ ТА РОЗПІЗНАВАННЯ ОБ'ЄКТІВ НА ЗОБРАЖЕННЯХ РІЗНОСПЕКТРАЛЬНИХ ОПТИКО-ЕЛЕКТРОННИХ СИСТЕМ РОЗВІДКИ**

Застосування різноспектральних оптико-електронних систем розвідки (спостереження), у більшості випадків телевізійних (ТВ) та інфрачервоних (ІЧ), дозволяє контролювати ситуацію у визначених областях простору та забезпечувати своєчасне виявлення та розпізнавання об'єктів. У той же час досвід застосування різноспектральних засобів оптико-електронної розвідки на лінії розмежування сторін під час ведення бойових дій в операції Об'єднаних сил, що проводиться в окремих районах Донецької та Луганської областей України, при охороні державного кордону України вказує на низьку їх ефективність в складних умовах спостереження. Це характерно для випадків застосування противником аерозольних засобів маскування, зменшення помітності об'єктів на оточуючому фоні, використання природних умов (вечірніх та ранкових сутінок, димки над морською поверхнею та береговою лінією). У таких умовах використання окремо ТВ та ІЧ засобів розвідки як окремих каналів оптико-електронних систем не завжди забезпечує потрібні імовірності виявлення та розпізнавання об'єктів на зображеннях, особливо при неоднорідному фоні зображень.

Імовірність виявлення та розпізнавання об'єктів в складних умовах спостереження може бути покращена за рахунок та комплексування різноспектральних зображень, отриманих ТВ та ІЧ каналами оптико-електронних систем розвідки. Серед методів комплексування виділяється група методів з відносно простим математичним апаратом таких як усереднення, або максимумів яскравості, однак застосування таких методів не дає змогу відобразити в повній мірі відмінні риси різноспектральних зображень на результуючому. Більш складний математичний апарат мають методи морфологічного комплексування, вагових коефіцієнтів, аналізу основних компонент, маски, які мають кращі показники комплексування та підвищення інформативності.

У той же час, застосування відомих методів комплексування різноспектральних зображень не дозволяє отримати максимальне значення відношення об'єкт/фон (сигнал/шум) на комплексованому зображенні і тим самим забезпечити потенційні значення імовірностей виявлення та розпізнавання об'єктів в складних умовах спостереження, оскільки не враховує локальні зміни фоново-об'єктового складу різноспектральних зображень.

Забезпечення максимального відношення сигнал/шум на результуючих зображеннях оптико-електронних систем, отриманих в умовах складної фоново-об'єктової обстановки, обумовило розвиток методів комплексування, в основу яких покладено урахування яскравісних, контрастних та структурних особливостей різноспектральних зображень.

УДК 372.862

**Лазарев В.Д.**, старший викладач кафедри Національної академії Національної гвардії України  
**Козлов В. Є.**, доцент кафедри Національної академії Національної гвардії України, кандидат військових наук, доцент

## **ПІДВИЩЕННЯ ГНУЧКОСТІ ТА ОПЕРАТИВНОСТІ УПРАВЛІННЯ ЧАСТИНАМИ НГУ ЗА ДОПОМОГОЮ ІНТЕРКОМУНІКАЦІЙНОЇ СИСТЕМИ ІНТЕРКОМ RF-7800I ВИРОБНИЦТВА КОМПАНІЇ HARRIS**

На озброєння НГУ почала надходити система інтерком Harris RF-7800I. Це сучасна, гнучка, багатофункціональна цифрова система внутрішнього зв'язку для бронетехніки та інших транспортних засобів, в яку інтегруються автомобільні радіостанції Harris та засоби зв'язку інших виробників

При якісному налаштуванні відповідно до потреб бойового управління, Harris RF-7800I дозволяє значно покращити координацію екіпажу бойової машини та підвищити її бойові можливості. Крім бойових машин, системи інтерком можуть встановлюватись на командно-штабних машинах та командних пунктах.

Система інтерком Harris RF-7800I має гнучку модульну структуру. Ядро системи - центральний блок, який містить промисловий комп'ютер. До нього за допомогою системи кабелів під'єднуються блоки екіпажу з різним набором функцій: від клавішно-дисплейного блоку управління до простих трикнопових абонентських блоків. До блоків членів екіпажу підключаються гарнітури з активним шумоподавленням та комп'ютери, оснащені послідовним портом. Також до центрального блоку під'єднуються радіостанції бойової машини та гучномовець.

Органи управління системою - функції клавіш, дії поворотного перемикача, значення піктограм на дисплеї тощо - налаштовуються згідно з набором підключеного обладнання та завдань екіпажу бойової машини, щоб максимально спростити бойове управління.

Система інтерком для транспортних засобів Harris RF-7800I складається з центрального блоку, блоків екіпажу, допоміжних блоків, з'єднувальних кабелів та системи електроживлення. Функції системи визначаються конкретним набором блоків, встановлених на об'єкті, і підключеними до них радіостанціями та зовнішніми лініями, а також конфігураційним файлом.

В командно-штабних машинах та на стаціонарних командних пунктах, як правило, монтуються системи на основі центрального блоку RF-7800I-CU100. В них, зокрема, входять два блоки управління RF-7800I-KD400 та блок телефонії, до якого може бути підключена стаціонарна зовнішня телефонна лінія. Також центральний блок інтеркому може бути підключений до зовнішнього IP-каналу через роз'єм Ethernet. Блок виклику встановлюється на робочому місці військового начальника, в інтересах якого працює КШМ або пункт управління. Блок дистанційного підключення через польовий кабель може в цьому випадку використовуватись для організації радіовиносу.

В пунктах управління можуть використовуватись конфігурації інтеркому з декількома центральними блоками, з'єднаними у локальну мережу; в таких конфігураціях може взаємодіяти велика кількість блоків екіпажу. Аналогічну конфігурацію можна створити, об'єднуючі центральні блоки командно-штабних машин, які входять в склад мобільного пункту управління.

Система інтерком Harris RF-7800I тільки починає застосовуватись в підрозділах НГУ. Її функціональність найбільше розкривається при застосуванні в командно-штабних машинах, які експлуатує більш підготований персонал, і на яких встановлено дві або більше радіостанцій.. Розгорнуто систему інтерком на деяких стаціонарних пунктах управління вищої ланки.

## УДК 621.391

**Лютов В.В.**, старший викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба

**Дзюба І.В.**, викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба

**Колесник С.В.**, курсант Харківського національного університету Повітряних Сил імені Івана Кожедуба

## АНАЛІЗ ЕФЕКТИВНОСТІ ЗАСОБІВ РАДІОЗВ'ЯЗКУ ВІЙСЬКОВОГО ПРИЗНАЧЕННЯ ПРИ ВИКОРИСТАННІ МІМО ТЕХНОЛОГІЇ В ЗАСОБАХ ТА КОМПЛЕКСАХ РАДІОЗВ'ЯЗКУ УКХ ДІАПАЗОНУ У СКЛАДНІЙ ЗАВАДОВІЙ ОБСТАНОВЦІ

Аналіз інфраструктури телекомунікаційної системи ЗС України та її використання в ході АТО та ООС показав, що у тактичній ланці управління спостерігається недостатня швидкість передачі інформації каналами радіозв'язку. Для вирішення цієї проблеми, створюється автоматизована система управління рівня С4ISR, технічною основою якої є, в тому числі і засоби радіозв'язку. В той же час, досвід проведення ООС свідчить про недостатню пропускну здатність каналів радіозв'язку БПЛА.

В роботі запропоновано використовувати МІМО технологію для підвищення пропускну здатності засобів УКХ радіозв'язку. З цією метою програмою MATLAB проведено моделювання можливих варіантів топології антенних систем. За результатами аналізу обґрунтовано доцільність впровадження МІМО технології для підвищення пропускну здатності засобів радіозв'язку.

З метою оцінки ефективності впровадження МІМО технології, розраховано потенційний вигравш у швидкості передачі даних радіостанції RF 7800V-НН від впровадження МІМО технології. Результати аналізу свідчать (рис. 1), що для МІМО системи зв'язку 4×4, підвищення пропускну здатності у смузі полоси пропускання 25 кГц, збільшується з 64 кбіт/с до 245 кбіт/с, а для смуги частот 75 кГц, підвищується з 192 кбіт/с до 737 кбіт/с.

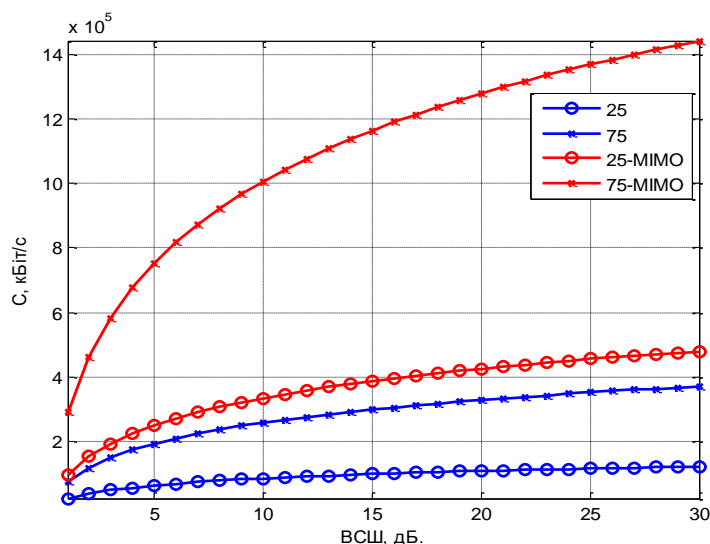


Рисунок 1 – Пропускна здатність радіостанції RF-7800V-НН на смугах 25 кГц та 75 кГц (синім кольором) та RF-7800V-НН з технологією МІМО на смугах 25 кГц та 75 кГц (червоним кольором) в залежності від відношення сигнал/шум

**УДК 621.396**

**Майборода І.М.**, доцент кафедри Національної академії Національної гвардії України, кандидат військових наук, доцент

**Оленченко В.Т.**, заступник начальника кафедри Національної академії Національної гвардії України, кандидат технічних наук, доцент

### **АНАЛІЗ СИСТЕМИ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ ЦИФРОВИХ ЗАСОБІВ ЗВ'ЯЗКУ «HARRIS»**

Враховуючи суттєві зміни в технічному оснащенні системи зв'язку Національної гвардії України (НГУ), а саме прийняття на озброєння цифрових засобів зв'язку виробництва HARRIS, виникає необхідність щодо наближення системи експлуатації та технічного обслуговування (ТО) техніки зв'язку до стандартів НАТО.

Проведений аналіз заходів технічного забезпечення, які наведені в інструкціях з експлуатації радіостанцій виробництва HARRIS, показав, що основними для них вважається два види технічного обслуговування (профілактичне і позапланове), та три рівні обслуговування. Профілактичне обслуговування (ПрО) – це вид обслуговування, який здійснюється за графіком. Під час профілактики проводиться перевірка обладнання з метою запобігання виходу з ладу і зменшення часу простою. ПрО полягає в утриманні обладнання в чистому та сухому стані, очищеному від пилу. Обладнання, яке використовується має оглядатися щоденно, при цьому потрібно виконати вбудовані тести, перевірити надійність під'єднання батарейного відсіку і чистоту вентиляційного клапана, а також надійність під'єднання кабелів та роз'ємів до трансівера і антенної системи. Якщо обладнання щодня не використовується, то його огляд та виконання відповідних процедур має проводитися щотижня. Перелік робіт при цьому включає в себе огляд антени на наявність зламів і розтягнень (за потреби необхідно відремонтувати чи замінити), огляд роз'ємів на предмет корозії чи пошкоджень, перевірку роз'ємів, які не використовуються, на наявність захисних ковпачків. ПрО крім щоденного та щотижневого обслуговування передбачає і щорічне обслуговування, під час якого проводиться перевірка в повному обсязі роботи радіостанції та заміна батареї HUB. Позапланове технічне обслуговування (ПЗО) проводиться, коли під час ПрО, чи під час роботи радіостанції, були виявлені ті чи інші несправності, або той чи інший дефект, тобто за необхідністю.

Компанією Harris, на відміну від системи ТО, що діє в НГУ, передбачається три рівні обслуговування. Перший рівень передбачає визначення рівня працездатності обладнання (виконується оператором без застосування додаткового обладнання). На другому рівні визначається працездатність обладнання радіостанції (виконується оператором із застосуванням додаткового обладнання). Третій рівень передбачає визначення працездатності обладнання до модуля у пристрої (виконується сертифікованим персоналом із застосуванням обладнання спеціалізованого автомобіля).

Таким чином, результати порівняння діючої в НГУ системи та видів ТО засобів зв'язку з тими видами, що застосовуються в ЗС країн членів НАТО, та неухильний процес нарощування системи зв'язку НГУ виробами компанії Harris, обслуговування яких значно відрізняється від обслуговування аналогової техніки зв'язку, і є підтвердженням необхідності вдосконалення діючої системи ТО в НГУ. Отже, напрямками удосконалення системи ТО цифрових засобів зв'язку в НГУ пропонується вважати: визначення головної мети ТО в процесі експлуатації засобів зв'язку на новій елементній базі, які надходять на озброєння; визначення сукупності взаємопов'язаних засобів, виконавців і документації з ТО, призначеної для підтримання справного і працездатного стану техніки зв'язку; оптимізація періодичності та видів ТО цифрових засобів зв'язку з визначенням методик проведення кожного із них.



**УДК 004.056.**

**Нещерет І.Г.**, провідний науковий співробітник Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут

**Штонда Р.М.**, начальник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут

## **ПРОПОЗИЦІЇ ЩОДО БЛОКУВАННЯ ВІРУСУ ШИФРУВАЛЬНИКА В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ**

У 2013-2017 роках кібератаки проти України здійснювалися з використанням АРТ-атак (Snake, Urobogor, Sofacy/APT28, Epic Turla, Black Energy 2 і 3, Arma-geddon та інші), характерних саме для України. Перші системні атаки були зафіксовані у травні 2014 року на об'єкти критичної інформаційної інфраструктури України (Укрзалізницю та сервери Центральної виборчої комісії під час проведення президентських виборів). Також відбулися кібератаки на енергетичний сектор: у грудні 2015 року – на ПАТ “Прикарпаття обленерго” і ПАТ “Київ обленерго”; у грудні 2016 року – на компанію “Укренерго” (споживачі частини правого берега Києва та прилеглих районів області залишилися без струму). У червні 2017 року об'єкти критичної інфраструктури України зазнали масштабної атаки комп'ютерного вірусу Petya.A.

Основні світові аналітики визнають, що 30 відсотків сучасних кіберзагроз становлять спроби шифрування інформації в системі з подальшою вимогою надати викуп за можливість її відновлення.

Відома розширена модель проведення атаки Cyber-Kill Chain [1] визначає кроки, які реалізує зловмисник для досягнення можливості виконати несанкціоновані дії на кінцевих точках у визначених ним мережах. При цьому зловмисник реалізує наступні кроки:

**1. Кроки зовнішньої Cyber-Kill Chain:**

- зовнішня розвідка мережі;
- озброєння – вибір інструментів;
- доставка шкідливого програмного забезпечення (далі – ШПЗ);
- зовнішнє зараження; встановлення ШПЗ;
- досягнення можливості управління;
- дії в мережі.

**2. Кроки внутрішньої Cyber-Kill Chain:**

- внутрішня розвідка в мережі;
- озброєння – вибір інструментів;
- доставка ШПЗ; внутрішнє зараження;
- підвищення прав;
- горизонтальне переміщення;
- маніпуляції з цільовою машиною.

**3. Cyber-Kill Chain маніпуляції з цільовою машиною:**

- розвідка цілі;
- зараження цілі;
- озброєння інструментами;
- встановлення ШПЗ;
- досягнення цілі зловмисника.

Експерти вважають що зловмисники досконало відпрацьовують всі кроки ланцюжка моделі Cyber-Kill Chain необхідні для вдалого вторгнення до цільової інформаційно-телекомунікаційної системи (далі – ІТС) та потім успішно виконують заплановані шкідливі дії на цільовій машині. На кожному етапі моделі Cyber-Kill Chain застосовуються необхідні заходи кіберзахисту, але зловмисники постійно та впевнено долають цей захист.

Автори пропонують зосередити зусилля захисту на блокуванні процесу шифрування ще на його початку, щоб потім не було потреби в надскладному розшифруванні інформації.

Пропозиція полягає в тому, щоб заздалегідь розгорнути в ІТС зразки спеціального програмного забезпечення (далі – СПЗ), які здатні до своєчасного виявлення ознак шифрування, блокування процесу шифрування, аварійного копіювання, пошуку ключової інформації, відновлення видалених або зашифрованих файлів та відновлення працездатності системи в цілому.

Пропонується комплексно застосувати наступні СПЗ:

- СПЗ для недопущення проникнення ВШ в ІТС;
- СПЗ для екстреного резервного копіювання образу ІТС;
- СПЗ для контролю за існуючими “процесами” в ІТС;
- СПЗ для контролю за навантаженням CPU;
- СПЗ для контролю за файлами;
- СПЗ для виявлення ознак шифрування інформації в ІТС;
- СПЗ для екстреної при зупинки CPU або уповільнення його роботи;
- СПЗ для оповіщення підрозділів ІТС про загрозу дії ВШ;
- СПЗ для блокування спроб несанкціонованого пере завантаження системи;
- СПЗ для пошуку паролів інформації;
- СПЗ для відновлення ІТС (ОС, додатків та даних).

Головна пропозиція авторів полягає у концентрації зусиль на недопущенні початку шифрування інформації. Застосування такого СПЗ дозволить адміністраторам ІТС вчасно виявити та призупинити процес шифрування інформації, провести аналіз інциденту та зберегти працездатність ІТС.

Використання запропонованого СПЗ дозволить адміністраторам своєчасно заблокувати дії ВШ та підвищити захищеність ІТС від дій ВШ.

Для унеможливлення роботи ВШ в ІТС доцільно заздалегідь підготувати засоби захисту та забезпечити повну обізнаність адміністраторів а саме:

- досягати повної обізнаності адміністраторів та користувачів щодо загрози від ВШ та відпрацьовувати їх практичні навички для протидії загрозам дій ВШ;
- постійно оновляти актуальне СПЗ для можливості ефективного блокування початку роботи ВШ;
- постійно резервувати інформацію системи, щоб у вас було декілька бекапів: один у хмарі, наприклад Dropbox, Google Drive та інших спеціалізованих сервісах, а також на змінному носії (знімний жорсткий диск, USB-флеш або резервний комп’ютер);
- проводити навчання для підвищення навичок адміністраторів системи практично нейтралізувати дії ВШ;
- для захисту ІТС слід застосовувати обидва комплекти засобів захисту від дії ВШ для недопущення початку шифрування та можливості ефективного розшифрування інформації.

Наслідком таких зусиль стане ріст захищеності ІТС від дій ВШ.

Подальші напрямки досліджень дозволять поширити запропонований підхід на блокування різноманітних класів ШПЗ – руткітів, хробаків, бекдорів, різноманітних вірусів та систем вторгнень, враховуючи при цьому особливості їх дій.

**УДК 621.391**

**Онипченко П.М.** професор кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат педагогічних наук, доцент

**Невзоров Р.В.**, начальник кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат педагогічних наук

**Ушань В.М.**, доцент кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук

## **УПРАВЛІННЯ БЕЗПІЛОТНИМИ ЛІТАЛЬНИМИ АПАРАТАМИ ПРИ ЇХ ЗАСТОСУВАННІ У СКЛАДІ ГРУПИ**

На сьогодні безпілотні літальні апарати (БПЛА) широко застосовуються для вирішення як військових, так й цивільних завдань. Одним з перспективних варіантів застосування БПЛА є застосування їх у складі групі. Для забезпечення ефективного виконання завдань та управління групою БПЛА необхідно створення системи управління цією групою. Розв'язання даного завдання спрямоване на створення системи, що розширює автономність БПЛА й спрощує їх групове застосування в складних фізико-географічних умовах і (або) під впливом активної радіоелектронної протидії з боку противника. Основною метою при цьому вважається розвиток можливостей “спільної автономності” під якою розуміється синхронізація інформації всередині групи БПЛА, розробка декількох варіантів спільних дій та їхнє корегування при зміні обстановки. Оператор має лише вибрати один із запропонованих йому варіантів дій.

Перевагою такого підходу є підвищення живучості окремих БПЛА за рахунок можливості обміну необхідними даними з іншими БПЛА групи при виході з ладу або придушенні яких-небудь систем (наприклад, навігації або цілевказівки). У якості пріоритетної вимоги до системи управління БПЛА визначається можливість функціонування групи без постійного контролю.

Інтерфейс користувача і алгоритми автономності мають розроблятися на базі відкритої архітектури, заснованої на вже наявних стандартах. Така уніфікація дозволить проводити інтегровані операції з максимальними можливостями по взаємодії. Оператору, що керує групою БПЛА, необхідно мати актуальні дані про її стан, статус виконаних і чергових завдань, а також про можливі алгоритми дій. Також необхідно забезпечити можливість виділяти частину групи БПЛА, присвоювати їм позивні й відправляти нову сформовану групу на виконання нового завдання. При цьому завдання, покладені на них до цього, автоматично перерозподіляються між БПЛА, що залишилися.

Після виконання завдання група має продовжувати діяти за основним планом або очікувати на нове завдання відповідно до заздалегідь розробленого алгоритму дій. Має бути можливість передачі управління групами БПЛА іншим операторам.

На відміну від управління поодинокими БПЛА, де є тільки мережа зв'язку “оператор – БПЛА”, в групах необхідно створити мережі “БПЛА – БПЛА”.

До теперішнього часу більшість систем керування групою БПЛА характеризувалися відсутністю можливості автономної постановки нових завдань, що не дозволяло групі оперативно приймати ефективні рішення щодо зміни сценарію виконання поточного завдання. Для вирішення подібних проблем доцільно застосовувати мультиагентні технології. В основі цих технологій лежить поняття “агента”, тобто програмного об'єкта, здатного сприймати ситуацію, приймати рішення і взаємодіяти із собі подібними. При мультиагентному методі БПЛА виконують функції “агентів”, які за допомогою спеціального програмного забезпечення та сенсорів (датчиків) оцінюють ситуацію, приймають рішення та взаємодіють з іншими “агентами”, а також з рештою апаратів. Мультиагентний метод колективного управління дозволить керувати незалежними, автономними БПЛА, які виконують різні задачі.

Функції оператора обмежуються постановкою загальної задачі, але в будь-який момент часу він може втручатись в управління окремим БПЛА.

**УДК 629.7.058**

**Флорін О.П.**, доцент кафедри Національної академії Національної гвардії України, кандидат технічних наук, доцент

**Сальніков О.М.**, доцент кафедри Національної академії Національної гвардії України, кандидат технічних наук, доцент

### **МОЖЛИВОСТІ ЗАСТОСУВАННЯ СИСТЕМ БОРТОВИХ ВИМІРЮВАНЬ ДЛЯ ПРОВЕДЕННЯ ВИПРОБУВАНЬ БЕЗПЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ**

На сучасному етапі до військових формувань України надходить багато безпілотних літальних апаратів (БпЛА) різного функціонального призначення, як вітчизняного так і іноземного виробництва. Спектр завдань, які виконують безпілотні літальні апарати досить широкий починаючи від цивільних – доставки пошти, перевезення вантажів, спостереження, охоронних операцій на об'єктах нафтогазового комплексу та енергетики, в зонах надзвичайних ситуацій, ведення геологорозвідки, до військових – розвідка, постановка радіоперешкод, управління вогнем і цілевказівки, ретрансляції повідомлень і даних тощо. Виконання функціонального призначення БпЛА під час експлуатації залежить від багатьох факторів, одним з них є кількісна оцінка характеристик дослідного зразка БпЛА під час випробувань та підконтрольної експлуатації. Що в свою чергу можливо тільки з використанням вимірювальної техніки.

Кількість таких БпЛА чимала, принципи побудови різні, параметри, які підлягають випробуванням різноманітні. Провідними розробниками (виробниками), які здійснюють розробку в сфері інформаційно-вимірювальних систем, створено багато зразків, в тому числі для використання на повітряних суднах. Вони потребують досконалого вивчення з метою можливості використання для проведення випробувань БпЛА.

Наведені обставини та стрімкий розвиток технічних засобів вимірювань, перетворення та обміну даними всередині систем та між ними вимагають вдосконалення методів розробки і застосування бортових інформаційно-вимірювальних комплексів та реєструвальних систем для забезпечення проведення випробувальних робіт, які враховують особливості розвитку електронного обладнання на даному етапі розвитку БпЛА, будуються на єдиному підході до проблеми оптимального використання ресурсів систем збору і обробки параметричної інформації.

Метою досліджень було вивчення можливостей застосування систем бортових вимірювань для проведення випробувань безпілотних літальних апаратів.

Аналіз використання систем бортових вимірювань для проведення випробувань показав, що можливі наступні варіанти реалізації систем бортових вимірювань для безпілотних літальних апаратів:

- програмно-алгоритмічна реалізація з передачею інформації з борту безпілотного літального апарату на наземну частині комплексу для її подальшої обробки;
- реалізація систем бортових вимірювань на самому борту безпілотного літального апарату за рахунок обладнання бортовими засобами реєстрації параметрів польоту. В цьому варіанті розглядається можливість передачі параметрів польоту в реальному масштабі часу на наземну частину комплексу та накопичення її на борту для наступного зчитування (списування) та аналізу після здійснення польоту;
- використання в якості систем бортових вимірювань для проведення випробувань безпілотних літальних апаратів малогабаритних сучасних універсальних систем об'єктивного контролю на базі реєстраторів параметрів польоту.

Результати роботи доцільно використовувати при проведенні випробувань безпілотних літальних апаратів та інших типів озброєння та військової техніки науково-дослідними установами та підприємствами промисловості.

**УДК 621.391**

**Макаров С.А.**, начальник факультету Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент

**Чекунова О.М.**, старший науковий співробітник науково-дослідної лабораторії Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук

**Чекунов В.В.**, заступник начальника факультету Харківського національного університету Повітряних Сил імені Івана Кожедуба

## **ОБГРУНТУВАННЯ ЄДИНОГО ПІДХОДУ ЩОДО ОЦІНКИ ЗАВАДОСТІЙКОСТІ СИСТЕМИ ЗВ'ЯЗКУ В ІНТЕРЕСАХ УПРАВЛІННЯ ВІЙСЬКАМИ**

Широке застосування комплексів РЕБ РФ в зоні проведення ООС (АТО) призводить до дезорганізації управління військами (силами) Збройних Сил (придушення ліній радіозв'язку) та введення дезінформації до системи радіозв'язку. Масове використання цифрових засобів телекомунікації загального призначення (цивільного виконання) у системі зв'язку та автоматизації управління (АУ), збільшення кількості застосовуваних сучасних засобів зв'язку та розширення смуги частот випромінюваного сигналу призвело до зниження завадостійкості системи зв'язку та АУ повітряного командування (ПвК) в оборонній операції оперативного угруповання військ (сил).

З метою підвищення завадостійкості системи зв'язку та АУ ПвК авторами проведено аналіз оперативно-тактичних факторів, що впливають на завадостійкість системи зв'язку та АУ ПвК. Основними з яких є: можливі форми та способи дій і впливу противника; основні завдання ПвК; існуюча система пунктів управління і особливості в організації інформаційних процесів; топологія системи зв'язку; стан засобів зв'язку та АУ та їх відповідність сучасним інформаційним технологіям; морально-психологічний стан і рівень підготовки особового складу військових частин та підрозділів зв'язку та АУ ПвК; фізико-географічні та метеорологічні умови операційної зони.

Існуюча методика оцінки завадостійкості системи зв'язку та АУ дозволяє визначити просторові обмеження забезпечення зв'язком, але ця методика спрямована на визначення ступеню впливу навмисних завад та не передбачає оцінку ступеню впливу ненавмисних (пасивних) завад, що здійснюється на підставі аналізу електромагнітної сумісності (ЕМС) радіоелектронних засобів (РЕЗ) ОВТ, розміщених на обмеженій ділянці місцевості.

Удосконалення методики оцінки завадостійкості системи зв'язку та АУ здійснено авторами введенням показника ЕМС РЕЗ ОВТ в операційному районі (зоні). Методика оцінки ЕМС РЕЗ ОВТ складається із наступних етапів: а) частотного аналізу РЕЗ; б) енергетичного аналізу РЕЗ; в) визначення норм частотно-територіального рознесення (ЧТР).

Частотний аналіз визначає канали проникнення ненавмисних завад у приймальний пристрій. Енергетичний аналіз визначає рівень потужності ненавмисної завади на вході приймача з урахуванням коефіцієнту спрямованої дії антени. Визначення норм ЧТР полягає у розрахунку для кожного каналу проникнення ненавмисної завади необхідного частотного рознесення на основі характеристики частотної вибіркової приймального пристрою для різних значень відстані між РЕЗ і варіантів взаємної орієнтації діаграми спрямованості антени (ДСА), при яких виконується детермінований критерій ЕМС РЕЗ. Рівень допустимої потужності кожного виду завад отримується тільки експериментально.

**УДК 004.056.5**

**Штонда Р.М.**, начальник науково-дослідного відділу Наукового центру зв'язку та інформатизації Військового інституту телекомунікацій та інформатизації імені Героїв Крут

## **ЗАВДАННЯ ТА ЕТАПИ ПРОВЕДЕННЯ НЕЗАЛЕЖНОГО АУДИТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВІЙСЬКОВИХ ЧАСТИН (УСТАНОВ) ЩОДО ЕФЕКТИВНОСТІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ**

Згідно з Постановою Кабінету Міністрів України від 19 червня 2019 року № 518, власник та/або керівник об'єкта критичної інфраструктури організовує проведення незалежного аудиту інформаційної безпеки на об'єкті критичної інфраструктури згідно з вимогами законодавства в сфері захисту інформації та кібербезпеки. Кіберзахист об'єкта критичної інфраструктури забезпечується шляхом впровадження на об'єкті критичної інформаційної інфраструктури об'єкта критичної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю [1].

До об'єктів критичної інфраструктури можуть бути віднесені також військові частини та установи, які включені до переліку, як такі, що мають стратегічне значення для економіки і безпеки держави. Виходячи з вище зазначеного виникає необхідність проведення незалежного аудиту інформаційної безпеки в військових частинах та установ Збройних сил України (далі – військові частини (установи)).

Незалежний аудит інформаційної безпеки військових частин (установ) необхідно проводити згідно з нормами чинного законодавства України, національних стандартів, а також з урахуванням рекомендацій міжнародних стандартів проведення аудиту.

Предметом незалежного аудиту є стан інформаційної безпеки у військових частинах (установах) щодо ефективності забезпечення кібербезпеки, інформаційно-телекомунікаційних системах та системах зв'язку Збройних сил України (далі – ІТС ЗС України). Метою проведення незалежного аудиту інформаційної безпеки у військових частинах (установах) щодо ефективності забезпечення кібербезпеки, ІТС ЗС України є отримання об'єктивної оцінки стану інформаційної безпеки (кібербезпеки), стан захищеності та її відповідності встановленим вимогам національних та рекомендаціям міжнародних стандартів інформаційної безпеки (кіберзахисту) і надання рекомендацій щодо їх уникнення (зменшення, перекладання чи прийняття).

Основними завданнями незалежного аудиту інформаційної безпеки військових частин (установ) щодо ефективності забезпечення кібербезпеки, ІТС ЗС України є:

- аналіз поточного рівня захищеності інформації, що обробляється та циркулює на об'єктах інформаційної діяльності військових частин (установ);
- оцінка інформаційної безпеки відповідно до загальноприйнятих стандартів;
- визначення ймовірних ризиків для інформаційно-телекомунікаційних систем (автоматизованих систем);
- виявлення слабких місць з можливістю їх усунення в майбутньому;
- формування звіту для спеціалістів із забезпечення інформаційної безпеки.

Етапи незалежного аудиту інформаційної безпеки військових частин (установ): внутрішній незалежний аудит; зовнішній незалежний аудит; технічний незалежний аудит; позаплановий незалежний аудит.

Основними етапами проведення внутрішнього незалежного аудиту інформаційної безпеки у військових частинах (установах) є:

- попередній аналіз документів необхідних для проведення незалежного аудиту інформаційної безпеки у військових частинах (установах);
- підготовка внутрішнього плану незалежного аудиту інформаційної безпеки у військових частинах (установах) аудитором інформаційної безпеки;
- збір відомостей незалежного аудиту інформаційної безпеки у військових частинах

(установах);

- аналіз зібраних даних під час незалежного аудиту інформаційної безпеки у військових частинах (установах);
- підготовка звіту за результатами незалежного аудиту інформаційної безпеки у військових частинах (установах).

Основними етапами проведення зовнішнього незалежного аудиту інформаційної безпеки у військових частинах (установах) є:

- попередній аналіз документів необхідних для проведення незалежного аудиту інформаційної безпеки у військових частинах (установах);
- підготовка внутрішнього плану незалежного аудиту інформаційної безпеки у військових частинах (установах) аудитором інформаційної безпеки;
- проведення тестування на проникнення з використанням програмно-апаратних засобів пошуку та аналізу вразливостей;
- аналіз зібраних даних під час незалежного аудиту інформаційної безпеки у військових частинах (установах);
- підготовка звіту за результатами незалежного аудиту інформаційної безпеки у військових частинах (установах).

Основними етапами проведення технічного незалежного аудиту інформаційної безпеки у військових частинах (установах) є:

- попередній аналіз документів необхідних для проведення незалежного аудиту інформаційної безпеки у військових частинах (установах);
- проведення тестування на виявлення вразливостей в мережах на об'єктах незалежного аудиту інформаційної безпеки;
- підготовка звіту за результатами технічного незалежного аудиту інформаційної безпеки у військових частинах (установах).

Під час проведення позапланово незалежного аудиту, необхідно враховувати основні етапи проведення внутрішнього, зовнішнього та технічного незалежних аудитів інформаційної безпеки у військових частинах (установах). Рекомендується проводити позапланового незалежний аудит інформаційної безпеки способом поєднання етапів проведення внутрішнього, зовнішнього та технічного незалежних аудитів інформаційної безпеки.

Проведення незалежного аудиту інформаційної безпеки є обов'язковим для всіх військових частин (установ). Чітке виконання зазначених етапів незалежного аудиту інформаційної безпеки надасть можливість визначити ефективність забезпечення кібербезпеки військових частин (установ).

Незалежний аудит інформаційної безпеки – один з найбільш ефективних сьогодні інструментів для отримання незалежної і об'єктивної оцінки поточного рівня захищеності військових частин (установ) від загроз інформаційної безпеки. Крім того, результати незалежного аудиту дають основу для формування стратегії розвитку системи забезпечення інформаційної безпеки військових частин (установ). Однак необхідно розуміти, що незалежний аудит інформаційної безпеки – це не разова процедура, він повинен проводитися на регулярній основі. Тільки в цьому випадку незалежний аудит буде приносити реальну віддачу і сприяти підвищенню рівня інформаційної безпеки військових частин (установ).

**УДК 621.391**

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

**Збежховська У.Р.**, ад'юнкт Харківського національного університету Повітряних Сил імені Івана Кожедуба

**Слободянюк В.В.**, викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба.

## **МЕТОД ПРИХОВАНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ В СИСТЕМАХ З OFDM МОДУЛЯЦІЄЮ**

Сьогодні однією з найважливіших вимог до сучасних систем передачі інформації (СПІ) в умовах ведення радіоелектронної розвідки є скритність. Тому з урахуванням стрімкого розвитку інформаційно телекомунікаційних систем нового покоління виникає завдання пошуку та розробки нових методів забезпечення високого рівня скритності СПІ. Наприклад, за допомогою використання в якості носіїв інформації хаотичних процесів та послідовностей. Одним з найефективніших методів забезпечення інформаційної, енергетичної і спектральної ефективності сучасних систем зв'язку є сигнали з OFDM-модуляцією (Orthogonal frequency division multiplexing). Використання сигналів з OFDM-модуляцією дозволяє підвищити швидкість прийому-передачі даних та інформаційну ємність системи в умовах багатопроменевого поширення при обмеженій смузі пропускання.

В роботі проаналізовано IID-скритність сигналів з OFDM-модуляцією, тобто оцінено їх близькість до “білого” шуму, за допомогою непараметричної BDS-статистики. Аналіз отриманих результатів показав, що такі сигнали не володіють ознаками IID-скритності, оскільки їх значення знаходяться за межами інтервалу  $(-1,96; 1,96)$ . Наявність замкнутих траєкторій в “образах” гармонічних сигналів з OFDM-модуляцією в псевдофазовому просторі, свідчить про структурованість та залежність значень сигналу один від одного та відрізняє їх від “образу” “білого” шуму.

Тому для подальшого використання OFDM сигналів у перспективних системах спеціального радіозв'язку запропоновано підвищити їх скритність, за допомогою хаотичних послідовностей з властивостями близькими до “білого” шуму. Для цього на основі поліномів Чебишева 1 роду 3 та 4 порядків було сформовано хаотичні піднесучі. Далі здійснено перетворення отриманих піднесучих в аналоговий сигнал обмежений в деякій смузі частот та перенесено кожен з них на свою піднесучу частоту. Аналіз BDS-статистик отриманих хаотичних сигналів з OFDM модуляцією показав, що їх значення знаходяться ближче до інтервалу  $(-1,96, 1,96)$ , ніж у гармонічних сигналів з OFDM модуляцією, що може свідчити про можливе підвищення IID скритності. При цьому, “образ” сигналу в псевдофазовому просторі та енергетичний спектр сформованих хаотичних сигналів з OFDM-модуляцією підтверджує їх близькість до “білого” шуму.

Виходячи з проведених розрахунків та моделювання можна зробити висновок, що використання хаотичних сигналів з OFDM модуляцією дозволяє підвищити IID – скритність, в порівнянні з традиційними сигналами з OFDM – модуляцією. Це стимулює проведення подальших досліджень властивостей хаотичних сигналів з OFDM-модуляцією і можливостей їх використання при організації скритного радіозв'язку в СПІ спеціального призначення.



**УДК 621.391**

**Рисаков М.Д.**, старший науковий співробітник Наукового центру Повітряних Сил Харківського національного університету Повітряних Сил ім. Івана Кожедуба, кандидат технічних наук  
**Воронов Д.М.**, заступник начальника відділу Наукового центру Повітряних Сил Харківського національного університету Повітряних Сил ім. Івана Кожедуба, кандидат технічних наук  
**Лопатін А.В.**, старший науковий співробітник Наукового центру Повітряних Сил Харківського національного університету Повітряних Сил ім. Івана Кожедуба

### **ПРОПОЗИЦІЇ ЩОДО ПРИНЦИПІВ ПОБУДОВИ РЕТРАНСЛЯТОРІВ НА БЕЗПЛОТНОМУ ЛІТАЛЬНОМУ АПАРАТІ ДЛЯ УПРАВЛІННЯ АВІАЦІЄЮ ВІЙСЬКОВИХ ФОРМУВАНЬ УКРАЇНИ**

У доповіді пропонуються технічні рішення, що вирішують завдання забезпечення зниження маси та забезпечення надійності роботи апаратури ретранслятора.

Наземні і бортові радіостанції працюють на фіксованих (заданих) частотах. Для забезпечення ретрансляції сигналів радіостанцій у прямому напрямку – від наземних пунктів управління до бортових радіостанцій літальних апаратів та в зворотному напрямку – до радіостанцій наземних пунктів управління пропонується виконати частотне рознесення радіосигналів цих радіостанцій та бортового комплексу ретрансляції БПЛА. Для реалізації цього необхідно мати два комплекти приймально-передавальної апаратури, яку пропонується будувати за трансиверною схемою.

Трансиверний принцип побудови трактів означає, що окремі каскади підсилення використовуються в режимах передачі і прийому.

Для зниження маси та енергоживлення апаратури ретранслятора пропонується використати направлені антени з високим коефіцієнтом підсилення та вузькою направленістю. Це дасть змогу знизити взаємовплив обох комплектів приймально-передавальної апаратури та знизити потрібну потужність передавачів, а з нею необхідне енергоживлення та масу апаратури ретранслятора, що має особливе значення при розміщенні її на БПЛА.

**УДК. 519.711.3**

**Рудковський О.М.**, науковий співробітник Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного  
**Ільницький І.Л.**, молодший науковий співробітник Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

### **ПЕРСПЕКТИВИ РОЗВИТКУ ТА ЗАСТОСУВАННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ ВІЙСЬКАМИ**

Аналіз ведення бойових дій в ході операції Об'єднаних сил на тимчасово окупованій території Сходу України показав, що ефективність застосування підрозділів ЗС України, Національної гвардії та інших військових формувань значною мірою залежить від рівня розвитку системи управління військами. В свою чергу, можливість суттєво підвищити бойові можливості військ, скоротити витрати часу роботи органів управління на планування дій та доведення до підлеглих підрозділів, надає автоматизація процесу управління.

Система управління вимагає від системи зв'язку та АСУ своєчасного проходження і опрацювання всіх видів інформації у реальному масштабі часу, достовірності відтворення повідомлень із заданою точністю, здатності протистояти порушенням обміну інформацією.

Виконання завдань розвитку системи управління військами надасть можливість створити єдиний інформаційний простір та надійний обмін різними видами інформації в закритому вигляді. Забезпечити використання ресурсів цифрової транспортної мережі зв'язку, скоротити

кількість термінального обладнання, створити економічні та організаційні умови для інтенсифікації розвитку і розповсюдження вітчизняних технологій.

Кожна автоматизована система управління ЗС України є складовою частиною системи управління Збройними Силами і включає до себе відповідні види забезпечення, а саме: інформаційне, математичне, лінгвістичне, програмне, організаційне, нормативно-правове, метрологічне і технічне.

Заходи, що здійснюються найближчим часом з метою вдосконалення системи зв'язку та АСУ ЗС України, нададуть можливість значного підвищення рівня якості управління військами і озброєнням. Але на даний час існує низка проблемних питань, що гальмують розвиток системи, а саме: відсутність уніфікованих засобів зв'язку і єдиної програмної платформи; уніфікованого інформаційного забезпечення, єдиної транспортної мережі, побудованої на сучасних цифрових стандартах.

Головною метою розвитку та вдосконалення системи зв'язку та АСУ Збройних Сил є забезпечення відповідності оперативно-технічних характеристик вимогам системи управління ЗС в мирний і воєнний час.

#### **УДК 621:681.65**

**Єльчанинов О.Д.**, професор кафедри Національної академії Національній гвардії України, кандидат технічних наук, доцент.

### **ПРОБЛЕМА ОЦІНКИ СТАНУ АДАПТИВНОЇ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНОЇ СИСТЕМИ РОБОТОТЕХНІЧНОГО КОМПЛЕКСУ**

Інформаційно-вимірювальна система (ІВС) є невід'ємною структурною складовою будь-якого робототехнічного комплексу (РК). У загальному випадку така система являє собою сукупність функціонально об'єднаних апаратно-програмних засобів, призначених для отримання поточної інформації про власний стан РК та стан зовнішнього середовища з подальшим перетворенням цієї інформації у сигнали керування. Ефективність функціонування РК у цілому в значній мірі залежить від якості його ІВС.

В процесі оцінювання якості стану ІВС виникає необхідність розв'язання багатокритеріальних (векторних) оптимізаційних задач. При цьому найбільш складними є багатокритеріальні задачі, що розв'язуються в умовах ситуаційної (ап'юріорної) невизначеності та відносяться до класу некоректних задач. У таких задачах незначні варіації спостережуваних реалізацій вибірок призводять до непередбачених результатів їх розв'язання.

Ситуаційна невизначеність оцінки стану зумовлена впливом непередбачуваних дестабілізуючих факторів середовища її перебування – зовнішня невизначеність, а також існуванням різноманітних ресурсних обмежень – внутрішньосистемна невизначеність. Притаманні будь-якій реальній системі дестабілізуючі фактори та непереборні ресурсні обмеження на фізичному рівні проявляються у вигляді випадкових зовнішніх і внутрішньосистемних збурень. За такої детермінації степінь ситуаційної невизначеності стану ІВС буде різним в будь-які довільні моменти часу.

Вибір інтегрального показника ІВС РК передбачає формування тим чи іншим способом критерія оцінки якості стану досліджуваної системи. Згідно основних положень теорії системного аналізу інтегральний або глобальний (узагальнений) показник стану і критерій оцінки якості будь-якої технічної системи мусять бути функцією всіх найважливіших характеристик системи, у фізичному сенсі конструктивними і простими, відображати якість виконання системою поставлених завдань. Суперечливість вимог та умов формування інтегрального показника оцінки якості такої системи ускладнюється тим, що для більшості

реальних процесів характерним є неперервність змінювання параметрів, які визначають критерії її оптимальності. У подібних ситуаціях простір стратегій прийняття рішень стає нескінченним, що обмежує застосування методів приведення векторної оптимізації до скалярної та введення глобального показника якості.

**УДК. 623.396**

**Кубрак В.Г.**, начальник науково-дослідного відділу наукового центру Повітряних Сил Харківського національного університету Повітряних Сил ім. Івана Кожедуба

### **ВПРОВАДЖЕННЯ СУЧАСНИХ ФОРМ І СПОСОБІВ ОРГАНІЗАЦІЇ МЕРЕЖ ТАКТИЧНОГО ЗВ'ЯЗКУ ОБ'ЄДНАНОГО УГРУПУВАННЯ ВІЙСЬК (СИЛ)**

Впродовж останніх років у ЗС США та країн НАТО приділяється посилена увага розробці та практичній реалізації технології побудови самоорганізованих мереж зв'язку, які отримали умовне найменування MANET (Mobile Ad-Hoc NETworking), (бездротові децентралізовані самоорганізовані мережі з мобільних пристроїв). Вони складаються з мобільних пристроїв (радіостанцій) зі стандартними IP-інтерфейсами і зі збереженням широких можливостей по модернізації програмного забезпечення. Впровадження подібних систем для забезпечення інформаційного обміну об'єднаного угруповання військ (сил) дозволить отримати можливість передачі даних на великі відстані без збільшення потужності передавача. При цьому підвищиться стійкість до змін в інфраструктурі мережі зв'язку. З'явиться можливість швидкої реконфігурації мереж зв'язку в умовах складної перешкодової і радіочастотної обстановки, збільшиться швидкість їх розгортання.

**УДК 004.8**

**Чопенко Д.А.**, молодший науковий співробітник Наукового центру Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба

### **КОНТРОЛЬ КОРЕКТНОСТІ ВАРІАНТІВ РІШЕНЬ ПО РЕСУРСАМ ТА ЧАСУ У ВІДКРИТИХ ЕКСПЕРТНИХ СИСТЕМАХ РЕАЛЬНОГО ЧАСУ**

Виходячи з аналізу інформації, яка характеризує обстановку, що склалася і яка використовується в процесі вироблення рішень у відкритих експертних системах реального часу, неможливо однозначно визначити, як надалі буде розвиватися ситуація. Це обумовлено як цілеспрямованим дією, так і наявністю величезної кількості зовнішніх випадкових факторів. Тому кожній ситуації відповідає деяка множина варіантів розвитку обстановки, які характеризують різні шляхи досягнення актуальних цілей, обумовлені наявністю дій з невизначеним результатом. Під можливим варіантом рішення розуміється один з варіантів досягнення цілей, що реалізується за необхідним запасом ресурсів і часу.

Варіант розвитку обстановки вважається коректним (здійсненим), якщо в даній ситуації система володіє достатнім запасом ресурсів, які необхідні для досягнення цілей управління, і час досягнення поставлених цілей не перевищує встановленого граничного значення. Іншими словами варіант розвитку обстановки, коректний, якщо для нього можна сформулювати, принаймні, один можливий варіант рішення. Висновок про коректність варіантів рішень робиться виходячи з результатів аналізу реалізуєності по ресурсам та часу складових його варіантів досягнення цілей. Тому необхідно розглядати особливості подання варіантів досягнення цілей, які визначають послідовність аналізу його реалізуєності.

Сформульована задача аналізу реалізуємості варіантів досягнення цілей, яка включає в себе складання здійсненого плану реалізації варіантів досягнення цілей при відповідних обмеженнях на час досягнення поставлених цілей управління і запасу ресурсів, наявних у розпорядженні.

Розрахунок часових параметрів робіт і розподіл ресурсів обраними методами мережевого планування і управління запропоновано безпосередньо здійснювати на графі варіанту досягнення цілей, так як він повністю задовольняє вимогам до структури мережевої моделі. У загальному випадку час реалізації робіт, які необхідно виконати для досягнення поставлених цілей управління, може бути задано точковим значенням або інтервалом можливих значень.

Визначений порядок аналізу реалізуємості варіанту досягнення цілей у випадку, якщо час виконання складових його робіт заданий тільки точковими значеннями та у випадку, коли час використання ресурсів може бути заданий інтервалом можливих значень. Надалі визначений порядок аналізу реалізуємості варіанту досягнення цілей по ресурсам і часу. Описана процедура перерозподілу ресурсів, заснована на методах евристичного планування.

Якщо в процесі вироблення рішень для певного виду розвитку обстановки не вдалося сформулювати жодного реалізуємого варіанту досягнення цілей, то досягнення поставлених цілей управління в даній ситуації неможливо. У цьому випадку повинна бути сформульована задача, яка відповідна складу та запасу ресурсів, який маєтсья, шляхом відповідного коригування узагальненої мережевої моделі.

#### **УДК 621.391**

**Корольок Н. О.**, заступник начальника кафедри Харківського національного університету Повітряних Сил ім. Івана Кожедуба, кандидат технічних наук, доцент

**Коршець О. А.**, заступник начальника кафедри Національного університету оборони України ім. І. Черняхівського, кандидат технічних наук

**Першин О. В.**, викладач кафедри Харківського національного університету Повітряних Сил ім. Івана Кожедуба

### **ФОРМАЛЬНЕ ПРЕДСТАВЛЕННЯ ПРОЦЕСІВ ПЛАНУВАННЯ МАРШРУТУ БПЛА**

Планування повітряної розвідки представляє собою ряд послідовних процесів, які на даний час є неавтоматизованими. З огляду на розглянуту послідовність основних етапів процесу планування маршруту польоту БПЛА і притаманну знанням невизначеність пропонується в подальшому розглядати знання, якими оперує когнітолог при розробці і супроводі бази знань: знання про прогнозовану операцію, тактичні умови проведення розвідки, вплив зовнішнього середовища (опаді, туман, температура повітря, швидкість и напрямлення вітру на рівні землі, висоті польоту, рельєф) на дальність польоту БПЛА під час підготовки до бойових дій; знання про найбільш важливі ті об'єкти, які приймають участь в системі управління протилежної сторони та інформаційній протидії в операції; знання про прогнозовану систему ППО противника (місцезнаходження, значення пунктів управління системою ППО, угруповання ЗРК великої та середньої дальності, військових та об'єктових засобів ППО); знання щодо визначення доцільної стратегії польоту БПЛА з урахуванням виду операції (за результатами зіставлення прогнозованої і реальної наземної обстановки).

При розробці моделі предметної області завдання планування маршруту польоту БПЛА на етапі концептуалізації пропонується використання методології об'єктно-орієнтованого аналізу - методу для ототожнення важливих сутностей в задачах реального світу, для розуміння і пояснення того, як вони взаємодіють між собою. Сучасні підходи до створення програмного забезпечення АСУ базуються в основному на двох основних технологіях: структурної і об'єктно-орієнтованої. Основна відмінність цих технологій полягає в способі декомпозиції предметної

області. У структурній технології використовується представлення програми у вигляді ієрархічної структури блоків інструкцій. При об'єктно-орієнтованій технології основною одиницею є не функція, а клас програмних об'єктів, тобто операційна категорія, яка об'єднує як конкретні значення даних, так і методи (операції) в програмному кодї, які маніпулюють цими значеннями.

Таким чином, в якості базової технології програмної реалізації бази знань системи управління БПЛА пропонується використовувати об'єктно-орієнтовану технологію, що дозволить сформулювати попередній опис знань за результатами виконання процедури концептуалізації, створити модель, яка буде використана при об'єктно-орієнтованому проектуванні, розробити схему програмної реалізації бази знань з використанням об'єктно-орієнтованого програмування.

#### **УДК. 621.39**

**Опалінський В.Б.**, викладач кафедри Національної академії сухопутних військ

**Давіденко С.В.**, доцент кафедри Національної академії сухопутних військ, кандидат технічних наук, доцент

**Бойчук Б.М.**, старший викладач кафедри Національної академії сухопутних військ

### **ПЕРСПЕКТИВИ РОЗВИТКУ НОВІТНІХ ТЕХНОЛОГІЙ ТА ЗАСОБІВ ЗВ'ЯЗКУ В ІНТЕРЕСАХ УПРАВЛІННЯ ВІЙСЬКАМИ**

Сьогодні в умовах високого рівня інформаційного забезпечення бойових дій військ стає визначальним чинником досягнення стратегічної і оперативної переваги над противником. У сучасній війні виграє той, хто витрачає менше часу на проведення збору інформації, аналіз та розрахунки, і, відповідно, більш оперативно, ефективно та оптимально приймає рішення в умовах обстановки, що склалася.

Як показує досвід, провідні країни світу, з точки зору системи управління, розвиваються в напрямку створення багатофункціональної інформаційно-управляючої системи, яка інтегрує функції управління військами, зброєю, розвідкою, радіоелектронною боротьбою, а також зв'язку, навігації, орієнтування тощо. Тобто йде мова про ведення бойових дій в єдиному інформаційно-комунікаційному просторі, а саме концепцію мережецентричної організації управління.

Гібридна війна на Сході України відчутно змінила не лише ставлення до управління частинами і підрозділами, а й використання сучасних засобів управління та зв'язку. Так, на момент початку ООС (АТО), на озброєнні в підрозділах Збройних Сил України стояли переважно аналогові комплекси та засоби зв'язку виробництва колишнього СРСР, які вже на той час давно технічно та морально застаріли. Тому одним із важливих питань, яке потребувало негайного вирішення, було питання переведення системи зв'язку на цифрові канали і засоби зв'язку та створення якісної цифрової системи зв'язку, яка б забезпечувала потреби як Збройних Сил України, так і усіх силових структур держави у цілому.

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 радіозв'язку у ЗС України є актуальним. В рамках реалізації положень Стратегічного оборонного бюлетеня України керівництвом ЗС України ведеться робота щодо створення ефективної системи оперативного управління, зв'язку, розвідки та спостереження (C4ISR), яка б відповідала стандартам НАТО, та забезпечення її інтеграції з Єдиною системою управління оборонними ресурсами (Defense resources management information system – DRMIS). Сьогодні у Збройних Силах України

величезна увага приділяється розвитку та вдосконаленню стаціонарної та польової компоненти системи зв'язку та автоматизації управління всіх ланок управління в частині їх повного переоснащення новітніми засобами, переходу на цифрові системи передачі та обробки інформації. У ЗС України С4ISR створюватиметься у відповідності до прийнятої в країнах НАТО мережецентричної концепції управління військами в ході ведення бойових дій. Технологічно основою для реалізації даної системи стане єдина автоматизована система ЗС України, яка буде інтегрувати автоматизовані системи бойового управління, обчислювальну техніку, засоби зв'язку, радіоелектронної боротьби, розвідки, навігації та засоби вогневого ураження.

Застосування новітнього високотехнологічного обладнання зв'язку дало змогу відмовитись від застарілих та слабоефективних принципів організації і забезпечення зв'язку 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.

Забезпечення ефективного управління підрозділами Збройних Сил України доцільно організовувати за допомогою комплексного підходу – розробці сучасних засобів зв'язку та комутації вітчизняного виробництва, а також застосування передових технологій і засобів телекомунікації провідних країн світу. Це, в свою чергу, в подальшому дасть можливість впровадити в ЗС України концепцію ведення бойових дій в єдиному інформаційному просторі.

#### **УДК 004.8**

**Хижняк І.А.**, викладач кафедри Харківського національного університету Повітряних Сил ім. Івана Кожедуба, кандидат технічних наук

### **ВИКОРИСТАННЯ МЕТОДІВ РОЙОВОГО ІНТЕЛЕКТУ ПРИ КЕРУВАННІ ГРУПОЮ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ**

На сьогоднішній день в зоні проведення операції Об'єднаних сил на території Донецької та Луганської областей для виконання завдань спостереження активно застосовуються безпілотні літальні апарати (БпЛА). Так як традиційні види озброєння протиповітряної оборони розраховані на віддалені та великі за розміром цілі, тому доцільним є застосування нано-, мікро- та мініБпЛА, які літають на малих висотах. На даний час активно використовуються автономні БпЛА та БпЛА з комбінованою системою управління, які виконують поставлені завдання при мінімальному втручанні оператора.

Масове виробництво та відносна дешевизна малорозмірних БпЛА на сьогоднішній день дає можливість їх групового застосування. Тому перспективним є створення груп з взаємодіючих один з одним БпЛА та безпілотних авіаційних комплексів (БпАК) або групою з БпЛА, які можуть приєднуватися у будь-які складні системи, такі як мережецентричні системи управління, що дозволить більш спрямовано та якісно виконувати поставлені завдання.

Однією з основних проблем при використанні групи БпЛА (БпАК) є складності в забезпеченні радіозв'язку з пультом керування оператора у зв'язку з тим, що потужність радіопередавачів та розмір антени обмежені через невеликий розмір самого апарату. Використання націлених наземних антен для супроводження апарату вирішить таку проблему, але обмежить зону використання малорозмірного БпЛА. А використання груп БпЛА (БпАК) робить проблему забезпечення радіозв'язку ще більш актуальною.

Для вирішення даної проблеми у групах БпЛА пропонується використовувати методи ройового інтелекту. Так, при взаємодії БпЛА у групах на основі методів ройового інтелекту, кожний апарат взаємодіє лише з найближчими у даний момент до нього БпЛА. Отже дальність зв'язку та енерговитрати на інформаційний обмін значно малі.

Ройовий підхід при взаємодії БпЛА у групі можна також застосовувати для вирішення задачі пошуку та виявлення перешкод та зон дії протиповітряної оборони противника, а також для прокладання найкращого маршруту руху польоту БпЛА з урахуванням таких обмежень.

Також використання методів ройового інтелекту може вирішити задачу ретельного збору інформації групою БпЛА про територію, тобто мінімізувати перекриття робочих зон сенсорних пристроїв, при цьому не допускаючи пропуску ділянок або приділяти значну увагу об'єктам інтересу.

#### **УДК 621.396**

**Васюта К.С.**, заступник начальника Харківського національного університет Повітряних Сил імені Івана Кожедуба з навчальної роботи, доктор технічних наук, професор, заслужений діяч науки і техніки

**Кацшин О.Л.**, ад'юнкт Харківського національного університет Повітряних Сил імені Івана Кожедуба

### **МЕТОДИ ПОБУДОВИ СКЛАДЕНИХ ХАОТИЧНИХ СИГНАЛІВ ДЛЯ ПІДВИЩЕННЯ РОЗДІЛЬНОЇ ЗДАТНОСТІ**

На сьогоднішній день велика увага приділяється методам передачі, в яких в якості носія інформації використовують не гармонійні коливання, а шумоподібні сигнали. Особливість такого виду передачі інформації, як шум, пояснюється новою перспективою їх застосування в різних інформаційних технологіях, в тому числі й в радіолокації.

Шумоподібні сигнали на основі динамічного хаосу є широкосмуговими та володіють властивостями випадкових шумових сигналів: широкий спектр, змінюється за зовнішнім виглядом при кожній вибірці реалізація такого сигналу, та має головну особливість – їх можливо реалізувати з використанням розробленого математичного алгоритму, тобто володіють властивістю відтворення.

Широкосмугові сигнали, крім того, отримали широке застосування, тому як дозволяють в повній мірі реалізувати переваги оптимальних методів обробки сигналів, забезпечують високу завадостійкість, дозволяють успішно боротися з багатопроменевим поширенням радіохвиль шляхом розділення промінів, дозволяють підвищити скритність роботи системи та її роздільну здатність.

Одною з переслідуваних цілей при застосуванні складних сигналів є підвищення роздільної здатності радіолокаційних засобів. Такі радари в іноземних джерелах мають назву Low Probability of Intercept (LPI) Radar, тобто в перекладі з англійської радар с низькою вірогідністю перехвату або з підвищеною скритністю функціонування.

Пропонується формувач хаотичних несучих складеного хаотичного сигналу, який виконано на базі генератору тактових імпульсів, сигнального процесору та цифро-аналогового перетворювача.

Структурна схема системи передачі та прийому зондуючого радіолокаційного сигналу, дозволяє привести цифрову хаотичну послідовність, що згенерована за допомогою сигнального процесора, до аналогового вигляду.

Отримана часова реалізація хаотичної несучої подібна до білого шуму (шуму спостереження). При застосуванні сформованої складеної хаотичної несучої з'являється можливість підвищити роздільну здатність та скритність функціонування радіолокаційних систем посадки.

**УДК 621.391**

**Мельніков І.С.**, молодший науковий співробітник наукового центру Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба

**Кулик О.П.**, провідний науковий співробітник наукового центру Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат військових наук

### **ПРОБЛЕМНІ ПИТАННЯ УПРАВЛІННЯ ПОЛЬОТАМИ ЛІТАКІВ ВИРОБНИЦТВА КРАЇН-ЧЛЕНІВ НАТО**

Максимальна реалізація можливостей авіації військових формувань України багато в чому залежить від наявності стійкого, безперервного, оперативного та скритого управління військами (силами). Таке управління може бути досягнуте лише у разі побудови високоефективної, багаторівневої системи управління, функціонування якої об'єктивно залежить від ефективності функціонування однієї з її основних складових – системи зв'язку.

Для управління польотами літаків виробництва країн-членів НАТО при участі їх екіпажів у навчаннях, що проводяться на території України, а також при нарощуванні спроможностей авіації військових формувань України шляхом закупівлі (лізингу, оренди) авіаційної техніки у країн-членів НАТО виникає потреба в забезпеченні повітряного радіозв'язку з літаками виробництва країн-членів НАТО.

Наземні авіаційні засоби радіозв'язку, які застосовуються для управління авіацією військових формувань України, працюють в діапазоні 100-150 МГц та 220-400 МГц з видами модуляції АМ, ЧМ і ЧТ і за своїми характеристиками можуть бути тільки частково застосовані для забезпечення управління літаками виробництва країн-членів НАТО.

До складу бортового обладнання літаків виробництва країн-членів НАТО входять пристрої системи розподілу тактичної інформації JTIDS або аналогічної по сфері застосування системи Link 16, у ВПС Швеції використовується система CDL 39. Проведений аналіз основних технічних характеристик, загальних даних про принципи побудови систем JTIDS, Link 16 і CDL 39 свідчить, що вони відповідають вимогам стандарту НАТО STANAG 5516, використовують множинний доступу з часовим розподілом, працюють в діапазоні 960-1215 МГц та за своїми протоколами є частково сумісними між собою.

В зв'язку з цим існує необхідність закупівлі спеціалізованих наземних засобів, які б забезпечували роботу у вказаних системах.

**УДК 621.391**

**Литвин А.В.**, викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба

**Попович Б.Р.**, курсант Харківського національного університету Повітряних Сил імені Івана Кожедуба

### **ПРОПОЗИЦІЇ ЩОДО ЗАСТОСУВАННЯ МЕТОДУ ЗМЕНШЕННЯ ПОЗАСМУГОВОГО ВИПРОМІНЕННЯ OFDM-СИГНАЛІВ В СУЧАСНИХ ЦИФРОВИХ РРС**

Використання сучасних засобів радіозв'язку та їх аналіз показав, що забезпечення ефективного управління підрозділами Збройних Сил потребує використання новітніх систем, спрямованих на підвищення ефективності використання радіомереж в ході сучасних бойових дій.



В першу чергу потрібно розглянути переваги сучасних безпроводних систем стандарту WiMAX і методи її використання в цифрових РРС під час проведення реальних бойових дій та проаналізувати, як саме можна забезпечити високоефективний радіозв'язок.

Радіорелейний зв'язок час ведення ООС можна організувати за допомогою сучасних цифрових радіорелейних станцій в обмежений термін при порівняно невеликій кількості особового складу і транспорту, а також у таких умовах, за яких проводний зв'язок організувати важко або неможливо.

Система стандарту WiMAX є оптимальним рішенням для підвищення пропускної спроможності, мобільності і надійності РРС, за рахунок використання сучасних видів модуляції, таких як: QPSK (Quadraturephase-shiftkeying), QAM (Quadrature Amplitude Modulation), OFDM (Orthogonal Frequency-Division Multiplexing). Наряду з чисельними перевагами застосування технології OFDM існують її суттєві недоліки, такі як: високий пік-фактор (peak-to-average power ratio – PAPR), нелінійні спотворення в радіотракті засобів радіозв'язку, помилки синхронізації, висока чутливість до помилок компенсації фазових зсувів в каналі, що порушує ортогональність несучих.

Для зменшення позасмугового випромінення сигналів пропонується застосувати віконну обробку часового сигналу вікон типу припіднятий косинус. На практиці спектр OFDM-сигнала має велику кількість бокових лепестків, які поступово згасають в частотній мірі, що призводить до збільшення позасмугового випромінення. Окрім застосування захищених піднесучих, які доповнюються по краях OFDM-сигналу, для зниження побічного випромінення OFDM-символу застосовується обробка сигналу за допомогою віконної обробки інформації. Використання віконної функції здійснюється з метою локалізації сигналу OFDM у частотно-часовій області.

Запропонований метод зменшення рівня бічних пелюсток піднесучих, у розробляємій цифровій РРС з використанням технології WiMAX, дозволить зменшити рівень позасмугового випромінювання, що є актуальним з точки зору забезпечення електромагнітної сумісності радіотехнічних систем передачі інформації в зоні проведення ООС.

#### **УДК 621.391**

**Литвин А.В.**, викладач кафедри радіоелектронних систем пунктів управління Повітряних Сил Харківського національного університету Повітряних Сил;

**Громова Т.В.**, курсант Харківського національного університету Повітряних Сил.

### **МЕТОД ПІДВИЩЕННЯ ЖИВУЧОСТІ СИСТЕМИ НАЗЕМНОГО УКХ РАДІОЗВ'ЯЗКУ З УРАХУВАННЯМ УМОВ ПРОВЕДЕННЯ ООС**

Використання сучасних засобів радіозв'язку та їх аналіз показав, що забезпечення ефективного управління підрозділами Збройних Сил України потребує реалізація новітніх військових концепцій, спрямованих на підвищення ефективності використання збройних сил в ході сучасних бойових дій, особливо в тактичному ланці управління, потребує вирішення великої кількості завдань як організаційного так і технічного характеру.

В першу чергу потрібно розуміти переваги сучасних радіомереж, розглянути їх побудову під час реальних бойових дій та проаналізувати, як саме можна забезпечити високоефективний радіозв'язок між пунктами управління.

Мережа MANET є оптимальним рішенням для підтримки роботи оперативних служб та підрозділів тактичної ланки в екстремальних ситуаціях, під час виконання спеціальних завдань. Висока надійність такої мережі обумовлена відсутністю загального центру управління, який може вийти з ладу в результаті руйнівних зовнішніх або внутрішніх впливів. Живучість даної мережі є більш високою порівняно із іншими, що дає змогу більш вірогідно забезпечити зв'язком Збройні Сили.

Проаналізувавши різні види топологій мереж, прийшли до висновку, що живучість системи залежить від кількості маршрутів та кількості цінних вузлів в ній. Чим більша кількість маршрутів, тим більша живучість всієї системи, так як мережа буде зберігати та виконувати свою функцію що до передачі інформації.

Запропонований алгоритм підвищення живучості призводить до зросту надійності, пропускнуої спроможності та живучості мереж, за рахунок додавання більш простих але корисних маршрутів від пункту А до пункту Б. Таким чином, розглянувши дві основні властивості показника живучості мереж зв'язку, а саме структурну і функціональну живучість, було наведено методичку розрахунку та дослідження показників живучості та підвищення живучості сучасних мереж. Досягнення достатнього рівня живучості дозволить вважати технологію побудови мереж класу MANET найбільш перспективною в найближчі десятиріччя при побудови систем зв'язку тактичного рівня.

#### **УДК 62-512**

**Оборнєв С.І.**, науковий співробітник Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

### **ПЕРСПЕКТИВИ РОЗВИТКУ ТА ЗАСТОСУВАННЯ СУЧАСНИХ СИСТЕМ З УДОСКОНАЛЕННЯ ЗБЕРЕЖЕННЯ МАТЕРІАЛЬНИХ ЗАПАСІВ ПРИ ВІДНОВЛЕНІ БОЄДАТНОСТІ ОЗБРОЄННЯ**

Бойова готовність та боєдатність озброєння, військової техніки напряму пов'язано з складовими управління і технологією відновлення. Удосконалення системи управління логістичним забезпеченням, відповідно до вимог стандартів країн-членів НАТО, з удосконалення системи збереження матеріальних запасів та нарощування пропускнух можливостей з відновлення озброєння, передбачає отримання кращих результатів при тих же витратах ресурсів. Ідентифікація предметів постачання це найважливіший елемент системи кодифікації тому, що вона встановлює унікальний опис кожного предмету постачання. Вона складається з мінімуму даних, необхідних для чіткого визначення основних характеристик предмету, тобто тих характеристик, які надають предмету унікальний характер і відрізняють його від інших предметів.

Створення номенклатурного каталогу предметів постачання в Збройних Силах України, який постійно буде наповнюватися відповідно до принципів системи кодифікації НАТО, дасть змогу забезпечити точною інформацією про предмет постачання (характеристики), джерела постачання, інші дані, що забезпечить оперативність вирішення завдань матеріально-технічного забезпечення, розподілу та використання фінансових, матеріальних й інших ресурсів для забезпечення боєдатності військ.

Створення каталогу ідентифікації предметів постачання в системі управління Збройними Силами України, дозволить провести інтеграцію в єдиний функціонально-інформаційний простір на єдиній програмній платформі автоматизованих систем, за єдиними стандартами з країнами альянсу.

**УДК 621.391**

**Королюк Н.О.**, заступник начальника кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент

**Королюк А.О.**, здобувач вищої освіти факультету міжнародних економічних відносин та туристичного бізнесу Харківського національного університету імені В. Каразіна

**Романюк А.О.**, науковий співробітник наукового центру Повітряних Сил Харківського національного університету Повітряних Сил імені Івана Кожедуба

### **ОСОБЛИВОСТІ ОЦІНКИ РИЗИКУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ НА ОСНОВІ ТЕОРІЇ НЕЧІТКИХ МНОЖИН**

Забезпечення інформаційної безпеки (ІБ) є частиною управління інформаційною системою (ІС) в цілому. При цьому однією з найважливіших складових системи управління ІБ є оцінка ризиків, яка призначена для визначення ефективності застосовуваних механізмів захисту на основі конкретних метрик. Актуальним залишається завдання удосконалення існуючих методів оцінки ризику ІБ у зв'язку з виникненням нових видів небезпек. Ризики безпеки ІС дуже тісно пов'язані з невизначеністю. При цьому можна виділити два випадки невизначеності: ідентифікації поточних і майбутніх станів систем. При вирішенні завдань, пов'язаних з оцінками ризику безпеки, дуже часто постає питання про якісну інтерпретацію тих чи інших рівнів параметрів. Лінгвістична оцінка рівня безпеки зрозуміліша і найкращим чином описує стан безпеки ІТ-інфраструктури, що, в свою чергу, спонукає керівника до прийняття якісних рішень.

Особливості загроз інформаційно-телекомунікаційних мереж у зв'язку з неможливістю формалізації наслідків реалізацій загроз вимагають застосування методу оцінки ризиків на основі теорії нечітких множин. Цей математичний апарат дозволяє визначити кількісні характеристики суб'єктивним методом.

Таким чином, застосування теорії нечітких множин дає можливість формалізації процесу оцінки ризиків і збитку при різних загрозах ІБ. Враховуючи актуальність і новизну підходу щодо оцінки ризику інформаційної безпеки центру управління та оповіщення на основі теорії нечітких множин планується продовжити дослідження в області аналізу ризику ІБ в інформаційно-телекомунікаційній мережі.

**УДК 621.396. 97**

**Жук О.В.**, викладач кафедри Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

**Матала І.В.**, науковий співробітник Наукового центру Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

### **ОСОБЛИВОСТІ КЛАСИФІКАЦІЇ МОБІЛЬНИХ СИСТЕМ ТРАНКІНГОВОГО ЗВ'ЯЗКУ**

Суть транкінгового радіозв'язку полягає у забезпеченні голосового зв'язку між великою кількістю рухомих абонентів при обмеженій кількості радіоканалів.

Поняття мобільних систем зв'язку охоплює велику кількість різноманітних систем. Загалом до мобільних систем зв'язку відносяться територіальні, транкінгові, лінійні, космічні системи зв'язку та інші.

Мобільні систем транкінгового зв'язку, що існують на сьогоднішній день, можна класифікувати за наступними ознаками:

- за типом протоколу (стандарту);

- за принципом доступу організації до системи;
- за організацією управління базовим обладнанням та програмним забезпеченням;
- за принципом організації радіоканалу;
- за способом утримання радіоканалу;
- за способом організації радіоканалу;
- за способом конфігурації радіомережі;
- за призначенням;
- за кількістю абонентів.

Останнім часом з'явилась перспективна тенденція щодо створення на базі транкінгових систем – гами систем радіозв'язку загального користування, які є продовженням телефонних мереж загального користування. Разом з тим такі системи можуть знайти чільне місце у системах зв'язку Збройних Сил та інших силових структур України.

Таким чином, принцип транкінгового зв'язку полягає у вільному доступі абонентів до декількох радіоканалів, що дозволяє суттєво підвищити дієвість системи управління Збройних Сил України та адаптувати її до системи управління, що застосовується в країнах – членах НАТО.

#### **УДК 621.391**

**Чечуй О.В.**, доцент кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент

**Дудко Г.С.**, курсант Харківського національного університету Повітряних Сил імені Івана Кожедуба

### **МЕТОДИ ПОБУДОВИ АНТЕННО-ФІДЕРНИХ СИСТЕМ В МЕРЕЖАХ ПОВІТРЯНОГО УКХ РАДІОЗВ'ЯЗКУ ДЛЯ БОРОТЬБИ З НАПРАВЛЕНИМИ ЗАВАДАМИ**

Досвід ведення бойових дій при проведенні АТО та ООС свідчить про застосування супротивником засобів РЕБ у всіх ланках управління військами, при чому особливої актуальності набувають питання забезпечення якісного зв'язку в мережах повітряного УКХ радіозв'язку при створенні супротивником складної заводової обстановки. Відмінною рисою таких мереж є те, що для забезпечення управління літальними апаратами (ЛА), які виконують завдання у повітрі, радіостанції УКХ зв'язку являють собою єдиний засіб зв'язку, який повинен забезпечувати стійкий інформаційний обмін при застосуванні супротивником засобів РЕП.

Аналіз існуючих антенно-фідерних систем (АФС) радіостанцій УКХ радіозв'язку показує, що їхні характеристики не відповідають сучасним вимогам, які пред'являються АФС військового призначення та постає необхідність побудови антен, які повинні мати додаткові, більш жорсткіші вимоги до розвід захищеності та формуванню направлених діаграм спрямованості з одного боку, та залишатися простими, надійними та зручними для розгортання з іншого.

Розроблено пропозиції щодо модернізації АФС для радіостанцій Р-845М та ІСОМ із застосуванням нових конструктивних рішень, які дозволяють забезпечувати кращу якість зв'язку у складній заводовій обстановці за рахунок формування направлених діаграм спрямованості. Результати розрахунків підтверджені проведенням моделювання АФС за допомогою програми MMANA.

На основі принципів та методів побудови сучасних антенних систем запропоновано АФС радіостанції Р-845М з використанням секторних елементів антени та діаграмо утворюючої схеми, яка здійснює формування управляючих команд на ці елементи з метою зміни їх діаграм спрямованості.

Застосування запропонованих АФС в системі повітряного УКХ радіозв'язку надасть можливість забезпечувати управління ЛА, які виконують завдання в районах ведення бойових дій, в зоні проведення ООС з більшою стійкістю та розвідзахищеністю.

#### **УДК 629.735**

**Чечуй О.В.**, доцент кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент

**Комін Д.С.**, старший викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук

**Панхохін О.С.**, курсант Харківського національного університету Повітряних Сил імені Івана Кожедуба

**Павловський В.А.**, курсант Харківського національного університету Повітряних Сил імені Івана Кожедуба

### **ФОРМАЛІЗОВАНА МОДЕЛЬ ОЦІНКИ ГАРАНТІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ**

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 розглядається 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 355/359. 002:004**

**Троценко О.Я.**, старший науковий співробітник Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного  
**Пашковський В.В.**, начальник науково-дослідного відділу Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного, кандидат технічних наук, старший науковий співробітник, підполковник

**ТЕНДЕНЦІЇ УДОСКОНАЛЕННЯ ПРОЦЕСУ УПРАВЛІННЯ ВІЙСЬКАМИ (СИЛАМИ) З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ**

В сучасних умовах успіх бойових дій залежить не тільки від бойових спроможностей військ (сил) але і в якості управління ними. Досвід воєнних конфліктів показує, що надійне управління завжди було одним з основних чинників досягнення перемоги в бою. Чим складніше ставала структура і технічне оснащення військ, умови, форми і способи ведення бойових дій, тим вищі вимоги пред'являлися до систем військового управління.

Домогтися вирішення головної проблеми управління військами – забезпечення повного використання потенційних можливостей, управління військами (силами) і засобами в інтересах успішного і своєчасного виконання поставлених перед ними завдань неможливо без впровадження в роботу органів управління нових інформаційних технологій.

Вирішення цієї проблеми слід шукати в: упорядкуванні потоку інформації; вироблення нових підходів до прийняття рішення і планування операції (бою); систематизації методик розробки і впровадження оперативно-тактичних розрахунків; застосування засобів механізації та автоматизації при розробці бойових документів; переході до цифрових інформаційних технологій; розробці математичних моделей рекомендаційного і прогностичного характеру; створення бібліотек даних з автоматизованого управління військами з можливістю коригування планів бойового застосування військ; розробці можливостей забезпечення автоматизованого контролю за виконанням прийнятих рішень (розроблених планів) з наданням порівняльних результатів реальних дій військ (сил) з очікуваними; забезпеченні здійснення автоматизованого контролю за збором даних обстановки з наданням попередження про інформацію, яка не надійшла до встановленого часу; підвищення рівня автоматизації (за рахунок використання досягнень в створенні штучного інтелекту) з вироблення рекомендацій на раціональне застосування сил і засобів при різних варіантах дій противника, моделюванні бойових дій, розробці планів бойового застосування військ, доведення до них бойових завдань в автоматизованому режимі.

Саме вирішення вищезазначених проблемних питань сприятиме забезпеченню високої ефективності управління військами і зброєю, і дасть змогу домогтися переваги в управлінні перед потенційним противником.

**УДК 355/359].07**

**Троценко О. Я.**, старший науковий співробітник Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного  
**Кізло Л. М.**, науковий співробітник Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

**ОСОБЛИВОСТІ ОПТИМІЗАЦІЇ ПРОЦЕСУ УПРАВЛІННЯ ВІЙСЬКАМИ**

Сучасний розвиток засобів збройної боротьби загострює низку проблемних питань з організації діяльності органів управління щодо керівництва військами, які обумовлені не лише

удосконаленням озброєння і військової техніки, а й зміною вимог до якості підготовки військовослужбовців, з врахуванням їх сумісності зі стандартами збройних сил країн-членів НАТО і ЄС.

По-перше, вирішального значення набуває фактор часу, який визначається швидкістю сучасної зброї, зростанням мобільності військ, їх здатності в стислі терміни готуватися до бою, швидко здійснювати маневр, раптово завдавати удари.

По-друге, постійно збільшується обсяг управлінських робіт, пов'язаних з появою нових способів управління військами. До їх числа можна віднести, планування і підготовку застосування високоточної зброї у військових частинах (підрозділах), оснащених високо маневреними засобами пересування; планування захисту військ, оперативного та тактичного маскування; боротьби з незаконними збройними формуваннями; новими видами забезпечення та інше. До того ж збільшилася і кількість і якість необхідної інформації в ході управління військами, що обумовлено великим просторовим розмахом бойових дій, різноманітністю застосування бойових засобів, збільшенням кількості об'єктів управління, різкими змінами обстановки.

По-третє, зростають вимоги щодо достовірності відомостей (оперативної інформації) і швидкості прийняття рішень, а також відповідності їх повноти і актуальності, що ґрунтуються не тільки на інтуїції і досвіді командира, але, перш за все, на чітких розрахунках, об'єктивних кількісно-якісних оцінках можливостей сторін і оперативного прогнозування.

Виходячи з цього, можна з повною впевненістю стверджувати, що основні зусилля для оптимізації процесу управління військами доцільно спрямовувати на підвищення оперативності управління; покращення розрахункового обґрунтування прийнятих рішень в процесі планування бойових дій; забезпечення прихованості потоку інформації і безперервного контролю за ходом виконання бойових завдань.

#### **УДК 623.55.02**

**Іохов О.Ю.**, начальник кафедри Національної академії Національної гвардії України, доктор технічних наук, доцент, старший науковий співробітник

**Ткаченко К.М.**, ад'юнкт Національної академії Національної гвардії України, кандидат технічних наук, доцент

**Малюк В.Г.**, професор кафедри Національної академії Національної гвардії України, кандидат технічних наук, доцент

### **ВИЗНАЧЕННЯ ЗОН РОЗТАШУВАННЯ ЗАСОБІВ АКТИВНОГО РАДІОМАСКУВАННЯ В УМОВАХ ЗАСТОСУВАННЯ ПРОТИВНИКОМ ЗАСОБІВ РАДІОРОЗВІДКИ ДЛЯ ЗАХИСТУ СИСТЕМИ РАДІОЗВ'ЯЗКУ ПІД ЧАС ВИКОНАННЯ ЗАВДАНЬ ЗА ПРИЗНАЧЕННЯМ ПІДРОЗДІЛАМИ НГУ**

Особливості ведення сучасних воєнних конфліктів призводять до ускладнення задач зв'язку щодо забезпечення безперервного управління частинами (підрозділами), що посилює вимоги до зв'язку в умовах застосування противником засобів радіорозвідки.

Аналіз існуючих методів захисту системи радіозв'язку показав, що одним із шляхів вирішення завдання забезпечення розвідуваності є проведення комплексу організаційних і технічних заходів радіомаскування, серед яких застосування засобів активного радіомаскування відіграє досить важливу роль.

Адаптація до змін умов оперативної обстановки потребує вирішення низки завдань, зокрема: визначення точок розміщення засобів радіорозвідки противника та маршруту їх руху, оптимізації розташування засобів активного радіомаскування, розрахунку їх мінімальної потужності, необхідної для забезпечення маскування корисних сигналів власних засобів

радіозв'язку в усіх точках можливої траєкторії руху засобів розвідки. При цьому істотно важливим є той факт, що під час проведення заходів радіомаскування, мають виконуватись умови електромагнітної сумісності між власними радіозасобами.

В дисертаційній роботі запропоновано метод, який дозволяє обґрунтувати порядок розміщення засобів радіомаскування на місцевості та просторового орієнтування їх антен, враховуючи, при цьому, збереження працездатності системи радіозв'язку при проведенні заходів пасивного та застосуванні засобів активного радіомаскування.

#### **УДК 355.3:654.623.61**

**Кізло Л.М.**, науковий співробітник Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

**Ніколасва Л.Я.**, молодший науковий співробітник Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

### **ОСОБЛИВОСТІ ПІДГОТОВКИ ФАХІВЦІВ ДЛЯ ВІЙСЬК ЗВ'ЯЗКУ В УКРАЇНІ**

Сьогодні для армії будь-якої країни світу військовий зв'язок важливий як ніколи. Це технічна основа роботи військових, яка забезпечує зв'язок і управління військами, а воїни-зв'язківці входять до складу всіх родів військ і працюють над створенням надійної єдиної системи управління Збройними Силами (ЗС) як в умовах війни, так і в мирний час. Під час Другої світової війни практично десята частина солдатів була зв'язківцями. Питома вага представників цієї професії в загальному штаті армії стрімко зростає і зараз. В сучасній армії зв'язківців вже близько 12%, наразі їхня робота одна з найбільш затребуваних та важливих в районі проведення бойових дій на сході України.

В ЗС України ведеться робота щодо удосконалення не лише технічних складових зв'язку і кібербезпеки у напрямку збільшення можливостей і впровадження сучасних засобів зв'язку, модернізації існуючих апаратних та інших засобів зв'язку та розроблення і застосування нових зразків та програмного забезпечення, а також, суттєво оптимізується процес підготовки персоналу для обслуговування новітньої апаратури і засобів зв'язку ЗС, бо застосування сучасних технологій на війні вимагає належної кваліфікації персоналу. Зокрема, для підготовки фахівців у ЗС запроваджено: Курси академії Cisco з мережевих технологій; Курси підготовки спеціалістів з експлуатації засобів зв'язку виробництва компаній Harris і Aselsan. Для оптимізації цього процесу, з метою удосконалення здатності виконувати професійні завдання за призначенням в будь-яких умовах обстановки, докорінно оновлені програми підготовки сучасних фахівців-зв'язківців, які спрямовані на поглиблене вивчення різних способів (мов) програмування, з врахуванням особливостей застосування в роботі найсучасніших засобів зв'язку та телекомунікаційного обладнання, досвіду, набутого під час проведення бойових дій в районі ООС та передових технологій і засобів телекомунікації провідних країн світу.

Найкращі армії світу – професійні, ефективні, добре оснащені формування, що вирізняються високотехнологічним зв'язком та автоматизованим управлінням усіх підрозділів, а також надійною системою захисту від кіберзагроз. Саме тому підготовка висококваліфікованих кадрів в Збройних Силах є пріоритетом – це головне завдання, що стоїть перед військами зв'язку і від реалізації якого залежить підвищення обороноздатності держави.



**УДК 355.3:654**

**Кізло Л.М.**, науковий співробітник Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

**Троценко О.Я.**, старший науковий співробітник Наукового центру Сухопутних військ Національної академії сухопутних військ імені гетьмана Петра Сагайдачного

**СУЧАСНІ ТЕНДЕНЦІ РОЗВИТКУ ВІЙСЬК ЗВ'ЯЗКУ В УКРАЇНІ**

У Збройних Силах (ЗС) України зв'язок – високотехнологічна основа системи управління військами (СУВ), без належної організації якої неможливо забезпечити якісну перевагу над ворогом.

Процес становлення СУВ в ЗС України відбувався за активної участі професіоналів-зв'язківців з розрізних систем зв'язку військових округів, Чорноморського флоту, повітряних, протиповітряних сил та ракетних військ і артилерії, які залишилися в Україні після розпаду СРСР та видався непростим. Проте найскладніший, але і найефективніший етап цього шляху пройдено тоді, коли Україна зіштовхнулася з російською агресією. В умовах обмеженості ресурсів і безперервної бойової роботи, долаючи об'єктивні труднощі, вдалося сформувати абсолютно нову, збудовану на сучасних цифрових рішеннях єдину систему зв'язку ЗС України, здатну виконувати поставлені завдання на противагу діям, оснащеного сучасними засобами радіорозвідки і РЕБ, противника.

На теперішній час війська зв'язку повністю позбавилися від радянського спадку не лише у питаннях технічного оснащення, а й на рівні ухвалення управлінських рішень та структури в цілому. Також потрібно відзначити, що вагомий внесок у оснащення військ сучасними захищеними засобами зв'язку зробили наші партнери – країни НАТО. На сьогодні підрозділи, що виконують бойові завдання в районі проведення ООС, забезпечуються сучасною цифровою технікою зв'язку, високотехнологічними засобами і програмним забезпеченням до нього, а з боку Міноборони та Головнокомандувача ЗСУ є повне розуміння і сприяння у вирішенні питань забезпечення військ зв'язку необхідними ресурсами, проте безпекова ситуація навколо нашої держави потребує пришвидшення цього процесу.

Отже завдання, які стоять перед військами зв'язку сьогодні відповідальні та складні і вимагають від особового складу професіоналізму, організованості та дисципліни, що стане надійним гарантом миру, стабільності та зміцнення обороноздатності України.

**УДК 621.391**

**Дудко М.В.**, науковий співробітник Наукового центру Повітряних Сил Харківського національного університету Повітряних Сил ім. Івана Кожедуба

**Тимочко О.І.**, професор кафедри Харківського національного університету Повітряних Сил ім. Івана Кожедуба, доктор технічних наук, професор

**Павленко М.В.**, начальник кафедри Харківського національного університету Повітряних Сил ім. Івана Кожедуба, доктор технічних наук, професор

**ОСОБЛИВОСТІ ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ ПРИ ПОБУДОВІ СИСТЕМ УПРАВЛІННЯ БПЛА**

Аналіз збройних конфліктів останніх десятиріч свідчить про те, що перед системами розвідки постають все більш складні та багатогранні завдання, пред'являються жорсткі вимоги та набуває розвитку тенденція широкого впровадження безпілотної техніки. Повітряна розвідка є одним із видів військової розвідки та найважливішою умовою успіху бойових дій авіації. Вона

ведеться частинами розвідувальної авіації, розвідувальними підрозділами авіаційних з'єднань, екіпажами, що виконують бойові завдання, безпілотними літальними апаратами з метою одержання даних про противника (об'єкти, сили і засоби, місцевість) необхідних для своєчасного забезпечення командування і штабів повними і достовірними даними, успішного ведення воєнних дій всіма видами Збройних сил.

Основні зусилля розвідки зосереджують на головному напрямку для виконання найважливіших завдань, на своєчасному виявленні засобів масового ураження, високоточної зброї противника, його головного угруповання, виявленні бойових (похідних) порядків, артилерії, мінометів, резервів і пунктів управління. Знати замисел противника, розташування його засобів ураження й угруповання, відповідно реагувати – значить досягти успіху в бою. Особа, що приймає рішення, (ОПР) не здатна прийняти правильне рішення або ефективно застосувати вогневі засоби, якщо вона не організує безперервну активну і цілеспрямовану розвідку й не отримує достовірні відомості про противника.

Таким чином, висока вразливість БПЛА від різних факторів бойової обстановки, низька "інтелектуальність" в автономному режимі через відсутність таких незамінних людських якостей, як оперативне ухвалення рішення, можливість перенесення основних зусиль на нові, більш важливі об'єкти, вміння ухилятися від небезпеки і оперативно застосувати заходи щодо ведення в оману противника, є сьогодні нерозв'язними проблемами, що знижують ефективність бойового застосування сучасних БПЛА та потребують врахування вищеперерахованих факторів на етапі планування повітряної розвідки.

#### **УДК 621.391**

**Женжера С.В.**, старший викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук

**Мироненко О.С.**, курсант Харківського національного університету Повітряних Сил імені Івана Кожедуба

### **ШЛЯХИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ D2D (device-to-device) СТАНДАРТУ 5G ПРИ ОРГАНІЗАЦІЇ ВИСОКОШВИДКІСНИХ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ В ПІДРОЗДІЛАХ ТА ЧАСТИНАХ ЗБРОЙНИХ СИЛ УКРАЇНИ**

В Збройних Силах України (у тому числі у зоні ведення бойових дій) можливо та доцільно запровадити розгортання мереж 5G для забезпечення безпроводової роботи різноманітних пристроїв, а саме: різноманітних датчиків, пристроїв цифрового телефонного та відеозв'язку, системи відеоспостереження, засобів об'єктивного контролю, засобів високошвидкісної передачі даних, систем та засобів управління боєм, систем управління БПЛА та передачі розвідувальної фото та відеоінформації оператору БПЛА, систем та засобів дистанційного управління зброєю.

У Повітряних Силах найбільш ефективним є використання мереж 5G при перебазуванні на новий чи польовий аеродром коли час розгортання такої мережі буде значно меншим у порівнянні з стандартними способами забезпечення передачі інформації у зоні аеродрому, що дозволить швидше організувати польоти авіації.

На теперішній час можливо використовувати дискретні 5G-модулі, вартість яких менше у 2...3 рази у порівнянні з мобільними телефонами. Такі модулі задовольняють необхідним вимогам. У роботі були обґрунтовані схеми застосування технологій мереж 5G:

- у Сухопутних військах біля лінії розмежування та запропоновано використання у якості резерву для оптоволоконної лінії – ЦРПЛ;

- у Повітряних Силах в зоні розташування авіаційної бригади, де запропоновано використання трьох базових станцій, що забезпечить суцільне покриття.

При заданих вихідних даних було розраховано зону покриття однієї базової станції, радіус якої складає 3374 м, що задовольняє вимогам при організації мережі 5G на аеродромі. Три такі станції дають змогу забезпечити високошвидкісним доступом до мережі 5G всіх об'єктів аеродрому.

Проаналізувавши частоти, відстані до об'єктів і провівши розрахунки, було розраховано мінімальну швидкість передачі даних (196,49 Мбіт/с) в зонах покриття базових станцій на аеродромі, що задовольняє необхідним вимогам та забезпечить передачу даних та відеоінформації високої якості.

Результати роботи можуть бути використанні при модернізації існуючих і створення новітніх мереж зв'язку і передачі даних, як у Сухопутних військах так і у Повітряних Силах.

#### **УДК 355.421**

**Заболотнюк В.І.**, заступник начальника з наукової роботи Наукового центру Сухопутних військ Національної академії Сухопутних військ, кандидат історичних наук

**Мокоївець В.І.**, провідний науковий співробітник Наукового центру Сухопутних військ Національної академії Сухопутних військ, працівник ЗСУ

**Федоров О.Ю.**, провідний науковий співробітник Наукового центру Сухопутних військ Національної академії Сухопутних військ, працівник ЗСУ

### **ОСНОВНІ ВЛАСТИВОСТІ ЄДИНОЇ АВТОМАТИЗОВАНОЇ СИСТЕМИ УПРАВЛІННЯ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ**

У XXI столітті людство не перестає вирішувати нагальні проблеми і протиріччя шляхом використання сили і застосування воєнних засобів боротьби. У світі не припиняються війни, міжнаціональні збройні конфлікти і внутрішньодержавні сутички. Держави змушені витратити величезні ресурси на утримання військових структур та сил, призначених для підтримання громадського порядку. Це примушує політичне і військове керівництво провідних країн світу шукати інші шляхи підвищення ефективності застосування своїх силових структур. Одним з таких шляхів став напрямок інтенсифікації процесів управління.

Матеріальною основою збору, узагальнення і аналізу інформації, проведення оперативних розрахунків, моделювання способів дій, контролю стану підрозділів та обміну інформацією стали засоби автоматизації управління. В сучасних арміях світу такі засоби об'єднані в автоматизовані комплекси управління силовими структурами.

Не залишається осторонь від процесу автоматизації управлінської діяльності і Україна. Поряд із модернізацією та удосконаленням інформаційних систем, які вже розроблені і експлуатуються в органах управління і підрозділах силових структур України, в державі запроваджена цільова програма створення єдиної автоматизованої системи управління сектору безпеки і оборони України. Обрана стратегія створення такої загальнодержавної системи не відрізняється від загальносвітових тенденцій. Суть її полягає у поєднанні сукупності управлінських процесів на основі єдиного комплексу матеріальних засобів і програмних продуктів, що узгоджено керують функціями суб'єкту управління.

На жаль, під час реалізації стратегічно правильного напряму удосконалення процесу управління військами (силами) за допомогою впровадження засобів автоматизації, представники різних компонентів сектору безпеки і оборони України не завжди дотримуються єдиних підходів до загальних вимог щодо створення і функціонування такої єдиної автоматизованої системи. Не рідко обирається хибний шлях створення розрізнених, не пов'язаних єдиним логічним принципом та автономно функціонуючих засобів, що призводить до відхилення від принципу єдності виконання управлінських функцій.

Роботу щодо розробки і створення єдиної автоматизованої системи управління сектору безпеки і оборони України необхідно здійснювати системно і комплексно за єдиною програмою

та під загальним керівництвом після визначення єдиних для всіх елементів вимог і загальних критеріїв оцінки ефективності кінцевого продукту, який повинен відповідати визначеним вимогам і володіти певними властивостями. До основних властивостей автоматизованої системи управління можуть відноситися: бойова готовність, ємність, пропускна спроможність, оперативність, якість рішення завдань управління, завадостійкість, живучість, мобільність, ефективність.

Сукупність перелічених властивостей, реалізованих у відповідних елементах єдиної автоматизованої системи управління забезпечить ефективне функціонування всієї системи управління силами сектору безпеки і оборони України та підвищить результативність дій і якість виконання завдань кожним із його компонентів.

#### **УДК 623.618:519.686**

**Яценко В.Ж.**, заступник начальника кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук, доцент

**Бекіров А.Е.**, старший викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук

**Корепанов В.В.**, викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба

### **ЗАВАДОСТІЙКЕ КОДУВАННЯ МОВНОГО ПОВІДОМЛЕННЯ З ДОДАТКОВИМ ВБУДОВУВАННЯМ ДАНИХ**

Функціонування засобів обміну інформації для структур сектору безпеки пов'язано з ризиками, які обумовлені високою значимістю інформації. Одночасно з авторизованими користувачами у інформаційному просторі присутні зловмисники, ціллю яких є доступ до синтаксичної та семантичної складової інформаційних повідомлень. Сьогодні сучасні засоби зв'язку, якими оснащені підрозділи Збройних Сил України та Національної гвардії України, мають захищені канали передачі інформації.

Для цифрових засобів передачі інформації широко застосовуються криптографічні алгоритми, в яких для авторизації використовується ключова інформація. Для аналогових засобів передачі інформації можливо застосування вокодерів, заснованих на перемішуванні складових мовного повідомлення у просторовому або спектральному представленні.

В той же час для авіаційних бортових засобів зв'язку та передачі інформації характерним є обмін повідомленнями у аналоговому вигляді: для передачі мовного повідомлення застосовується амплітудна або частотна модуляція, для передачі формалізованих команд та кодових слів – частотна телеграфія. При цьому фактично відсутня можливість одночасно забезпечити обмін мовними повідомленнями і передачу інформації. Процес прямого та зворотнього криптографічного перетворення при цьому передбачає проведення аналого-цифрового перетворення і як результат значно впливає на оперативність та якість зв'язку.

Сучасні тенденції ведення збройного протистояння передбачають наявність систем інформаційної підтримки сил та військ у режимі реального часу. Для авіаційного компоненту інформаційна підтримка передбачає надання інформації про навігаційні координати та параметри, інформацію про ціль та бойові вказівки, інформацію про засоби протиповітряної оборони в зоні операції, обмін інформаційними повідомленнями, інформацію про погодні умови в районі проведення операції.

Застосування сучасних зразків бортового обладнання передачі інформації на повітряних судна Збройних Сил України ускладнюється організаційно-нормативними заходами. Також важливою є економічна складова. Звідси, важливими є дослідження, які сфокусовані на модернізації та використанні існуючих зразків обладнання для передачі інформації.

Аналіз існуючих методів вбудовування інформації в мовні повідомлення засновані на опосередкованій модифікації компонент частотного спектру складових мовного повідомлення. У таких методах застосовується зміна значень параметрів повідомлення у відповідності до інформації, яка вбудовується. Серед обмежень таких методів є внесення спотворень в вихідне повідомлення і необхідність значних обчислювальних потужностей. Також недоліком є відсутність можливості застосування завадостійкого кодування і, як наслідок, значні спотворення мовного повідомлення і вбудованої інформації.

Пропонується метод вбудовування двійкової інформації в елементи повного повідомлення після аналого-цифрового перетворення і кодування Хеммінга. На етапі аналого-цифрового перетворення значення амплітуди фрагменту мовного повідомлення перетворюється в площину миттєвих значень амплітуди з частотою дискретизації значень, що задовольняє критерій Найквіста-Шенона.

Наступне перетворення площини миттєвих значень передбачає представлення їх у двійковому вигляді у синтаксичній формі, що задовольняє забезпечити взаємооднозначність прямого та зворотного перетворень. Тут, враховуючі різний рівень миттєвих значень амплітуди, для забезпечення однакової кількості біт для представлення кожна складова у двійковому вигляді доповнюється нульовими бітами на позиції старших бітів двійкового представлення. Це не змінює абсолютного значення складової, але дозволяє сформувавши бітову площину для наступної обробки.

Наступна обробка передбачає формування кодових слів для кодування Хеммінга. Кодові слова формується по рядках від старших бітів складових до молодших бітів. Кодування Хеммінга передбачає додавання до кодової послідовності перевірочних елементів, звідси кінцева послідовність для вбудовування буде мати більшу кількість біт у порівнянні з вихідною.

Наступний етап включає вибір позиції бітів кодового слова у які буде здійснюватись вбудовування даних. Правило вибору бітів уявляє собою ключову інформацію і повинна бути відома на приймальній та передавальній стороні. В умовах неавторизованого доступу інформація про наявність вбудовування та позиції вбудованих бітів відсутня.

Після вбудовування біт додаткової інформації здійснюється композиція кодових слів у вихідну форму, цифро-аналогове перетворення з наступною передачею фрагментів до каналу передачі.

Метод декодування та вилучення відбувається у зворотній послідовності і включає наступні етапи:

- декомпозицію отриманого мовного повідомлення;
- здійснення аналого-цифрового перетворення фрагментів мовного повідомлення із заданим значенням частоти дискретизації;
- формування кодових слів для вилучення інформації;
- визначення позиції вбудованих бітів на основі ключового правила;
- вилучення бітів вбудованого інформаційного повідомлення;
- зворотне кодування Хеммінга та відновлення мовного повідомлення.

В умовах неавторизованого доступу у противника відсутня інформація про наявність та правило вбудовування даних. При здійсненні зворотного перетворення Хеммінга, вбудовані біти будуть сприйматись алгоритмом як помилки, які виникли в процесі обробки та передачі інформації та будуть знищені шляхом виправлення.

Оцінка ефективності розробленого методу скритої передачі інформації здійснювалось на основі розрахунку кількості бітів, які можуть бути вбудовані в мовне повідомлення. Так для мовного повідомлення довжиною 1 секунда, при визначеній частоті дискретизації 22,5 кГц кількість вбудованої інформації дорівнює 22501 біт.

**УДК 629.052.3**

**Красноручий А.О.**, доцент кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба, кандидат технічних наук

**Дігтярь М.М.**, старший викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба

**Казьміров І.В.**, викладач кафедри Харківського національного університету Повітряних Сил імені Івана Кожедуба

**Троян В.С.**, курсант Харківського національного університету Повітряних Сил імені Івана Кожедуба

### **РОЗРОБКА ПРОГРАМНОЇ МОДЕЛІ ФОРМУВАННЯ І ПРИЙОМУ СИГНАЛІВ З ПСЕВДОВИПАДКОВОЮ ПЕРЕБУДОВОЮ РОБОЧОЇ ЧАСТОТИ**

Системи радіозв'язку, що використовують для передачі інформації метод псевдовипадкової перебудови робочої частоти (ППРЧ), відносяться до систем радіозв'язку з розширеним спектром. Системи подібного плану володіють не тільки підвищеною складністю у виявленні, а й в перехопленні. Такі позитивні риси системи радіозв'язку з розширеним спектром обумовлюються тим, що щільність корисного сигналу розподіляється на велику смугу частот псевдовипадковими послідовностями, використовуваними для розширення спектра, відомими тільки на приймальній і передавальній сторонах.

Згодом ситуація змінилася і системи радіозв'язку з розширеним спектром стали доступні не тільки військовим структурам, а й сфері цивільного зв'язку. Наприклад, практично всім відомий спосіб передачі інформації через Bluetooth використовує метод псевдовипадкової перебудови робочої частоти з частотою перебудови рівної 1600 стрибків в секунду і дворівневої частотної маніпуляцією. Wi-Fi, без якого вже не можна уявити жоден сучасний смартфон, використовує розширення спектра методом прямої послідовності (стандарти 802.11 і 802.11b). Метод прямої послідовності теж розширює спектр сигналу і має схожі характеристики з методом псевдовипадкової перебудови робочої частоти.

Проте, не дивлячись на те, що системи з розширеним спектром щільно увійшли в наше життя, у відкритому доступі відсутні не тільки готові системи радіозв'язку, що використовують розширення спектра методом псевдовипадкової перебудови робочої частоти або прямої послідовності, для передачі інформації на коротких хвилях, а й їх моделі. Тому розробка програмної моделі формування та прийому сигналів з псевдовипадковою перебудовою робочої частоти є першим кроком на шляху до побудови повноцінної системи радіозв'язку, здатної вести передачу і прийом інформації через реальний канал зв'язку.

В ході досліджень було розроблено програмну модель формування та прийому сигналів з псевдовипадковою перебудовою робочої частоти. Програмна модель реалізована високорівневою мовою програмування з використанням інтерактивного середовища для програмування, чисельних розрахунків і візуалізації результатів – MATLAB. Отримана ширина смуги сформованого широкосмугового сигналу становить більше 384 кГц, щоб не виходити за сумарну смугу, що формується 8 знижувальними перетворювачами частоти (digital down converters (DDC)). Кожен DDC виділяє смугу рівну 48 кГц, використовувану в реальному приймально-передавальному устаткуванні короткохвильового радіозв'язку. В ході дослідження було виконано:

- аналіз процесу розширення спектра і його структури;
- порівняння процесів розширення спектра сигналу псевдовипадковою перебудовою робочої частоти і прямою послідовністю;
- вибір структурної схеми для реалізації моделі і проаналізовано процес її роботи;
- складено блок-схеми формування та прийому ППРЧ сигналу;
- реалізовано модель формування та прийому ППРЧ сигналу;
- проведено оцінку реалізованої моделі за допомогою графіка bit error rate (BER).

## ЗМІСТ

<b>Власов К.В., Фик О.І.</b> Основні терміни та принципи зв'язку та інформаційних систем на сучасному етапі за стандартами НАТО.	3
<b>Горєлишев С.А., Волков П.Ю., Баулін Д.С.</b> Геометричні та енергетичні характеристики системи спостереження у бістатичній радіолокації при зовнішньому підсвічуванні.	4
<b>Воронін О.І., Сальніков О.М.</b> Варіанти застосування цифрових радіорелейних станцій Р-425С3 у системі зв'язку та інформатизації НГУ.	6
<b>Новикова О.О., Глущенко М.О.</b> Спеціальна підготовка особового складу із технічного забезпечення.	7
<b>Женжера С.В., Бровко А.А.</b> Шляхи збільшення надійності охорони військових об'єктів при протидії тактичним БПЛА шляхом застосування засобів РЕП.	8
<b>Казіміров О.О., Малюк В.Г., Потіхенський А.І.</b> Сучасне телекомунікаційне обладнання, що застосовується підрозділами зв'язку національної гвардії України.	9
<b>Василишин В.І., Коваль О.В.</b> Аналіз ефективності подавлення шуму в мовних сигналах методом спектрального віднімання.	10
<b>Костенко І.Л., Блащук С.М., Поздняк В.П.</b> Пропозиції щодо автоматизованого розрахунку радіолінії при зв'язку земною хвилею для визначення граничної дальності забезпечення радіозв'язку.	11
<b>Шмаков В.В., Красноручський А.О., Олексін О.О., Федоровський О.В.</b> Тенденції розвитку та існуючі можливості авіаційного радіозв'язку вертольотів силових структур.	12
<b>Таршин В.А., Танцюра О.Б., Куравський М.В.</b> Підвищення імовірності виявлення та розпізнавання об'єктів на зображеннях різноспектральних оптико-електронних систем розвідки.	13
<b>Лазарев В.Д., Козлов В. Є.</b> Підвищення гнучкості та оперативності управління частинами НГУ за допомогою інтеркомунікаційної системи Інтерком RF-7800і виробництва компанії HARRIS.	14
<b>Люттов В.В., Дзюба І.В., Колесник С.В.</b> Аналіз ефективності засобів радіозв'язку військового призначення при використанні МІМО технології в засобах та комплексах радіозв'язку УКХ діапазону у складній завадовій обстановці.	15
<b>Майборода І.М., Оленченко В.Т.</b> Аналіз системи технічного обслуговування цифрових засобів зв'язку «HARRIS».	16
<b>Нещерет І.Г., Штонда Р.М.</b> Пропозиції щодо блокування вірусу шифрувальника в інформаційно-телекомунікаційних системах.	17
<b>Онипченко П.М. Невзоров Р.В., Ушань В.М.</b> Управління безпілотними літальними апаратами при їх застосуванні у складі групи.	19
<b>Флорін О.П., Сальніков О.М.</b> Можливості застосування систем бортових вимірювань для проведення випробувань безпілотних літальних апаратів.	20
<b>Макаров С.А., Чекунова О.М., Чекунов В.В.</b> Обґрунтування єдиного підходу щодо оцінки завадостійкості системи зв'язку в інтересах управління військами.	21
<b>Штонда Р.М.</b> Завдання та етапи проведення незалежного аудиту інформаційної безпеки військових частин (установ) щодо ефективності забезпечення кібербезпеки.	22
<b>Васюта К.С, Збежховська У.Р., Слободянюк В.В.</b> Метод прихованої передачі інформації в системах з OFDM модуляцією.	24
<b>Рисаков М.Д., Воронов Д.М., Лопатін А.В.</b> Пропозиції щодо принципів побудови ретрансляторів на безпілотному літальному апараті для управління авіацією військових формувань України.	25
<b>Рудковський О.М., Ільницький І.Л.</b> Перспективи розвитку та застосування автоматизованої системи управління військами.	25

<b>Сльчанінов О.Д.</b> Проблема оцінки стану адаптивної інформаційно-вимірjuвальної системи робототехнічного комплексу.	26
<b>Кубрак В.Г.</b> Впровадження сучасних форм і способів організації мереж тактичного зв'язку об'єднаного угруповання військ (сил).	27
<b>Чопенко Д.А.</b> Контроль коректності варіантів рішень по ресурсам та часу у відкритих експертних системах реального часу.	27
<b>Королюк Н. О., Коршець О. А., Першин О. В.</b> Формальне представлення процесів планування маршруту БПЛА.	28
<b>Опалінський В.Б., Давіденко С.В., Бойчук Б.М.</b> Перспективи розвитку новітніх технологій та засобів зв'язку в інтересах управління військами	29
<b>Хижняк І.А.</b> Використання методів ройового інтелекту при керуванні групою безпілотних літальних апаратів.	30
<b>Васюта К.С., Кашишин О.Л.</b> Методи побудови складених хаотичних сигналів для підвищення роздільної здатності.	31
<b>Мельніков І.С., Кулик О.П.</b> Проблемні питання управління польотами літаків виробництва країн-членів НАТО.	32
<b>Литвин А.В., Попович Б.Р.</b> Пропозиції щодо застосування методу зменшення позасмугового випромінення OFDM-сигналів в сучасних цифрових РРС.	32
<b>Литвин А.В., Громова Т.В.</b> Метод підвищення живучості системи наземного УКХ радіозв'язку з урахуванням умов проведення ООС.	33
<b>Оборнєв С.І.</b> Перспективи розвитку та застосування сучасних систем з удосконалення збереження матеріальних запасів при відновленні боєздатності озброєння.	34
<b>Королюк Н.О., Королюк А.О., Романюк А.О.</b> Особливості оцінки ризику інформаційної безпеки інформаційно-телекомунікаційних мереж на основі теорії нечітких множин.	34
<b>Жук О.В., Матала І.В.</b> Особливості класифікації мобільних систем транкінгового зв'язку.	35
<b>Чечуй О.В., Дудко Г.С.</b> Методи побудови антенно-фідерних систем в мережах повітряного укх радіозв'язку для боротьби з направленими завадами.	36
<b>Чечуй О.В., Комін Д.С., Панхохін О.С., Павловський В.А.</b> Формалізована модель оцінки гарантій інформаційної безпеки комплексної системи захисту інформації.	36
<b>Троценко О.Я., Пашковський В.В.</b> Тенденції удосконалення процесу управління військами (силами) з використанням інформаційних технологій.	37
<b>Троценко О. Я., Кізло Л. М.</b> Особливості оптимізації процесу управління військами.	38
<b>Іохов О.Ю., Ткаченко К.М., Малюк В.Г.</b> Визначення зон розташування засобів активного радіомаскування в умовах застосування противником засобів радіорозвідки для захисту системи радіозв'язку під час виконання завдань за призначенням підрозділами НГУ.	39
<b>Кізло Л.М., Ніколаєва Л.Я.</b> Особливості підготовки фахівців для військ зв'язку в Україні.	39
<b>Кізло Л.М., Троценко О.Я.</b> Сучасні тенденції розвитку військ зв'язку в Україні.	40
<b>Дудко М.В., Тимочко О.І., Павленко М.В.</b> Особливості використання інтелектуальних технологій при побудові систем управління БПЛА.	41
<b>Кізло Л.М., Троценко О.Я.,</b> Сучасні тенденції розвитку військ зв'язку в Україні.	40
<b>Женжера С.В., Мироненко О.С.</b> Шляхи використання технологій D2D (device-to-device) стандарту 5G при організації високошвидкісних мереж передачі даних в підрозділах та частинах Збройних сил України.	42



<b>Заболотнюк В.І., Мокоївець В.І., Федоров О.Ю.</b> Основні властивості єдиної автоматизованої системи управління сектору безпеки і оборони.	43
<b>Ященок В.Ж., Бекіров А.Е., Корепанов В.В.</b> Завадостійке кодування мовного повідомлення з додатковим вбудовуванням даних.	44
<b>Красноруцький А.О., Дігтярь М.М., Казьміров І.В., Троян В.С.</b> Розробка програмної моделі формування і прийому сигналів з псевдовипадковою перебудовою робочої частоти.	46

**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*