УДК: 621.396:623.4.02:355.4

А.В. Колесник, Ю. В. Георгієв

ВАРІАНТИ РЕАЛІЗАЦІЇ ЗАХИСТУ РАДІОЛОКАЦІЙНИХ СТАНЦІЙ ВІД ПОТЕНЦІЙНОГО ПРОТИВНИКА В УМОВАХ ВІЙСЬКОВИХ ДІЙ

Анотація: д*ослідження та аналіз варіантів реалізації захисту радіолокаційних станцій (РЛС) від впливу потенційного противника в умовах ведення військових дій є запорукою успішного виконання поставлених військових завдань. Особлива увага приділена методам забезпечення стійкості та надійності РЛС у складних бойових умовах, а також засобам активного та пасивного захисту. Розглянуто основні загрози, пов'язані з впливом засобів радіоелектронної боротьби (РЕБ), та запропоновані можливі контрзаходи для зниження їх ефективності. Аналізуються сучасні технології маскування та укриття, системи самозахисту РЛС.*

Ключові слова: *захист РЛС, засоби активного та пасивного захисту, повітряний противник, протиповітряна оборона.*

Abstracts: *The study and analysis of options for the protection of radar stations (RS) from the influence of a potential enemy in the conditions of military operations is a guarantee of successful fulfilment of military tasks. Particular attention is paid to the methods of ensuring the stability and reliability of radars in difficult combat conditions, as well as to the means of active and passive protection. The main threats associated with the impact of electronic warfare (EW) are considered, and possible countermeasures to reduce their effectiveness are proposed. Modern technologies of camouflage and concealment, as well as radar self-defence systems are analysed.*

Keywords: *radar defence, active and passive defence means, air enemy, air defence*.

Вступ

Одним із ключових елементів систем протиповітряної оборони (ППО) та розвідки, які використовуються для виявлення, відстеження і класифікації повітряних, наземних і об'єктів. В умовах військових дій ефективність РЛС стає вирішальною, тому забезпечення їх захисту є критичним завданням. Однак, радіолокаційні системи піддаються значним загрозам з боку засобів радіоелектронної боротьби (РЕБ), протирадарних ракет, а також фізичних атак. У цій статті розглядаються основні варіанти захисту РЛС, які можна реалізувати в умовах сучасного конфлікту. [1, 2].

Основна частина

Через важливість ефективному веденні бойових дій РЛС стають мішенню для засобів ураження противника, таких як ракети, авіація або електронні системи боротьби. Для забезпечення їх захисту застосовують як активні, так і пасивні засоби [1, 2]. Розглянемо спочатку пасивні засоби захисту, які є критично важливими для зниження вразливості РЛС без активного застосування зброї чи засобів придушення, до яких можна віднести:

Маскування та розосередження. Один із ключових пасивних засобів захисту радіолокаційних станцій – це використання маскування та розосередження. Розміщення РЛС в природних укриттях, таких як лісові масиви, гірські райони або штучні споруди, може значно зменшити ризик їх виявлення противником. Крім того, розосередження кількох РЛС на великій відстані одна від одної дозволяє знизити ефективність масованих ударів. Маскування РЛС може включати використання камуфляжних сіток

або спеціальних матеріалів, що поглинають радіовипромінювання. Таким чином, зменшується ефективність ворожих систем виявлення та наведення зброї.

Поглинальні покриття. Для зменшення радіолокаційної помітності РЛС застосовуються спеціальні матеріали, що поглинають електромагнітні хвилі. Це дозволяє значно зменшити відбитий сигнал, що ускладнює виявлення станції ворожими радарами. Такі покриття можуть бути нанесені як на саму антену, так і на допоміжні елементи інфраструктури. Поглинальні матеріали на основі метаматеріалів або радіопоглинаючих полімерів є одним з сучасних напрямів розвитку в цій сфері.

Використання відбивачів та приманок. Ще одним ефективним пасивним засобом захисту є використання відбивачів та приманок. Відбивачі здатні створювати хибні сигнали, які імітують реальні РЛС або інші об'єкти, відволікаючи на себе ворожі засоби ураження. Приманки можуть бути наземними чи повітряними і використовуються для імітації роботи справжніх станцій. Таким чином, противник витрачає свої ресурси на хибні цілі, залишаючи основні об'єкти непошкодженими.

Використання укриттів та мобільність. Стаціонарні РЛС часто використовують спеціально підготовлені укриття або бункери, що захищають їх від ударів. Ці споруди здатні витримувати удари високоточної зброї або артилерійські обстріли. Укриття також можуть бути обладнані системами охолодження для зниження теплового сліду, що робить станцію менш вразливою для теплових або інфрачервоних засобів наведення.

Мобільні РЛС мають перевагу в тому, що можуть швидко змінювати своє розташування, знижуючи ризик їх ураження. Швидке розгортання і згортання мобільних комплексів дозволяє уникати попадання під удари після виявлення. Зміна позицій також ускладнює противнику здійснення ефективного планування атаки.

Радіотехнічне маскування. Цей метод включає зниження інтенсивності випромінювання РЛС або його тимчасове вимкнення, щоб уникнути виявлення противником. Окрім того, можливе використання режимів роботи, які зменшують відбиток радіолокаційного сигналу або змінюють його частотний діапазон, що ускладнює роботу засобів радіоелектронної боротьби противника. Важливим є також використання радіолокаційних станцій з низьким енергоспоживанням, що робить їх менш помітними.

Захист від електромагнітного імпульсу (ЕМІ). Електромагнітні імпульси, створювані в результаті ядерного вибуху або спеціальних засобів ЕМ-випромінювання, можуть вивести з ладу електронні системи РЛС. Для захисту від цього застосовуються спеціальні екрани, фільтри та заземлення, які знижують вплив ЕМІ на електроніку. Ефективне захист від ЕМІ є важливим для збереження працездатності РЛС у складних бойових умовах.

Одним з основних методів активного захисту РЛС є використання перешкод, що викликають радіоелектронні збої в роботі засобів ураження противника [2, 3].

Активне радіоелектронне заглушення: спеціальні системи створюють радіочастотні сигнали, які перекривають або спотворюють радіосигнали противника. Це робить виявлення та наведення на ціль менш точними або неможливими.

Засоби постановки перешкод: системи, що генерують штучні сигнали на тих самих частотах, що й радіолокаційна станція противника, заважають її роботі. Такі системи можуть працювати як з власними, так і з сторонніми РЛС, щоб забезпечити широке покриття.

Зміна робочих частот і адаптивні системи: змінюючи частоту роботи РЛС, можна уникнути виявлення або заглушення її роботи засобами противника. Ця техніка відома як «частотна гнучкість» і дозволяє станції оперативно перемикатися між різними частотними діапазонами, коли противник намагається створити перешкоди на певному

діапазоні. Деякі сучасні РЛС оснащені «адаптивними системами», які здатні аналізувати спектр і автоматично вибирати найменш загрозливу частоту для роботи.

Хибні цілі та дезінформація: ефективним методом захисту є створення хибних радіолокаційних відображень або «імітацій». Такі системи вводять противника в оману щодо місцезнаходження реальної РЛС або об'єктів, що захищаються. Це може бути реалізовано за допомогою декількох варіантів, таких як: хибні передавачі та активних ретрансляторів. Перші в свою чергу створюють додаткові сигнали, що імітують роботу справжньої РЛС. Другі – це спеціальні прилади, які відображають радіолокаційні хвилі таким чином, що створюється враження наявності додаткових об'єктів. Ці методи спрямовані на те щоб противник витрачав свої ресурси і час на ураження несправжніх цілей, знижуючи ймовірність знищення реальної РЛС.

Окремо слід відзначити, що розвиток кіберзагроз змушує приділяти увагу захисту програмного забезпечення РЛС [4]. Засоби кіберзахисту включають в себе ряд заходів, зокрема: шифрування даних, для запобігання доступу до конфіденційної інформації; захист від зламу – це впровадження протоколів безпеки, що унеможливлюють злам системи і використання її вразливостей для виведення РЛС з ладу.

Висновки

Пасивні та активні засоби захисту радіолокаційних станцій є невід'ємною складовою їх безпеки на полі бою. Використання маскування, поглинальних матеріалів, приманок, укриттів та радіотехнічного маскування дозволяє значно зменшити ймовірність ураження РЛС противником. Поєднання методів радіоелектронної боротьби, частотної гнучкості, створення хибних цілей, фізичного захисту та кібербезпеки дозволяє забезпечити надійну роботу РЛС і зменшити ризик їх ураження противником Сучасні технології продовжують вдосконалювати ці методи, роблячи радіолокаційні системи більш стійкими до зовнішніх загроз та зберігаючи їхню ефективність у бойових умовах.

Список використаних джерел:

1. Гризо А. А., Костиря О. О., Лісогорський Б. А., Ткаченко В. І. Аналіз характеристик та оцінка ефективності застосування потенційних засобів вогневого ураження елементів системи протиповітряної оборони у російсько-українській війні. Наука і техніка Повітряних Сил Збройних Сил України. 2023. № 1 (50). С. 70-81. https://doi.org/10.30748/nitps.2023.50.08.

2. Олійник В. В., Данилюк І. А., Оцінювання важливості об’єктів противника в ході планування рейдових дій з використанням методу аналізу ієрархії. Сучасні інформаційні технології у сфері безпеки та оборони. Київ, 2020. Вип.2 (38). С. 107–112. DOI: 10.33099/2311-7249/2020-38-2-107-112.

3. Толюпа С.В., Дружинін В. А., Наконечний В.С., Цьопа Н.В., Батрак Є.О. Методи та алгоритми обробки радіолокаційної інформації у багатопозиційних системах зі змінною просторовою конфігурацією / Толюпа С.В., Дружинін В. А., Наконечний В.С., Цьопа Н.В., Батрак Є.О. - К.: Логос, 2014. – 230 с. ISBN978-966-171-860-8.

4. Вплив штучного інтелекту на стратегії захисту інформаційних систем від нових типів кіберзагроз. (2024). Herald of Khmelnytskyi National University. Technical Sciences, 337(3(2), 366-372. https://doi.org/10.31891/2307-5732-2024-337-55

Колесник Андрій Вікторович **–** аспірант кафедри будівництва, міського господарства та архітектури; Вінницький національний технічний університет, Вінниця, e-mail: andrey.enginer@gmail.com.

Георгієв Юрій Вікторович – старший викладач кафедри авіаційного обладнання літаків і вертольотів, Харківський національний університет Повітряних Сил імені І. М. Кожедуба, м. Харків, e-mail: yura.georgiev.74@ukr.net

Kolesnik Andrii V. - PhD student of the Department of Civil Engineering, Municipal Economy and Architecture; Vinnytsia National Technical University, Vinnytsia, e-mail: andrey.enginer@gmail.com

Yuriy Viktorovych Georgiev *– senior lecturer at the Department of Aircraft and Helicopter Aviation Equipment, I.M. Kozhedub Kharkiv National University of the Air Force, Kharkiv, e-mail: yura.georgiev.74@ukr.net*