УДК 621.391

О.Ю. Іохов, В.Є. Козлов, В.Г. Малюк, К.М. Ткаченко, М.Д. Ткаченко

Національна академія Національної гвардії України. Харків

РАДІОМАСКУВАННЯ ВІЙСЬКОВИХ ПІДРОЗДІЛІВ ЗА УМОВ ЗАСТОСУВАННЯ ШТАТНИХ ТА ІМПРОВІЗОВАНИХ ЗАСОБІВ

В статті розглянуто спосіб комплексного застосування заходів активного радіомаскування з використанням спеціальних засобів радіоелектронного придушення (РЕП), що може бути використаний для побудови локальних систем радіозв'язку, призначених для обміну конфіденціальною інформацією в діапазоні ультракоротких хвиль в умовах штучних радіозавад і спроб несанкціонованого доступу до інформації, що передається.

Ключові слова: *система радіозв'язку, активне радіомаскування, розвідзахищеність, ультракороткі хвилі.*

Аналіз публікацій та постановка проблеми

Ведення радіоелектронної розвідки є невід'ємною частиною процесу отримання розвід даних. Аналіз досвіду проведення антитерористичної операції в Донецькій та Луганській областях України виявив неспроможність існуючої системи радіозв'язку НГУ забезпечити захист від дії засобів радіорозвідки противника (ЗРРПр). Це обумовлено використанням у військових підрозділах таких радіо засобів як Vertex VX-1210, MOTOTRBO DM 4601, MOTOTRBO DP 4801, MTR3000, що не пристосовані до захисту від ЗРРПр. Таким чином, використання зазначених радіозасобів вимагає ретельного вибору технічних засобів та/ або проведення організаційних заходів з радіомаскування (РМ).

Висунемо наукову гіпотезу про можливість забезпечення розвідзахищеного радіообміну підрозділи НГУ в обмеженому просторі шляхом застосування штатних та імпровізованих засобів пасивного та активного маскування.

Проведений у роботі [1] аналіз показав, що виконання окремих заходів пасивного РМ не забезпечує досягнення необхідного рівня захищеності за умови стабільної роботи радіомережі.

Орієнтовні розрахунки дають можливість стверджувати про необхідність комплексного застосування заходів маскування з використання спеціальних засобів радіоелектронного придушення (РЕП) [2, 3], що здатні створювати на вході приймача радіорозвідки перешкоди з необхідним рівнем потужності.

У роботах [4, 5] надані практичні рекомендацій щодо підвищення безпеки радіомереж тактичної ланки управління НГУ, однак вони не враховують необхідність постановки завад декількома джерелами для декількох засобів зв'язку підрозділів НГУ та розташування засобів радіоелектронної розвідки (РЕР) на висотах або на повітряних носіях.

Викладене вище зумовлює **актуальність та мету статті** – розглянути спосіб радіомаскування військових підрозділів за умов застосування штатних та імпровізованих засобів активного маскування.

Виклад основного матеріалу

Термін активне радіомаскування, як він розуміється в даний час, означає протидію радіо- і радіотехнічній розвідці шляхом створення спеціальних полів перешкод, що ускладнюють несанкціонований прийом сигналу засобами радіотехнічної розвідки і виділення повідомлень засобами радіорозвідки. Потребує уточнення істотно важливе обмеження:: перешкоди не повинні заважати роботі систем, що маскуються, тобто не повинні знижувати показники якості і ефективності радіозв'язку нижче деякого прийнятного рівня.

В [6] розглянуто спосіб захисту інформаційного обміну в локальній системі радіозв'язку, заснований на зменшені відношення сигнал/ шум для приймачів, що здійснюють спробу несанкціонованого доступу до інформації, яка передається, за рахунок того, що під час роботи системи радіозв'язку неперервно випромінюють за периметр системи і вгору шумові сигнали, які мають потужність більшу потужності робочих сигналів в системі радіозв'язку, що перекривають усю смугу частот, використовуваних в системі. Цей спосіб складний для побудови, потребує великих матеріальних та енергетичних витрат, а його фізичні (у смузі частот, використовуваних в системі) та візуальні (специфічний вигляд та розміри антен захисту і каналів зв'язку) якості є демаскуючими ознаками, що унеможливлюють скритне застосування.

Спосіб захисту інформації, розглянутий в роботі [7], передбачає використання окремо або в різних сполученнях будови системи зв'язку, при якій канали зв'язку мають мінімальний витік енергії за рахунок зменшення відношення сигнал/ шум для приймачів, що здійснюють спробу несанкціо-

нованого доступу до інформації, яка передається, шляхом зниження потужності робочих сигналів і неперервного випромінювання за периметр системи і вгору шумових сигналів, і канали передавання інформації з конфігурацією, що управляється. Недоліком цього способу є складність побудови системи зв'язку, зумовлена необхідністю використання абонентських радіостанцій зі спеціальними засобами формування, передавання, приймання та фільтрації шумових сигналів, і неможливість скритного застосування, обумовлена візуальними (специфічний вигляд та розміри антен каналів зв'язку) демаскуючими ознаками.

Спосіб захисту інформаційного обміну в локальній системі радіозв'язку [8], на відміну від попереднього, передбачає застосування сумісно скритних антенних пристроїв захисту і каналів передавання інформації з конфігурацією, що управляється.

Цей спосіб не забезпечує захист від спроб несанкціонованого доступу до інформації, яка передається, розвідувальних приймачів, розміщених на повітряних носіях, що переміщаються вище верхнього рівня основної пелюстки діаграми направленості (ДН) в площині кута місця антенних пристроїв захист, тобто розміщених у будь-якій точці простору.

Для реалізації сформульованої наукової гіпотези доцільним є сумісне застосування скритних антенних пристроїв захисту і каналів передавання інформації з конфігурацією, що управляється; при цьому, антенні пристрої захисту мають забезпечувати орієнтування діаграми направленості в визначених азимутальному напрямку β та куті місця ε.

На рис. 1 наведено в азимутальній площині варіант побудови локальної системи радіозв'язку (ЛСР), а на рис. 2 – фрагмент ЛСР в площині кута місця.

У кампусі – обмеженій території з постійним складом і місцем розміщення (студентське або військове містечко, майдан тощо) – розташовують один або декілька абонентів (А) 1 зв'язку, один або декілька пунктів управління (ПУ) 2, що удвох створюють канал передавання інформації (КПІ), та один або декілька пристроїв захисту (ПЗ) 3 відносно одного або декількох розвідувальних приймачів (РП), розміщених на площині 4 або на повітряних носіях 5 (безпілотні літальні апарати, квадрокоптери, повітряні змії або кулі) таким чином, щоб забезпечити надійний захист від спроб несанкціонованого доступу до інформації, яка передається, і електромагнітну сумісність засобів (ЕМС) ЛСР та мереж бездротового зв'язку легальних користувачів.

Конфігурація ЛСР змінюється зі зміною обстановки (переміщенні РП) шляхом взаємного переміщення відносно РП і один до одного ПЗ та КПІ (абонентів і, при необхідності, ПУ) таким чином, щоб директриси ДН ПЗ були спрямовані на розміщений у просторі або рухомий РП при умові забезпечення ЕМС.

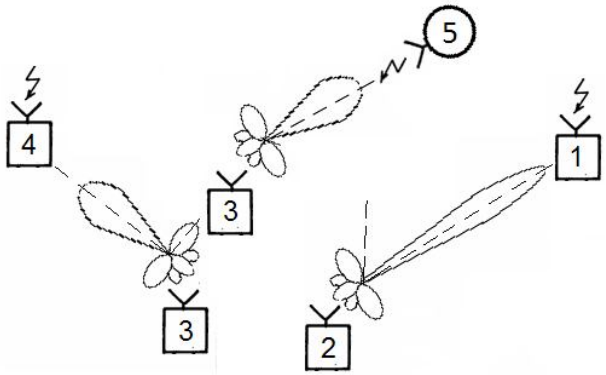

Рис. 1. Варіант побудови
локальної системи радіозв'язку

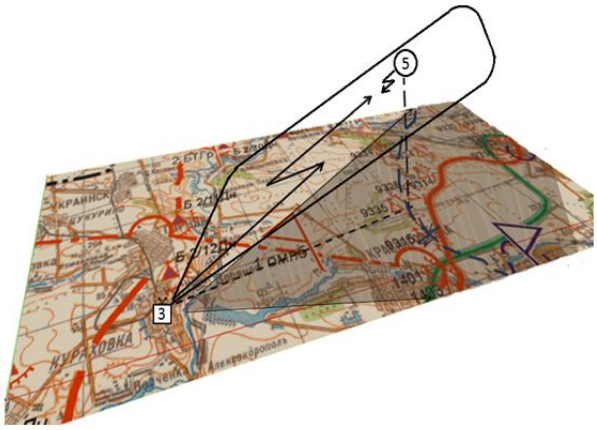

Рис. 2. Фрагмент ЛСР в площині кута місця

Адаптація до змін умов функціонування ЛСР потребує вирішення низки завдань, зокрема, визначення точок розміщення РП, оптимізації розташування ПЗ, розрахунку їх мінімальної потужності, розрахунку покриття, інтерференцій.

Перелічені завдання вирішує програмний виріб (ПВ) HTZ warfare, який може використовуватися на обчислювальному засобі (ноутбук, планшет тощо) ПУ. Результати розрахунків відображаються в 3D-форматі, що дозволяє уявити радіоелектронну обстановку у будь-якій точці об'єкта аналізу та визначити азимут β та кут місця ε окремого розвідувального приймача або зони його баражування, як показано на рис. 2.

В якості антен абонентів зв'язку 1 та пристроїв захисту 3 можуть застосовуватися антенні пристрої [9] або їм подібні, що забезпечують скритність застосування. Для пунктів управління 2 доцільне використання антенних пристроїв з більш вузькою діаграмою направленості [5].

Захист від засобів РР, розміщених у просторі можна забезпечити антенний пристрій [12], зовнішній вигляд якого наведено на рис. 3, що склада-

ється із куткового дзеркала (рефлектора) 1, утвореного двома пласкими металевими пластинами, і вібратора або системи колінеарних вібраторів 2, містить шарнірно приєднану усередині вершини дзеркала лінійку 3, розташовану у площині бісектриси кута дзеркала, з повзунком 4, який з обох боків з'єднаний шарнірно з пластинами дзеркала, та оптичного візиру 5, розташованого зверху рефлектора у площині бісектриси його кута.

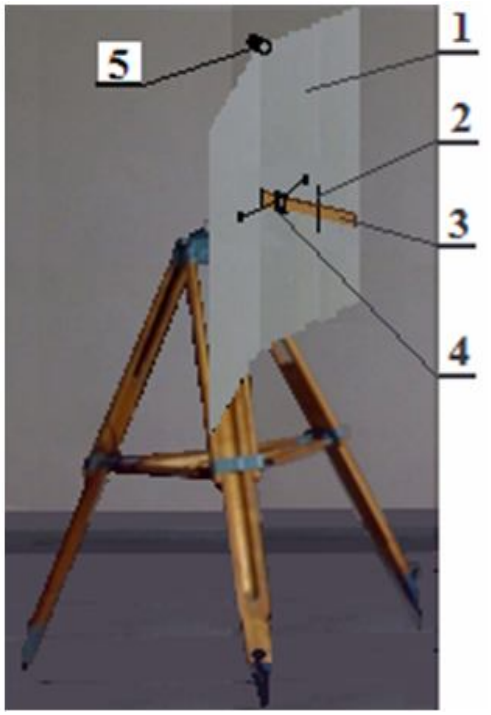

Рис. 3. Антенний пристрій

На рис. 4 наведено зовнішній вигляд повзунка 4 з нанесеною шкалою 6 кута нахилу рефлектора у площині кута місця, стрілкою-виском 7 і фіксатором 8.

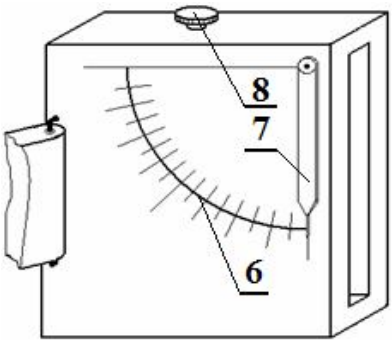

Рис. 4. Зовнішній вигляд повзунка 4

Переміщенням повзунка 4 встановлюють потрібний кут φ розкриву дзеркала, який фіксують фіксатором 8.

Кут місця ε можна також встановити за шкалою 6 і стрілкою-виском 7 без використання візиру (у випадку відсутності візуального контакту з ціллю).

Рис. 5 – частина лінійки 3 із градуюванням кутової шкали у значеннях кута розкриву дзеркала для довжини плеча шарнірного з'єднання повзунка 77 мм.

Наведення ДН антенного пристрою в потрібних азимутальному напрямку β та куті місця ε здійснюють за допомогою візиру 5, оптична вісь якого співпадає з бісектрисою кута дзеркала і перпендикулярна до нього; положення дзеркала фіксують, при цьому стрілка-висок 7 показує на шкалі 6 значення кута місця ε у напрямку максимуму ДН.

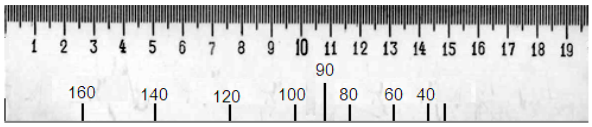

Рис. 5. Частина лінійки 3

При зміні кута розкриву дзеркала з φ_1 на φ_2 лінійка залишається у площині бісектриси кута завдяки рівноплечому шарнірному з'єднанню повзунка з пластинами дзеркала (рис. 6).

Зміна кута розкриву φ та відстані вібратора (системи вібраторів) від вершини дзеркала дозволяє змінювати ширину ДН та кількість її пелюстків в азимутальній площині з метою визначення азимуту цілі однопелюстковим методом максимуму або двохпелюстковим методом мінімуму.

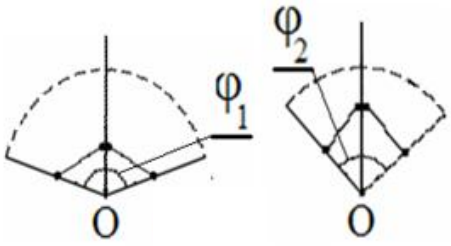

Рис. 6. Кута розкриву дзеркала

Розглянуте технічне рішення забезпечує точне наведення діаграми направленості у напрямку цілі (об'єкта спостереження) і може бути використана для пеленгування та/або придушення джерела радіовипромінювання (завад), розміщеного на повітряному носії.

Це гарантує адаптованість до будь-якої обстановки, що склалася в системі, і захист локальної системи радіозв'язку.

Антенний пристрій можна встановлювати на поворотному пристрої (наприклад, тринозі) на ґрунті, авто-та бронетехніці тощо.

На рис. 3 наведено зовнішній вигляд розміщеного на тринозі антенного пристрою у складі куткового дзеркала 1, вібратора (системи вібраторів) 2, лінійки 3 із повзунком 4 та оптичного візиру 5.

Аналіз характеристик перешкод показав [2, 3], що за характером впливу найбільш ефективними є імітуючі або прицільні активні перешкоди, які

ускладнюють виявлення і розпізнавання корисного сигналу та дозволяють вносити неправдиву інформацію.

На озброєнні підрозділів НГУ відсутні будь-які засоби постановки навмисних завад. У застосовуваних радіостанціях MOTOTRBO використовується два режими роботи: цифровий та аналоговий. Виходячи з цього, в якості навмисної завади можна використовувати сигнал радіостанції в аналоговому режимі для подавлення цифрового корисного сигналу та навпаки.

Проведений натурний експеримент з побудови розглянутого способу активного радіомаскування підтвердив його працездатність.

Висновки

Розглянутий спосіб радіомаскування з використанням імпровізованих антенних пристроїв та штатних засобів радіозв'язку може забезпечити розвідзахищений радіообмін підрозділів НГУ в обмеженому просторі, що дає змогу вважати доведеною висунуту в постановчій частині статті наукову гіпотезу.

Список літератури

1. Журавський Ю.В. Аналіз впливу заходів радіомаскування на розвідзахищеність радіоелектронних засобів / Ю. В. Журавський, Р. М. Жовноватюк, Г. Д. Носова, А. А. Завада // Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. - 2015. - Вип. 10. - С. 43-50.

2. Куприянов А.И. Теоретические основы радиоэлектронной борьбы [Текст]/ А. И. Куприянов, А. В. Сахаров. – М.: Вузовская книга, 2007.- 356 с.

3. Активная радиомаскировка. Режим доступу: http://studopedia.media4biz.ru /2_46668_aktivnaya-radiomaskirovka.html.

4. Розроблення рекомендацій щодо підвищення безпеки радіомереж тактичної ланки управління ВВ МВС України: науково-дослідна робота [Текст]/ О.Ю. Іохов, І.В. Кузьминич, О.М. Горбов, О.О. Казіміров, О.М. Орлов, С.А. Горєлишев та інші – № держреєстрації 0112U000529. – Х.: Академія внутрішніх військ, 2012. – 175 с.

5. Іохов О.Ю. Основні аспекти радіоелектронного захисту системи радіозв'язку тактичної ланки управління внутрішніх військ МВС України під час виконання завдань за призначенням в умовах міста[Текст] / О.Ю. Іохов, В.В. Антонець, О.М. Горбов, І.В. Кузьминич, В.В. Овчаренко // Честь і закон. – Х. : Акад. ВВ МВС України, 2012. - № 4. – С. 40-47.

6. Пат. РФ №2114513, МПК (2006. 01) H04K 3/00. Способ защиты информационного обмена в локальной системе радиосвязи/ Опубл. 27.06.1998 [Электронный ресурс]. – Режим доступа: http://www.freepatent.ru.

7. Левин В.Н. Концептуальная основа информационной безопасности компьютерных сетей, технология электронных коммуникаций [Текст]/ В.Н. Левин, Д.М. Платонов, Ю.А. Тимофеев// Информационная безопасность компьютерных сетей. – Т. 45. – М.: Экотрендз, 1993. – С. 5-43.

8. Пат. України №104505 на корисну модель, МПК (2015.01) H04B 7/00. Спосіб захисту інформаційного обміну в локальній системі радіозв'язку/ Опубл. 10.02.2016, Бюл. №3.

9. Пат. України №95314 на корисну модель, МПК (2015.01) H04B 7/00. Антенний пристрій/ Опубл. 25.12.2014, Бюл. №24.

10. Кочержевский Г.И. Антенно-фидерные устройства [Текст]/ Г.И. Кочержевский. – М.: Связь, 1972. – 472 с.

11. Пат. РФ №2288528, МПК (2006. 01) H01 Q19/13. Уголковая антенна с повышенным коэффициентом направленного действия/ Опубл. 27.11.2006/ [Електронний ресурс]. – Режим доступу: http://www.freepatent.ru.

12. Пат. України на корисну модель №105732, МПК (2016. 01) H01Q 19/00, 9/00. Антенний пристрій/ Опубл. 11.04.2016, бюл. №7.

Надано до редколегії 24.12.2016

Рецензент: д-р техн. наук, проф. О.О. Морозов, Національна академія Національної гвардії України. Харків.

РАДИОМАСКИРОВКА ВОЕННЫХ ПОДРАЗДЕЛЕНИЙ В УСЛОВИЯХ ПРИМЕНЕНИЯ ШТАТНЫХ И ИМПРОВИЗИРОВАНЫХ СРЕДСТВ

А.Ю. Иохов, В.Є. Козлов, В.Г. Малюк, К.Н. Ткаченко, Н.Д., Ткаченко

В статье рассмотрены способ комплексного применения мер активной радиомаскировки с использованием специальных средств радиоэлектронного подавления, который может быть использован для построения локальных систем радиосвязи, предназначенных для обмена конфиденциальной информацией в диапазоне ультракоротких волн в условиях искусственных радиопомех и попыток несанкционированного доступа к передаваемой информации.

Ключевые слова: *система радиосвязи, активная радиомаскировка, разведзащищенность, ультракороткие волны.*

DECEPTION MILITARY UNITS THE CONDITIONS OF APPLICATION OF STANDARD AND IMPROVISED MEANS

A.Yu. Iohov, V.Ye. Kozlov, V.H. Maluk, K.N. Tkachenko, N.D. Tkachenko

The article describes the method of complex application of the active radio camouflage measures using special jamming devices. The method can be used to build a local radio communication systems for the exchange of confidential information in the VHF range in terms of artificial interference and unauthorized access to the transmitted information.

Keywords: *radio communication system, active deception, intelligence as protected, VHF.*