УДК 621.391

Ю.П. Белокурський[2], О.Ю. Іохов[1], В.Є. Козлов[1], О.О. Щербина[2]

[1] *Національна академія Національної гвардії України, Харків*
[2] *Харківський Національний університет радіоелектроніки, Харків*

ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ РАДІОЕЛЕКТРОННОГО ЗАХИСТУ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ГВАРДІЇ УКРАЇНИ ПІД ЧАС ВИКОНАННЯ ЗАВДАНЬ ЗА ПРИЗНАЧЕННЯМ

Проаналізована термінологія в галузі радіоелектронної боротьби і відмінності підходів до її ведення в збройних силах та силах охорони правопорядку, зокрема, Національній гвардії України. Застосування методу морфологічного аналізу дозволило запропонувати склад системи радіоелектронного захисту. На основі результатів моделювання різних типів антен зроблено висновок про доцільність використання конструкції кутової антени як базового елемента та антен інших розглянутих в статті типів в комплексі зі штатними засобами військового призначення та пристроями Hi-Tech для побудови системи захисту радіозв'язку підрозділу Національної гвардії України при виконанні завдань за призначенням.

Ключові слова: *радіоелектронний захист, Hi-Tech-технології.*

Вступ

Постановка проблеми та аналіз публікацій. Датський філософ С. К'єркегор (1813–1955) сформулював афоризм: "Визначиться із поняттями і ви позбавите людство від половини його помилок (рос. заблуждений)". Тому спочатку визначимося з дефініціями.

Керівні документи Армії США [1–2] визначають радіоелектронну війну (РЕВ) як дії військ (сил) з використання електромагнітної енергії і засобів спрямованої енергії з метою здійснення управління (контролю) випромінюваннями електромагнітного спектру частот (у тому числі й використання самого спектру частот) або дії (атаки) на особовий склад, радіоелектронні системи і засоби, об'єкти, озброєння та військову техніку противника. Радіоелектронна війна включає три основних взаємозв'язаних і взаємодоповнюючих один одного елементи: радіоелектронну атаку, радіоелектронний захист і забезпечення ведення РЕВ. Радіоелектронний захист як один з елементів РЕВ одним із напрямків передбачає підсилення захисних якостей об'єктів (цілей), зокрема, створення спеціальних схем, екранів, сховищ, технічних засобів захисту (у першу чергу мова йде про фізичні та технічні засоби захисту від дії електромагнітних випромінювань радіоелектронних засобів (РЕЗ) своїх військ або військ противника). Для забезпечення ведення РЕВ визначені склад сил і засобів – органи управління, розвідки, тилового та технічного забезпечення, – а також напрямки оперативної та бойової підготовки. Підкреслюється [2], що РЕВ є одним з елементів інформаційних операцій.

У Збройних силах України під терміном радіоелектронна боротьба (РЕБ) розуміють [3] сукупність узгоджених за метою, завданнями, місцем і часом одночасних і послідовних дій з радіоелектронного подавлення систем управління військами та зброєю противника і заходів щодо радіоелектронного захисту РЕЗ своїх систем управління, які спрямовані на забезпечення переваги у використанні електромагнітного спектру. Радіоелектронне подавлення (РЕП) розглядають як сукупність узгоджених за метою, завданнями, місцем і часом радіоелектронних впливів на радіоелектронні системи і засоби управління військами та зброєю, які здійснюються силами та засобами РЕБ за єдиним замислом і планом відповідно з радіоелектронною обстановкою, що склалася. У свою чергу, радіоелектронний захист (РЕЗах) – це комплекс організаційно-технічних заходів і дій, спрямованих на забезпечення стійкої роботи своїх систем управління військами і зброєю з метою забезпечення переваги у використанні електромагнітного спектру. Окремо розглядають радіоподавлення як дії щодо порушення роботи радіо-, радіорелейних, тропосферних і супутникових ліній зв'язку, засобів радіолокації і радіонавігації противника шляхом впливу на них електромагнітними випромінюваннями, застосуванням оманних радіолокаційних цілей і пасток, передачі повідомлень, що дезінформують, у радіомережах противника або своїх військ, демонстрації (помилкової) роботи своїх радіоелектронних засобів або імітація роботи РЕЗ противника, а також зміни умов розповсюдження радіохвиль. Для ведення РЕБ залучають спеціальні сили та засоби – батальйони, вузли РЕБ, індивідуальні і групові засоби РЕБ, у тому числі літальних апаратів, пристрої (прилади) радіоелектронного захисту засобів військ.

Аналогічний підхід до тлумачення понять і дій РЕБ прослідкується і в інших джерелах [4].

Загалом, короткий аналіз стану питання радіоелектронного протистояння [5–9] дозволяє зробити

висновок, що радіоелектронна боротьба знаходиться на стику забезпечення інформаційної та воєнної безпеки держави.

В Національній гвардії України, на відміну від Збройних сил, відсутні спеціальні сили та засоби РЕБ, що й обумовлює актуальність та мету статті – розглянути варіант побудови системи радіоелектронного захисту підрозділів Національної гвардії України під час виконання завдань за призначенням.

Виклад основного матеріалу

Широке застосування в житті суспільства знайшли пристрої Hi-Tech: засоби зв'язку, обробки інформації, навігації, Wi-Fi камери, тепловізори, безпілотні літальні апарати (БПЛА) невеликих розмірів і т.д. Ці пристрої є засобами подвійного призначення і породжують масу проблем збройним силам (ЗС) і силам охорони правопорядку (СОП), до яких відноситься Національна гвардія України (НГУ). Пристрої Hi-Tech використовують терористичні угруповання і незаконні збройні формування (НЗФ) [10, 11] для зв'язку і протидії підрозділам сил охорони правопорядку і ЗС. Основними доступними засобами зв'язку Hi-Tech у вільному продажу є: аналогові і цифрові портативні і автомобільні радіостанції діапазонів VHF (146-174 МГц), UHF (400-480 МГц), мобільні телефони GSM і CDMA, супутникові телефони, Wi-Fi, скануючі приймачі, вбудовані пристрої GPS-навігації, зв'язок з віддаленим доступом (Internet Radio).

До засобів Hi-Tech в останні роки додалися радіокеровані моделі БПЛА, зокрема квадрокоптери, з відеокамерами високої роздільної здатності та професіональними функціями. Їх технології удосконалюються, поліпшуються надійність, безпека, керованість та інші характеристики. У цих "іграшок" з'явились такі функції, як "повернення додому", системи FPV з відстеженням "положення голови" (спосіб управління БПЛА за допомогою відеокамери на борту – відео реального часу дозволяє оператору управляти апаратом, який знаходитися поза зором оператора), 3D FPV окуляри, режим огинання перешкод, функція "слідуй за мною" та інші. Навіть при невеликому часі польоту (15-30 хвилин) "іграшка" в руках терориста перетворюється на ефективний засіб розвідки і протидії підрозділам СОП, особливо в міських умовах.

Аналіз дій НЗФ в Лівані показав можливості використання радіоелектронних засобів Hi-Tech в умовах інформаційного протиборства, коли ведуться радіоелектронна розвідка і радіопротидія, застосовуються радіомаскування і захист від спеціальних перешкод [10–14]. Це дозволило визначити доцільність створення просторово-розподілених систем розвідки і перешкод, їх структуру, види і характеристики перешкод, що випромінюються малогабаритними модулями [14].

Виконання завдань за призначенням підрозділами НГУ потребує виконання заходів РЕБ, зокрема, забезпечення захисту інформації в радіоканалах. З точки зору технічної реалізації системи РЕБ і захисту мають вузли однакового функціонального призначення, тому доцільно розглянути питання мінімізації кількості складових за рахунок їх функціональної сумісності й можливості побудови локальної і просторово-розподіленої системи РЕЗах за агрегатно-модульним принципом. Такий підхід дозволяє проводити ремонт, модернізацію, нарощування функціональних можливостей системи з урахуванням морального та фізичного ресурсів її елементів (модулів, агрегатів) протягом усього життєвого циклу, враховувати вимоги до елементів системи – узгодження за енергетичними, частотними, інформаційними, електричними і конструктивними параметрами.

Для оптимізації складу системи за критерієм мінімізації кількості функціонально сумісних елементів застосуємо метод морфологічного аналізу [15], який передбачає виконання такої послідовності дій:

– точне формулювання проблеми;

– визначення найважливіших елементів системи – об'єкта аналізу;

– визначення варіантів можливого виконання елементів і занесення їх до таблиць (морфологічна скритність);

– оцінювання всіх наявних в таблицях варіантів;

– вибір структури з кращих варіантів.

Результати морфологічного аналізу приведені в табл. 1–6.

Аналіз змісту табл. 1–6 дозволяє запропонувати мінімальну структурну схему системи радіоелектронного захисту підрозділу НГУ (рис. 1), де 1, 3, 5, 7 – антена; 2 – розвідувальний приймач (пеленгатор); 4 – генератор перешкод подавлення, 6 – радіостанція зв'язку; 8 – генератор перешкод активного радіомаскування.

Підкреслимо, що наведено структуру локальної системи. Для просторово-розподіленої системи необхідний модуль управління, що дозволить застосовувати канали дезінформації для збільшення ефективності активного радіомаскування (розширення простору розвідувальних ознак). Для реалізації функцій управління можна застосувати персональних комп'ютерів (ПК), що входить до комплекту розвідувального скануючого приймача. У складі системи можна використовувати пристрої як військового, так і цивільного призначення, зокрема Hi-Tech.

Таблиця 1

Заходи при виконанні завдань за призначенням

Умови	Особливості заходів	Види зв'язку
Кампус	Існує контрольована зона, відомо R_{min} до засобів радіорозвідки, активне радіомаскування, ЕМС*	Волоконні оптичні лінії, дротовий зв'язок, радіозв'язок
Блок-пост	Маскування спрямованих антен, радіомаскування	Радіозв'язок, супутниковий зв'язок
Місто	Захист і подавлення по вертикалі і горизонталі, ЕМС*	Радіозв'язок, ретранслятори, GSM, CDMA
Сільська місцевість	Маскування, радіомаскування	Радіозв'язок, ретранслятори, супутниковий зв'язок
На марші	Мінімальна контрольована зона, захист від радіокерованих вибухових пристроїв	Радіозв'язок, ретранслятори, супутниковий зв'язок
Масові заворушення	Локальність простору захисту і подавлення, ЕМС*	Радіозв'язок, ретранслятори, GSM, CDMA, супутниковий зв'язок
Надзвичайні ситуації	ЕМС*	Радіозв'язок, ретранслятори, супутниковий зв'язок

* Дотримання норм ЕМС є необхідною умовою при виконанні усіх видів завдань за призначенням

Таблиця 2

Засоби зв'язку підрозділів НГУ

Радіостанції портативні,автомобільні штатні	Мобільні телефони	Супутникові телефони	Антени радіостанцій
Радіостанції професійні1, 5, 20,40,6 0 Вт	GSM, CDMA, 3G	В спеціальних випадках	Штатні
Підсилювачі потужності,			Зовнішні пеленгаційні, з керованою діаграмою

Таблиця 3

Засоби РЕБ підрозділів НГУ

Приймачі розвідки радіозв'язку	Радіостанції зв'язку	Антени*	Радіоукриття*
Радіостанції з функцією сканунування	Передавачі перешкод*	Пеленгаційні	На основі куткової антени
Скануючі приймачі*	Передавачі перешкод з віддаленим доступом	Спрямовані для подавлення	Екрануючий шатер з металізованої тканини
Скануючі приймачі з віддаленим доступом	Передавачі подавлення БПЛА**	З керованою діаграмою	Площинний екран розмірами n λ_{max}·m λ_{max}

*VHF, UHF, 3G, Wi-Fi, GPS L1, L2, L3, L4, L5

** Передавачі перешкод видимого та IR діапазонів

Таблиця 4

Антени РЕБ

Завдання	Діаграма	Поляризація	Діапазон
Радіомаскування активне	Секторна*	Вертикальна, горизонтальна	VHF,UHF,3G, Wi-Fi
Радіорозвідка (пеленгація)	Двопелюсткова	Вертикальна	VHF,UHF,3G, Wi-Fi
Подавлення радіостанцій зв'язку	Секторна, однопелюсткова	Вертикальна	VHF,UHF,3G, Wi-Fi
Подавлення каналів управління рухомих командних пунктів	Кругова, секторна*	Вертикальна, кругова	VHF,UHF,3G, Wi-Fi
Подавлення каналів управління і передавання інформації БПЛА	Секторна, однопелюсткова, косекансна	Вертикальна, горизонтальна	VHF, UHF, 3G, Wi-Fi, GPS L1, L2, L3, L4, L5

* Передавачі перешкод видимого та IR діапазонів

Таблиця 5

Антени захисту інформації

Завдання	Діаграма	Поляризація	Діапазон
Радіомаскування активне від наземних засобів радіорозвідки	Секторна	Вертикальна, горизонтальна	VHF,UHF,3G, Wi-Fi
Радіомаскування активне від БПЛА	Секторна	Вертикальна, горизонтальна	VHF,UHF,3G, Wi-Fi

Таблиця 6

Діапазони та смуги частот БПЛА

Діапазон	Смуга	Призначення
WiFi 5.8 ГГц	5.7-5.9 ГГц	Передавання відео
WiFi 2,4 ГГц	2400-2480 МГц	Управління
GPS L1	1575.42 МГц	Навігація
GPS L2	1227.60 МГц	Навігація
433 МГц		Пульт управління
800/900 М, 850-965МГц		Пульт управління

В розглянутій структурі (рис.1) найбільшу кількість відмінностей мають антени.

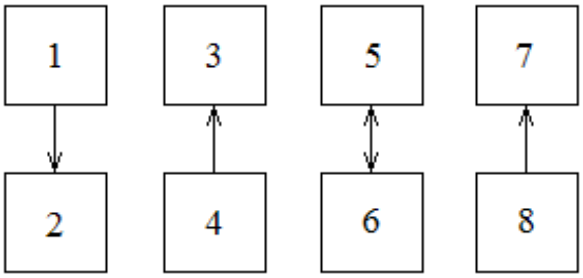

Рис. 1. Мінімальна структурна схема системи радіоелектронного захисту підрозділу НГУ

Зазначимо, що до параметрів антен систем радіозв'язку, радіорозвідки, радіомоніторингу, активного радіомаскування та подавлення висуваються різні вимоги, тому реалізація універсальної антени для різних застосувань і умов виконання службових завдань проблематична. До того ж, при експлуатації радіоелектронних засобів з часом вимоги до властивостей та значень їх параметрів можуть змінюватися (підвищуватися), в той час як серійні антени РЕЗ є закінченими пристроями і модернізація їх неможлива без дозволу розробника. Взагалі, ідеальною для застосування антеною можна вважати таку, яка могла б адаптуватись до умов експлуатації. Важливими є також вимоги до технологічності базової конструкції, мінімізації кількості елементів. Додатково необхідно враховувати можливість встановлення (монтування) антени на транспортні засоби або захисне оснащення, а також малу чутливість до відхилень геометричних розмірів конструкції, можливість її виготовлення в умовах ремонтних органів та відсутність демаскуючих ознак. Антени повинні працювати в діапазонах VHF, UHF, GSM, CDMA, 3G, Wi-Fi, GPS L1, L2, L3, L4, L5 бажано при мінімальній номенклатурі типів (конструкцій).

Вибір типів антен приведено в [16]. У сенсі анотованої мети уваги заслуговують антени типу "випромінювач над циліндричною поверхнею" та найпростіша за конструкцією кутова антена, що складається з двох пласких відбивачів і випромінювача, яку доцільно використати як базовий елемент.

Можливість поліпшення характеристик кутових антен за рахунок управління формою та шириною діаграми спрямованості розглянута в [17].

Аналіз характеристик та конструкція кутової антени в залежності від частотного діапазону, який визначає випромінювач, описані в [18]. У зв'язку з тим, що відбивачі кінцеві в розмірах, антени мають бічні пелюстки, що негативно впливає на ефективність і безпеку системи захисту. Установка металевих прямокутних або круглих перемичок на кутовий відбивач в певних положеннях дозволить знизити рівень бічних пелюсток [19], як показали результати машинного моделювання на основі FEKO та практичні дослідження [20], приблизно на 20–25 дБ. Практичність описаного підходу полягає в його дешевизні: він не змінює первісну форму антени, не вимагає суттєвих змін існуючої конструкції, крім оптимального розміщення і фіксації перемичок.

Викладене в [16–20] дало змогу запропонувати варіант побудови системи захисту радіообміну в локальній системі радіозв'язку [21].

В табл. 7 наведені результати моделювання імпровізованої антени з пласким відбивачем розмірами $m\lambda max \cdot n\lambda max$ (mmin>2, nmin>1), за основу конструкції якої взята антена типу "випромінювач над площиною" [22].

Зміна відстані від випромінювача до екрану згідно з діапазоном хвиль дозволяє трансформації – змінювати вид та ширину діаграми спрямованості.

Антена може встановлюватися над корпусом бронетехніки або металевого кузова автомобіля.

Таблиця 7

Характеристики антени “випромінювач над площиною”

Відстань до дзеркала S/ λ	Довжина вібратора l/λ	Ширина головної пелюстки, град	Діаграма спрямованості	G, дБ
0,20	0, 46	77	1 пелюстка	7,6
0,40	0,48	105	1 пелюстка	6,1
0,50	0,48	–	2 пелюстки	6,3
0,70	0,47	–	головний+2 бокових	7,5

Вигляд квазірупорної антени дециметрового діапазону показаний на рис. 2.

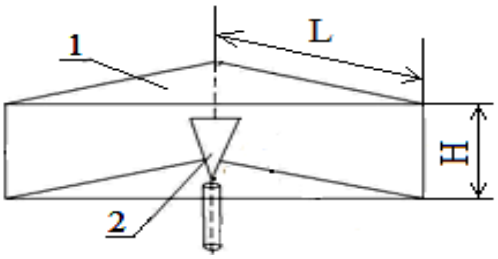

Рис. 2. Квазірупорна антена дециметрового діапазону

Антена, що складається з металевого корпусу відбивача 1 та широкосмугового випромінювача 2, забезпечує можливість істотного зниження габаритів при збереженні значень електричних параметрів (коефіцієнта корисної дії (КСД) і коефіцієнта стоячої хвилі (КСХ)) в порівнянні з кутовою (табл. 8).

Висота ребра відбивача становить H=(0,22-0,24)λсер., H/ L= ,3-0,4, кут розкриття α=45-900, кут при вершині випромінювача обраний в інтервалі 30–400, а його висота h = (0,75-0,85)H.

Антена дозволяє перекривати смугу частот GSM 900-1800, 3G при розмірах H=52мм, L=125мм. У чотирьох- або шестисекторному варіанті антена може встановлюватися на бронетехніці й використовуватися для пеленгування, ретрансляції, локального подавлення, активного радіомаскування, створення оманних сигнатур сигналів засобів зв’язку.

Таблиця 8

Порівняльні характеристики антен для діапазону UHF

Параметри	Кутова антена UHF, розмір	Квазірупорна антена UHF,розмір
H	850 мм	172мм
L	890мм	490мм
F/B	25–30	25–35
F_{max}/F_{min}	1,6	2,5
КСХН	<2	<2

Особливості виконання завдань за призначенням підрозділами НГУ визначаються умовами місцевості: сільська (рівнинна, пересічена), сільський населений пункт, місто тощо. Рельєф місцевості, нерівність поверхні, рослинність, будівлі та їх висота, відстань між засобами зв’язку здійснюють різний вплив на формування діаграми спрямованості (ДС) антен та зон покриття. Очевидно, що повністю детерміністські методи розрахунку цих характеристик нездійсненні не тільки через дуже великий обсяг обчислень, але й через відсутність коректних електродинамічних методів урахування всіх локальних особливостей. Реальні ДС і зони покриття можна встановити, використовуючи наземні й повітряні носії джерел вимірювальних сигналів. При обльоті зони з радіусом 500 м на швидкості 5 м/с така процедура реалізується у термін до 10 хв. Вибір можливих типів повітряних носіїв, наприклад, квадрокоптерів визначається вагою корисного навантаження, часом польоту, швидкістю, умовами виконання завдань за призначенням, наявністю необхідних функцій (ActiveTrack, Tap fly, Obstacle Sensing System, GPS, Positioning hangs, Return home тощо), комплекту обладнання та економічними чинниками [23]. Але знання ДС антен і зон покриття підвищує можливості реалізації ефективного захисту і надійності зв’язку підрозділу НГ України.

Висновки

У сенсі анотованої мети при побудові системи радіоелектронного захисту підрозділів Національної гвардії України при виконанні службово-бойових завдань доцільно використовувати конструкції кутової антени як базового елемента та антени інших розглянутих в статті типів в комплексі зі штатними засобами військового призначення та пристроями Hi-Tech.

Авторами протягом декількох років в теорії і на практиці доводилось вирішувати завдання захисту радіообміну і РЕБ для підрозділів Національної гвардії України і створення просторово-розподілених систем. Отриманий досвід підтвердив можливість поетапної побудови системи захисту і РЕБ за агрегатно-модульним принципом: від мінімально необхідного складу з поступовою модернізацією системи "на ходу" за умов появи нових тактичних завдань і технічних рішень у розглянутій галузі.

Список літератури

1. FM 3 – 38 Cyber Electromagnetic Activities. Headquarters Department of the Army Washington, DC, 12 February 2014. – 96 p.
2. Information security standards [Електронний ресурс]. – Режим доступу: http://www.iso27001security.com. – Назва з екрану.
3. Мельников Ю.П. Радиотехническая разведка. Методы оценки эффективности местоопределения источников радиоизлучения / Ю.П. Мельников, С.В. Попов. – М.: Радиотехника, 2008. – 432 с.
4. Борьба радиоэлектронная. Термины и определения: ГОСТ РВ 0158-002-2008: Изменение N 1. – Введ. 2012-01-01. – М.: Стандартинформ, 2011.
5. Радиоэлектронные системы: Основы построения и теория. Справочник / [Ширман Я.Д., Багдасарян С.Т., Маляренко С.А. и др.]; под ред. Я.Д. Ширмана. [2-е изд.]. – М.: Радиотехника, 2007. – 512 с.
6. Роль и место РЭБ в вооружённой борьбе. [Електронний ресурс]. – Режим доступу: http://www.military-informant.com/index.php/other /analytic/1478-reb.html.
7. Иванов И. Содержание и роль радиоэлектронной борьбы в операциях XXI века / И. Иванов, И. Чадов. [Електронний ресурс]. – Режим доступу: http://pentagonm.ru/pub/soderzhani_i_ujl_radioehlekronnoj_borby_v_operacijakh_xxi_veka/ 80-1-0-1700.
8. Electronic Warfare. Joint Publication 3-13.1, U. S. Army, 2007. – 129 p.
9. Adam T. Electronic warfare I / T. Adam. –: Nova Science Publishers. 2009. – 192 p.
10. Biddle Stephen The 2006 lebanon campaign and the future of warfare: implications for army and defense policy [Електронний ресурс] / Stephen Biddle, Jeffrey A. Friedman // September 2008, p 90. – Режим доступу: http://www.StrategicStudiesInstitute.army.mil.
11. Ларин Д.А. Электронная война в Ливане летом 2006 года / Д.А. Ларин // Защита информации. Інсайд. – 2008. – № 3. – С. 92-96.
12. Куприянов А.И. Теоретические основы радиоэлектронной борьбы / А.И. Куприянов, А.В. Сахаров. – М.: Вузовская книга, 2007. – 356 с.
13. Куприянов А.И. Радиоэлектронная борьба. Основы теории / А.И.Куприянов, Л.Н. Шустов. – М.: Вузовская книга, 2011. – 800 с.
14. Радзиевский В.Г. Сетецентрическая пространственно-распределенная система на основе малогабаритных модулей разведки и помех [Текст] / В.Г. Радзиевский // Радиотехника. – 2012. – № 6. – С. 4-12.
15. Основы научных исследований / А.П. Болдин, В.А. Максимов, Э.Ф. Бабуров, Э.П. Куликов, В.К. Маригодов. – М.: Академия, 2012. – 336 с.
16. Антени для захисту каналів радіозв'язку підрозділів Національної гвардії України / Ю.П. Белокурський, О.Ю. Іохов, В.Є. Козлов, О.О. Щербина // Зб. наук. праць Нац. акад. Нац. гвардії України. – 2015. – Вип. 2 (26). – С 65-68.
17. Пат. України №105732, МПК (2016.01) H01Q 19/00. Антенний пристрій / Ю.П. Белокурський, О.Ю. Іохов, В.Є. Козлов, І.В. Кузьминич, О.О. Морозов, О.О. Щербина (Україна). – Опубл. 11.04.2016, Біл. №7.
18. Організація захисту каналів радіозв'язку підрозділів охорони правопорядку України / Ю.П. Белокурський, О.Ю. Іохов, В.Є. Козлов, О.О. Щербина // Зб. наук. праць Акад. внутр. військ МВС України. – 2014. – Вип. 1(23). – С. 46-49.
19. Підвищення ефективності антен для активного захисту інформації / Ю.П. Белокурський, О.М. Горбов, О.Ю. Іохов, В.Є. Козлов, О.О. Щербина // Тези наук.-практ. конф. – Х.: Нац. акад. Нац. гвардії України, 2015. – С. 4-5.
20. Дослідження імпровізованих діаграмоутворюваючих пристроїв для захисту інформації / Ю.П. Белокурский, В.Є. Козлов, В.В. Лишенко, О.О. Щербина // Тези наук.-практ. конф. – Х.: Акад. внутр. військ МВС України, 2011. – С. 24.
21. Пат. України №104505, МПК (2016.01) H04B 7/00. Спосіб захисту інформаційного обміну в локальній системі радіозв'язку / Ю.П. Белокурський, О.М. Горбов, О.Ю. Іохов, В.Є. Козлов, О.О. Морозов, О.О. Щербина (Україна). – Опубл. 10.02.2016, Біл. № 3.
22. Радіоелектронний захист каналів службового радіозв'ку / Ю.П. Белокурський, О.Ю. Іохов, В.Є. Козлов, О.О. Щербина // Тези наук.-практ. конф. – Х.: Нац. акад. Нац. гвардії України, 2016. – 62 с.
23. Кадем Р.К. Компонентный анализ беспилотных летательных аппаратов / Р.К. Кадет // Електроніка та системи управління. – 2010. – № 2 (24). – С. 45-51.

References

1. FM 3 – 38 Cyber Electromagnetic Activities. Headquarters Department of the Army Washington, DC, 12 February 2014. – 96p.
2. Information security standards, www.iso27001security.com.

3. Mel'nikov, Yu.P. and Popov, S.V. (2008), "*Radiotekhnicheskaya razvedka. Metody ocenki ehffektivnosti mestoopredeleniya istochnikov radioizlucheniya*" [*Radio technical intelligence. Methods for estimating the efficiency of the location of radio emission sources*], Radiotekhnika, Moscow, 432 p.

4. GOST RV 0158-002-2008 (2011), "*Bor'ba radioehlektronnaya. Terminy i opredeleniya*" [*Electronic Warfare. Terms and Definitions*], Standartinform, Moscow.

5. Shirman, Ya.D., Bagdasaryan, S.T. and Malyarenko, S.A. (2007), "*Radioelektronnyie sistemyi: Osnovyi postroeniya i teoriya. Spravochnik*" [*Radioelectronic Systems: Fundamentals of Construction and Theory. Directory*], Radiotehnika, Moscow, 512 p.

6. "*Rol i mesto REB v vooruzhYonnoy borbe*" [*The role and place of EW in armed struggle*], http://www.military-informant.com/index.php/other /analytic/1478-reb.html.

7. Ivanov, I. and Chadov, I. "*Soderzhanie i rol radioelektronnoy borbyi v operatsiyah XXI veka*" [*The content and role of electronic warfare in the operations of the 21st century*], http://pentagonm.ru/pub/soderzhani_i_ujl_radioehlekronnoj_borby_v_operacijakh_xxi_veka/80-1-0-1700.

8. Electronic Warfare. Joint Publication 3-13.1, U. S. Army, 2007. – 129 p.

9. Adam, T. (2009), *Electronic warfare*, Nova Science Publishers, New York, 192 p.

10. Biddle Stephen and Friedman Jeffrey, A. (2008), *The 2006 lebanon campaign and the future of warfare: implications for army and defense policy*, www.StrategicStudiesInstitute.army.mil, p 90.

11. Larin, D.A. (2008), "Elektronnaya voyna v Livane letom 2006 goda" [Electronic war in Lebanon in the summer of 2006], *Protection of information, Inside*, No. 3, pp. 92-96.

12. Kupriyanov, A.I. and Sakharov, A.V. (2007), "*Teoreticheskie osnovyi radioelektronnoy borbyi*" [*Theoretical basis of electronic warfare*], The college book, Moscow, 356 p.

13. Kupriyanov, A.I. and Shustov, L.N. (2007), "*Radioelektronnaya borba. Osnovyi teorii*" [*Electronic warfare. Fundamentals of the theory*], The University Book, Moscow, 800 p.

14. Radzievsky, V.G. (2012), "Radioelektronnaya borba. Osnovyi teorii" [Network-centric spatially-distributed system based on small-scale reconnaissance and interference modules], *Radio engineering*, No. 6, pp. 4-12.

15. Boldin, A.P., Maksimov, V.A., Baburov, E.F., Kulikov, E.P. and Marigodov, V.K. (2012), "*Osnovyi nauchnyih issledovaniy*" [*Fundamentals of Scientific Research*], Academy, Moscow, 336 p.

16. Belokurskiy, Yu.P., Iohov, O.Yu., Kozlov, V.Ye. and Scherbina, O.O. (2015), "Anteni dlya zahistu kanaliv radiozv'yazku pidrozdiliv Natsionalnoyi gvardiyi Ukrayini" [Antennas for protection of radio communication channels of the units of the National Guard of Ukrainet], *Collection of scientific works of the National Accademy of the National Guard of Ukraine*, No. 2 (26), pp. 65-68.

17. Belokurskiy, Yu.P., Iohov, O.Yu., Kozlov, V.Ye., Kuzminich, I.V., Morozov, O.O. and Scherbina, O.O. (2016), "*Antenniy pristriy*" [*Antenna device*], Ukraine, МПК (2016.01) H01Q 19/00.

18. Belokurskiy, Yu.P., Iohov, O.Yu., Kozlov, V.Ye. and Scherbina, O.O. (2014), "Organizatsiya zahistu kanaliv radiozv'yazku pidrozdiliv ohoroni pravoporyadku Ukrayini" [Organization of protection of radio communication channels of the Ukrainian law enforcement units], *Collection of scientific works of the National Accademy of the National Guard of Ukraine*, No. 1 (23), pp. 46-49.

19. Belokurskiy, Yu.P., Gorbov, O.M., Iohov, O.Yu., Kozlov, V.Ye. and Scherbina, O.O. (2015), "Pidvischennya efektivnosti anten dlya aktivnogo zahistu informatsiyi" [Increasing the efficiency of antennas for active protection of information], *Abstracts of the scientific and practical conference*, National Accademy of the National Guard of Ukraine, Kharkiv, pp. 4-5.

20. Belokurskiy, Yu.P., Kozlov, V.Ye., Lishenko, V.V. and Scherbina, O.O. (2011), "Doslidzhennya improvizovanih diagramoutvoryuvayuchih pristroyiv dlya zahistu informatsiyi" [Research of improvised directional devices for information protection], *Abstracts of the scientific and practical conference*, Academy of Internal Troops of the Ministry of Internal Affairs, Kharkiv, p. 24.

21. Belokurskiy, Yu.P., Gorbov, O.M., Iohov, O.Yu., Kozlov, V.Ye., Kuzminich, I.V., Morozov, O.O. and Scherbina, O.O. (2016), "*SposIb zahistu InformatsIynogo obmInu v lokalnIy sistemI radIozv'yazku*" [*A way to protect information exchange in the local radio system*], Ukraine, МПК H04B 7/00.

22. Belokurskiy, Yu.P., Iohov, O.Yu., Kozlov, V.Ye. and Scherbina, O.O. (2016), "Radioelektronniy zahist kanaliv sluzhbovogo radiozv'ku" [Radio-electronic protection of channels of official radio communication], *Abstracts of the scientific and practical conference*, National Accademy of the National Guard of Ukraine, Kharkiv, p. 62.

23. Kadem, R.K. (2010) "Komponentnyiy analiz bespilotnyih letatelnyih apparatov" [Component analysis of unmanned aerial vehicles], *Electronics and control systems*, No. 2 (24), pp. 45-51.

Надійшла до редколегії 3.11.2017
Схвалена до друку 7.12.2017

***Відомості про авторів*:**

Белокурський Юрій Павлович
Асистент кафедри
Харківського національного університету
радіоелектроніки,
Харків, Україна
https://orcid.org/0000-0002-8311-5297
e -mail:urpalbel@gmail.com

***Information about the authors*:**

Yuriy Belokurskyi
Assistant of Lecturer
Kharkiv National University
of Radio Electronics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-8311-5297
e-mail:belokurskyi.y.p@gmail.com

Іохов Олександр Юрійович
кандидат технічних наук доцент
старший науковий співробітник,
начальник кафедри Національної академії
Національної гвардії України,
Харків, Україна
https://orcidid0000-0002-1718-0138
e-mail: iohov@ukr.ne

Козлов Валентин Євгенович
кандидат технічних наук доцент,
доцент кафедри Національної академії
Національної гвардії України,
Харків, Україна
https://orcid.org/0000-0003-4452-3009
e-mail: kozlov1945ve@gmail.com

Щербина Олександр Олексійович
кандидат технічних наук доцент,
доцент кафедри Харківського національного
університету радіоелектроніки,
Харків, Україна
https://orcid.org/0000-0001-5931-8994
e-mail:jul-46@i.ua

Oleksander Iohov
Candidate of Technical Science Associate Professor
Senior Research,
Head of the Department of National Academy
of the National Guard of Ukraine,
Kharkov, Ukraine
https://orcidid0000-0002-1718-0138
e-mail: iohov@ukr.ne

Valentin Kozlov
Candidate of Technical Sciences Associate Professor,
Senior Lecturer of the Department of National Academy
of the National Guard of Ukraine,
Kharkov, Ukraine
https://orcidid0000-0003-4452-3009
e-mail: kozlov1945ve@gmail.com

Alexander Shcherbyna
Candidate of Technical Sciences Associate Professor,
Senior Lecturer of the Department
Kharkiv National University of Radio Electronics,
Kharkiv, Ukraine
https://orcid.org/0000-0001-5931-8994
e-mail:jul-46@i.ua

ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ РАДИОЭЛЕКТРОННОЙ ЗАЩИТЫ ПОДРАЗДЕЛЕНИЙ НАЦИОНАЛЬНОЙ ГВАРДИИ УКРАИНЫ ВО ВРЕМЯ ВЫПОЛНЕНИЯ СЛУЖЕБНО-БОЕВЫХ ЗАДАЧ

Ю.П. Белокурский, А.Ю. Иохов, В.Е. Козлов, А.А. Щербина

Рассмотрен вариант построения системы радиоэлектронной защиты подразделения Национальной гвардии (НГ) Украины при выполнении служебно-боевых задач (СБЗ) с использованием импровизированных антенн и устройств Hi-Tech. Проанализированы вопросы, касающиеся терминологии в области радиоэлектронной борьбы и различия подходов к ее ведению в вооруженных силах и силах охраны правопорядка, в частности, Национальной гвардии Украины. На основе метода морфологического анализа предложен состав системы радиоэлектронной защиты (СРЭЗ), минимальная структура которой включает антенны, разведывательный приемник (пеленгатор), генератор помех подавления, радиостанцию связи, генератор помех активной радиомаскировки. Рассмотрена одна из важнейших составляющих СРЭЗ – антенное устройство. Приведены результаты моделирования различных типов антенн. Сделан вывод о целесообразности использования конструкции уголковой антенны как базового элемента и антенн других рассмотренных в статье типов в комплексе со штатными средствами военного назначения и устройствами Hi-Tech для построения системы защиты радиосвязи подразделения НГ Украины при выполнении СБЗ.

Ключевые слова: *радиоэлектронная защита, Hi-Tech-технологии.*

PRINCIPLES OF THE SYSTEM OF ELECTRONIC PROTECTION UNITS OF THE NATIONAL GUARD OF UKRAINE DURING THE PERFORMANCE OF SERVICE AND COMBAT MISSIONS

Yu. Belokurskiy, O. Iohov, V. Kozlov, O. Scherbina

A brief analysis of the electronic opposition question leads to the conclusion that electronic warfare is located at the intersection of information and military security.

In the National Guard of Ukraine, in contrast to the armed forces, no special forces and means of warfare that determines the relevance and purpose of the article-consider the option of constructing a system of electronic defense units of the National Guard of Ukraine during the performance of service and combat missions. Analyzed issues related terminology in electronic warfare and differences in approaches to the conduct of the armed forces and law enforcement forces, including the National Guard of Ukraine. On the basis of morphological analysis proposed composition of electronic protection systems, the minimum structure which includes antenna reconnaissance receiver (direction finder), generator noise suppression, radio communication, radio jammers active camouflage. Considered one of the most important components of electronic protection-antenna device. The results of modeling different types of antennas. Determined that the construction of electronic systems protection units of the National Guard of Ukraine to the performance of service and combat missions should be used as a design angle antenna base element and the other antenna types discussed in the article together with regular means, military devices and Hi-Tech.

The authors for several years in the theory and practice had to solve the problem of protection for radio communications and electronic warfare units of the National Guard of Ukraine and the creation of spatially distributed systems. The experience confirmed the possibility of phased construction of protection systems and electronic warfare for the aggregate-modular principle of the minimum required of the gradual modernization of "on the go" in terms of new tactical problems and technical solutions in the field considered.

Keywords: *radio-electronic protection, Hi-Tech-technology.*