РОЗДІЛ 12
ВІЙСЬКОВЕ ПРАВО

УДК 356/358
DOI https://doi.org/10.32782/2524-0374/2024-12/102

АНАЛІЗ ТА УЗАГАЛЬНЕННЯ ДОСВІДУ ЗАБЕЗПЕЧЕННЯ РАДІОЕЛЕКТРОННОГО ЗАХИСТУ СИСТЕМ ЗВ'ЯЗКУ ТА ПРОТИДІЇ РАДІОЕЛЕКТРОННІЙ РОЗВІДЦІ ПРОТИВНИКА ОРГАНАМИ УПРАВЛІННЯ ЗВ'ЯЗКОМ І ПІДРОЗДІЛАМИ ЗВ'ЯЗКУ ЗБРОЙНИХ СИЛ УКРАЇНИ, ІНШИХ ВІЙСЬКОВИХ ФОРМУВАНЬ ТА ПРАВООХОРОННИХ ОРГАНІВ

ANALYSIS AND GENERALIZATION OF THE EXPERIENCE OF PROVIDING RADIO-ELECTRONIC PROTECTION OFCOMMUNICATION SYSTEMS AND ANTI-RADIO-ELECTRONIC INTELLIGENCE OF THE ADVERSARY BY COMMUNICATION MANAGEMENT BODIES AND COMMUNICATION UNITS OF THE ARMED FORCES OF UKRAINE, OTHERS MILITARYFORMS AND LAW ENFORCEMENT BODIES

Зміївський Г.А., викладач кафедри загальновійськових дисциплін
Військово-юридичний інститут
Національного юридичного університету імені Ярослава Мудрого

Пугач В.В., викладач кафедри загальновійськових дисциплін
Військово-юридичний інститут
Національного юридичного університету імені Ярослава Мудрого

Власов К.В., старший викладач кафедри військового зв'язку та інформатизації
Командно-штабний факультет
Національної академії Національної гвардії України

Горбунов В.І., старший викладач кафедри підготовки офіцерів запасу
Військово-юридичний інститут
Національного юридичного університету імені Ярослава Мудрого

Стаття присвячена аналізу та узагальненню досвіду забезпечення радіоелектронного захисту систем зв'язку та протидії радіоелектронній розвідці противника органами управління зв'язком і підрозділами зв'язку Збройних Сил України, інших військових формувань та правоохоронних органів в ході участі в Операції об'єднаних сил (раніше антитерористичній операції) на території Донецької та Луганської областей, російсько-Українській війні з метою ефективного використання цього досвіду в процесі планування і забезпечення зв'язку.

Наведено дані щодо підвищення активності використання збройними силами російської федерації раідоелектронної боротьби у ході широкомасштабного вторгнення, розширення можливостей засобів радіоелектронної боротьби щодо радіорозвідки та радіоподавлення інтегральних систем зв'язку і передачі даних колективного користування, збільшення вірогідності селекції об'єктів подавлення та розмірів зони ефективної дії, блокування абонентських терміналів стільникового зв'язку, а також скорочення часу реакції.

На основі проведеного аналізу для узагальнення (систематизації) отриманого досвіду запропоновано класифікувати заходи радіоелектронного захисту систем зв'язку та протидії радіоелектронній розвідці противника за ознаками впливу радіоелектронної боротьби, радіоелектронної розвідки та засобів вогневого ураження на систему зв'язку: зменшення ймовірності виявлення джерел радіовипромінювання; забезпечення стійкої роботи засобів радіозв'язку в умовах навмисних радіоперешкод; зменшення ймовірності вогневого ураження засобів зв'язку; зниження можливостей радіоелектронної розвідки противника з радіоперехоплення.

Здійснено розподіл основних заходів захисту і протидії, які аналізувалися, за ознаками запропонованої класифікації. Обґрунтовано проведення саме такого розподілу.

Установлено, що така класифікація буде сприяти забезпеченню єдиних підходів до організації заходів захисту і протидії та підвищить ефективність впровадження отриманого бойового досвіду в процес планування і забезпечення зв'язку.

Ключові слова: система зв'язку, радіоелектронна боротьба, радіоелектронна розвідка, радіоелектронний захист, радіоелектронне виявлення, радіоелектронне подавлення, перехоплення.

The article is devoted to the analysis and generalization of the experience of providing radio-electronic protection of communication systems and countering the enemy's radio-electronic intelligence by communication control bodies and communication units of the Armed Forces of Ukraine, other military formations and law enforcement agencies during the participation in the Joint Forces Operation (formerly the anti-terrorist operations) on the territory of Donetsk and Luhansk regions, the Russian-Ukrainian war in order to effectively use this experience in the process of planning and ensuring communication.

Data are given on the increase in the activity of the use of radio-electronic warfare by the armed forces of the Russian Federation during a large-scale invasion, the expansion of the capabilities of radio-electronic warfare in relation to radio reconnaissance and radio suppression of integrated systems of communication and data transmission of collective use, an increase in the probability of the selection of suppression objects and the size of the zone of effective action. blocking of subscriber terminals of cellular communication, as well as reduction of reaction time.

On the basis of the conducted analysis, in order to generalize (systematize) the experience gained, it is proposed to classify the measures of radio-electronic protection of communication systems and countermeasures against the enemy's radio-electronic intelligence according to the signs of the effect of radio-electronic warfare, radio-electronic intelligence, and means of fire damage on the communication system: reducing the probability of detecting sources of radio radiation; ensuring stable operation of radio communications in conditions of intentional radio interference; reducing the probability of fire damage to communication equipment; reduction of the enemy's radio-electronic intelligence from radio interception.

The distribution of the main measures of protection and countermeasures, which were analyzed, was carried out according to the features of the proposed classification. Such distribution is justified.

It has been established that such a classification will contribute to the provision of uniform approaches to the organization of protection and countermeasures and will increase the effectiveness of the implementation of the acquired combat experience in the process of planning and ensuring communication.

Key words: communication system, radio-electronic warfare, radio-electronic reconnaissance, radio-electronic protection, radio-electronic detection, radio-electronic suppression, interception.

Постановка проблеми у загальному вигляді. Воєнна доктрина росії передбачає активне використання раідоелектронної боротьби (РЕБ) у різних видах воєнних конфліктів, що підтверджується широким спектром розроблених та впроваджених систем, а також досвідом їх використання у збройних конфліктах на Північному Кавказі, в Грузії, Сирії та російсько-Українській війні.

За оцінками військових експертів [1], нові засоби РЕБ російської федерації дозволяють забезпечити можливість радіорозвідки та радіоподавлення інтегральних систем зв'язку та передачі даних колективного користування та в 1,5–1,8 рази збільшити вірогідність селекції об'єктів подавлення, скоротити час реакції в 10 разів. Крім того, вони здатні забезпечити приховане, вибіркове за місцем і (або) системною адресою блокування абонентських терміналів стільникового зв'язку та збільшити розмір зони ефективної дії завдяки застосуванню нетрадиційних (неенергетичних) способів інтелектуального блокування абонентських терміналів зв'язку.

У свою чергу росією здійснюються заходи з розширення можливостей і наземної радіоелектронної розвідки (РЕР).

Під час виконання завдань за призначенням в Операції об'єднаних сил (раніше антитерористичній операції) на території Донецької та Луганської областей, російсько-Українській війні органи управління зв'язком і підрозділи зв'язку Збройних Сил України, інших військових формувань та правоохоронних органів отримали самий різноманітний досвід забезпечення стійкої роботи зв'язку в умовах впливу засобів радіоелектронної боротьби та радіоелектронної розвідки противника. Але для ефективного впровадження цього досвіду в процес планування і забезпечення зв'язку виникає необхідність його систематизації і виробленні єдиних підходів до організації заходів захисту і протидії.

Отже, **метою статті є** проведення аналізу та узагальнення досвіду забезпечення радіоелектронного захисту систем зв'язку та протидії радіоелектронній розвідці противника органами управління зв'язком і підрозділами зв'язку в ході участі в Операції об'єднаних сил (раніше антитерористичній операції) на території Донецької та Луганської областей, російсько-Українській війні для ефективного використання в процесі планування і забезпечення зв'язку.

Виклад основного матеріалу. Для узагальнення і систематизації отриманого досвіду доцільно провести класифікацію заходів забезпечення радіоелектронного захисту систем зв'язку та протидії радіоелектронній розвідці противника. Ознаками ж для класифікації, на думку авторів, мають стати завдання РЕБ і РЕР щодо впливу на систему зв'язку, виходячи із їх визначень.

Радіоелектронна боротьба – сукупність узгоджених за метою, завданням, місцем і часом дій військ (сил) щодо виявлення систем і засобів управління військами та зброєю противника, їх радіоелектронного подавлення, радіоелектронного захисту своїх систем і засобів управління, а також виконання заходів електронної підтримки радіоелектронної боротьби [2].

Радіоелектронна розвідка здійснюється з метою добування, обробки, аналізу, узагальнення і доведення розвідувальної інформації про противника шляхом виявлення (пеленгування), перехоплення та аналізу випромінювань його радіоелектронних засобів [3].

У загальному вигляді процес впливу РЕБ, РЕР та засобів вогневого ураження на систему зв'язку та інформаційних систем, а також запропоновану класифікацію заходів радіоелектронного захисту та протидії радіоелектронній розвідці противника на основі цього впливу відображено на рис. 1.

Отже, виходячи зі змісту визначень, першим завданням як РЕБ, так і РЕР є *радіоелектронне виявлення (пелен-*

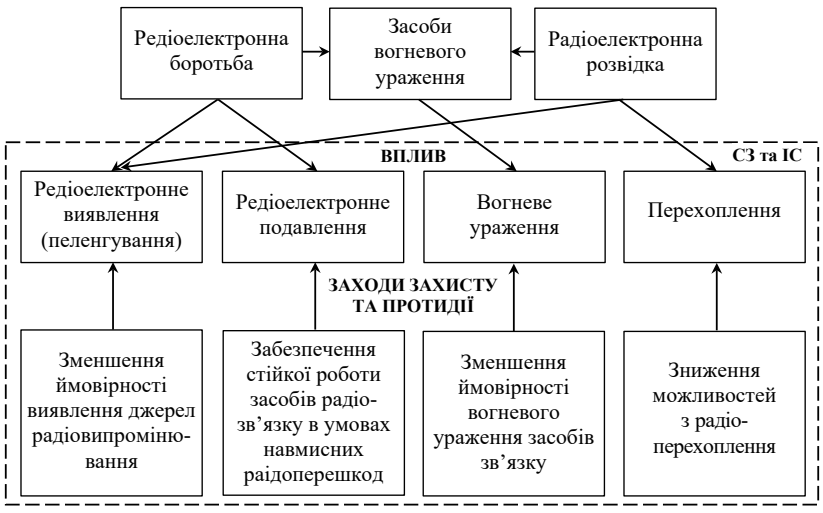

Рис. 1. Класифікація заходів радіоелектронного захисту системи зв'язку та протидії радіоелектронній розвідці противника

гування). Відповідно, першою ознакою для класифікації має стати зменшення ймовірності виявлення джерел радіовипромінювання (рис. 1).

Виявлення радіовипромінювального засобу залежить від перевищення рівня сигналу над реальною чутливістю приймача радіоелектронної розвідки та інших факторів, пов'язаних із забезпеченням розвідзахищеності системи зв'язку. Виходячи з цього, *для зменшення ймовірності виявлення джерел радіовипромінювання* здійснюються (дотримуються) такі основні заходи (правила) [1; 4–6]:

– відведення переваги для передавання важливої інформації проводовим засобам зв'язку;

– скорочення часу роботи випромінювальних засобів на передачу;

– використання режимів роботи засобів радіозв'язку на мінімальній потужності;

– використання для радіопередач малопомітних засобів радіозв'язку (малої потужності, зі широкосмуговими сигналами);

– спрямовування антен так, щоб найбільші промені (пелюстки) на діаграмі спрямованості перекривали лише саме необхідний сектор фронту або кореспондента;

– використання спрямованих антен або встановлення металевих відбивачів (рефлекторів) зі сторони антени в напрямку противника;

– екранування (за можливості) за допомогою огороджувальних конструкцій зі струмопровідного матеріалу («клітка Фарадея») для радіоізоляції антени в певному напрямку;

– використання природних та штучних перешкод поширенню радіохвиль (геометрії місцевості, будівель та ін.), які обмежують потенційні дії засобів РЕБ противника (при цьому перешкода повинна розташовуватися між радіозасобом і лінією фронту);

– розміщення УКХ антен всередині будівель чи споруд або за перепадами рельєфу так, щоб вони були прикриті зі сторони потенційних дій РЕБ або радіорозвідки противника;

– використання замість Wi-Fi точок доступу ETHERNET та USB адаптерів для пристроїв без ETHERNET виходів;

– недопущення скупчення абонентів радіосистем (радіо-, стільниковий зв'язок, Wi-Fi та ін.) на невеликій території;

– розміщення точок радіодоступу (Wi-Fi та ін.) у захищених (екранованих) приміщеннях;

– мінімізація користування стільниковими телефонами, в крайньому випаду використання їх тільки в режимі польоту та через модем 4G (роутер) установлений у захищених (екранованих) приміщеннях (Wi-Fi);

– періодична зміна робочих частот (каналів);

– використання станцій-приманок.

Другим завданням РЕБ противника є *радіоелектронне подавлення*, яке полягає у дезорганізації роботи радіо-, радіорелейних, тропосферних та космічних систем і засобів зв'язку, систем і засобів радіолокації, радіонавігації та радіоуправління шляхом впливу радіоперешкодами, застосування хибних цілей та пасток, зміни умов поширення радіохвиль. Радіоподавлення, як складова частина радіелектронного подавлення, включає також передачу повідомлень, команд і сигналів, що дезінформують, у радіомережах (радіонапрямках) [2].

Відповідно, ознакою для класифікації має стати забезпечення стійкої роботи зв'язку та інформаційних систем в умовах навмисних радіоперешкод противника, що є одним із завданням радіоелектронного захисту системи зв'язку [4].

З метою *забезпечення стійкої роботи засобів радіозв'язку в умовах навмисних радіоперешкод противника* виконуються такі основні заходи (правила) [1; 4–6]:

– здійснення групового методу призначення частот та маневру ними;

– проведення аналізу робочого спектру завади, її характеру;

– здійснення переходу на інші робочі частоти (наприклад, на частоти, які знаходяться поза межами або на краю спектра радіоперешкоди);

– завчасне програмування резервних каналів зв'язку на радіостанціях та проведення навчання з оперативного переходу на резервні частоти;

– передавання одного і того ж повідомлення на декількох частотах одночасно;

– проведення зміни поляризації сигналу, а у разі відсутності технічної можливості зробити це – повертання антени в напрямку кореспондента на 90 градусів;

– використання антен спрямованої дії;

– забезпечення під час використання ретранслятора в комплексі з дуплексером наявність другого (резервного), а за можливості – й третього дуплексера, налаштованого на інші частоти;

– передбачення при плануванні зв'язку в підрозділі резервних каналів – тобто радіостанцій (каналів) на інших діапазонах частот та додаткових ретрансляторів, розгорнутих в прихованих локаціях, які активуються у випадку подавлення або знищення основного;

– застосування радіостанцій з нестандартним діапазоном частот, наприклад HIMERA, які працюють на частотах 900 МГц, що зменшує ризики подавлення стандартними засобами;

– організація зв'язку на радіостанціях, які можуть працювати в якості ретранслятора (таж HIMERA), що дозволяє швидко розширити покриття радіомережі без використання дорогих засобів транкінгового зв'язку;

– використання аналогових радіостанцій замість цифрових;

– використання радіозасобів, що працюють за технологією псевдовипадкового перелаштування робочої частоти (military grade радіостанції такі як Harris, Aselsan, HIMERA);

– диверсифікація зв'язку різних ланок управління з відведення переваги більш стійкому та надійному зв'язку (наприклад, супутниковому зв'язку по типу STARLINK) але і забезпечивши більш універсальними та стандартними засобами;

– скорочення інтервалів на радіорелейних і тропосферних лініях зв'язку;

– проведення в процесі планування зв'язку розвідки та виявлення навмисних і ненавмисних перешкод безпосередньо на місцевості за допомогою аналізаторів спектру та інших засобів РЕР і вживання відповідних заходів для їх уникнення;

– використання даних моніторингу та обробки підрозділами РЕР Збройних Сил України інформації щодо електромагнітної обстановки на лінії зіткнення, яка включно із потенційними районами застосування засобів РЕБ противника з'являється у відповідних шарах системи ситуаційної обізнаності DELTA, для прийняття рішення про застосування того чи іншого обладнання та засобів зв'язку а також про заходи, які можна вжити для нейтралізації впливу РЕБ противника.

Виходячи з того, що заходи радіоелектронного подавлення проводяться у поєднанні з *вогневим ураженням та захопленням* (виведенням з ладу) пунктів управління і радіоелектронних об'єктів, наступною ознакою для класифікації досвіду повинен бути захист від вогневого ураження засобів зв'язку як складова частина радіоелектронного захисту.

Для *зменшення ймовірності вогневого ураження засобів зв'язку*, у тому числі і самонавідною (на випромінення) зброєю, передбачається здійснення (дотримання) таких основних заходів (правил) [1; 4–6]:

– недопущення скупчення будь-яких одночасно працюючих на передачу радіовипромінюючих засобів на маленькій площі;

– використання об'єктів випромінювань, що відволікають;

– регламентування роботи радіоелектронних засобів за часом, територією й частотами;

– раціональний вибір напрямків розгортання ліній зв'язку, які виключають (знижують до мінімуму) випромінювання в бік противника;

– вибір позицій радіо-, транкінгових, радіорелейних, тропосферних станцій і станцій супутникового зв'язку на місцевості з урахуванням її маскувальних і захисних властивостей та їх інженерне обладнання;

– винесення радіостанцій, ретрансляторів та антен за межі пунктів управління та місць розташування особового складу;

– використання дистанційного управління радіозасобами по дротах на максимально допустимій дистанції;

– організація взаємодії із сусідніми підрозділами, підрозділами розвідки та РЕБ для обміну інформацією щодо застосування противником засобів вогневого ураження та РЕБ;

– організація постійного візуального та радіомоніторингу бойової та електромагнітної обстановки на лінії зіткнення (у зоні відповідальності).

У зв'язку з тим, що одним із основних способів ведення радіоелектронної розвідки з метою добування розвідувальної інформації є *перехоплення*, наступною ознакою для класифікації має стати зниження можливостей противника щодо його здійснення.

Основними заходами (правилами) щодо *зниження можливостей радіоелектронної розвідки противника з радіоперехоплення* є [1; 4–6]:

– зміна радіоданих при кожній зміні районів зосередження підрозділів і переміщенні пунктів управління

– приховування інтенсивності, важливості, часу і характеру передавання оперативної інформації шляхом застосування маскувального обміну та стабільної і рівної інтенсивності переговорів перед проведенням важливих заходів;

– суворе дотримання правил ведення зв'язку і користування апаратурою засекречування;

– уникнення перевірок радіозв'язку за щоденними графіками та за однією черговістю;

– дотримання однакової довжини радіопередачі як радіостанціями командирів, так і радіостанціями підлеглих;

– планування при організації радіозв'язку радіомереж з невеликою кількістю кореспондентів;

– забезпечення спеціального захисту технічних засобів обробки, передачі і зберігання інформації;

– використання для радіообміну по відкритих радіоканалах та каналах цифрових систем транкінгового зв'язку (стандарти шифрування DMR, ARC4, AES 256) документів прихованого управління військами, кодованих карт;

– організація передачі в радіомережах (розмовних групах) на радіостанціях системи транкінгового зв'язку MOTOTRBO ID радіостанції тільки у зашифрованому вигляді, періодичної зміни ID або переходу на один ID, виключення при формуванні ID нумерації військовослужбовців, підрозділів по черзі (штату).

Висновки. Таким чином, на основі проведеного аналізу досвіду, з метою його узагальнення та систематизації запропоновано класифікувати заходи радіоелектронного захисту системи зв'язку та протидії технічним засобам розвідки противника за ознаками впливу РЕБ, РЕР та засобів вогневого ураження на систему зв'язку: зменшення ймовірності виявлення джерел радіовипромінювання; забезпечення стійкої роботи засобів радіозв'язку в умовах навмисних радіоперешкод; зменшення ймовірності вогневого ураження засобів зв'язку; зниження можливостей радіоелектронної розвідки противника з радіоперехоплення.

Такий підхід до класифікації заходів радіоелектронного захисту системи зв'язку та протидії технічним засобам розвідки противника дозволить більш ефективно використовувати отриманий бойовий досвід у процесі планування і забезпечення зв'язку.

ЛІТЕРАТУРА

1. Довідник військового зв'язківця. Засоби радіоелектронної боротьби та розвідки, які використовуються російською федерацією» : військова навчально-методична публікація військовим організаційним структурам, ВВНЗ, НЦ, ЦПП, школам ЗС України та іншим складовими сил оборони України з практичного використання під час підготовки та застосування. Київ : Командування військ зв'язку та кібербезпеки Збройних Сил України спільно з Військовим інститутом телекомунікацій та інформатизації імені Героїв Крут, 2024. 68 с.

2. Бойовий статут Сухопутних військ «Радіоелектронна боротьба Сухопутних військ Збройних Сил України» : бойова публікація військовим організаційним структурам з порядку організації та забезпечення РЕБ. Київ : Командування Сухопутних військ Збройних Сил України, 2021. 196 с.

3. Бойовий статут Сухопутних військ «Розвідка Сухопутних військ та Десантно-штурмових військ Збройних Сил України» : бойова публікація військовим організаційним структурам з порядку організації та забезпечення РЕБ. Київ : Розвідувальне управління Командування Сухопутних військ Збройних Сил України, 2021. 208 с.

4. Настанова «Тактичний зв'язок» : військова керівна деталізована публікація військовим організаційним структурам зв'язку в Збройних Силах України. Київ : Командування військ зв'язку та кібербезпеки Збройних Сил України, 2020. 64 с.

5. Захист каналів від впливу РЕБ (для підрозділів зв'язку та БпЛА). *Sprotyv G7* : Офіційний веб-сайт Сил територіальної оборони України. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://sprotyvg7.com.ua/wp-content/uploads/2024/02/%D0%97%D0%90%D0%A5%D0%98%D0%A1%D0%A2_%D0%9A%D0%90%D0%9D%D0%90%D0%9B%D0%86%D0%92_%D0%97%D0%92%D0%AF%D0%97%D0%9A%D0%A3_%D0%92%D0%86%D0%94_%D0%92%D0%9F%D0%9B%D0%98%D0%92%D0%A3_%D0%A0%D0%95%D0%91.pdf (дата звернення: 04.12.2024).

6. Флеш Сергій. Яку небезпеку становить радіоелектронна розвідка противника. *ArmyInform* : веб-сайт. URL: https://armyinform.com.ua/2023/05/31/yaku-nebezpeku-stanovyt-radioelektronna-rozvidka-protyvnyka/ (дата звернення: 04.12.2024).