ЗМІСТ

РОЗДІЛ 3. ВОЄННІ ПРАКТИКИ КРИПТОСИСТЕМИ ВІЙСЬК РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ УКРАЇНИ

ПЕРЕДМОВА

Написання цього навчального посібнику є справою честі та відданості у житті для одного із авторів, що є воєнною людиною у сфері практичної радіоелектроніки. Не випадково, що цей автор із екзистенційних та логічних уподобань ще в ранньому дитинстві мріяв бути воєнним пілотом, жадібно притуляючи радіоприймач до голови та досить уважно слухаючи програму: «Польова пошта» на замовлення слухачів. Особливо любив автор слухати повідомлення про такі вищі військові навчальні заклади на той час в Україні як: «Чернігівське Вище Військове Льотне училище» та «Житомирське Вище Військове училище Радіоелектроніки». Так. Цей автор нелегко здійснив свою мрію, пройшовши тернистий шлях. Проте, здобув, врешті-решт, омріяну професію **воєнного пілота** (зокрема, борт-інженера), навчаючись на той час за спеціальністю: «Прикладна радіоелектроніка: динаміка та аеродинаміка бойового пілотування», а саме: крім навчання у Вінницькому технікумі електронних приладів (1975-1979 рр.), Вінницькому політехнічному інституті (1981 р.) та Київському політехнічному інституті (1982-1987 рр.), успішно навчався у 90-х роках минулого століття – спеціалізованих вищих військових навчальних закладах закритого типу. **Тому і не зрадив мирного неба України.**

Проте, сьогодні російсько-українська війна, на жаль, переходить у довготривалий формат. Для цього і потрібно всім нам негайно згуртовувати інтелектуальний людський ресурс. При цьому, створювати інноваційні ідеї щодо вітчизняного виробництва, насамперед, у криптосистемі військ радіоелектронної боротьби України. Адже це високо-технологічна війна, в якій фундаментальною матрицею є саме кібервійська як квантове програмне забезпечення штучного інтелекту. Це є ефективно діючою

константою у філософії контррадіоелектронної протидії ворожову супротивнику, криптосистемно дезорганізуючи та вводячи в оману такого ворога в квантовому електромагнітному середовищі на всіх ділянках фронту… Перерозподілений геополітичний та геоекономічний світ знову переходить, у нову, циклічно обумовлену, фазу протидії демократії і автократії. Це і є біополярне здійснення філософії як багатогранної формули мудрості щодо інтегративної ідеї Перемоги Добра над Злом.

Від авторів

РОЗДІЛ 1. СПЕЦИФІКА ТА ПРЕДМЕТ КРИПТОСИСТЕМИ ВІЙСЬК РАДІОЕЛЕКТРОННОЇ БОРОТЬБИ УКРАЇНИ

1.1. Сутність криптосистеми військ радіоелектронної боротьби України

Як ніколи, війська радіоелектронної боротьби України під час повномасштабного вторгнення російської агресії 24 лютого 2022 року на нашу рідну землю відіграють надто ключову роль у Захисті мирного неба як дискретна математика війни.

При цьому, варто озвучити сутність військ радіоелектронної боротьби України. Це індивідуальний захист озброєння і військової техніки (зокрема, ракетних комплексів, бойових літаків, гелікоптерів, кораблів, броньованих автомобілів тощо) від ворожого впливу засобів розвідки та його технологічної зброї. За цих обставин, радіоелектронна боротьба – це сукупність узгоджених дій військових сил щодо:

– здобуття інформації про розташування радіоелектронних засобів, систем радіонавігаційного управління військами і зброї противника, їх знищення, захоплення, виведення з ладу, радіоелектронне придушення;

– захисту власних радіоелектронних засобів і систем керування військами та зброєю, від застосованих противником радіоелектронної розвідки і ведення контррадіоелектронної протидії.

Отже, на наш погляд, криптосистема військ радіоелектронної боротьби України є окремою структурною одиницею бойового забезпечення ведення війни, що завдяки її дискретної математики, як фундаментальної матриці, набирає критичних обертів у воєнному середовищі. При цьому, автори, невипадково, у надто

скороченому вигляді подають сутність означеної тематики, оскільки її критеріальна криптосистема саме у воєнних реаліях становить державну таємницю.

1.2. Різновидна характеристика криптосистеми військ радіоелектронної боротьби України

У криптосистемі військ радіоелектронної боротьби України саме під час російсько-української війни варто озвучити різновидну характеристику РЕБ (радіоелектронної боротьби). Із відкритих інформаційних джерел витікає, що РЕБ (англ. electronic warfare) – це сукупність узгоджених щодо мети, завданнями, місцем і часом заходів і дій військ (сил) зі здобування інформації про розташування радіоелектронних засобів (РЕЗ), систем керування військами (силами) і зброї противника, їх знищення всіма видами зброї або захоплення (виведення з ладу) і радіоелектронному придушенню, а також захист власних РЕЗ і систем керування військами та зброєю від радіоелектронної розвідки і радіоелектронної протидії, застосованих противником (контррадіоелектронна протидія); вид бойового забезпечення [8].

Стратегічне значення РЕБ нагально оцінюється як фундаментальний засіб у протиповітряно-оборонному комплексі держав світу. Ці заходи спрямовано проти так званої інфраструктури (командування, керування, зв'язку і розвідки) противника, без якого сучасна війна, не є можливою.

Заходи радіоелектронної боротьби поділяють на:

Електронні заходи підтримки – полягають у пасивному використанні електромагнітного спектра, задля отримання даних про противника та використання їх для прямих тактичних дій. Ця інформація може, наприклад, служити як підґрунтя для застосування артилерійського вогню або ударів з повітря, але також і для

електронної протидії або захисних заходів. Вони також доповнюють збирання сигналів інтелекту (SIGINT) [8].

Радіоелектронну протидію (радіоелектронне придушення) – стосується активного використання електромагнітного спектра, шляхом створення завад (заклинювання) для електронних засобів противника, або введення його в оману. Активні заходи, це зокрема електронні захисні технічні рішення, що стосуються самого передавання (радіоприймачі зі стрибкоподібною перебудовою частоти) або з точки зору переданих даних (криптографічних) [8].

Радіоелектронне (РЕ) придушення розподіляється на:

- дії з тимчасового порушення роботи РЕ апаратури противника (постановка радіоперешкод);
- дії, пов'язані з довготерміновим (або постійним) виведенням з ладу цієї апаратури (силове ураження).

Метою РЕБ є дезорганізація керування силами (військами), зниження дієвості ведення розвідки, використання зброї і бойової техніки противника, а також забезпечення стійкості роботи систем і засобів керування власними військами і зброєю. Завдання РЕ розвідки – виявлення РЕ засобів противника за їх випромінюванням, визначення їх координат, визначення й вивчення характеристик випромінюваних ними сигналів. Ці відомості використовують на користь військової розвідки і під час створення радіоелектронної протидії.

Електромагнітне середовище

Військові операції, які виконуються в інформаційному середовищі з використанням електромагнітного (ЕМ) спектра, все більш ускладнюються. Електромагнітна частина спектра інформаційного середовища, називається електромагнітним середовищем (ЕМЕ).

У межах побудови інформаційної операції, РЕБ (EW) є складовою інформаційної війни; більш конкретно, вона є елементом наступальної та оборонної інформаційної протидії [8].

НАТО має всеосяжний і комплексний підхід до EW. Військовий комітет, з 2007 року ухвалив концептуальний документ (MCM 0142: Трансформація концепції майбутньої радіоелектронної боротьби НАТО) де EME визнається як оперативний простір маневру та ведення бойових дій. У НАТО, радіоелектронна боротьба EW, вважається війною в електромагнітному середовищі (EME). НАТО прийняло спрощену мову, за зразком тієї, яка використовуються в інших середовищах, наприклад, електронна атака є протидійним використанням EM енергії. ED є електронним захистом, і ES – електронне спостереження.

РЕБ, як і будь-які військові дії, пов'язані з використанням EM спектра, передбачають спрямовану енергію (DE) для керування спектром EM, або атаки противника. Це не обмежується радіо- або радарними частотами, а також охоплює: ІЧ, видимий, ультрафіолетовий та інші менш використовувані ділянки EM спектра.

Мета EW полягає у протидії противнику, отриманні переваги у EM спектрі, та забезпеченні власного безперешкодного доступу до частини EM спектра інформаційного середовища. EW може бути застосовано: з повітря, моря, землі, з використанням пілотованих і безпілотних систем. EW використовується для підтримки військових операцій за допомогою різних рівнів виявлення, виведення з ладу, обману, порушення роботи, придушення, захисту та знищення [8].

EW сприяє успіху інформаційних операцій за допомогою наступальних та оборонних тактик і способів у різних поєднаннях з метою створювати, порушувати, і здійснювати змагальне використання спектра EM, захищаючи власну свободу дій у цьому середовищі [8].

Складові частини РЕБ

Радіоелектронна протидія

Радіоелектронна протидія, радіоелектронне придушення (РЕП) – сукупність заходів і дій, спрямованих на порушення

роботи або зниження ефективності бойового застосування радіоелектронних засобів противника шляхом дії на них електромагнітним або акустичним випромінюванням. Складова частина радіоелектронної боротьби [9].

РЕП можна застосовувати проти радіотехнічних засобів (радіолокаційних станцій, радіоліній телеуправління, радіонавігаційних систем, обладнання радіозв'язку, інфрачервоних, оптико-електронних, лазерних, телевізійних та ін. установок.

РЕП радіотехнічним засобам досягається застосуванням навмисних радіоперешкод, зміною характеристик відбитих об'єктами сигналів, створенням удаваних цілей, використанням самонавідних на джерело випромінювання ракет. Робота інфрачервоних установок порушується головним чином за допомогою удаваних цілей і теплового маскування об'єктів (зниженням теплового контрасту між об'єктом та навколишнім середовищем). Для оптико-електронних, лазерних і телевізійних установок застосовуються й розробляються аналогічні засоби РЕП [9].

Апаратура РЕП:

- Р–330 – радянський автоматизований комплекс радіоелектронного придушення;
- «Лиман» – радянський / український наземний мобільний комплекс радіоелектронного придушення ліній наведення авіації;
- БКО «Талісман» – бортовий комплекс оборони для індивідуального захисту бойових літаків від керованої ракетної зброї;
- «Алтаец»;
- «Р–330МР»;
- «Арбалєт МР»;
- «Борісоглєбськ 2» російський багатоцільовий комплекс, використовувався проросійськими формуваннями у війні на Донбасі;
- Артилерійський боєприпас постановки активних завад Starshel (Болгарія) [9].

Історія застосування РЕП

Російсько-українська війна

Російські підрозділи вторгнення користувались засобами радіоелектронної боротьби і придушення в протистоянні з силами українських військ. Так, наприклад, станції РЕБ Р–330Ж «Житєль» були виявлені на озброєнні проросійських сил щонайменше з літа 2014 року. Системи Р–330Ж були також помічені влітку 2015 року. За даними активістів групи ІнформНапалм комплекси Р–330Ж «Житєль» були використані російськими військами під час боїв за Дебальцеве взимку 2015 року. Як встановили активісти ІнформНапалм, станція знаходилась на території пожежної частини №28 міста Горлівки (48.3103372° пн. ш. 38.1189859° сх. д.) орієнтовно в період з 24 січня 2015 до 27 лютого 2015 року, якраз у розпал боїв за місто Дебальцеве, яке потрапляє в 25-ти кілометрову зону дії даної АСП [9].

Були також ідентифіковані комплекси радіоконтролю, пеленгування, та придушення РП–377ЛА «Лорандит», комплекси радіорозвідки та радіопридушення РБ–531Б «Інфауна».

За інформацією Головного управління розвідки Міністерства Оборони України в квітні 2016 року, під час загострення бойових дій навколо Авдіївки, російські бойовики розгорнули біля Макіївки обладнання для радіоелектронної боротьби: станції РЕБ Р–330Ж «Житєль» та комплекс РЕБ «Лєєр–3» [9].

Радіоелектронний захист

Радіоелектронний захист – сукупність заходів і дій військ (сил) із послаблення впливу на свої РЕ об’єкти засобів РЕ ураження противника, захисту від ураження самонавідною (по випроміненню) зброї, захисту від ненавмисних сумісних радіоперешкод і від технічних засобів РЕ розвідки противника, тобто передбачає дії, вжиті для захисту персоналу, об’єктів та обладнання від будь-яких наслідків партнерського або ворожого використання впливу електромагнітного спектра.

Методи радіоелектронного захисту (ECCM) для протидії навмисним перешкодам

Засоби радіоелектронного захисту захищають радіоканали від електронної протидії (ECM), такої як навмисні перешкоди. Метод радіоелектронного захисту, заснований на швидкій перебудові частоти (frequency hopping, FHSS), використовується, наприклад, у всіх радіостанціях R & S ® M3AR, як додаткова можливість. У сімействі R & S ® M3AR застосовуються прийнятий в НАТО метод HAVE QUICK II і новітній метод SATURN, реалізовані відповідно до стандартів STANAG 4246 і STANAG 4372. Ці методи дозволяють створювати захищені від перешкод радіоканали.

Крім того, компанія Rohde & Schwarz розробила метод SECOS, який забезпечує надійний захист від перешкод навіть при високих швидкостях польоту. Він може шифрувати голос і дані зі швидкістю до 16 кбіт/с. Метод SECOS використовується у всьому світі протягом багатьох років і відмінно себе зарекомендував. Цей метод можна інтегрувати в трансивери Rohde & Schwarz паралельно з методом HAVE QUICK I / II , що дозволяє брати участь, як в національних, так і в міжнародних операціях. При використанні методу SECOS або SATURN голосова інформація стискується вокодером CVSD і передається в цифровому вигляді.

Захист від прослуховування і впливу помилкових сигналів за допомогою вбудованої системи шифрування голосу і даних

Для захисту радіоканалів від прослуховування і впливу завад, передану інформацію можна шифрувати. Випустивши R & S ® MR6000A з сімейства R & S ® M3AR, компанія Rohde & Schwarz стала першим виробником, що запропонував вбудоване шифрування НАТО. Це дозволяє обійтися без додаткового зовнішнього пристрою шифрування. Таким чином R & S ® MR6000A економить місце, знижує вагу і спрощує установку обладнання на повітряні судна. R & S ® MR6000A

сумісний із зовнішніми криптографічними пристроями, такими як KY57, KY58, KY99, KY100 і ELCRODAT 4–2.

Розроблений компанією Rohde & Schwarz надійний метод шифрування R & S ® SECOS може використовуватися всіма трансиверами сімейства R & S ® M3AR [11].

Радіоелектронна розвідка

Радіоелектронна розвідка (РЕР) – вид технічної розвідки. Добування розвідувальних відомостей про противника шляхом перехоплення і аналізу випромінювань його радіоелектронних засобів із застосуванням спеціальних технічних пристроїв. Як правило, термін «радіоелектронна розвідка» використовується для позначення розвідки засобів зв'язку і радіотехнічної розвідки у випадках, коли немає необхідності поділяти ці два види розвідки, або для підкреслення їх єдності. Радіоелектронна розвідка поділяється на радіорозвідку, радіотехнічну, радіолокаційну, радіотеплову (тепловізійну), теплову (інфрачервону), лазерну, телевізійну, звукову, гідроакустичну розвідки.

Види радіоелектронної розвідки

Радіоелектронна розвідка є найважливішою частиною державної та воєнної розвідки різних країн і являє собою основний, а в багатьох випадках, єдиний спосіб добування розвідувальної інформації. За різними оцінками засобами РЕР добувається 80–90 % первинної інформації.

Радіоелектронна розвідка класифікується за кількома ознаками.

За цільовим призначенням і характером інформації, що добувається:

1. Стратегічна радіоелектронна розвідка ведеться в інтересах урядових органів та вищого військового командування з метою добування всебічної інформації про розвідувані країні через випромінювання радіоелектронних засобів різних відомств і служб. Здійснюється радіотехнічними підрозділами центральних