Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"

ШОЛОХОВ С.М., САМБОРСЬКИЙ І.І.,ВАКУЛЕНКО О.В.,
НІКОЛАЄНКО Б.А.

ЗАВАДОЗАХИСТ РАДІОЕЛЕКТРОННИХ ЗАСОБІВ
Частина 1
Основи завадозахисту систем зв'язку

НАВЧАЛЬНИЙ ПОСІБНИК

За редакцією
д.т.н., професора Єрохіна В.Ф.

Київ – 2021

УДК 621.391
ББК 32.811

Рекомендовано Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського
(протокол № 16 від 28 грудня 2021)

Рецензенти: д.т.н., професор *Козловський* В.В., професор Спеціальної кафедри № 3 ІСЗЗІ КПІ ім. Ігоря Сікорського.
д.т.н., с.н.с. *Рома* Олександр Миколайович, завідувач Спеціальної кафедри № 1 ІСЗЗІ КПІ ім. Ігоря Сікорського.
к.т.н., с.н.с. *Ніколаєв* Сергій Миколайович, начальник управління військової частини А1906.

Шолохов С.М., Самборський І.І., Вакуленко О.В., Ніколаєнко Б.А. Завадозахист радіоелектронних засобів. Частина 1. Основи завадозахисту систем зв'язку: навчальний посібник. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 210 с.

Навчальний посібник розроблений авторським колективом спеціальної кафедри № 3 ІСЗЗІ КПІ ім. Ігоря Сікорського, за редакцією доктора технічних наук, професора В.Ф. Єрохіна, у складі: кандидата технічних наук, доцента С.М. Шолохова (вступ, заключення, гл. 1, гл. 2, гл. 3), кандидата технічних наук Б.А. Ніколаєнка (гл. 2, п. 2.6), кандидата технічних наук, старшого наукового співробітника Самборського І.І. (гл. 3), Вакуленка О.В. (гл. 3., п. 3.2).

У навчальному посібнику викладені систематизовані положення основ завадозахисту радіоелектронних засобів. Визначені складові завадозахищеності радіоелектронних засобів в умовах ведення противником радіоелектронної боротьби та радіоелектронної розвідки. Сформульовані показники енергетичної скритності та завадостійкості засобів зв'язку.

Перша частина навчального посібника саме забезпечує вивчення теоретичних основ завадозахищеності систем зв'язку, засад радіоелектронної боротьби та радіоелектронної розвідки, методів та способів завадозахисту засобів зв'язку за спеціальністю 172 Телекомунікації та радіотехніка, а також може використовуватися науково-педагогічними працівниками та інженерно-технічним складом.

Матеріал навчального посібника представлений в систематизованому вигляді, що сприяє засвоєнню навчального матеріалу.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АМ	–	амплітудна модуляція;
АОФП	–	акустооптичний Фур’є – процесор;
АПРЧ	–	адаптивне перелаштування робочої частоти;
АСЗ	–	автоматизована станція завад;
АСУ(В)	–	автоматизована система управління (військами);
АТО	–	антитерористична операція;
АФ	–	адаптивний фільтр;
БЕР	–	безпосередня електронна розвідка;
БІЦ	–	бойовий інформаційний центр;
БКК	–	багаторазовий космічний корабель;
БНС	–	багатонаціональні сили;
БОЕР	–	безпосередня оптико-електронна розвідка;
БПЛА	–	безпілотний літальний апарат;
БРЛС	–	бортова РЛС;
БРЕР	–	безпосередня радіоелектронна розвідка;
БФФН	–	багатоканальний фільтровий Фур’є – процесор;
ВЗ	–	вузол зв`язку;
ВКТК	–	вузол комплексного технічного контролю;
ВПЗ	–	вертоліт постановник завад;
ВТЗ	–	високоточна зброя;
ВУ	–	вогневе ураження;
ГАК	–	гідроакустичний комплекс;
ГАП	–	гідроакустичне подавлення;
ГАПД	–	гідроакустична протидія;
ГАС	–	гідроакустична станція;
ГАнК	–	гібридний антагоністичний конфлікт;
ГВД	–	гібридні військові дії;
ГСН	–	головка самонаведення;
ДВ	–	дипольні відбивачі;
ДМХ	–	дециметрові хвилі;
ДРЛВУ	–	дальнє радіолокаційне виявлення і управління;
ДСА	–	діаграма спрямованості антени;
ДФП	–	дисперсійний Фур’є – процесор;
ЕМ(Б)	–	електромагнітний (боєприпас);
ЕМ(В)	–	електромагнітне (випромінювання);
ЕМ(З)	–	електромагнітна (зброя);
ЕМ(І)	–	електромагнітний (імпульс);
ЕМ(С)	–	електромагнітна (сумісність);
ЕКЧР	–	еквівалентний канал частотного розрізнення;
ЕМП	–	електромагнітне подавлення;
ЕОМ	–	електронно-обчислювальна машина;

ЕПР – ефективна площа розсіювання;
ЗПЗ – закидуваний передавач завад;
ЗС(У) – збройні сили (України);
ЗКР – зенітна керована ракета;
ІГСН – інфрачервона головка самонаведення;
ІЧ – інфрачервоні;
КВ – кутові відбивачі;
КП – командний пункт;
КР – крилата ракета;
КТК – комплексний технічний контроль;
КЧР – канал частотного розрізнення;
КХ – короткохвильовий;
КЦ – командний центр;
ЛЧМ – лінійна частотна модуляція;
МАУ – масований авіаційний удар;
МВУ – масований вогневий удар;
МГД – магнітогідродинамічний генератор;
ММО – міжнародні миротворчі операції;
НДР – науково дослідна робота;
НСЗФ – незаконно-створені збройні формування;
НК – надводний корабель;
НЦУ(РУК) – наземні центри управління (розвідувально-ударним комплексом);
ОВТ – озброєння та військова техніка;
ОЕМП – об’єкт електромагнітного подавлення;
Об(РЕП) – об’єкт радіоелектронного подавлення;
ОЕЗ – оптико-електронні засоби;
ОЕП – оптико-електронне подавлення;
ООС – операція об’єднаних сил;
ОС – односмугова;
ОЗС – об`єднані збройні сили;
ПД(ТЗР) – протидія (технічним засобам розвідки);
ПЗРК – переносний зенітно-ракетний комплекс;
ПКБ – програмно-комп’ютерна боротьба;
ПКП – програмно-комп’ютерне подавлення;
ПКР – протикорабельна ракета;
ПТРК – протитанковий ракетний комплекс;
ПТКР – протитанкова керована ракета;
ПМ(ДПА) – податкова міліція Державної податкової адміністрації;
ПП – постановники завад;
ПС – повітряні сили;
ПУ – пункт управління;
ПУ(ЗК) – пункт управління (засобами комплексу);
ПУ(Т) – пункт управління (тактичний);
ПУ(ТА) – пункт управління (тактичною авіацією);

ППО – протиповітряна оборона;
ППРЧ – програмне перелаштування робочої частоти;
ПРР – протирадіолокаційні ракети;
ПФФП – послідовний фільтровий Фур’є – процесор;
ПЧ – підводний човен;
РВК – развідувально-вогневий комплекс;
РВП – радіовимірювальній пристрій;
РВіА – ракетні війська і артилерія;
РДГ – розвідувально-диверсійна група;
РЕ(А) – радіоелектронна (апаратура);
РЕБ – радіоелектронна боротьба;
РЕ(В) – радіоелектронний (вплив);
РЕ(ВУ) – радіоелектронний (вогневий удар);
РЕЗ(УЗ) – радіоелектронні засоби (управління зброєю);
РЕЗ – радіоелектронний захист;
РЕП – радіоелектронне подавлення;
РЕР – радіоелектронна розвідка;
РЕУ – радіоелектронний удар;
РЕЗ – радіоелектронний засіб;
РЕЗт – радіоелектронний захист;
РЕК – радіоелектронний конфлікт;
РЕО – радіоелектронна обстановка;
РЕОб – радіоелектронний об’єкт;
РЛП – радіолокаційне поле;
РЛС – радіолокаційна станція;
РНС – радіонавігаційна система;
РПд – радіопідривач;
РР – радіорозвідка;
РзПр – розвідприймач;
РСП – розвідувально-сигнальній пристрій;
РЛР – радіолокаційна розвідка;
РТЗ – радіотехнічні засоби;
РТВ – радіотехнічні війська;
РТР – радіотехнічна розвідка;
РУК – розвідувально-ударний комплекс;
РЧР – радіочастотний ресурс;
СБУ – служба безпеки України;
СВФ – спектральна вагова функція;
СЗН – станція завад наземна;
СЗР – станція завад радіопідривача;
СРЦ – селекція рухомих цілей;
СВ – сухопутні війська;
СМО – система масового обслуговування;
СНЗ – самонавідна зброя;
СНР – самонавідні ракети;

СНС	–	самонавідні снаряди;
СПр	–	спеціального призначення;
СПр(З)	–	спеціального призначення (засіб зв’язку);
СПр(К)	–	спеціального призначення (комплекс зв’язку);
СПр(СЗ)	–	спеціального призначення (система зв’язку);
СЦ	–	спеціальний центр;
СУ	–	система управління;
СУВ	–	система управління військами;
ТА	–	тактична авіація;
ТТХ	–	тактико-технічні характеристики;
УКХ	–	ультракороткохвильовий;
УТЦ	–	удавана теплова ціль;
ФП	–	Фур’є процесор;
ЦРЕП	–	ціль РЕП;
ЦУБД	–	центр управління бойовими діями;
ЦФ	–	цифровий фільтр;
ЧТР	–	частотно-територіальний розподіл;
ЧМ	–	частотна модуляція;
ШСЗ	–	штучний супутник землі;
ШШС	–	широкосмуговий шумоподібний сигнал.

ПЕРЕДМОВА

Навчальний посібник розроблений у відповідності до нормативної частини програми підготовки: курсантів ІСЗЗІ КПІ ім. Ігоря Сікорського згідно освітньо-професійних програм підготовки здобувачів вищої освіти спеціальності 172 Телекомунікації та радіотехніка: доктор філософії – відповідно до програми навчальної дисципліни “Методи завадозахисту засобів радіозв’язку”; магістр – відповідно до програми навчальної дисципліни “Електромагнітна сумісність та завадозахист радіоелектронних засобів”; бакалавр – відповідно до програми навчальної дисципліни “Радіорелейні, тропосферні та супутникові системи”.

У навчальному посібнику викладені систематизовані положення основ завадозахисту радіоелектронних засобів. Визначені складові завадозахищеності радіоелектронних засобів (РЕЗ) в умовах застосування противником навмисних завад. Сформульовані показники енергетичної скритності та завадостійкості засобів зв’язку.

Вперше за історію незалежної України застосування засобів зв’язку відбувається в умовах ведення гібридних військових дій на території України при комплексному застосуванні противником та нашими збройними формуваннями новітніх комплексів радіоелектронної боротьби та радіоелектронної розвідки. Теоретичні основи завадозахисту систем в умовах “дуельної” ситуації дуже добре висвітлені у науковій і спеціальній літературі. Однак, докорінна зміна ідеології ведення сучасної збройної боротьби, широке розповсюдження такої її форми, як гібридний антагоністичний конфлікт вимагає глибоко розуміння фахівцями зв’язку, не лише теоретичних лише основ завадозахищеності систем зв’язку в умовах “навмисна завада” – приймач, а й загальних основ тактики, форм та способів ведення радіоелектронної боротьби при порушенні функціонування саме системи зв’язку в умовах гібридного антагоністичного конфлікту. Окремим питання є врахування під час організації зв’язку бойових можливостей та тактики застосування частин (підрозділів) радіоелектронної боротьби ЗСУ для організації взаємодії та виключення взаємного заважаючого впливу на приймальні пристрої системи зв’язку в умовах гібридного антагоністичного конфлікту.

Саме такі знання дозволять фахівцям зв’язку забезпечити виконання завдань за призначенням саме системи зв’язку, при її функціонуванні в умовах протікання на території України гібридного антагоністичного конфлікту.

Це обумовило актуальність корегування змісту силабусів навчальних дисциплін “Методи завадозахисту засобів радіозв’язку”, “Електромагнітна сумісність та завадозахист радіоелектронних засобів”, “Радіорелейні, тропосферні та супутникові системи” в бік більш детального вивчення основ ведення радіоелектронної боротьби та радіоелектронної розвідки противником та своїми військами.

Тому, в частині першій навчального посібника основна увага приділяється основним поняттям теорії завадозахисту, розгляду сутності радіоелектронної боротьби, як виду бойового (оперативного) забезпечення противника та своїх військ в операціях (бойових діях), основам радіоелектронного захисту, як складових радіоелектронної боротьби з метою формулювання наукових основ для вивчення та розробки методів та способів завадозахисту засобів зв'язку від впливу навмисних завад в умовах ведення гібридних військових дій на території Луганської та Донецької областей.

Визначена суть радіоелектронної боротьби (РЕБ) як основного виду оперативного (бойового) забезпечення противника у боротьбі за панування у радіоефірі у гібридному антагоністичному конфлікті (ГАнК). Визначені напрямки розвитку РЕБ у збройній боротьбі майбутнього. Визначений склад та бойові можливості частин (підрозділів) РЕБ ЗСУ для їх врахування при організації завадозахищеного зв'язку в ООС (АТО).

Розкриті основні положення здійснення радіоелектронного подавлення засобів противником. Наведений аналіз досвіду застосування комплексів РЕБ противника у антитерористичних операціях (АТО) та операціях об'єднаних сил (ООС). Визначені задачі та методи ведення радіоелектронної розвідки для інформаційного забезпечення процесів РЕБ.

Конкретизовані задачі, види та методи радіоелектронного захисту своїх засобів зв'язку. Розглянуті технічні та організаційні методи радіоелектронного захисту. Розглянута адаптація до радіозавад та прогнозування випадкових процесів для адаптації. Наведена методика розробки можливих сценаріїв ведення радіоелектронного подавлення (РЕП) та електромагнітного подавлення (ЕМП) для розробки методів, способів та визначення заходів завадозахисту засобів зв'язку.

Навчальний посібник складається з чотирьох розділів.

В першому розділі викладені систематизовані положення основ завадозахисту радіоелектронних засобів. Визначені складові завадозахищеності радіоелектронних РЕЗ в умовах застосування противником навмисних завад. Сформульовані показники енергетичної потайливості та завадостійкості РЕЗ.

В другому розділі викладені загальні відомості про радіоелектронну боротьбу як вид оперативного (бойового) забезпечення гібридних дій. Конкретизовані бойові можливості частин (підрозділів) РЕБ Збройних Сил України для їх врахування в питаннях організації взаємодії між підрозділами Держспецзв'язку та РЕБ ЗС України під час виконання завдань за призначенням.

Проаналізований досвід застосування комплексів РЕБ Російської Федерації у АТО та ООС. Проаналізовані тенденції розвитку РЕБ та визначені шляхи зміни ідеології її ведення у війнах та збройних конфліктах майбутнього.

Розглянуті світові тенденції розвитку зброї РЕБ нового покоління. Розглянуті нові складові радіоелектронного подавлення – електромагнітне та програмно – комп'ютерне подавлення. Викладені основи трансформації форм

РЕБ та конкретизовані особливості їх ведення у збройній боротьбі сучасності та у майбутньому на прикладі радіоелектронного удару.

У третьому розділі визначені загальні положення та складові радіоелектронного подавлення радіоелектронних засобів противником. Розглянуті основні критерії, показники та методики оцінки ефективності ведення радіоелектронного подавлення.

У четвертому розділі викладені основи радіоелектронного захисту засобів зв'язку. Розглянуті технічні та організаційні методи радіоелектронного захисту. Конкретизовані заходи з радіоелектронного захисту РЕЗ у повсякденній діяльності підрозділів Держспецзв'язку.

Ведення гідридних воєнних дій на території окремих районів Донецької та Луганської областей робить необхідним докорінний перегляд підходів до забезпечення завадозахищеності спеціальних засобів радіозв'язку від навмисних завад противника. Проведений аналіз досвіду ведення АТО та ООС показав, що для досягнення інформаційної переваги російсько – терористичні війська активно застосовують новітні комплекси (засоби) радіоелектронної боротьби. Боротьба за перевагу в управлінні військами (силами) та її утримання стає невід'ємною складовою гібридних воєнних дій, а протиборство в сфері управління – важливою частиною ГАнК.

В сучасних умовах невід`ємною складовою сучасних військових конфліктів, операцій, гібридних воєнних дій є РЕБ. Питома вага сил і засобів РЕБ, які застосовуються у війнах і збройних конфліктах, постійно збільшується завдяки постійно зростаючій ролі радіоелектронних засобів у підвищенні бойових можливостей військ.

В умовах ведення нової форми збройної боротьби – ГАнК, у противника з'являються нові, раніше не притаманні РЕБ, задачі з подавлення об'єктів РЕП. Одним з таких нових завдань противника, що притаманні ГАнК є дезорганізація системи Державного управління шляхом впливу навмисними завадами (радіо та електромагнітного типу) на засоби радіозв'язку. Така ситуація є принципово новою для фахівців Держспецзв'язку, одним з основних завдань яких, традиційно була боротьба із ненавмисними завадами, що створюються «своїми» радіоелектронними засобами. Тому, сучасні умови вимагають більш детального вивчення фахівцями телекомунікацій основ РЕБ, тактики застосування, способів та засобів РЕБ для забезпечення успішного виконання завдань за призначенням в умовах масованого застосування противником різних типів радіоелектронних та електромагнітних завад. Ці питання у відомій авторам літературі з основ завадозахисту не розглянуті у повному обсязі, носять різнорідний характер та потребують узагальнення та систематизації.

Радіоелектронна боротьба виникла як результат діалектичного розвитку озброєння і військової техніки на етапі широкого впровадження досягнень радіоелектроніки у всі системи та ланки управління військами (силами) і зброєю. Вперше засоби РЕБ масовано були застосовані у війні в Кореї 1950-1953 рр. З того часу не проводилась жодна операція, де б в тих чи інших масштабах цей вид оперативного (бойового) забезпечення не

використовувався. В XXI столітті теоретики оперативного мистецтва та стратегії бачать РЕБ у складі більш загальних понять інформаційного протиборства, інформаційної боротьби, а комплекси (засоби) РЕБ відносять до нових видів інформаційної зброї. Вже зараз можна констатувати, що успішне вирішення завдань з РЕБ може визначити успіх всієї операції (бою) і навіть локальної війни та збройного конфлікту в цілому.

В сучасних умовах сили і засоби РЕБ залучаються до вирішення завдань тактичного, оперативного і навіть стратегічного рівня з глобальним просторовим розмахом. Фактично РЕБ поступово набирає риси специфічної форми бойових дій, що має за мету досягнення переваги або недопущення переваги противника в інформаційній компоненті збройної боротьби, яка забезпечується радіоелектронними засобами.

Зараз можна стверджувати, що відбувся перегляд поглядів на роль, сутність та основи ведення радіоелектронної боротьби у збройних конфліктах сучасності та у майбутньому. Сформована нова ідеологія ведення РЕБ на основі переоснащення частин (підрозділів) РЕБ зброєю функціонального ураження (електромагнітна, програмно-комп'ютерна), переходу від симетричних до асиметричних принципів розвитку РЕБ. Це призвело до активного розповсюдження РЕБ на інформаційну сферу та сферу впливу на особовий склад і населення противника. РЕБ набуває рис специфічного виду бойових дій та стає основною складовою інформаційної боротьби. Розвиваються і впроваджуються в практику операцій та бойових дій нові комбіновані форми РЕБ та вогневого ураження: радіоелектронний, радіоелектронно-вогневий удари, операція РЕБ.

Враховуючи тенденції розвитку радіоелектронної боротьби у збройній боротьбі сучасності та у майбутньому, досвід її організації та ведення у локальних війнах та збройних конфліктах, повсякденній діяльності військ (сил), в перший частині навчального посібника викладаються сучасні положення ведення радіоелектронної боротьби в умовах гібридних військових дій та у збройній боротьбі майбутнього.

Посібник розроблено на основі аналізу і узагальнення тенденцій розвитку радіоелектронної боротьби, положень керівних документів та результатів наукових досліджень спеціальної кафедри № 3 інституту.

Навчальний посібник може бути корисним для курсантів, аспірантів, викладачів та науковців ІСЗЗІ КПІ ім. Ігоря Сікорського, фахівців інших військових навчальних закладів, наукових організацій, частин та органів управління частинами і підрозділами радіоелектронної боротьби.

РОЗДІЛ 1
ОСНОВНІ ПОЛОЖЕННЯ ЗАВАДОЗАХИСТУ СИСТЕМ ЗВ'ЯЗКУ

1.1. Завадозахист систем спеціального зв'язку, його сутність та складові

Спроможність системи спеціального призначення (СПр) виконувати завдання у визначених умовах характеризують ефективністю.

Ефективність систем зв'язку залежить від великої кількості показників, зокрема, таких, як точність, живучість, надійність, вірність передавання інформації, завадостійкість, тощо [1-4]. В різних умовах застосування значущість відповідних показників (груп показників) може бути різною. Зокрема, при застосуванні комплексів (засобів) зв'язку, ведення гібридних воєнних дій різко зростає роль показників, що характеризують можливість виконання завдання за призначенням в умовах активного ведення противником (регулярними збройними формуваннями, зловмисниками, терористичними угрупованнями тощо) радіоелектронного подавлення ліній зв'язку із застосуванням навмисних радіоелектронних та електромагнітних завад. Можна говорити, що застосування систем СПр здійснюється в умовах складної сигнально-завадової обстановки, в яких значення показників, якими оцінюються завадозахищеність систем стають пріоритетними [5-8].

Що таке завадозахищеність системи СПр?

Під завадозахищеністю [1] системи СПр будемо розуміти її спроможність виконувати завдання за призначенням в умовах РЕП та ЕМП [4, 9-14]. При цьому зауважимо, що РЕП та ЕМП слід розглядати комплексно, як складові виду бойового (оперативного) забезпечення ГАнК – РЕБ [9-13, 15]. Більш детально сутність РЕБ та її складових розглянуті в розділах 2 та 3 цього посібника.

В якості основного показника ефективності, як міри успішності виконання завдань з передачі інформації можна обрати ймовірність її вірного (безпомилкового) передавання по радіоелектронних каналах зв'язку відповідним споживачами в умовах комплексного РЕП та ЕМП.

У загальному сенсі цикл РЕП та ЕМП елементів СПр(СЗ) містить етапи РЕР, РЕП та ЕМП, періодичний контроль їх ефективності.

Метою радіоелектронної розвідки є встановлення факту випромінювання радіоелектронних комплексів (засобів) та визначення їх параметрів, що необхідні для організації РЕП та ЕМП [8-9, 15].

Мета РЕП та ЕМП – створення таких умов, які б ускладнили або зірвали виконання завдань за призначенням СПр(СЗ) шляхом впливу навмисними радіоелектронними завадами та електромагнітним імпульсом.

В таких умовах завадозахищеність СПр(СЗ) може бути описана сукупністю ймовірнісних показників, що характеризують її скритність та завадостійкість [1, 4].

Прихованість (скритність) – це спроможність СПр(СЗ) чинити опір заходам РЕР противника (див. розділ 2.), що спрямовані на виявлення факту роботи СПр(СЗ), визначення її параметрів, перехоплення інформації для подальшої постановки навмисних радіоелектронних та електромагнітних завад [1].

Завадостійкість – це спроможність СПр (СЗ) виконувати завдання з передачі інформації з визначеними показниками якості в умовах дій навмисних радіоелектронних та електромагнітних завад (див. розділ 3) [1].

Нехай, – ймовірність розвідки параметрів СПр(СЗ), що необхідні для організації радіопротидії, а $P_{\text{п}}$ – ймовірність помилки (середня ймовірність помилки) при прийомі сигналу у СПр(СЗ) в умовах дії радіоелектронних завад комплексів РЕБ противника. Тоді показник завадозахищеності СПр (СЗ) може бути визначений у вигляді ймовірності $P_{звз}$ у вигляді (1.1):

$$P_{\text{звз}} = 1 - \text{P}_{\text{р}} \cdot \text{P}_{\text{п}}. \qquad (1.1)$$

1.2. **Показники прихованості (скритності) системи зв’язку**

Ймовірність $P_{\text{р}}$ виразу (1.1) кількісно відображає властивість СПр(СЗ) що може називатись скритністю. Під прихованістью (скритністю) [1] слід розуміти спроможність протистояти заходам радіоелектронної розвідки, що спрямовані на виявлення факту роботи СПр (СЗ) та визначення необхідних для організації РЕП та ЕМП параметрів сигналів СПр (СЗ). Тоді величину ймовірності можна розглядати як показник прихованості (скритності) [4, 8, 15-16]:

$$P_{\text{прих}} = 1 - P_{p}. \qquad (1.2)$$

Радіоелектронна розвідка противника вирішує задачі [17-19]:

– виявлення факту роботи РЕЗ (виявлення сигналу);
– визначення структури сигналів СПр(СЗ) (на основі множини його параметрів);
– викриття інформації, що міститься у сигналі СПр(СЗ).

Відповідно до сформульованих задач РЕР можна визначити три види прихованості (скритності) системи (комплекса, засобу) зв’язку [1]:

– енергетична;
– структурна;
– інформаційна.

1. Енергетична прихованість (скритність) характеризує спроможність протидіяти заходам, що спрямовані на виявлення факту випромінювання сигналу РзПр РЕР.

Відомо, що виявлення сигналу відбувається в умовах дій на приймач РЕР завад (шумів) та супроводжується помилками двох видів – не виявлення

сигналу за його наявності (або виявлення іншого, замість вірного) та хибне виявлення сигналу за його відсутності.

Помилки мають ймовірнісний характер. Тоді в якості кількісної міри енергетичної прихованості можна, наприклад, обрати ймовірність вірного виявлення сигналу:

$$P_{\text{вв}} = P_{ев} \cdot P_{ччз}(\tau_a), \tag{1.3}$$

де $P_{\text{ев}}$ – ймовірність енергетичного виявлення, що залежать від відношення сигнал-шум на виході лінійної частини приймача та від алгоритму прийняття рішення щодо виявлення; $P_{\text{ччз}}(\tau_a)$ – ймовірність частотно-часового збігу [20-22], що враховує випадковий характер співпадіння каналу частотного розрізнення РвПр та сигналу під час застосування в РвПр пошукових за частотою (напрямком) методів виявлення невідомого сигналу. Для РзПр, що реалізують без пошукові методи виявлення ймовірність $P_{\text{ччз}}(\tau_{\text{а}}) = 1$.

Особливу роль у сучасних умовах відграє врахування процесів частотно-часового пошуку сигналу у широкій смузі частот аналізу приймачем РЕР. Якість пошуку (виявлення) сигналів охарактеризуємо ймовірністю частотно-часового збігу $P_{\text{ччз}}(\tau_{\text{а}})$ за час аналізу $\tau_{\text{а}}$ смуги ΔF_a частот, що аналізуються РзПр [22].

Ймовірність виявлення сигналу $P_{\text{ев}}$ на виході лінійної частини розвідприймача залежить від відношення сигнал-шум q у смузі каналу частотного розрізнення $\Delta F_{\text{кчр}}$ (у випадку багатоканальної схеми побудови РвПр), смуги аналізу розвідприймача ΔF_a (у випадку одно канальної схеми побудови РвПр $\Delta F_{\text{кчр}} = \Delta F_a$), [22]:

$$q = \frac{P_{свх}}{P_{ш}} = \frac{P_{свх}}{W_0 \cdot \Delta F_{кчр}}, \tag{1.4}$$

де $P_{\text{свх}}, P_{ш}$ – потужність сигнала та шуму відповідно на виході лінійної частини РвПр (без врахування втрат енергії сигналу за рахунок неспівпадіння частотних характеристик приймального тракту та сигналу, часу існування сигналу на відповідній частотній позиції та її аналізу РзПр при здійсненні частотно (просторово)-часового пошуку); W_0 – спектральна щільність потужності шуму у смузі $\Delta F_{\text{кчр}}$ (за умови, що процес пошуку сигнала по частоті та простору вже здійснений, а його стохастичні показники будуть враховані при оцінці ймовірності $P_{\text{ччз}}\tau_{\text{а}})$).

При розгляді $P_{\text{вв}} = f(q)$ необхідно знайти залежність q від параметрів РЕЗ, сигналів та характеристик розвідприймача. Вважаємо, що форма сигналу,

що розвішується, невідома. Тоді, єдиною ознакою наявності сигналу є енергія реалізації процесу $y(t)$ (за час τ_a) на виході розвідприймача:

$$E_в = \int_0^{\tau_a} \big(y(t)\big)^2 dt, \qquad (1.4)$$

де

$$y(t) = \begin{cases} s(t) + n(t) - \text{за} \quad \text{наявності} \quad \text{сигналу}; \\ n(t) - \text{за} \quad \text{відсутності} \quad \text{сигналу}. \end{cases}$$

Оптимальним приймачем у цій ситуації (коли вважається, що завдання з частотно-часового та просторового пошуку виконані, $P_{\text{ччз}}(\tau_\text{а}) = 1$) буде добре відомий «енергетичний» приймач, що містить лінійний смуговий фільтр зі смугою $\Delta F_{кчр}$, квадратичний детектор, інтегратор з сталою інтегрування t_a та пороговий пристрій.

В сучасних умовах оцінка енергетичної скритності вимагає врахування $P_{\text{ччз}}(\tau_\text{а})$ та потребує окремо розгляду та розробки підходів до її оцінки.

Не гублячи загальності викладення, в якості прикладу розглянемо найбільш складний випадок – задачу визначення $P_{\text{ччз}}(\tau_\text{а})$ в умовах, коли в якості сигналу СПр (ЗЗ) використовуються сигнали з ППРЧ. Необхідність розгляду цього важливого з практичної точки зору прикладу обумовлена великим розповсюдженням цього виду сигналу у сучасних засобах зв'язку провідних країн світу та України.

Якість пошуку (виявлення) елементів сигналів з ППРЧ охарактеризуємо ймовірністю частотно-часового збігу $P_{\text{ччз}}(\tau_\text{а})$ [22], де $\tau_\text{а}$ – відрізок часу, визначений противником для вирішення задачі спостереження за СПр (ЗЗ). При цьому під $P_{\text{ччз}}(\tau_\text{а})$ будемо розуміти ймовірність того, що для кожного з $\xi = 1...\text{ent}\{t_{\text{сп}}/T_\text{е}\}$ елементів, що надійшли у смугу $\Delta F_\text{а}$ аналізу РвПр за відрізок часу $\tau_\text{а}$, на певному часовому інтервалі відбудеться збіг спектральних складових елемента сигналу з ППРЧ та частоти налагодження КЧР РПр під час реєстрації його стану [22]. Врахуємо найбільш складний з точки зору частотно-часового пошук випадок застосування сигналів з програмною перебудовою робочої частити (ППРЧ.)

Нехай пошук (виявлення) елементів сигналу з ППРЧ здійснюється РзПр на основі ФП (Фур'є – процесор – фізичний пристрій, в якому формується Фур'є - образ сигналу, що поданий на його вхід), що утримує $r_к = \Delta F_a / \delta_f$ еквівалентних каналів частотного розподілення (ЕКЧР), де $\Delta F_a, \delta_f$ – смуга аналізованих частот та розрізнювальна здатність за частотою ФП відповідно.

Еквівалентні канали частотного розподілення ФП характеризуються відповідно комплексними спектральними ваговими функціями (СВФ) $FW_i(j\varpi) = FW_i(\varpi)\exp\{j\phi_{ki}(\varpi)\}$ з центральними частотами ϖ_{ki}, смугами пропускання $\delta_{fki} = \delta_k$ та початковими фазами ϕ_{ki}, де $i = 1...m,\ \ m$ – кількість ЕКЧР ФП. Час накопичення сигналу $\tau_{\text{н}}$ у ЕКЧР дорівнює тривалості $\tau_{\text{в}}$ реалізації (вибірки), що обробляється.

Виявлення елементів сигналів з ППРЧ здійснюється на виході $n(n \le m)$, у загальному випадку неузгоджених з елементом сигналу статистично незалежних ЕКЧР ФП на фоні білого гаусівського шуму зі спектральною щільністю потужності $W(\varpi) = W_0 = \text{const}$. Діапазон $\Delta F_{\text{а}}$ - не менше смуги частот $\Delta F_{\text{ппрч}}$, що використовується у режимі ППРЧ. Час аналізу частотного діапазону $\Delta F_{\text{а}}$ ФП дорівнює [22]:

$$\tau_{\text{а}} = \frac{\Delta F_{\text{а}}}{\gamma_{\text{а}}} = r_k \cdot \tau_{\text{оп}}, \qquad (1.6)$$

де $\gamma_{\text{а}}, \tau_{\text{оп}}$ – швидкість аналізу ФП та час опитування ЕКЧР відповідно.

На вхід розвідприймача надходять елементи сигналу з ППРЧ $s(t)$ з тривалістю $\tau_{\text{е}}$, шириною спектра $\Delta f_{\text{е}}$, несівною частотою $\varpi_{\text{е}}$, початковою фазою $\phi_{\text{е}}$, комплексною спектральною щільністю $S(j\varpi) = S(\omega)\exp\{j\phi_{\text{е}}(\varpi)\}$ та періодом появи $T_{\text{е}}$.

Враховуючи результати [22], при оцінці енергетичної скритності, ймовірність $P_{\text{ччз}}(\tau_{\text{а}})$ визначимо у такому вигляді:

$$P_{\text{ччз}}(t_{\text{н}}) \ge \begin{cases} \left\{ \left\langle 1 - \left[1 - \dfrac{(\tau_{\text{оп}} + \tau_{\text{е}} + 2\tau_{\min})\tau_{\text{оп}}}{\tau_A{}^2} \right]^{r_k} \right\rangle^{\vartheta} \right\}^{\xi} & \text{при } \tau_{\text{а}} \le T_{\text{е}},\ \tau_{\min} \le \min\{\tau_{\text{е}}, \tau_{\text{оп}}\},\ \tau_{\text{опр}} \le T_{\text{е}} - \tau_{\text{е}} \\ \left\{ \left\langle 1 - \left[1 - \dfrac{(\tau_{\text{оп}} + \tau_{\text{е}} + 2\tau_{\min})\tau_{\text{оп}}}{\tau_A \cdot T_{\text{е}}} \right]^{r_k} \right\rangle^{\vartheta} \right\}^{\xi} & \text{при } \tau_{\text{а}} > T_{\text{е}},\ \tau_{\min} \le \min\{\tau_{\text{е}}, \tau_{\text{оп}}\},\ \tau_{\text{опр}} \le T_{\text{е}} - \tau_{\text{е}} \\ \left\{ \left\langle 1 - \left[1 - \dfrac{(\tau_{\text{оп}} + \tau_{\text{е}} + 2\tau_{\min})\tau_{\text{оп}}}{\tau_A \cdot (\tau_{\text{е}} + \tau_{\text{оп}})} \right]^{r_k} \right\rangle^{\vartheta} \right\}^{\xi} & \text{при } \tau_{\min} \le \min\{\tau_{\text{е}}, \tau_{\text{оп}}\},\ \tau_{\text{оп}} > T_{\text{е}} - \tau_{\text{е}} \end{cases} \qquad (1.7)$$

де

$$\vartheta = \begin{cases} \text{ent}(\tau_{\text{а}} / T_{\text{е}}) & \text{при } \tau_{\text{а}} \geq T_{\text{е}}; \\ 1 & \text{при } \tau_{\text{а}} < T_{\text{е}}, \end{cases} \tag{1.8}$$

Практичне застосування формул (1.7), (1.8) вимагає конкретизації параметрів $\tau_{\text{а}}$ та $\tau_{\text{оп}}$ до конкретного виду розвідприймача у такому порядку [22]:

– якщо засіб РР реалізований на основі послідовного фільтрового ФП (ПФФП), то $\tau_{\text{а}} = \Delta F_{\text{а}} / \gamma_{\text{пч}}$, а $\tau_{\text{оп}} = \Delta F_{\text{а}} / (\gamma_{\text{пч}} \cdot r_k)$, де $\gamma_{\text{пч}}$ – час перестроювання за частотою ПФФП;

– якщо засіб РР побудований на основі ПФФП з паралельним опитуванням k ЕКЧР, то $\tau_{\text{а}} = \Delta F_{\text{а}} / (\gamma_{\text{пч}} \cdot k)$;

– при аналізі акустооптичного з просторовим інтегруванням (АОФП) та багатоканального фільтрового ФП (БФФП) $\tau_{\text{а}}$ у формулі (1.7) слід вибирати рівним часу опитування лінійки фотодіодів АОФП та частотних каналів БФФП відповідно.

Ймовірність енергетичного виявлення сигналу $P_{\text{ев}}$ що залежить від відношення сигнал-шум q у смузі пошуку ΔF_a лінійної частини РвПр:

$$q = \frac{P_{свх}}{P_{ш} \cdot \varepsilon_k}, \tag{1.9}$$

де

$$P_{ш} = k \cdot T_{\text{о}} \cdot {q_{\text{пор}}}^2 \cdot \Delta f_{\text{еф}} \cdot \left(t_{\text{а}} - 1 + \frac{N}{K_{\text{пф}}} \right), \tag{1.10}$$

k – стала Больцмана, $k = 1{,}380649 \cdot 10^{-23}$ Дж·К^0;

T_0 –температура, С^0;

$\Delta f_{\text{еф}}$ – ефективна шумова смуга приймача, Гц;

$t_{\text{а}}$ – відносна шумова температура антени, С^0;

N – коефіцієнт шуму приймача;

$K_{\text{пф}}$ – коефіцієнт передачі фідерного тракту;

${q_{\text{пор}}}^2$ – потрібне порогове відношення потужності корисного сигналу до потужності завади на виході лінійної частини РзПр;

$\varepsilon_{\text{к}}$ – коефіцієнт, що враховує втрати потужності елемента сигналу за рахунок апріорного неузгодження спектральної годинної функції еквівалентного каналу частотного розподілення (ЕКЧР) ФП та сигналу [22]:

$$\varepsilon_{\text{к}} = \left[\int_{-\infty}^{\infty} \left| FW(\varpi - \varpi_{ki}) \right|^2 d\varpi \int_{-\infty}^{\infty} \left| S(\varpi - \varpi_c) \right|^4 \times \text{L} \right.$$

$$\text{L} \times \left[\left| \frac{1}{2\pi} S(\varpi - \varpi_c) \cdot FW(\varpi - \varpi_{ki}) \exp\left\{ j\left(\phi_c(\varpi) + \phi_{ki}(\varpi) + \varpi\tau_{\text{в}} \right) \right\} d\omega \right|^2 \times \text{L} \qquad (1.11)$$

$$\left. \text{L} \times \int_{-\infty}^{\infty} \left| S(\varpi - \varpi_c) \right|^2 d\varpi \right]^{-1},$$

де $FW(\varpi - \varpi_{ki})$ – спектральна вагова функція ЕКЧР РвПр; $S(\varpi - \varpi_c)$ – спектральна щільність сигналу, що надійшов на вхід РвПр.

На практиці при оцінці коефіцієнт $\varepsilon_{\text{к}}$ набуває різних для кожного i-го ЕКЧР ФП значень ε_{ki}, $i = 1\text{K}\ m$. Це обумовлено випадковим взаємним розташуванням ЕКЧР ФП та спектра сигналу, що трапляється на осі частот.

При розрахунках розвіддосяжності радіоелектронних засобів необхідно орієнтуватися на найменш вигідний, з точки зору виявлення, варіант взаємного розташування ЕКЧР ФП та сигналу на осі частот. При цьому величину коефіцієнта $\varepsilon_{\text{к}}$ для умови (1.7) необхідно вибирати рівною максимальному значенню $\varepsilon_{\text{к}}$ [22]:

$$\varepsilon_{\text{к}} = \max\left\{ \varepsilon_{ki} \right\}, \quad i = 1\text{K}\ m \qquad (1.12)$$

При застосуванні виразів (1.9), (1.10), (1.11) для оцінки виконання виразу (1.3) необхідно враховувати особливості обробки сигналу у ФП, вибираючи варіанти взаємного перекриття СВФ ЕКЧР та спектральної щільності корисного сигналу.

Якщо обробка сигналу проводиться у РвПр на основі ФП, що “дискретизує” сигнал за частотою (наприклад, багатоканальний фільтровий ФП), то визначати $\varepsilon_{\text{к}}$ доцільно для ситуації, за якої центральна частота елемента сигналу з ППРЧ попадає на перетин СЧФ суміжних ЕКЧР.

При розгляді РвПр, сигнал на виході яких не має дискретного характеру (наприклад, дисперсійний або акустооптичний з часовим інтегруванням ФП), та коли $\frac{\Delta f_{\text{е}}}{\delta f} \geq 1$, необхідно розраховувати $\varepsilon_{\text{к}}$ для випадку, при якому ЕКЧР квазіузгоджений із сигналом, що приймається за центральною частотою. Це обумовлено особливостями обробки сигналу у пристроях на основі алгоритмів ЛЧМ перетворення.

У разі, коли для РвПр, що вказаний у попередньому пункті, $\frac{\Delta f_{\text{е}}}{\delta f} < 1$, необхідно орієнтуватись на ситуацію, за якої центральна частота сигналу збігається з центральною частотою одного з ЕКЧР ФП.

У таблиці 1 наведені результати застосування виразів (1.11), (1.12) для визначення коефіцієнта ε_{k} при оцінці розвіддосяжності РЕЗ РвПр на основі багатоканального фільтрового ФП. Результати отримані для типових СВФ ЕКЧР ФП. При розрахунках величина співвідношення $\frac{\Delta f_{\text{е}}}{\delta f}$ складала відповідно 1…8, 1/2, 1/4, 1/6, 1/8. Як модель вхідного сигналу був обраний дзвоникоподібний (гауссів) імпульс.

Таблиця 1

Величина коефіцієнта ε_{k}

СВФ ФП	Величина коефіцієнта $\Delta f_{\text{е}} / \delta f$											
	1	2	3	4	5	6	7	8	1/2	1/4	1/6	1/8
Діріхле	33,1	1,35	1,99	7,2	77,2	20,6	108,5	39,1	12,1	104,5	487,7	2·103
Бартлетта	27,9	1,8	61,2	8,3	78,6	19,6	97,8	33,9	302,8	6·103	107	6·104
Парзена	93,4	3,03	40,5	6,7	52,4	13,8	66,5	23,8	21,1	17,7	22,1	27,4
Хеннінга	11,3	1,3	13,9	8,02	83,1	21,8	114,4	40,8	3,7	18,2	189,1	557,1
Хеммінга	12,4	1,4	14,7	7,8	81,8	21,5	113	40,4	3,9	18,6	185,9	550,3

Вираз для розрахунку рівня сигналу $P_{\text{свх}}$ на вході розвідприймача може мати традиційний вигляд [18-20]:

$$P_{\text{свх}} = \frac{P_{\text{пер}} \cdot G_{\text{пер}} \cdot G_{\text{пр}} \cdot F_{\text{ст}}{}^{2}(\alpha_{\text{ст}}, \Theta_{\text{ст}}) \cdot F_{\text{ср}}{}^{2}(\alpha_{\text{ср}}, \Theta_{\text{ср}})}{K_{\text{ослвп}}, K_{\text{огм,}} K_{\text{онп}}} \qquad (1.13)$$

де $F_{\text{ст}}{}^{2}(\alpha_{\text{ст}}, \Theta_{\text{ст}}), F_{\text{ср}}{}^{2}(\alpha_{\text{ср}}, \Theta_{\text{ср}})$ – нормовані діаграми спрямованості антен засобу з ППРЧ та радіорозвідки відповідно; $P_{\text{пер}}, G_{\text{пер}}, G_{\text{пр}}$ – потужність, коефіцієнт підсилення антен передавача та розвідприймача відповідно; $K_{\text{ослвп}}, K_{\text{огм,}} K_{\text{онп}}$ – коефіцієнти, що враховують втрати потужності сигналу при розповсюдженні у вільному просторі, гідрометеорах та за рахунок неспівпадіння поляризації відповідно.

2. Структурна прихованість (скритність) [1] характеризує спроможність системи зв'язку протистояти заходам РЕР противника, що спрямовані на викриття структурних ознак сигналу, розпізнавання його форми, способів кодування та модуляції (маніпуляції) тощо, віднесення його до одного з класів апріорі відомих. Відповідно, для підвищення структурної прихованості необхідно мати великий ансамбль сигналів, що застосовуються та мати можливість змінювати форму сигналу, вид модуляції (маніпуляції)

тощо. Завдання визначення структури сигналу також належить до статистичних даних, при цьому кількісною мірою структурної прихованості можна обрати ймовірність викриття структури сигналу $P_{\text{стр}}$ за умови що, сигнал виявлений.

3. Інформаційна прихованість (скритність) [1] визначається спроможністю протистояти заходам, що спрямовані на викриття змісту інформації, що передається за допомогою сигналів. Викриття змісту інформації – співставлення кожного сигналу (символу), що прийнятий або їх сукупності з тим повідомленням, що передається. Наявність апріорної та апостеріорної невизначеності робить цю задачу стохастичною, а у якості кількісної міри інформаційної прихованості можна обрати умовну ймовірність викриття змісту інформації, що передається $P_{\text{інф}}$ за умови що виконані етапи його виявлення та викриття структури. Тоді загальну (інтегральну) прихованість ССПр (КСПр, ЗСПр) можна визначити у вигляді:

$$P_{\text{прих}} = 1 - P_{р} \cdot P_{стр} \cdot P_{інф} \qquad (1.14)$$

В практичних застосуваннях для вирішення завдань РЕБ противника задача викриття змісту інформації системи зв’язку не передбачається. Тоді в (1.3) можна покласти $P_{\text{інф}} = 1$. Ключову роль при цьому починає відігравати енергетична прихованість. Справа в тому, що сучасні методи закриття інформації на основі методів криптографічного захисту практично унеможливили викриття змісту кодованої інформації в режимі часу близькому до реального. Це суттєво ускладнює виконання на практиці умов щодо недопущення «старіння» інформації, що викривається.

1.3. Показники завадостійкості та порядок їх оцінки

Під завадостійкістю [1] РЕЗ будемо розуміти спроможність виконувати задачу в умовах впливу завад, що створюються засобами РЕБ. Це спроможність РЕЗ протистояти РЕБ, тобто, зменшувати її негативний вплив на якість передавання інформації по каналах зв’язку [4].

Враховуючи, той факт, що сучасні системи зв’язку широко застосовують дискретні сигнали, подальше викладення матеріалу сконцентровано на завадостійкості цифрових засобів зв’язку.

1.3.1. Поняття потенційності завадостійкості радіоелектронних засобів. Підходи до оцінки завадостійкості РЕЗ із дискретними сигналами

Нехай будемо вважати, що коли на сигнал не накладаються коливання завади, приймач без помилок відтворить повідомлення, що передано. Якщо на сигнал накрадеться завада (далі буде розглянута завада у вигляді нормального флуктуаційного випадкового процесу), то на вході приймача буде діяти

сумарна напруга, що дорівнює напрузі сигналу плюс напруга завади. В цьому випадку приймач в залежності від сумарного коливання буде відтворювати те чи інше коливання, яке у загальному випадку може відрізнятись від переданого. Таким чином, кожному сумарному коливанню, що впливає на приймач, буде відповідати визначене повідомлення, що при цьому відтворюється.

У різних приймачів ця відповідність може бути різною. В залежності від цієї відповідності приймач буде у більшій або у меншій мірі підвернений впливу завад. Приймач, який має найкращу відповідність є ідеальним та має спотворення сигналу мінімальними з можливих.

Завадостійкість, що характеризується цими мінімально можливими спотвореннями є потенційною завадостійкістю. Ця завадостійкість може бути отримана й у реальному приймачі, якщо він близький до ідеального але вона не може бути перевищена.

Нехай у системі зв'язку передається повідомлення, що можуть приймати m значень [2, 3].

Будемо рахувати, що кожному значенню повідомлення буде відповідати визначений сигнал (коливання), що буде впливати на приймач при передаванні цього повідомлення в умовах відсутності завад.

Позначимо, m значень сигналу як:

$$A_1(t),\ A_2(t),....,\ A_m(t). \tag{1.15}$$

У частковому випадку один з цих сигналів може дорівнювати нулю.

Розкладемо ці сигнали за системою одиничних ортогональних функцій $I_i(t)$ з коефіцієнтами (координатами) $a_{kl} \in \{0,+\infty\}, k=1,...,m$:

$$A_k(t)=\sum_{l=l_1}^{l_2} a_{kl}\cdot I_l(t); \tag{1.16}$$

$$\overline{I_k^2(t)}=1,\ \overline{I_k(t)\cdot I_l(t)}=0,\ k\neq l; \tag{1.17}$$

$$\begin{cases} I_0(t)=1, \\ I_1(t)=\sqrt{2}\sin\dfrac{2\pi}{T}t, \\ I_2(t)=\sqrt{2}\cos\dfrac{2\pi}{T}t, \\ \ldots\ldots\ldots\ldots \\ I_{2m-1}(t)=\sqrt{2}\sin m\dfrac{2\pi}{T}t, \\ I_{2m}(t)=\sqrt{2}\cos m\dfrac{2\pi}{T}t. \end{cases} \qquad (1.18)$$

Коефіцієнти a_{kl} повністю характеризують відповідні функції в (1.16).

Ряд (1.16) по суті є звичайним дискретним перетвореннями Фур'є функції $A_k(t)$ на часовому відрізку $-\frac{T}{2},+\frac{T}{2}$. Покладемо, що всі коливання, що розглядаються лежать у інтервалі $-\frac{T}{2},+\frac{T}{2}$. Виконання цієї умови можливо забезпечити обираючи період T достатньо великим.

На коливання (1.16) накладається завада.

Нехай для усіх частот, що входять до суми, інтенсивність завади буде однаковою та дорівнює δ. У цьому випадку сумарне спостереження, що впливає на приймальний пристрій під час передавання сигналу $A_k(t)$, буде дорівнювати [2]:

$$X(t)=\sum_{l=l_1}^{l_2} x_l \cdot I_l(t)=W_{\mu,\nu}(t)+A_k(t), \qquad (1.19)$$

де: $W_{\mu,\nu}$ – коливання завади, що визначається моделлю нормального флуктуаційного коливання [2] та уявляє собою сукупність великої кількості n коротких імпульсів, що хаотично розташовані у часі та виділені у складову завади з частотами від $f_\mu=\frac{\mu}{T},\ \mu\geq 1$ до $f_\nu=\frac{\nu}{T}$.Таке завадове коливання – нормально флуктуаційне:

$$W(t)=\sum_{k=1}^{n} F_k(t-t_k), \qquad (1.20)$$

де: $F_k(t-t_k)$ – k-й імпульс завади, що потрапив на період часу $-\frac{T}{2},+\frac{T}{2},n\in\{1,+\infty\}$.

Враховуючи результати [1], модель коливання завади в (1.19), за умови представлення рядом Фур'є (відкинути постійну складову) має загальний вигляд [1]:

$$W_{\mu\nu}=\sum_{l=l_1}^{l_2}\frac{\delta}{\sqrt{2T}}I_l(t)\cdot\Theta_l=\frac{\delta}{\sqrt{T}}\sum_{l_1}^{l_2}\left(\Theta_{2l-1}\cdot\sin l\cdot\frac{2\pi}{T}t+\Theta_{2l}\cdot\cos l\cdot\frac{2\pi}{T}t\right), \qquad (1.12)$$

де: $l_1=2\mu-1,\quad l_2=2\nu$ - кількість можливих значень сигналів $A_1(t),A_2(t)$ відповідно.

Випадковий параметр Θ_l має стале значення на інтервалі $-\frac{T}{2},+\frac{T}{2}$, однак значення цього параметру буде змінюватись випадковим чином від досліду до досліду. Всі Θ_l взаємно незалежні, оскільки всі $I_l(t)$ взаємно ортогональні.

Коливання $W_{\mu,\nu}(t)$ є нормально флуктуаційним коливанням з постійною інтенсивністю та частотами від $-\frac{\mu}{T}$ до $-\frac{\nu}{T}$.

У цьому виразі здійснюється додавання по всіх частотах, на які може реагувати приймач.

Виходячи з формул (1.18) – (1.21), отримаємо [1]:

$$x_l=\frac{\delta}{\sqrt{2T}}\cdot\Theta_l+a_{kl}. \qquad (1.22)$$

Коливання (1.19), що впливає на приймач повністю визначається координатами $x_{l1},x_{l_1+1},...,x_{l_2}$.

Модель (1.16 – 1.20) дозволяє визначити "ідеальний" [1], з точки зору завадозахищеності приймач.

Будемо рахувати, що в залежності від загального коливання *X(t)* приймач обов'язково відтворить одне з можливих значень повідомлення. Для кожного приймача з усіх можливих значень *X(t),* тобто з усіх можливих значень сукупності $x_{l_1},x_{l_1+1},...,x_{l_2}$, можна виділити область таких значень, при яких приймач буде відтворюватись повідомлення, що відповідає сигналу $A_1(t)$. Ця область – область сигналу $A_1(t)$. Аналогічно, можна виділити області таких значень, за яких буде відтворюватись повідомлення, що відповідає сигналу $A_2(t)$. Це область сигналу $A_2(t)$ та т. д.

Усю область можливих значень *X(t)* можна розбити таким чином, на *m* не перетинаючи одна одну областей.

Нехай сигнал, що передається матиме вигляд $A_к(t)$. У цьому випадку коливання *X(t)*, що приймає приймач за умови наявності завади буде описуватись координатами (1.15), які можуть приймати випадкові значення. Це обумовлено тим, що Θ_l взаємно незалежні нормальні (розподілені за нормальним законом розподілу) величини. Таким чином, з певною ймовірністю $P^{зав}_{пом}(t)$ коливання *X(t)* може попасти в довільну область. Наприклад, коливання, за умови впливу завад, потрапило у область $A_l(t), i \neq k$. У цьому випадку приймач помилково відтворює повідомлення, що відповідає сигналу $A_i(t)$, замість повідомлення, що відповідає сигналу $A_к(t)$.

Ймовірність $P^{зав}_{пом}(t)$ може бути обраною в якості показника завадостійкості певного РЕЗ. Якщо поставити оптимізаційне завдання мінімізувати $P^{зав}_{пом}(t)$ за певних умов, то можна вирішити відому задачу щодо побудови “ідеального” приймача сигналу в умовах впливу завад. Такий приймач буде забезпечувати максимальну величину ймовірності вірного приймання сигналу в умовах завад $P^{зав}_{впр}(t)$, яку можна обирати в якості показника завадостійкості відповідного приймача сигналів. Ймовірності $P^{зав}_{пом}(t)$ та $P^{зав}_{впр}(t)$ складають повну групу подій:

$$P^{зав}_{впр}(t) + P^{зав}_{пом}(t) = 1 \qquad (1.23)$$

Використовуючи результати [2], конкретизуємо поняття “ідеального” приймача та відповідної до нього “потенційної завадостійкості”.

Зрозуміло, що в залежності від конфігурації областей, що визначаються приймачем, залежить кількість вірно відтворених повідомлень. Поставимо задачу при заданих сигналах (1.15) обрати області значень коливання X(t) так, щоб кількість не вірно відтворених била мінімальною (ймовірність правильного відтворення повідомлень булла максимальною). Приймач, що характеризується такими областями, має мінімальну кількість невірно відтворених повідомлень при накладанні завади та має назву “ідеальний”.

Навіть в “ідеальному” приймачі можуть мати випадки невірного відтворення повідомлень внаслідок викривлень коливання сигналу завадою, що накладається. Знайдена ймовірність невірного відтворення (ймовірність викривлення) повідомлення для “ідеального приймача” буде характеризувати його завадостійкість, яка носить назву - “потенційна завадостійкість”. Ймовірність викривлення під час прийому на реальний приймач може лише досягати цієї величини, але не може бути меншою.

Не гублячи загальності викладення, розглянемо в якості прикладу аналітичну модель “ідеального приймача” дискретних сигналів, що можуть

приймати два значення $A_1(t)$ та $A_2(t)$. Цей випадок являє великий практичний інтерес, оскільки дискретні сигнали часто складаються з слідуючих один за одним елементарних сигналів, кожний з яких має тільки два значення.

Відповідно [2], найбільша ймовірність вірного відтворення повідомлень досягається якщо у приймачі сигнал *X(t)* буде завжди відноситься до області того сигналу, для якого величина:

$$T \cdot \left[X(t) - A_k(t) \right]^2 - \delta^2 \ln P(A_k), \tag{1.24}$$

буде мати найменше значення, де $P(A_k)$ - апріорна ймовірность відправлення сигналу A_k.

Враховуючи результат (1.22), після перетворень маємо, що "ідеальний приймач" у випадку приймання сигналів з двома можливими значеннями повинен відтворити повідомлення, що відповідає повідомленню $A_1(t)$, якщо [2]:

$$T \cdot \left[X(t) - A_1(t) \right]^2 - \delta^2 \ln P(A_1) < T \cdot \left[X(t) - A_2(t) \right]^2 - \delta^2 \ln P(A_2), \tag{1.25}$$

та сигналу $A_2(t)$ у альтернативному випадку.

Ймовірність $P_{пом}^{зав}(t)$ викривлення при "ідеальному" приймальному пристрої та двох дискретних сигналах визначається виразом [2]:

$$P_{пом}^{зав}(t) = P(A_1) \cdot P_{21}(\alpha_{21}) + P(A_2) \cdot P_{12}(\alpha_{12}) \tag{1.26}$$

де $P(A_1)$, $P(A_2)$ – апріорні ймовірності відправлення повідомлення A_1 *та* A_2 відповідно; P_{21}, P_{12} – ймовірність $P(A_2$ *замість* A_1, *та* A_1 *замість* $A_2)$ відповідно [2]:

$$\alpha_{21} = -\alpha + \frac{1}{2\alpha} \ln \frac{P(A_1)}{P(A_2)}, \quad \alpha_{12} = \alpha + \frac{1}{2\alpha} \ln \frac{P(A_2)}{P(A_1)}, \tag{1.27}$$

$$\alpha^2(t) = \frac{T\left[A_1(t) - A_2(t) \right]^2}{2\delta^2}. \tag{1.28}$$

де δ^2 – квадрат інтенсивності завади.

Аналіз виразів (1.26)-(1.28) дозволяє зробити дуже важливі висновки щодо факторів від яких залежить потенційна завадостійкість приймача. Зрозуміло що потенційна завадостійкість залежить від двох факторів:

– відношення ймовірностей:

$$P(A_1)/P(A_2); \qquad (1.29)$$

– та параметру α(t) - (1.28).

Перший фактор залежить виключно від повідомлень, що передаються. Зокрема, для випадку двох сигналів доцільно покласти $P(A_1) = P(A_2) = 0{,}5$.

Другий фактор α залежить від відношення питомої енергії різниці сигналів до квадрату інтенсивності завади δ^2. Чим більше значення набуває це відношення, тим менше ймовірність $P_{пом}^{зав}(t)$ та тим краща потенційна завадостійкість РЕЗ. У цьому факторі, для заданої інтенсивності завад δ можна змінювати лише питому енергію різниці сигналів. З геометричної точки зору потенційна завадостійкість буде визначатись відстанню між точками, що зображують сигнали та буде тим більше, чим більше ця відстань.

Розглянуті у п.п.1.3.1 результати є верхньою межею завадостійкості та в цілому можуть використовуватись для оцінки потенційних (найкращих) значень цього показника, тому у наступному підрозділі посібника розглянуті підходи до оцінки завадостійкості в умовах впливу на практиці низки факторів, що взаємопов'язані між собою.

1.3.2. Оцінка завадостійкості передачі РЕЗ з дискретними повідомленнями за критеріями вірності.

Завадостійкість передачі дискретних повідомлень на практиці визначається сумісною дією великої кількості взаємопов'язаних факторів:

– видом та характеристиками завад та тактикою застосування комплексів РЕБ, сценаріями проведення РЕК, його цілями та динамічністю. Ці матеріали не розглянуті у відомій літературі з завадозахисту у повному обсязі та будуть поглиблені у розділах 2 та 3 навчального посібника;

– надлишковістю;

– способами кодування;

– властивостями сигналів, що передають повідомлення, видом та способами демодуляції (деманіпуляції) та декодування сигналу;

– порушенням синхронізації сигналів, що приймаються та передаються, тощо.

Оцінку завадостійкості в таких умовах доцільно проводити багатоетапною процедурою. На кожному етапі визначають вплив того, чи іншого фактору на показники завадостійкості. Визначають фактори, що є визначальними. Якщо можна, визначають вплив на показники завадостійкості декількох найбільш важливих факторів одночасно. Для цього доцільно застосовувати метод послідовних наближень до реальних умов застосування РЕЗ в умовах РЕК.

Одним з підходів до оцінки завадостійкості РЕЗ є застосування методологічних основ визначення критеріїв вірності передачі повідомлень в

умовах РЕК із застосуванням засобів РЕБ та електромагнітного подавлення [6-8, 9, 14].

Найбільш розвинутим у теоретичному плані є випадок, визначення завадостійкості повідомлень, коли спосіб передачі та характеристики каналу задані. У такому випадку задача оцінки завадостійкості може бути зведена до оцінки вірності різних способів прийому сигналів – способів обробки сигналів у приймальних пристроях.

При розгляді процедури приймання сигналів можуть виникати три добре відомих класів задач:

- виявлення сигналів;
- розрізнення (розділення) сигналів;
- відновлення сигналів.

При виявленні сигналів необхідно встановити, чи є сигнал та завада на вході приймача чи тільки завада. Ця задача типова для засобів радіолокації та може виникати у системах зв'язку з пасивною паузою.

Під час розрізнення (розділення) необхідно визначити, який сигнал з множини відомих, є на вході приймача. Під час вирішення задачі необхідно врахувати не тільки властивості сигналів та завад, а й відмінність сигналів за наявності завад та викривлень. Ця задача є типовою для систем зв'язку із активною паузою.

Задача відновлення сигналів істотно складніше за задачу перши двох типів. Сутність задачі – на основі аналізу прийнятого сигналу отримати сигнал, який найменше відрізняється від того, що переданий.

Показник завадостійкості РЕЗ – ймовірність $P_{\text{п}}$, (див. (1.1)), можна визначити як ймовірність того, що фактичне значення відношення сигнал-шум + завад на виході приймача РЕЗ стане менш деякого критичного $q_{\text{кр}}$ (для відповідного виду завади):

$$P_{\text{п}} = P(q \le q_{кр}), \tag{1.30}$$

при якому функціонування РЕЗ порушується.

У загальному випадку при оцінці $P_{\text{п}}$ необхідно враховувати велику кількість факторів – вид (форму) завади, її інтенсивність, форму корисного сигналу, структуру приймача, антени, способи боротьби із завадами тощо.

Враховуючи велику кількість публікацій щодо оцінки завадостійкості аналогових сигналів [3-15] та тенденцію щодо масового впровадження в практику зв'язку цифрових систем передачі інформації конкретизуємо основні критерії (показники) завадостійкості та прикладі дискретних повідомлень.

Під час аналізу завадостійкості застосовують наступні критерії вірності [5-7]:

- критерій Байєса (середнього ризику);
- критерій ідеального наглядача або критерій Котельникова (повної ймовірності вірного прийму);

- критерій максимум апостеріорної ймовірності;
- мінімаксний критерій;
- критерій Неймана – Пірсона;
- критерій максимальної правдоподібності;
- інформаційний критерій.

Розглянемо коротко ті з критеріїв, які найчастіше застосовуються в телекомунікація.

1.3.2.1. Критерій Байєса

Нехай передаються m-сигналів: $s_i(t), i=1,m$. Прийнятий сигнал позначимо $z(t)=s_i(t)+\xi(t), i=\overline{1,m}$, де $\xi(t)-$ адитивна завада. Введена багатомірна умовна щільність $f(z/s_i)$ розподілу z за умови, що переданий сигнал $s_i(t)$.

Для того щоб мати можливість прийняти рішення про сигнал, який прийшов на вхід приймача, потрібно простір G сигналів, що приймаються розбити на m підпросторів $G_i \in G, i=1,m$. Якщо сигнал $z(t) \in G_i$, приймається рішення що був переданий сигнал $s_i(t)$. Якщо насправді переданий сигнал $s_j(t)$, але сигнал попав до підпростору G_i під впливом завад, то має місце помилка у прийнятті рішення про переданий сигнал. Зрозуміло, що помилки при прийманні сигналу будуть обумовлені порядком ведення РЕП в умовах РЕК, характеристиками завадових сигналів противника та критеріями за якими обирається підпростір прийняття рішень у відповідній ситуації.

Умовна ймовірність вірного приймання сигналу має вигляд [6-7]:

$$p(s_i/s_i)=\int_{G_i} f(z/s_i)dz, \tag{1.31}$$

де інтеграл у загальному випадку є багатомірним.

Умовна ймовірність помилки може бути визначена виразом виду:

$$p(s_j/s_i)=\int_{G_j} f(z/s_i)dz, \tag{1.32}$$

Введемо поняття втрат π_{ij}, що виникають у випадку прийняття помилкового рішення, що був прийнятий сигнал $s_j(t)$, коли дійсно був переданий сигнал $s_i(t)$. У разі безпомилкового прийому доречно покласти $\pi_{ii}=0$.

Умовний риск при передачі сигналу $s_i(t)$ визначимо у вигляді:

$$\rho_i = \sum_{j=1}^{m} \pi_{ij} \cdot p(s_j / s_i), i \neq j. \quad (1.33)$$

Якщо $p(s_i)$ – апріорна ймовірність передачі сигналу $s_i(t)$, середній риск при передачі одного сигналу:

$$\rho = \sum_{j=1}^{m} \rho_i \cdot p(s_i) = \sum_{i=1}^{m} \sum_{j=1}^{m} \pi_{ij} p(s_i) p(s_j / s_i),\ j \neq i. \quad (1.34)$$

Враховуючи (1.32), маємо цільову функцію для оптимізації значення середнього ризику [2]:

$$\rho = \sum_{i=1}^{m} \sum_{j=1}^{m} \pi_{ij} \cdot p(s_i) \cdot \int_{G_i} f(z/s_i) dz \to \min, i \neq j. \quad (1.35)$$

Оптимальним правилом (1.35) прийняття рішення під час прийому повідомлення за критерієм середнього ризику є таке, що мінімізує середній ризик. Параметрами, що впливають на результат пошуку оптимального рішення (1.33) є: характеристики сигналів, структура та параметри операторів перетворення сигналів в каналах, межі областей прийняття рішення.

Вхідними даними для вирішення оптимізаційної задачі є: апріорні ймовірності $p(s_i)$, втрати π_{ij}, характеристики завадових сигналів або умовні щільності ймовірності $f(z/s_i)$.

Критерій середнього ризику є теоретично узагальнюючим. Часткові критерії від цього критерію є: критерій ідеального спостерігача, апостеріорної ймовірності вірного прийому, тощо.

Відмітимо, що для використання критерію (1.34) потрібно мати велику кількість вхідних даних, які отримати на практиці досить складно. Тому далі, не гублячи загальності викладення розглянемо інші критерії вірності, що не мають зазначених недоліків.

1.3.2.2. Критерій ідеального спостерігача (критерій Котельникова).

Нехай, у (1.34) всі помилки призводять до однакових наслідків, тоді можливо покласти $\pi_{ij} = 1, i \neq j$. Це дає змогу перейти від (1.34) до формули повної ймовірності виникнення помилки при прийомі:

$$p = \sum_{i=1}^{m} \sum_{j=1}^{m} p(s_i) \cdot \int_{G_i} f(z/s_i) dz,\ j \neq i. \quad (1.36)$$

Ймовірність вірного прийому, використовуючи поняття “повної” групи випадкових подій прийме наступний вигляд:

$$Q = 1 - p = \sum_{i=1}^{m} \int_{G_i} f(z/s_i) \cdot p(s_i) dz. \cdot \tag{1.37}$$

Оптимальним за критерієм ідеального спостерігача є той спосіб передачі повідомлення в умовах завад, за якого ймовірність виникнення помилки є мінімальною, відповідно ймовірність вірного прийому є максимальною. Параметри, що є змінними під час вирішення задачі оптимізації, є аналогічними п.1.3.2.1. Спрощення задачі досягаються завдяки тому, що не враховується різниця у наслідках помилок. Максимальне значення Q досягається тоді, коли рішення про те, що прийнятий сигнал відноситься до області рішень $z(t) \in G_i$, приймається за правилом:

$$f(z/s_i) \cdot p(s_i) > f(z/s_j) \cdot p(s_j),\ j \neq i. \tag{1.38}$$

Аналіз m-1 умов (1.35) відповідає алгоритму вигляду:

$$\max_i [f(z/s_j) \cdot p(s_j)] = p(z/s_i) \cdot p(s_i) \tag{1.39}$$

Регіструється той сигнал $s_i(t)$, для якого апріорна щільність розподілу максимальна. Оптимальний приймач, що побудований за цим правилом прийняття рішення є ідеальним приймачем Котельникова (див. п.п.1.3.1).

1.3.2.3. Критерій максимуму апостеріорної імовірності

Враховуючи що, $f(z/s_i) \cdot p(s_i) = p(s_i/z) \cdot f(z)$, де $p(s_i/z)$ – апостеріорна ймовірність того, що сигнал $s_i(t)$ був переданий за умови, що був прийнятий сигнал z; $f(z)$ – безумовна щільність розподілу прийнятого сигналу, що у відповідності з формулою Байєса:

$$p(s_i/z) = \frac{p(s_i) \cdot f(z/s_i)}{\sum_{i=1}^{m} p(s_i) \cdot f(z/s_i)}. \tag{1.40}$$

Якщо оптимальний приймач реалізує алгоритм:

$$\max_j [p(s_j/z)] = p(s_i/z). \tag{1.41}$$

та приймає в цьому випадку рішення про наявність сигналу $s_i(t)$, то говорять, що він забезпечує максимум апостеріорної ймовірності вірного прийому.

Порівняння алгоритмів (1.38) та (1.40) показує, що призводять до одного й того ж оптимального рішення. Відповідно, критерій ідеального спостерігача, максимум апріорної щільності розподілу та максимум апостеріорної ймовірності мають однакову силу. Для вирішення задач оптимізації за цими критеріями потрібно мати одні й ті самі вхідні дані, що відрізняються рівнем знань про апріорні ймовірності $p(s_i)$.

1.3.2.4. Критерій мінімакса

Цей критерій можна застосувати у тих випадках, коли апріорні ймовірності появи сигналів у формулі (1.32) невідомі. Задачу оптимізації вирішують для найгіршого випадку розподілу ймовірностей $p(s_i)$, $i=\overline{1,m}$, та припускають такий їх розподіл, який доставляє максимум середнього ризику. При цьому використовують критерій виду

$$\rho = \min_{G_j} \max_{p(s_i)} \sum_{i=1}^{m} \sum_{j=1}^{m} \pi_{ij} \cdot p(s_i) \cdot \int_{G_i} f(z/s_i) dz,\ j \neq i. \qquad (1.42)$$

Операція мінімізації максимального ризику може виконуватись шляхом вибору інших змінних. Мінімаксний критерій не потребує знання апріорних ймовірностей, але призводить до занадто обережних рішень.

1.3.2.5. Критерій максимальної правдоподібності

Основним поняттям при застосуванні цього критерію є функція правдоподібності. Під цим поняттям будемо розуміти умовну щільність розподілу ймовірностей $f(z/s_i)$, найбільш правдоподібна гіпотеза для якої:

$$f(z/s_i) = \max_{j} \left[f(z/s_j) \right]. \qquad (1.43)$$

Оптимальним є такий спосіб прийому повідомлення, при якому реалізований алгоритм (1.40). Алгоритм (1.40) є окремим випадком алгоритмом (1.36) при виконанні умови $p(s_i) = p(s_j) = \frac{1}{m},\ i,\ j = 1,2,3,...,m$.

Критерій максимальної правдоподібності отримав велике розповсюдження, тому що він є відносно простим, не потребує великого об'єму вхідних даних, непогано відображає більшість реальних умов передачі повідомлень. Апаратурна реалізація алгоритмів максимальної правдоподібності відносно нескладна, при цьому результати застосування алгоритмів в багатьох випадках практично співпадають з іншими, більш складними правилами прийняття рішення.

Розглянуті у п. п 3.1.1-3.1.2 основні критерії та підходи до оцінки завадостійкості побудовані на основі врахування статистичних властивостей завадових сигналів та на математичному апараті теорії статистичних рішень.

Таким чином, можливо узагальнити, що теорія завадостійкості, як основа статистичної теорії зв'язку зобов'язана своєю появою дисертаційній роботі В. Котельникова "Теорія потенційної завадостійкості" (1947 рік). У відповідній монографії була сформульована та вирішена задача статистичного

синтезу оптимальних приймальних пристроїв, визначена гранична завадостійкість, що асимптотично може бути досягнута, але не може бути перевершена.

У 1948 році була представлена основоположна робота К. Шеннона “Математична теорія зв’язку”. Об’єктом дослідження авторів робіт був “канал із завадами”. Пропозиції К. Шеннона базувались на цілеспрямованому перетворенні (кодуванні) повідомлень, що передаються із застосуванням основних положень теорії інформації.

Враховуючи той факт, що питання оцінки, забезпечення та підвищення завадозахищеності систем зв’язку в умовах ведення гібридної війни проти України не досліджені у повному обсязі, вони є актуальми для систем зв’язку в умовах масованого застосування противником комплексів (засобів) РЕБ і тому вимагають розробки сучасних ефективних пропозицій щодо радіоелектронного захисту своїх телекомунікаційних систем. Для цього необхідно детально ознайомитись з основними положеннями ведення РЕБ в сучасних гібридних діях та воєнних конфліктах, викласти основні положення теорії РЕБ для глибокого розуміння порядку організації деструктивного впливу на елементи систем зв’язку з метою їх радіоелектронного захисту. Це дозволить в подальшому проводити дослідження з розробки методів та способів забезпечення завадостійкості СпСз в умовах активного застосування противником угруповань новітніх комплексів РЕБ.

Контрольні запитання до 1 розділу:

1. В чому сутність поняття завадозахищеності РЕЗ?
2. Що таке енергетична прихованість, які її показники Вам відомі?
3. Що таке завадостійкість, які її показники Вам відомі?
4. Що таке “потенційна” завадостійкість? Дайте визначення.
5. Що таке “ідеальний” приймач В. Котельникова?
6. Як Ви розумієте вплив навмисного завадового коливання на ефективність застосування системи зв’язку?
7. Які фактори впливають на порядок оцінки завадостійкості РЕЗ в умовах дій активних завад?
8. Наведіть порядок оцінки завадостійкості передачі РЕЗ з дискретними повідомленнями за критеріями вірності
9. Наведіть визначення критерія середнього риска (Байєровий критерій)
10. Наведіть визначення Критерій ідеального спостерігача (критерій Котельникова)
11. Наведіть визначення критерія максимуму апостеріорної імовірності
12. Наведіть визначення Критерій мінімакса
13. Наведіть визначення Критерій максимальної правдоподібності
14. Наведіть визначення Критерії та підходи до оцінки завадостійкості повідомлень на основі теорії інформації та кодування.

15. Які Вам відомі показники завадостійкості, що сформульовані із застосуванням теореми К. Шеннона щодо перепускної здатності каналу в умовах дій завад?

РОЗДІЛ 2
ЗАГАЛЬНІ ПОНЯТТЯ, ПОЛОЖЕННЯ ТА СКЛАДОВІ ЧАСТИНИ РЕБ

2.1. Основні історичні етапи розвитку радіоелектронної боротьби

Перші кроки у веденні радіоелектронної боротьби були зроблені з початком застосування радіо у військовій справі. У 1903 році винахідник радіо професор О.С. Попов висловив думку про можливість ведення радіорозвідки, створення радіозавад і вперше запропонував приймати заходи захисту від них [9, 10-12, 17].

Радіозавади у бойових діях вперше були застосовані в ході **російсько-японської війни (1904-1905 рр.)**. В квітні 1904 р. під час артилерійського обстрілу японськими крейсерами внутрішнього рейду м. Порт-Артур радіостанції броненосця “Победа” ускладнили передачу даних з кораблів-корегувальників на крейсер “Такасаго”. Під час Цусімської битви (14-15.05.1905 р.) крейсер “Изумруд” і броненосець “Громкий” подавили радіозв’язок японських кораблів.

У 1911 році професором радіотехніки А.П. Петровським були теоретично обґрунтовані способи створення радіозавад і захисту радіозв’язку, які випробовувались на Чорноморському та Балтійському флотах.

Разом із порушенням радіозв’язку шляхом створення радіозавад в Першу світову війну (1914 р.) зародилися радіопеленгація, радіоперехоплення, радіодезінформація.

У період між Першою та Другою світовими війнами способи та засоби протидії радіоелектронним засобам набули ще більш широкого розвитку. З метою протидії лініям управління танками та літаками по радіо були розроблені станції активних завад “Шторм” на ультракоротких хвилях і “Шторм-2” на середніх хвилях. А у 1937 році була розроблена станція завад “Грім” для подавлення радіозв’язків у короткохвильовому діапазоні.

Під час **другої світової війни (1939-1945 рр.)** способи ведення РЕБ на різних театрах військових дій мали певні особливості: на Західно – Європейському ТВД РЕБ велася переважно для подавлення засобів радіолокації і радіонавігації систем ППО, ВПС і ВМС. На радянсько-германському фронті РЕБ велась, головним чином, для порушення радіозв’язку сухопутних військ.

Найбільш визначними подіями застосування засобів РЕБ в цей період були наступні.

В липні 1943 року авіація союзників під час нальоту на Гамбург вперше застосувала пасивні завади РЛС ППО, скидаючи смуги з алюмінієвої фольги. Під час нічного нальоту з англійських бомбардувальників було скинуто декілька тисяч пачок по 2000 смуг в кожній, що дозволило подавити роботу РЛС гарматного наведення і наведення винищувачів.

Починаючи з 1943 року майже всі держави коаліцій почали використовувати пасивні завади, внаслідок чого втрати союзної авіації інколи зменшувались в два-три рази.

В цей же період з літаків стали створюватись активні завади. Наприкінці війни засоби радіозавад були встановлені на усіх американських і на 10% англійських бомбардувальників.

За масштабами застосування засобів і різноманітності тактичних прийомів РЕБ найбільш визначною була операція по висадці союзницьких військ в Нормандії в червні 1944 року. Завдяки дезорганізації радіолокаційної системи розвідки Німеччини, союзники втратили з двох тисяч кораблів лише шість, з 105 літаків-постановників завад – три.

На Східному фронті вперше радіозавади були застосовані 6 вересня 1941 року при нанесенні військами Червоної Армії контрудару під м. Єльня.

Успішно радіозавади застосовувались при розгромі оточеного угруповання під Сталінградом. В цей час були сформовані спеціальні частини, а у 1944 році окремі радіодивізіони спеціального призначення, які стали прототипом сучасних частин РЕБ.

Радіодивізіони порушували радіозв'язок в битвах під Курським, в Смоленській, Корсунь-Шевченківській, Білоруській, ВіслоОдерській, Берлінській та інших операціях. В ході визволення Кенігсбергу вперше з'явився термін "радіоблокада" [10-12].

Під час **війни в Кореї (1951-1953 р.р.)** у ВПС США були створені ескадрильї постановників завад ТВ-25j "Мітчелл". Літаки РЕБ діяли із бойових порядків тактичних груп та у складі груп забезпечення. З'явилась апаратура сигналізації про опромінення РЛС, застосовувалося комплексне створення активних та пасивних завад для подавлення РЛС виявлення, наведення та ціле вказання, управління вогнем ЗА [10].

Внаслідок застосування авіацією США застарілої техніки РЕБ було втрачено біля 2200 літаків [9].

Результати війни в Кореї підштовхнули процес створення країнами НАТО засобів та систем РЕБ нового покоління, які були застосовані під час бойових дій авіацією США у **В'єтнамі (1964-1973 рр.).**

Для попередження екіпажів літаків про опромінення РЛС використовувались приймачі виявлення, на бомбардувальниках почали встановлювати засоби завад індивідуального захисту. З'явились контейнерні станції завад (на літаках F-4).

З метою ефективного застосування літаків РЕБ з бойових порядків тактичних груп був створений літак ЕА-6В "Проулер", на якому встановлювались станції завад, що маскують та імітують для подавлення станцій наведення ЗРК та РЛС дальнього виявлення і наведення; станції завад УКХ радіозв'язку та радіолініям наведення, автомати пасивних завад, станції радіорозвідки. Аналіз радіоелектронної обстановки та управління засобами РЕБ здійснювалось електронно – обчислювальними машинами (ЕОМ).

Важливу роль під час проведення повітряних операцій виконували літаки пошуку та ураження наземних РЛС F-4G "Уайлд Уізл". Вони були озброєні

ракетами “повітря – РЛС” “Шрайк”, які вперше були застосовані у 1966 році [10-12].

Крім вказаних засобів РЕБ застосовувалися передавачі завад одноразового використання, хибні теплові та радіолокаційні цілі і безпілотні літаки РЕБ.

Війська ППО застосовували радіомаскування та радіоелектронний захист своїх РЕЗ.

У війнах **на Близькому Сході** велика роль відводилась РЕБ. Ізраїлем велась безперервна і інтенсивна розвідка. З початком агресії у червні 1967 року був порушений радіозв’язок між арабськими державами, подавлені РЕЗ ППО, наведення зенітно-ракетні комплекси і зенітна артилерія. У жовтневій війні 1973 року Ізраїль розробив і застосував власні засоби РЕБ, широко застосовувались демонстративні дії авіації і безпілотні літаки РЕБ. Наземні частини РЕБ в основному порушували радіомережі управління частинами сухопутних військ арабських країн.

В ході **бойових дій в Лівані (червень 1982 року)** приймали участь літаки радіотехнічної розвідки, літаки РЕБ, засоби індивідуального захисту, наземні станції розвідки і радіозавад, аеростати. Комплексне застосування засобів розвідки і РЕБ дозволило знищити 17 ЗРК з 19, що були розгорнуті Сирією в долині Бека.

В **англо-аргентинському конфлікті на Фолклендських островах (1982 р.)** РЕБ велась переважно англійською стороною. В основному подавлялись РЛС управління вогнем ЗА і головки самонаведення крилатих ракет. Внаслідок 167 бойових вильотів без засобів РЕБ аргентинська авіація втратила 117 літаків. Англійська авіація втратила лише 10 літаків і вертольотів [10-12].

В квітні 1986 року США був нанесений авіаційний удар по об’єктах Лівії. Ударну авіацію підтримували дві групи РЕБ у складі літаків РЕБ EF-111A та EA-6B, винищувачі F/A-18 озброєні протирадіолокаційними ракетами. Контроль і управління забезпечували два літаки ДРЛВУ Е-2С “Хокай”. Розвідку вели штучні супутники землі і літаки стратегічної розвідки SR-71 і RC-135. Внаслідок застосування засобів РЕБ з 30 літаків був збитий лише один.

Радіоелектронна боротьба в бойових діях авіаційних частин на території **Афганістану (1979-1989 рр.)** велась з метою дезорганізації управління засобами ППО повстанців, захисту літальних апаратів від ураження самонавідною зброєю, зниження можливостей противника по веденню розвідки. Найбільш небезпечними виявились ПЗРК “Стінгер” і “Блоупайп”. Для захисту літаків і вертольотів виконувалось перенацілювання інфрачервоних головок самонаведення ракет на хибні теплові цілі. Середні витрати ЗРК на один уражений літак складали 2,4 ракети (27 ракет при застосуванні засобів РЕБ). В якості групових засобів створення УТЦ широке застосування знайшли освітлювальні авіаційні бомби. Для захисту вертольотів

була розроблена станція оптико-електронного подавлення “Іспанка”. Використовувались різноманітні тактичні прийоми [9].

Перед початком **операції багатонаціональних сил** анти Іракської коаліції в зоні Перської затоки проти Іраку **“Буря в пустелі”** було створено та почало активно діяти угруповання розвідки, яке включало космічну, повітряну та наземну компоненти. Повітряну радіолокаційну розвідку та наведення винищувачів, здійснювали 41 літак дальнього радіолокаційного виявлення (ДРЛВУ): 17 Е-3А системи AWACS та 24 Е-2С “Хокай”. Вперше була залучена система повітряної радіолокаційної розвідки і ціле вказання “JSTARS”.

Вперше в історії в межах операції “Буря в пустелі” була проведена операція РЕБ, до якої були залучені авіаційні, морські та наземні сили та засоби РЕБ.

Операція РЕБ складалась з узгоджених за часом та місцем, цілеспрямованих радіоелектронних, радіоелектронно-вогневих і вогневих ударів та радіоелектронного блокування з метою досягнення панування в електромагнітному просторі, дезорганізації системи управління та подавлення системи ППО Іраку. Літаки РЕБ діяли у зонах баражування поза зоною ураження. На кожному з трьох напрямків удару для подавлення РЕЗ ППО в зонах баражування діяло біля третини літаків РЕБ, залучених до масованого авіаційного удару, інші – у складі ударних груп. Добре організована РЕБ з боку багатонаціональних сил та недостатній рівень захищеності від завад застарілого парку РЛС ППО Іраку дозволили звести до мінімуму втрати авіації багатонаціональних сил (усього 60 літаків) [9, 11].

Спільна операція ВПС США та Великобританії проти Іраку **“Лис пустелі”** (1998 рік) у військовому відношенні стала розвитком форм та способів ведення РЕБ, які вперше були випробувані у 1991 році. Характерними рисами операції “Лис пустелі”, з точки зору застосування засобів РЕБ були:

- постановка завад у повітрі здійснювалась тільки із завчасно встановлених зон баражування літаками ЕА-6В;
- відсутність наземної компоненти РЕБ та виконання цих задач силами РЕБ морського базування;
- відсутність літаків РЕБ ЕС-130Н, призначених для подавлення радіоліній наведення винищувачів.

За оцінками західних фахівців операція “Лис пустелі” досягла своєї мети без втрат з боку ВПС США і Великобританії.

Особливістю операції об’єднаних збройних сил НАТО проти Союзної республіки Югославія **“Союзницька сила” (1999 р.)** було впровадження і широкомасштабне ведення інформаційної боротьби. Застосовувались літаки інформаційної боротьби типу ЕС-130Е.

В об’єднаних збройних силах (ОЗС) НАТО було створене угруповання сил та засобів РЕБ у складі 23 літаків (3 – ЕС-130Н, 14 – Торнадо - ECR, 6 – ЕА-6В). Для подавлення ППО вогнем використовувались літаки F-16CJ- носії протирадіолокаційних ракет HARM. Крім того, 100% авіації, яка приймала

участь в нанесенні ударів, була оснащена засобами індивідуального захисту. По мірі розширення сектору нанесення ударів кількість літаків РЕБ збільшувалась і на кінець операції склала 50 літаків.

У ході конфлікту планувались та проводились операції по подавленню ППО СРЮ, які представляли собою узгоджені дії літаків РЕБ та ударних літаків і складались з декількох етапів. Спочатку демонстративні групи (безпілотні літальні апарати) хибними вторгненнями в повітряний простір примушували включати радіолокаційні засоби ППО на випромінювання (цей етап мав назву "демонстрація" або "виклик"). На другому етапі літаки РЕБ ставили прицільні активні завади РЛС із зон баражування за межами зон ураження ЗРК (ця фаза мала назву "осліплення"). Під прикриттям завад літаки-носії керованих ракет "повітря – РЛС" досягали рубежу пуску, самонавідні головки ракет захоплювали цілі-випромінювачі на автоматичне супроводження, за сигналом захвату льотчик виконував пуск та розвертав літак від цілі (етап "ураження"). Таким чином, літаки трьох різних типів у тісній взаємодії виконували різні функції в рамках одного завдання.

При проведенні групових авіаударів до 15% літаків групи вирішували завдання подавлення ППО. На кожному напрямку повітряного удару діяло до 4 літаків ЕА-6В із зон баражування, а у складі бойових порядків ударних груп використовувались літаки Торнадо ECR (до 6 на кожному напрямку) та літаки-носії керованих ракет "повітря – РЛС" HARM. Всього за час операції було використано близько 800 ракет HARM. Для управління авіацією застосовувались повітряні КП ЕС-130Е, літаки ДРЛВУ Е-3А AWACS та літак РЛР і цілевказання Е-8С JSTARS. Для РЕП системи радіозв'язку Збройних Сил СРЮ активно застосовувались 3 літаки ЕС-130Н "Компас – Колл". Всього за період операції було зроблено до 240 вильотів загальною тривалістю біля 2100 годин.

Особливістю РЕБ **в операції "Непохитна свобода" у Афганістані (2001 р.)** було порівняно широке застосування засобів індивідуального та групового захисту літаків та вертольотів від оптико-електронної зброї. При атаках наземних цілей літаками тактичної та палубної авіації відстріл піропатронів здійснювався з моменту уведення в пікірування та на виході з пікірування з одночасним виконанням протизенітного і протиракетного маневрів з максимально можливим перевантаженням. В якості групових засобів створення удаваних теплових цілей широко застосовувались освітлювальні авіаційні бомби.

В операції "Свобода Іраку" (2003 р.) масованого подавлення РЕЗ систем ППО Іраку не здійснювалось, завади створювалися епізодично з зон баражування без входу в зону ППО Іраку. Суттєво підвищилась роль РЕБ у боротьбі з радіокерованою зброєю при виконанні тактичних завдань.

Виходячи з проведеного військово-історичного аналізу в розвитку радіоелектронної боротьби можна виділити чотири основних етапи [10-12].

Перший етап – зародження РЕБ (1904-1939 р.). Його характерними рисами є використання окремих впливів радіозавадами на РЕЗ противника в

обмежених районах із застосуванням, як правило, спеціальних станцій радіозв'язку із приставками завад.

Другий етап охоплює період від Другої світової війни до початку війни у В'єтнамі (1939-1964 р.).

Основним змістом даного етапу розвитку радіоелектронної боротьби у світовій практиці було розширення арсеналу засобів РЕБ і покращення їх тактико-технічних характеристик.

Третій етап – охоплює період з 1964 до 1991 року.

Аналіз показав, що на третьому етапі відбулась якісна трансформація як військового аспекту – перетворення радіоелектронної боротьби в самостійний вид оперативного (бойового) забезпечення з розширенням її масштабів до масштабів застосування сил, так і технічного – створення автоматизованих комплексів і систем РЕБ.

Четвертий етап – розпочався з 1991 року і триває по теперішній час.

У війні в Перській затоці 1991 року вперше в практиці воєнних дій такого масштабу США була здійснена інтеграція систем розвідки, управління силами і зброєю багатонаціональних сил усіх рівнів. Стійкість і ефективність роботи цих систем багато в чому визначила хід бойових дій. Вперше в історії в межах операції "Буря в пустелі" була проведена операція РЕБ.

Зазначимо, що основним джерелом розвитку та трансформації РЕБ на усіх етапах є постійне протиріччя між вдосконаленням систем управління всіх рівнів та спроможністю сил та засобів РЕБ щодо вирішення покладених на них завдань. При цьому роль РЕБ у досягненні мети збройної боротьби постійно зростає.

2.2. Визначення, мета, завдання та складові частини радіоелектронної боротьби

Радіоелектронна боротьба (РЕБ) – це сукупність узгоджених за метою, завданнями, простором і часом заходів та дій з електронного забезпечення, радіоелектронного подавлення (РЕП) та радіоелектронного захисту (РЕЗт) систем і засобів управління військами (силами) і зброєю відповідно противника та своїх, які організуються командирами і штабами всіх рівнів, проводяться частинами та підрозділами РЕБ, а також об'єднаннями, з'єднаннями, частинами, підрозділами родів військ і спеціальних військ та спрямовані на забезпечення потрібної ефективності застосування своїх військ (сил) та зброї при вирішенні завдань збройної боротьби [18-21].

Радіоелектронна боротьба є одним із основних видів оперативного (бойового) забезпечення операцій (бойових дій) і дозволяє досягти переваги над противником в управлінні військами (силами) та зброєю [18, 19].

Радіоелектронна боротьба організується і ведеться з метою створення умов для найбільш ефективного застосування своїх військ (сил) в операціях (бойових діях) за рахунок дезорганізації управління військами та зброєю противника, зниження його можливостей щодо ведення розвідки, радіоелектронного подавлення та вогневого ураження, а також забезпечення

стійкої роботи своїх радіоелектронних систем та засобів управління військами (силами) і зброєю.

Основним завданням РЕБ є [18-19]**:**

– дезорганізація управління противника шляхом РЕП (у перспективі, функціонального ураження електромагнітними імпульсами, спеціальними програмно-комп'ютерними засобами, які впроваджуються у комп'ютерні мережі) найбільш важливих радіоелектронних об'єктів систем управління військами (силами) та зброєю;

– організація та проведення заходів щодо радіоелектронного захисту своїх систем управління військами (силами) та зброєю, рис. 2.1.

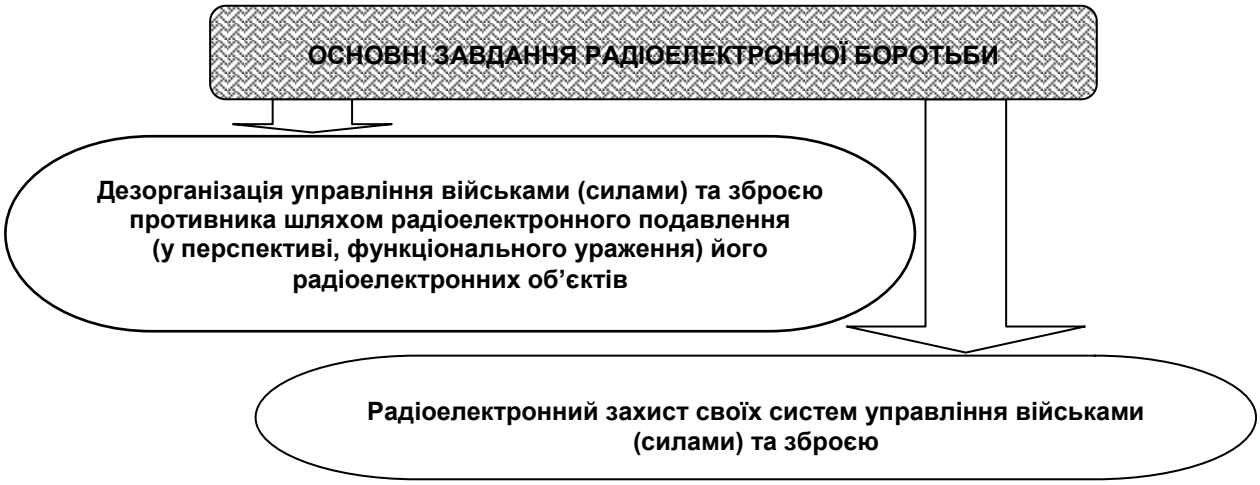


Рис. 2.1. Основні завдання РЕБ

Відповідно до визначених завдань, РЕБ включає **радіоелектронне подавлення** радіоелектронних об'єктів противника, **радіоелектронний захист** своїх систем та засобів управління військами і зброєю (рис. 2.2), радіоелектронне забезпечення та здійснюється у тісному поєднанні з діями об'єднань, з'єднань, частин і підрозділів видів Збройних Сил, родів військ і спеціальних військ по вогневому ураженню, знищенню (захопленню, виведенню з ладу) радіоелектронних об'єктів систем управління військами (силами) противника [18-21].

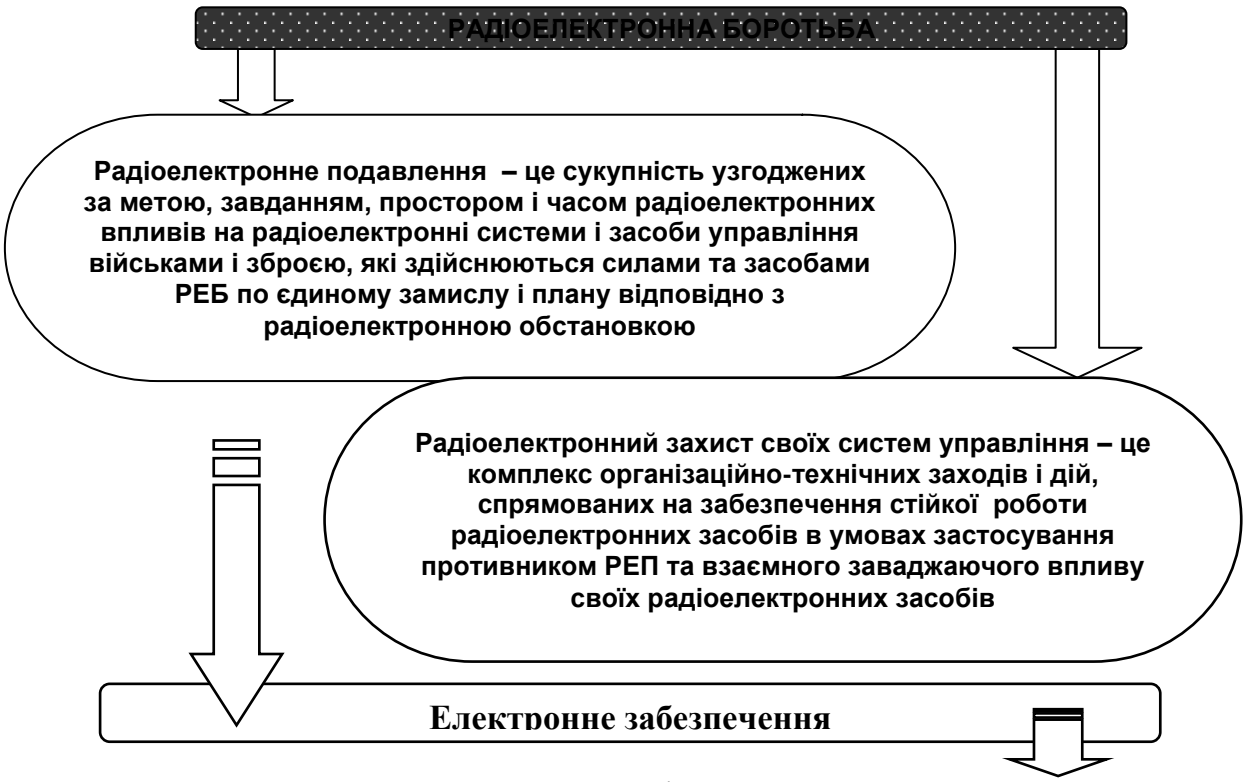


Рис. 2.2. Складові частини РЕБ

Для вирішення завдань з РЕБ створюється система РЕБ відповідного масштабу вирішення завдань. Зокрема, на рівні ЗСУ – система РЕБ Збройних Сил, в операції (бойових діях) – система РЕБ в операції (бойових діях).

Під системою РЕБ розуміють сукупність взаємопов'язаних елементів (підсистем), кожний з яких має особисті властивості та призначення, що забезпечує якісне вирішення завдань з РЕБ у відповідних масштабах та умовах обстановки.

У загальному вигляді система РЕБ відповідає усім властивостям та вимогам, що притаманні складним організаційно - технічним системам та може вміщати підсистеми: активного впливу (у перспективі, функціонального ураження) радіоелектронних систем та засобів противника в операції (бойових діях); радіоелектронного захисту своїх систем управління; електронного та всебічного забезпечення; управління (рис.2.3).

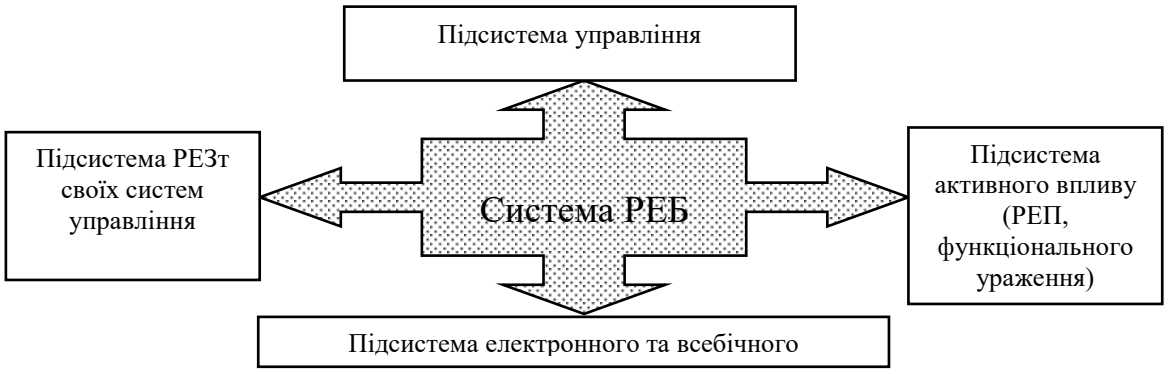


Рис. 2.3. Структура системи РЕБ

2.3. Принципи і форми радіоелектронної боротьби

Радіоелектронна боротьба організується і ведеться на основі визначених принципів, у відповідних формах, що забезпечують досягнення мети РЕБ.

Принципами РЕБ є загальні об'єктивні положення, на основі яких організується та ведеться радіоелектронна боротьба.

Основними **принципами РЕБ** в операціях (бойових діях) є [18-21]: відповідність; цілеспрямованість; активність; раптовість; випередження; масоване і комплексне застосування сил і засобів радіоелектронного подавлення в тісному поєднанні з вогневим ураженням і знищенням основних об'єктів систем і засобів управління військами і зброєю; неперервність і комплексність здійснення заходів з радіоелектронного захисту систем і засобів управління своїми військами і зброєю (рис. 2.4.).

Відповідність РЕБ виконанню завдань за бойовим призначенням досягається: підтриманням постійної готовності сил та засобів РЕБ; своєчасним оснащенням військ відповідними системами і засобами; розробкою сучасних способів їх ефективного застосування; безперечним виконанням військами (силами) заходів з РЕБ; розробкою декількох варіантів ведення РЕБ (моделюванням РЕБ); реалізацією бойових можливостей сил та засобів РЕБ в складній оперативній та радіоелектронній обстановці; завчасною підготовкою до ведення РЕБ в операціях (бойових діях) з урахуванням особливостей оперативного напрямку (району бойових дій); бойового досвіду противника та своїх військ.

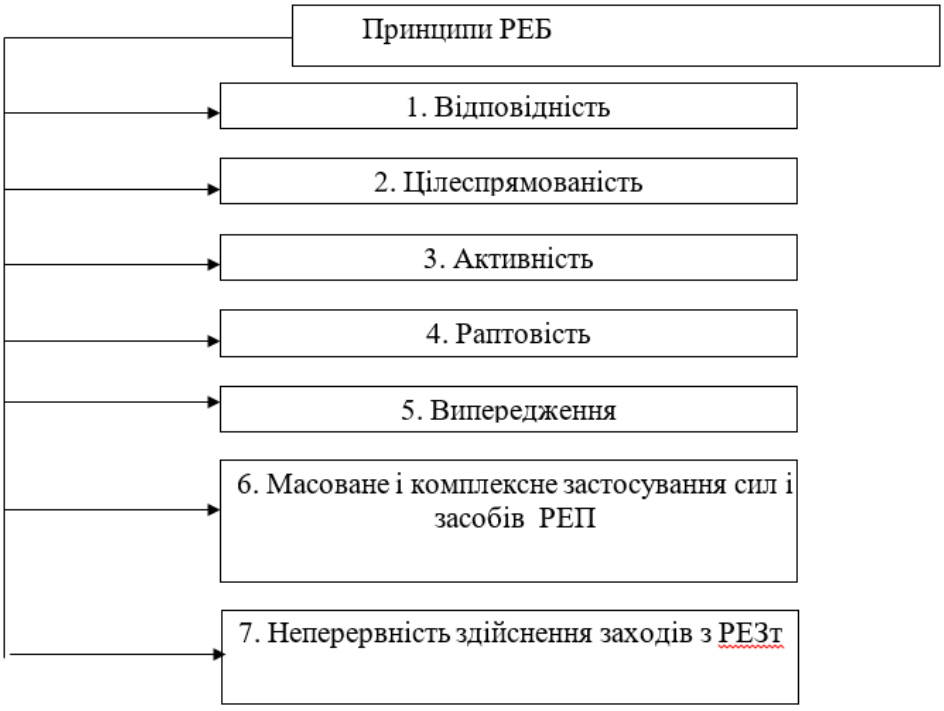


Рис 2.4. Принципи радіоелектронної боротьби.

Цілеспрямованість РЕБ містить в собі відповідність її мети, завдань та заходів замислу операції (бойових дій); зосередження основних зусиль у вирішальний момент на головному напрямку та важливих об'єктах (районах) для виконання головних завдань.

Вона досягається організацією РЕБ за єдиним замислом та планом; вмілим розподілом сил та засобів по напрямкам дій, оперативним (бойовим) завданням військ; централізованим, стійким, неперервним, оперативним та прихованим управлінням силами та засобами РЕБ; постійним уточненням військам завдань з РЕБ та контроля їх виконання.

Активність РЕБ полягає в постійному пошуку найбільш ефективних способів вирішення завдань РЕБ щодо дезорганізації управління противника, готовності та спроможності штабів та військ у будь-яких умовах обстановки вміло організовувати та наполегливо здійснювати дезорганізацію управління противника, виконувати заходи щодо радіоелектронного захисту своїх систем управління.

Вона досягається своєчасним добуванням даних про системи і засоби управління військами, розвідки та РЕБ, РУК противника; аналізом та оцінкою їх можливостей; прогнозуванням їх способів бойового застосування; прихованою своєчасною підготовкою до бойового застосування сил та засобів, що залучаються до виконання завдань РЕБ; їх рішучими та ініціативними діями в ході операцій (бойових дій); організацією та підтримкою чіткої та неперервної взаємодії штабів усіх ланок управління з питань РЕБ з частинами радіо- та радіотехнічної розвідки; об'єднаннями, з'єднаннями видів Збройних Сил, родів військ і спеціальних військ; забезпечення найбільшої ефективності радіоелектронного захисту РЕЗ; відповідною підготовкою органів та частин РЕБ.

Раптовість РЕБ включає дії щодо дезорганізації системи управління противника, а також заходи з РЕЗ радіоелектронних засобів, які не очікуються противником. Раптовість досягається збереженням в таємниці запланованих дій та заходів і дезінформацією противника щодо планів ведення РЕБ; завчасною підготовкою сил та засобів РЕБ, військ до дій; своєчасністю і прихованістю їх розгортання (перегрупування); застосуванням нових, невідомих противнику засобів РЕП, форм і способів ведення РЕБ.

Випередження ведення РЕБ полягає у рішучому вирішенні завдань РЕБ, які упереджують дії противника по відношенню до бойових завдань в операції (бойових діях) своїх військ, що обумовлені ключовою роллю радіоелектронних систем і засобів у забезпеченні дій військ і визначають можливість реалізації їх бойового потенціалу.

Воно досягається: прогнозуванням можливих змін РЕО та намірів противника; своєчасною постановкою завдань силам та засобам РЕБ; своєчасним нарощуванням зусиль, вмілим використанням резервів у поєднанні з маневром; постійним виявленням слабких місць в системі управління військами та зброєю, використання їх для дезорганізації управління; створенням оманної РЕО (проведенням радіоелектронної

дезінформації); своєчасним відновленням боєздатності частин РЕБ та їх всебічним забезпеченням.

Масоване і комплексне застосування сил і засобів РЕП полягає у використанні на найважливіших напрямках (в районах) і у вирішальні моменти операції (бою) більшої частини сил і засобів, що залучаються до ведення РЕБ, в поєднанні з вогневим ураженням найбільш важливих пунктів управління і радіоелектронних об'єктів противника.

Неперервність і комплексність здійснення заходів з радіоелектронного захисту систем і засобів управління військами і зброєю забезпечується одночасним застосуванням узгоджених за метою, місцем і часом заходів і дій, постійному їх проведенні в усіх видах бойової діяльності військ, у будь-яких умовах обстановки, з урахуванням особливостей ведення радіоелектронної розвідки, РЕБ і застосування противником високоточної керованої зброї.

Завершивши викладення принципів РЕБ, доцільно перейти до розгляду такого важливого поняття як форми РЕБ.

Форма РЕБ – це зовнішній вираз (масштабно-просторова та часова характеристика) відповідних варіантів застосування сил та засобів РЕБ з метою виконання конкретного завдання РЕБ в умовах обстановки, що склалася.

Формами РЕБ, які використовуються в сучасних умовах, є: радіоелектронний вплив (окремий, періодичний, систематичний); радіоелектронно-вогневий вплив; радіоелектронний удар; радіоелектронно-вогневий удар; радіоелектронно-уражаючий удар; стримування радіоелектронного впливу; радіоелектронно-вогневий бій; систематичні дії з радіоелектронної боротьби; радіоелектронна блокада; маневр засобами РЕБ; операція РЕБ (рис. 2.5.) [10-12].

Радіоелектронний вплив – це форма впливу окремими, періодичними, систематичними радіоелектронними завадами на системи управління військами і зброєю, яка здійснюється силами та засобами РЕБ за єдиним замислом і планом відповідно з поточною РЕО, на одному або декількох окремих напрямках [10].

Радіоелектронно-вогневий вплив – це форма комплексної дії радіоелектронними завадами на РЕЗ управління військами і зброєю, їх вогневе ураження самонавідною на випромінювання зброєю. Цей вплив проводиться різнорідними силами та засобами за єдиним замислом і планом відповідно до поточної обстановки з метою вирішення завдань дезорганізації управління противника на окремому напрямку (об'єкті).

Радіоелектронний удар – це особлива форма відносно короткочасного, досить потужного впливу засобів РЕБ у встановлений термін по окремому радіоелектронному об'єкту.

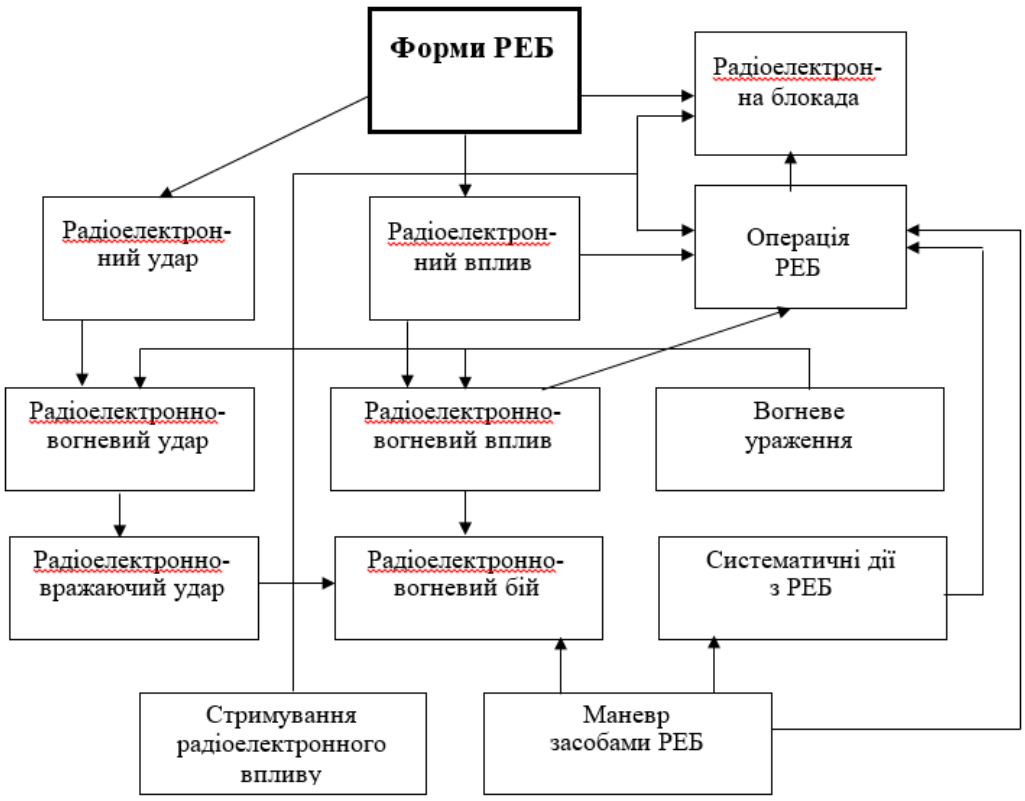


Рис. 2.5. Форми РЕБ

Радіоелектронно-вогневий удар – це сукупність узгоджених за метою, завданнями, місцем і часом радіоелектронних і вогневих ударів по радіоелектронних системах і засобах управління військами і зброєю та об'єктам противника, які здійснюються різнорідними силами і засобами за єдиним замислом і планом відповідно з радіоелектронною (оперативною) обстановкою.

Радіоелектронно-уражаючий удар представляє собою відносно короткочасну, потужну комплексну дію різноманітних засобів РЕБ на противника шляхом застосування променевої зброї, спеціальних (електромагнітних) боєприпасів, створення радіоелектронних завад, які приводять до тимчасового виведення з ладу або функціонального ураження РЕЗ і об'єктів.

Стримування радіоелектронного впливу – форма дій, комплекс заходів щодо забезпечення стійкого функціонування радіоелектронних засобів і об'єктів в умовах радіоелектронного впливу противника, застосування самонавідної на випромінювання зброї**.**

Радіоелектронно-вогневий бій – це сукупність узгоджених за метою, завданнями, місцем і часом окремих радіоелектронних впливів, радіоелектронних і радіоелектронно-вогневих ударів, стримування радіоелектронних впливів противника, маневру РЕЗ для завдання збитків противнику і (або) запобігання збитку своїм військам силам.

Систематичні дії з радіоелектронної боротьби – це форма комплексних, завчасних, неперервних і послідовних дій та заходів з РЕБ при підготовці до операцій (бойових дій) та в ході їх ведення.

Радіоелектронна блокада – це специфічна форма РЕБ, один або декілька узгоджених за метою, місцем і часом радіоелектронних впливів (ударів), радіоелектронно-вогневих впливів, які здійснюються визначеним складом різнорідних сил РЕБ, або утворенням в атмосфері (космічному просторі) штучних зон підвищеної іонізації з метою дезорганізації функціонування РЕЗ локального району або об'єкту.

Маневр засобами РЕБ – це складова частина радіоелектронної боротьби в операції, бойових діях (бою), що включає: завчасно сплановану зміну позицій, режимів роботи, напрямків випромінювання, а також використання резервних засобів та систем, створення оманних позицій і угруповань РЕЗ, які здійснюються у відповідності до завдань військ.

Маневр засобами радіоелектронної боротьби, радіоелектронним впливом, радіоелектронними ударами, напрямками випромінювання завад, а також виконанням різноманітних заходів РЕБ дозволяє захоплювати і утримувати ініціативу у використанні електромагнітного спектру, дезорганізувати управління противника й успішно вести РЕБ в умовах обстановки, що постійно змінюється.

В сучасних умовах сили і засоби РЕБ залучаються до вирішення завдань оперативного і стратегічного рівня з глобальним просторовим розмахом і практично миттєвим часом реакції на зміну обстановки, тому РЕБ набуває рис специфічного виду бойових дій. В цих умовах за наявності необхідних сил та засобів РЕБ можливе проведення операцій РЕБ.

Операція РЕБ – сукупність узгоджених за метою, завданнями, місцем і часом одночасних і послідовних радіоелектронно-вогневих, радіоелектронних (радіоелектронно-уражаючих) ударів і маневру засобами РЕБ, які проводяться за єдиним замислом і планом для дезорганізації систем управління і об'єктів противника, а також заходів, що спрямовані на зниження ефективності впливу засобів РЕБ противника і ураження ВТЗ та зброєю НФП своїх радіоелектронних засобів [10-12].

Операція РЕБ, як правило, буде розпочинатися до початку нанесення першого вогневого удару і проводитися у декілька етапів.

2.4. Тенденції розвитку РЕБ за досвідом локальних війн та збройних конфліктів сучасності

Аналіз війн і збройних конфліктів останніх десятиріч дозволяє виділити наступні основні тенденції розвитку змісту, форм, способів і засобів радіоелектронної боротьби.

Перша тенденція. РЕБ постає не стільки як вид оперативного і бойового забезпечення, скільки як специфічна форма бойових дій та перетворюється у складову інформаційної боротьби, яка ведеться з метою

досягнення переваги в управлінні військами (силами) та зброєю (див. рис. 2.6) [10-12].

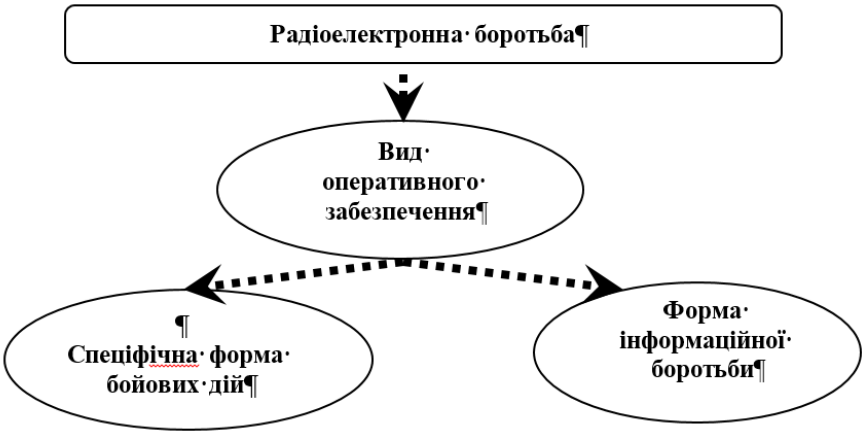


Рис. 2.6. Перша тенденція

Інформаційна перевага визначається як спроможність керувати поведінкою противника шляхом контролю за кількістю та якістю інформації, яку він намагається отримувати і обробляти для її ефективного використання в реальному масштабі часу, з гарантованою забороною інформаційного втручання з боку противника.

Для досягнення інформаційної переваги та виконання задач інформаційної боротьби, в Збройних Силах України визначені наступні її складові: комплексні заходи радіоелектронної боротьби, психологічної боротьби, стратегічного (оперативного) маскування, порушення нормального функціонування або повне знищення інформаційних систем противника, інформаційно-комп'ютерна боротьба.

Конкретизуємо завдання, які покладені на сили та засоби РЕБ та напрямки їх вирішення.

Завданнями радіоелектронної боротьби, які виконуються для здобуття інформаційної переваги є:

– радіоелектронне подавлення засобів масової інформації (радіомовлення та телебачення), систем зв'язку та передачі даних, комп'ютерних радіомереж систем управління військами (силами) та зброєю противника;

– радіоелектронний захист свого особового складу та систем управління від негативного інформаційного впливу противника.

Але з появою нових видів зброї РЕБ відмічається тенденція розвитку завдань РЕБ у нетрадиційних для даного виду оперативного (бойового забезпечення) напрямках. Зокрема суттєво підвищується роль РЕБ у вирішенні завдань впливу на особовий склад збройних сил противника та населення. Наприклад, вже зараз є чимало фактів застосування електромагнітної зброї (ЕМЗ) для руйнування теле- та радіоефіру (війна у Перській затоці 1991 р.),

виклику у особового складу у потрібні терміни часу нелетальних шокуючих больових відчуттів [8, 9, 10-12].

Суттєво підвищується роль РЕБ при вирішенні завдань введення політичного і військового керівництва противника в оману відносно намірів та можливостей збройних сил [10].

Стрімко зростає обсяг завдань РЕБ при веденні програмно-комп'ютерної боротьби (ПКБ). Зокрема, тенденції розвитку систем зв'язку та передачі даних призвели до зростання ролі РЕБ при вирішенні завдань з руйнування інформації, що передається по комп'ютерним радіомережам. Ця тенденція особливо підсилюється при вирішенні завдань інформаційної боротьби під час ведення операцій (бойових дій), коли радіоканал стає основним засобом доступу до програмного забезпечення в комп'ютерних системах різного призначення.

Суттєво підвищується роль РЕБ при вирішенні завдань інформаційної боротьби, що пов'язані із захистом власного інформаційного простору від впливу наступальних складових інформаційної боротьби противника. Зокрема, РЕБ відіграє провідну роль в частині:

– захисту власного особового складу від психологічного впливу противника;

– радіоелектронного захисту інформаційної інфраструктури при вирішенні завдань з протидії радіоелектронному продавленню з боку противника;

– захисту своєї інформаційної інфраструктури від зброї РЕБ функціонального ураження;

– зниження ефективності ведення противником радіоелектронної розвідки при вирішенні завдань введення його в оману.

Здійснюється трансформація радіоелектронної боротьби у самостійну форму оперативно-стратегічних дій. Трансформація форм введення РЕБ здійснюється в напрямку переходу від поодиноких (окремих) радіоелектронних впливів до масованих радіоелектронних ударів та операцій РЕБ. Зазначимо, що під формою РЕБ слід розуміти зовнішній вираз (масштабну, просторову та часову характеристику) відповідних варіантів застосування сил та засобів РЕБ з метою виконання конкретного завдання РЕБ в умовах обстановки, що склалася.

Враховуючи визначення форми РЕБ, р**адіоелектронний вплив (РЕВ)** можна охарактеризувати як дії окремих засобів з радіоелектронного подавлення радіоелектронних об'єктів противника, які проводяться за єдиним замислом і планом на одному або декількох окремих напрямках для вирішення завдань з дезорганізації управління військами (силами) і зброєю противника в операціях (бойових діях). Свій подальший розвиток ця форма РЕБ отримала за рахунок початку комплексування завдань РЕП та вогневого ураження. Виникла нова форма РЕБ – радіоелектронно-вогневий вплив, яка є сукупністю дій окремих засобів вогневого ураження, радіозавад з ураження та радіоелектронного подавлення радіоелектронних об'єктів противника, які проводяться за єдиним замислом і планом на одному або декількох окремих

напрямках для вирішення завдань з дезорганізації управління військами (силами) і зброєю противника в операціях (бойових діях).

В локальних війнах та збройних конфліктах 70-80–х років активно застосовується така форма РЕБ, як радіоелектронне блокування. Ця форма РЕБ представляє собою узгоджені за метою, завданням, місцем та часом дії по дезорганізації управління військами (силами) та зброєю противника у конкретному районі місцевості шляхом нанесення окремих радіоелектронних та радіоелектронно-вогневих впливів в спеціальних операціях (бойових діях).

Розвиваються і впроваджуються в практику бойових дій нові комбіновані форми ведення РЕБ та вогневого ураження [10-12]: радіоелектронний та радіоелектронно-вогневий удар (див. рис. 2.7.). Більш детально наслідки цих змін та нові форми проаналізовані у п. 3.2. навчального посібника.

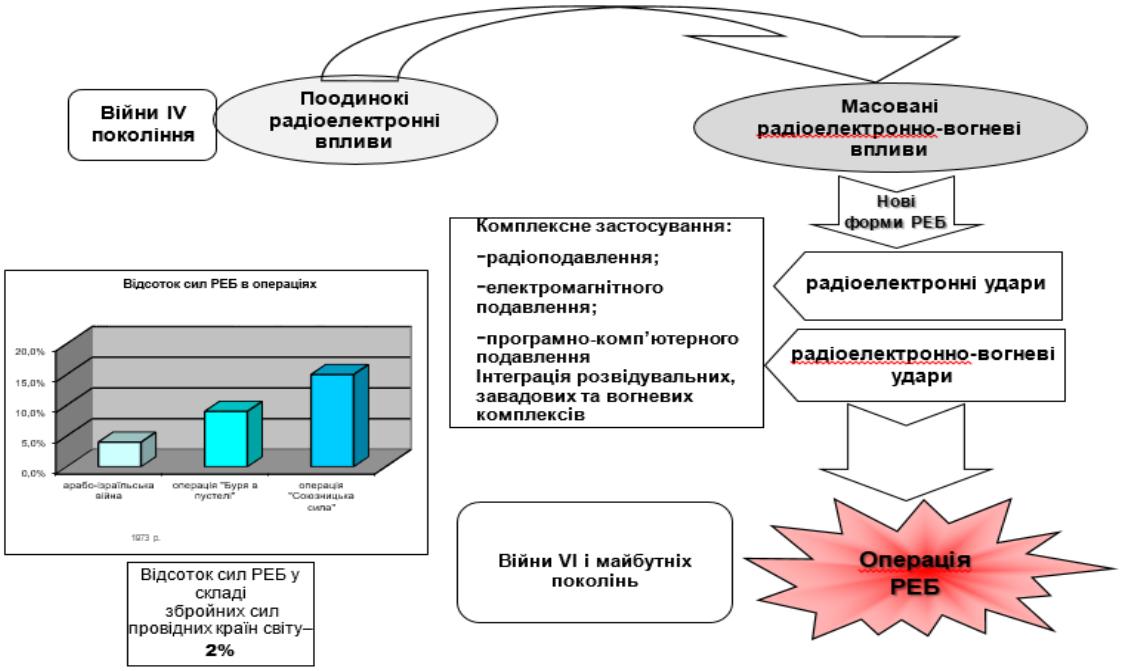


Рис. 2.7. Продовження розвитку першої тенденції

Сили і засоби РЕБ залучаються до вирішення завдань оперативного і оперативно-стратегічного рівнів з глобальними наслідками для противника. Збільшується відносна кількість сил і засобів РЕБ в операціях, при цьому загальна кількість сил РЕБ у збройних силах провідних країн світу залишається стабільною на рівні біля 2% (рис. 2.7.).

Друга тенденція. Розширення просторового розмаху і поступове розповсюдження методів ведення РЕБ на космічний простір. Застосування космічних систем для організації і ведення РЕБ на землі, в повітрі, на морі і в космосі дає підстави характеризувати дії РЕБ як глобальні [10-12].

Разом з тим, відмічається тенденція збільшення ролі РЕБ при виконанні завдань в тактичній ланці. Це обумовлено двома факторами.

По-перше, до цього призводить впровадження у збройних силах провідних країн світу ідеології комплексного інформаційного забезпечення окремого солдата на полі бою. Це викликало активне використання у тактичній ланці управління супутникових систем зв'язку, оповіщення та навігації, комп'ютерних радіомереж, стільникового та транкінгового зв'язку. В таких умовах окремий солдат або тактичні підрозділі можуть вирішувати практично будь-які завдання у автономному режимі. Тому боротьба з системами управління тактичної ланки за пріоритетністю починає конкурувати з аналогічними завданнями оперативно-тактичної та стратегічної ланок.

По-друге, за останні десятиріччя стрімко зросли об'єми завдань РЕБ при застосуванні військових контингентів під час міжнародних миротворчих операцій та у антитерористичній діяльності. Це обумовлено необхідністю боротьби з радіокерованою зброєю, застосування якої проти миротворчих контингентів останнім часом набуло масованого характеру.

Третя тенденція. Інтеграція сил і засобів РЕБ із засобами розвідки і вогневого ураження при нанесенні комбінованих радіоелектронно-вогневих ударів, а також різке підвищення ступеню автоматизації процесів розвідки і радіоподавлення, застосування методів штучного інтелекту в системах управління комплексами РЕБ, використання системи радіотехнічної розвідки і контролю в якості інформаційної компоненти комплексів РЕБ. Прикладом такого підходу є створення у США і постійна модернізація інтегрованого комплексу розвідки і РЕБ типу "ВУЛФПАК", АСУ силами та засобами розвідки і РЕБ типу "АСАС".

Відбувається трансформація складових радіоелектронної розвідки. Зокрема, в умовах масового криптозахисту радіоканалів передачі інформації, активно впроваджуються методи радіотехнічної розвідки для автоматизації процесів виявлення (пошук у широкій смузі частот), режекції (селекції) та розпізнавання джерел випромінювань у радіорозвідці [10-12].

Четверта тенденція. Підвищення бойових можливостей сил та засобів РЕБ за рахунок розширення діапазону робочих хвиль, в якому ведеться радіоелектронне подавлення, зростання потужності випромінювання.

П'ята тенденція. Відмічається випереджена розробка засобів РЕБ з урахуванням прогнозів розвитку військової радіоелектроніки, а не лише реагування на розвиток РЕЗ противника (так званий, принцип несиметричної адекватності). Розробляються комплекси РЕБ з високим ступенем адаптації, які здатні автоматично в реальному масштабі часу оцінювати радіоелектронну обстановку і здійснювати вибір оптимального впливу на РЕЗ.

Велика увага приділяється безпілотним літальним апаратам, як засобам радіоелектронної боротьби. Останнім часом великий інтерес виявляється до малих (мініатюрних) безпілотних літальних апаратів (БПЛА) – передавачів завад для застосування в оперативно-тактичній та тактичній ланках управління противника.

Крім того, розвиток комп'ютерної техніки і глобальне поширення комп'ютерних радіомереж викликали активну розробку засобів та способів

впровадження програмних засобів, що руйнують інформацію, яка поступає до комп'ютерних мереж через радіоканали.

Шоста тенденція. Збільшення ролі засобів РЕБ у боротьбі з ВТЗ противника. Засоби РЕБ спроможні створювати завади як ГСН крилатих ракет, так і системам космічної навігації типу GPS. Активно застосовуються протирадіолокаційні ракети та керовані бомби.

Сьома тенденція. Масоване застосування зброї РЕБ нового покоління (електромагнітні бомби і боєприпаси, лазерні промені, деструктивні програмно - комп'ютерні засоби та ін.) для впливу на радіоелектронні компоненти та особовий склад систем управління військами (силами) і зброєю противника. Застосовуються геофізичні засоби формування в атмосфері та космосі штучних областей підвищеної іонізації, які блокують роботу радіолокаційних систем і радіозасобів. Впливи такої зброї РЕБ на особовий склад, споруди й устаткування стають компонентом радіоелектронних ударів і застосовуються паралельно з традиційними засобами РЕП.

Головним принципом розвитку систем та засобів РЕБ на сучасному етапі стає принцип несиметричної адекватності. Згідно з цим принципом в галузі РЕБ розробляється техніка функціонального ураження, а саме – електромагнітна зброя (ЕМЗ).

Визначені тенденції розвитку РЕБ у світовій практиці призвели до необхідності корінного перегляду ідеології ведення РЕБ у збройній боротьбі сучасності та у майбутньому.

Аналіз тенденцій розвитку збройної боротьби вказує що сучасний стан систем управління військами (силами) та зброєю відносно війн четвертого покоління зазнав революційних змін у бік підвищення завадозахищеності ліній зв'язку та передачі інформації усіх ланок, масованого застосування космічних систем, комп'ютерних технологій, інтелектуалізації та глобальної автоматизації усіх процесів управління військами (силами) та зброєю, рис. 2.8 [10-12].

Для боротьби з системами управління, рис. 3.3. з 60-тих років минулого століття провідними країнами світу використовувалась концепція, сутністю якої є вплив радіозавадами на приймальні радіоелектронні засоби противника. Технічною основою цієї концепції було застосування досить великогабаритних та дорогих у експлуатації та модернізації комплексів РЕП, які є "гарною" мішенню для сучасних засобів ураження. На період 70-80 років минулого століття використання таких комплексів дозволяло частинам та підрозділам РЕБ виконувати до 80 % задач з дезорганізації управління військами (силами) та зброєю. Але застосування вказаного підходу у збройній боротьбі сучасності та майбутнього дозволяє вирішити не більш за 25 % завдань, рис. 2.8.

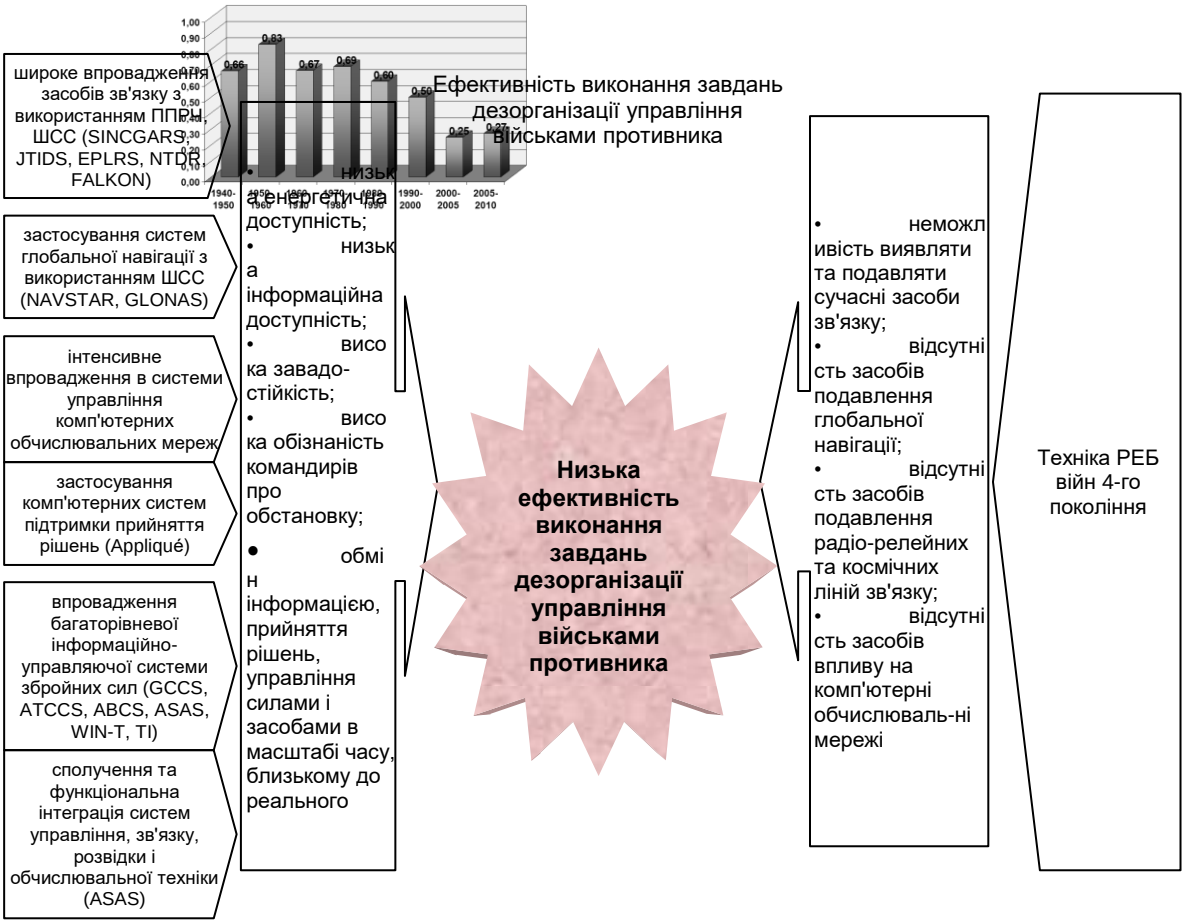


Рис. 2.8. Тенденції розвитку систем та засобів управління, зв’язку і автоматизації та їх вплив на ефективність ведення РЕП

Вже зараз, наприклад у ЗС Російської Федерації, якісне вирішені питання дезорганізації управління військами (силами) та зброєю в сучасних операціях за рахунок впливу завадами на приймальні пристрої:

– новітніх систем супутникового, радіорелейного, КХ та УКХ зв’язку нового покоління;

– супутникових навігаційних систем;

– радіокомандних систем наведення ВТЗ, РЛС РУК типу “Джисак”;

– оптичних, оптико-електронних та радіолокаційних головок самонаведення ВТЗ;

– багатофункціональних бортових РЛС засобів повітряного нападу;

– комп’ютерних радіомереж тактичної ланки;

– систем стільникового та транкінкового зв’язку (особливо під час проведення миротворчих операцій та у антитерористичній діяльності, операцій по локалізації та нейтралізації збройного конфлікту).

Модернізація та проведення доробок техніки РЕБ війн 4-ого покоління у бік збільшення потужності випромінювання, оптимізації завад, розробки та реалізації нових методів частотного пошуку та обробки сигналів може підвищити ефективність вирішення лише окремих часткових завдань та не вплине суттєво на загальну ефективність дезорганізації управління військами

(силами) в операціях (бойових діях) у війнах майбутнього. За рахунок реалізації старого підходу економіка відповідної держави лише буде втягнута у низькоефективне вкладання ресурсів в утримання частин (підрозділів) РЕБ, бойові можливості яких неухильно знижуються із року в рік.

Така ситуація потребує корінної зміни ідеології ведення РЕБ у війнах майбутнього.

Аналіз тенденцій розвитку РЕБ у світі вказує що на шлях революційних змін в галузі РЕБ вже стали такі провідні країни як США, Китай, Росія, Англія та Франція.

В світі іде активна розробка зброї РЕБ нового покоління та переозброєння на її основі частин (підрозділів) РЕБ.

Наприклад, ще на початку 90-х років США розробили концепцію застосування ЕМЗ середньої потужності й створення на її основі надпотужних постановників активних завад. Результат - випробування в ході бойових дій проти Іраку в 1991-1992 роках окремих зразків електромагнітної зброї. Це - крилаті ракети "Томахок" (морського базування), які були випущені по позиціях ПВО Іраку. Радіовипромінювання, що виникли внаслідок підриву бойових частин крилатих ракет, порушили роботу електронних систем озброєнь, особливо комп'ютерної мережі системи ПВО. Електромагнітні бомби неодноразово застосовувалися США й в ході бойових дій у Югославії (1999 рік), проте використання боєприпасів цього типу носило поки дослідницький, епізодичний характер. Є дані, що США прийняли на озброєння бойові зразки електромагнітних боєприпасів і високоточних крилатих ракет та почати їх масоване використання для вирішення завдань РЕБ [12].

Відповідно з наявною відкритою інформацією, в 1998 році на шведському полігоні російські фахівці провели показові випробування "електронного" боєприпасу з демонстрацією його уражаючої дії на РЕА літака, що перебував на літному полі (Російське телебачення, канал НТВ, 28.02.98). У тому ж році на виставці ОВТ сухопутних військ "Евросатори – 98" Росія запропонувала закордонним покупцям унікальну лабораторію, розроблену у Федеральному ядерному центрі "Арзамас 16", що надає можливість досліджувати дії високочастотного електромагнітного випромінювання на інформаційні й енергетичні системи, а також на канали передачі даних. У пресі опубліковані повідомлення про створення в Росії дослідних зразків ЕМЗ у вигляді активних гранат, призначених для електромагнітного подавлення системи активного захисту танка. Вже є зразки 100 мм й 130 мм електромагнітних снарядів, 40 мм, 105 мм й 125 мм реактивних електромагнітних гранат, 122 мм електромагнітних бойових частин некерованих ракет. На виставці ЛІМА 2001 у Малайзії (2001 рік) Росія продемонструвала діючий зразок бойового ЕМЗ генератора «Ранець Е» (Defence Systems Daily, 26.10.2001). Цей комплекс був створений як засіб оборони мобільних РЕЗ від високоточної зброї. Зафіксовані факти застосування електромагнітної зброї у зоні проведення АТО та ООС на території незалежної України.

В 1992 році газета “Санди телеграф” повідомила про вступ у ряди власників ЕМЗ й Великобританії. У публікації говорилося про розробку в Агентстві оборонних досліджень Великобританії (м. Фарнборо) “мікрохвильової бомби” для ураження електронного обладнання. За задумом, така бомба може приводитися в дію в середніх шарах атмосфери й повністю виводити з ладу комп’ютерні системи й телефонні лінії на площі одного кварталу (Агентство ИТАР ТАСС, 12.10.92). В 2001 році компанія Matra BAE Dynamics з успіхом продемонструвала британському МО артилерійський снаряд калібру 155 мм, здатний вражати бортові комп’ютери танків або літаків, переривати роботу радіостанцій і радарів. Об’єктами поразки можуть бути також засоби національної телефонної, телевізійні й радіомережі, система електропостачання всієї країни супротивника.

Досвід ведення РЕБ провідними країнами світу, аналіз світових досягнень у цій галузі дозволяє зробити висновок, що **технічною основою формування зброї РЕБ нового покоління** в сучасних збройних силах стають, рис. 2.9.[10-12]:

– електромагнітна зброя та її аналоги (зброя РЕБ функціонального ураження радіоелектронних об’єктів та особового складу противника), яка за рівнем важливості і ступенем впливу на результати бойових дій зрівнюється з вогневим ураженням об’єктів противника високоточною та тактичною ядерною зброєю;

– інтеграція розвідувальних, завадових, вогневих комплексів та комплексів функціонального ураження у єдині системи, що працюють у реальному масштабі часу, яка є основою реалізації “електронно-вогневої” концепції ведення збройної боротьби майбутнього;

– програмно-комп’ютерна зброя для руйнування інформаційної інфраструктури комп’ютерних радіомереж;

– акустична зброя, що здатна впливати на психіку та поведінку людини. Незважаючи на віддалення людини від поля бою та зменшення її впливу на хід бойових дій, актуальність впливу саме на людину в інтересах дезорганізації управління постійно зростає;

малогабаритна зброя радіоелектронного подавлення, що має модульну структуру, основними засобами доставки якої є легкі безпілотні літальні апарати БПЛА).

Поруч з традиційними з’являються та починають домінувати нові складові РЕП, рис. 2.10 [10-12]:

– електромагнітне продавлення, яке полягає у порушенні роботи радіоелектронних систем та засобів противника шляхом їх функціонального ураження потужними електромагнітними імпульсами;

– програмно-комп’ютерне подавлення що полягає у порушенні роботи програмно-комп’ютерних мереж та засобів противника шляхом їх ураження деструктивними програмними засобами.

Рис. 2.9. Технічна основа формування зброї РЕБ нового покоління в сучасних збройних силах

Характерними рисами зброї РЕБ нового покоління, які впливають на форми та способи ведення РЕБ в операціях (бойових діях) є:

Таким чином, в операціях (бойових діях) майбутнього необхідно розглядати зброю РЕБ нового покоління як зброю з сукупністю властивостей зброї масового ураження, ВТЗ та традиційних засобів вогневого ураження.

Аналіз бойових можливостей нових видів зброї РЕБ вказує на неможливість вирішення у сучасних операціях завдань з дезорганізації управління військами (силами) та зброєю противника на основі застосування лише якогось одного виду зброї.

Тільки втілення принципу комплексування різних видів зброї РЕБ, видів радіоелектронного подавлення може дозволити одержати перевагу в управлінні військами (силами) та зброєю в операціях майбутнього. Так, на рис. 2.11/, проілюстроване співвідношення кількості завдань з дезорганізації управління противника які необхідно виконати в операції до потенційних можливостей частин РЕБ, щодо їх виконання в умовах застосування тільки сучасних завадових комплексів, комплексування таких комплексів та електромагнітної зброї, електромагнітної зброї та дій з програмно-комп'ютерного впливу відповідно [10-12];

– універсальність та масштабність ураження: наприклад, ЕМЗ діє на різні радіоелектронні засоби, комп'ютери, електронні прилади та електричне обладнання, кабелі, та силові лінії та за масштабами ураження є аналогом тактичної ядерної зброї;

– програмно-комп'ютерна зброя (спеціальне програмне забезпечення, комп'ютерні віруси, логічні бомби, "троянські програми") по структурі складається з двох частин – розмноження та ударної. При цьому перша частина вірусу є "голівкою наведення" та служить для вибору цілей и доставляє його до об'єкту ураження. Інформація про цілі добувається системами комп'ютерної розвідки.

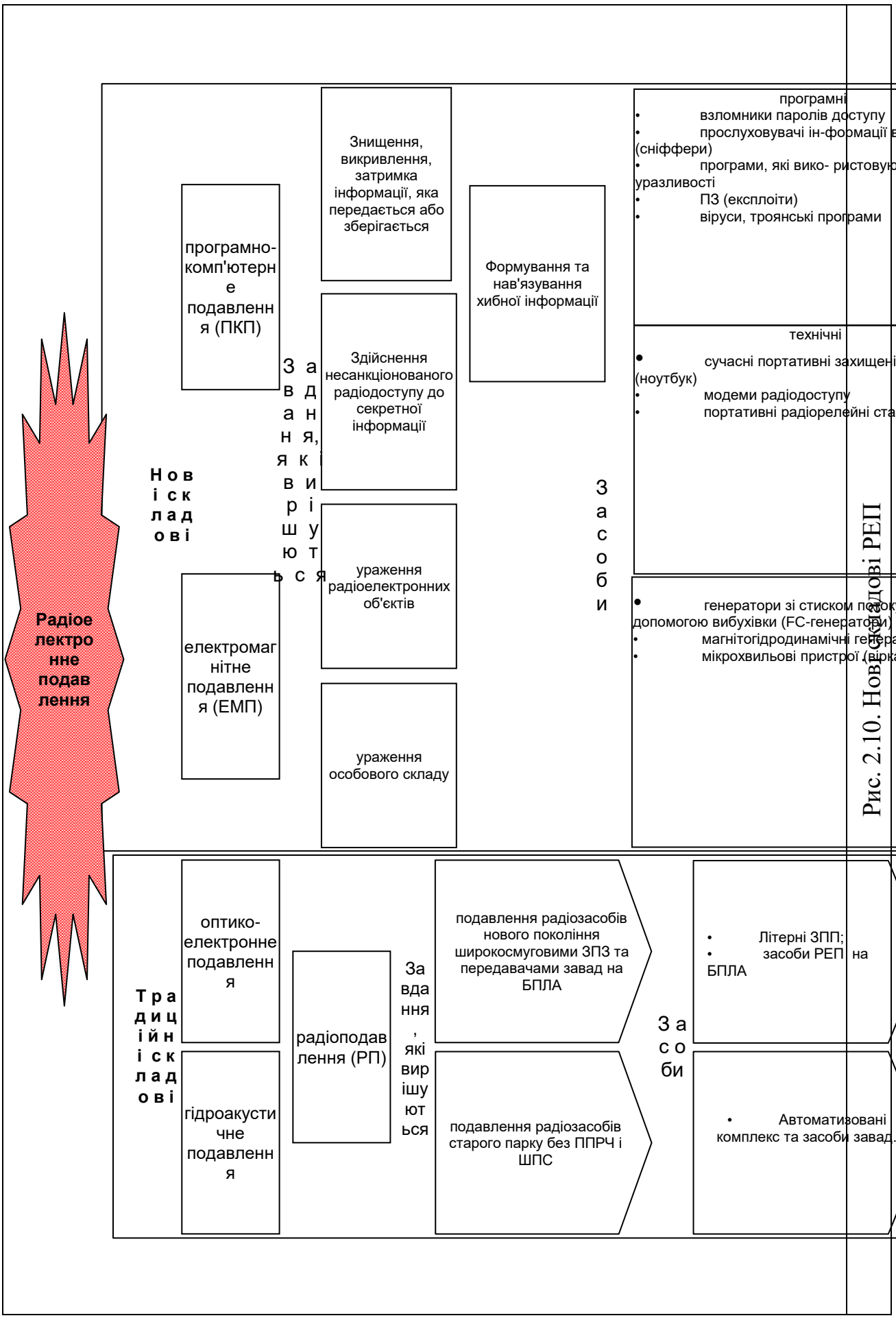


Рис. 2.10. Новий складові РЕП

При цьому засоби впливу на програмне забезпечення можуть за властивостями розглядатись як аналоги високоточної зброї у інформаційному просторі;

– носіями нової зброї РЕБ можуть бути крилаті ракети, керовані та некеровані бомби, безпілотні літальні апарати, ракети класу “поверхня-повітря” та “повітря-повітря”, літаки-снаряди, радіосигнали, що несуть програмні засоби;

– низька вартість. Наприклад, приблизна вартість одного генератору ЕМВ -2000...5000 $;

– висока живучість в умовах застосування сучасних засобів ураження;

– керований руйнуючий ефект, зокрема, дія ЕМЗ, програмно - комп’ютерної зброї може призводити як до тимчасового виведення з ладу елементів інформаційної інфраструктури противника, так і до її повного знищення.

Висвітлені світові тенденції у зміні ідеології ведення РЕБ створюють основи для формування частин (підрозділів) РЕБ Збройних сил провідних країн світу у недалекому майбутньому.

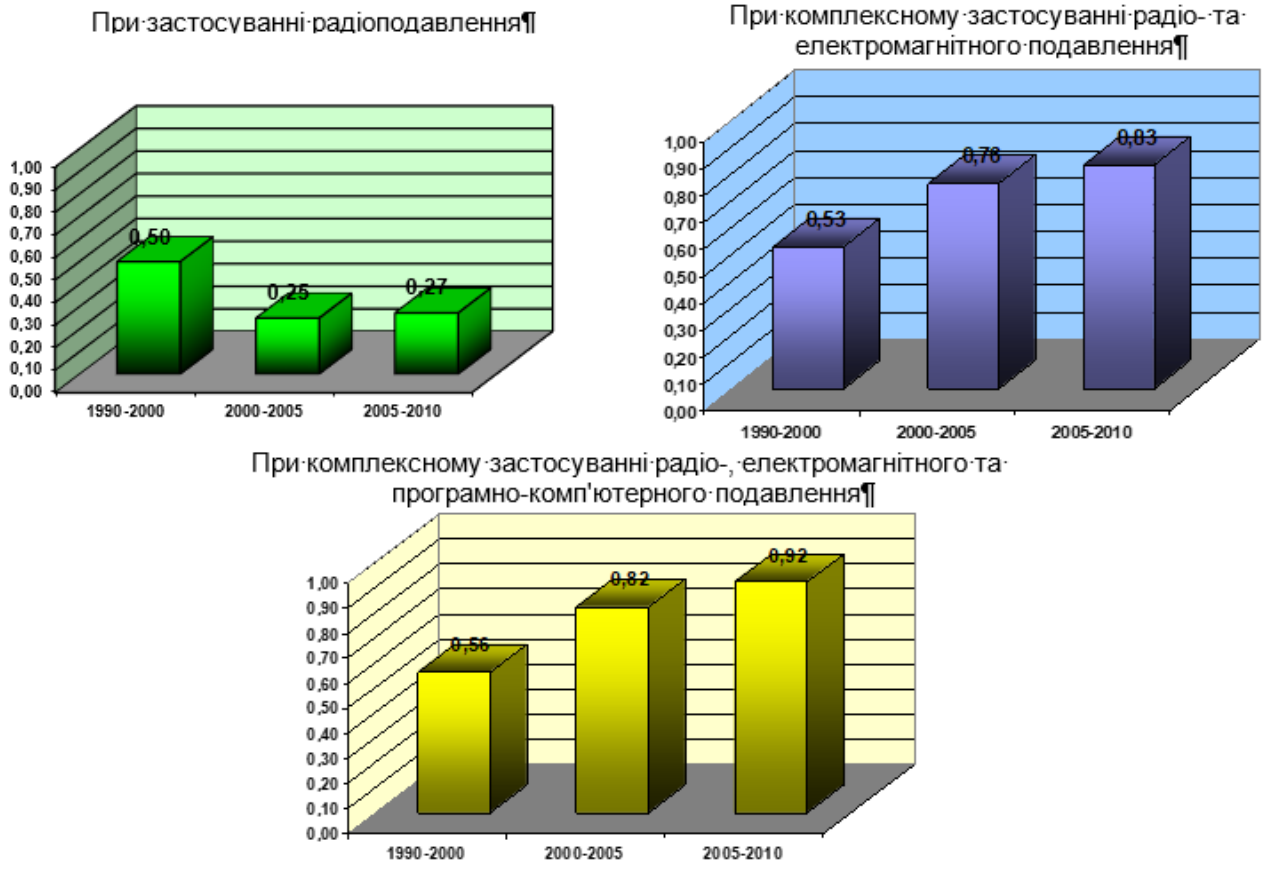


Рис. 2.11. Ефективність виконання завдань дезорганізації управління військами противника

Основою формування нової ідеології, у такий нетрадиційні сфері збройної боротьби як РЕБ, в світі стає створення на основі принципу асиметричної адекватності та втілення в практику військ нових видів зброї

РЕБ, розробка нових форм та способів застосування частин (підрозділів) РЕБ, (див. рис. 2.12) [10-12].

Рис. 2.12. Основи формування нової ідеології ведення РЕБ у війнах майбутнього

Як визначалось у п. 3.2., активне впровадження зброї РЕБ нового покоління призвело до появи нових складових РЕП – програмно - комп'ютерного та електромагнітного подавлення.

Під **програмно-комп'ютерним продавленням (ПКП) в операціях (бойових діях)** будемо розуміти сукупність узгоджених за метою, завданнями, місцем і часом заходів і дій частин (підрозділів) РЕБ (розвідувально-диверсійних груп) противника по виявленню комп'ютерних засобів і радіомереж, здійсненню доступу та впровадження до них спеціальних програмних засобів, які порушують нормальне функціонування комп'ютерних засобів і мереж, секретність та цілісність інформації, яка в них циркулює [13].

Об'єктами ПКП в операціях (бойових діях) є наступні елементи комп'ютерних мереж оперативно-тактичної (тактичної) ланки управління [13]:

– комп'ютерні засоби посадових осіб, які застосовуються для формування, отримання, передачі, відображення даних оперативно-тактичної (тактичної) обстановки, підтримки прийняття рішень;
– сервери центрів управління бойовими діями;
– сервери управління локальними мережами та маршрутизації.

Метою програмно-комп'ютерного подавлення можуть бути: отримання секретної електронної інформації, запровадження електронної дезінформації (спотворення електронної інформації), порушення нормального функціонування комп'ютерних засобів і мереж (програмне ураження) [13].

Ведення програмно-комп'ютерного подавлення комп'ютерної мережі противника тактичної ланки в операціях (бойових діях) включає [13]:

1) визначення мети та завдань програмно-комп'ютерного подавлення;
2) здійснення фізичного доступу до комп'ютерної мережі противника;
3) подолання процедури ідентифікації - автентифікації в мережі;
4) визначення топології мережі (сканування) та цілі впливу (атаки);
5) проведення інвентаризації мережевих ресурсів;
6) розширення права доступу до ресурсів мережі;
7) запровадження у мережу деструктивних програмних засобів.

2.5. Електромагнітне подавлення систем управління військами та зброєю

Сутність електромагнітної зброї полягає в створенні короткочасних електромагнітних випромінюваннь великої потужності з метою впливу на радіоелектронні пристрої і виведення їх з ладу [14-16].

Ключовими технологіями, створення ЕМЗ є:

– генератори зі стиском потоку за допомогою вибухівки, що працюють на вибухівці (наприклад, пороховому заряді);

– магнітогідродинамічні (МГД) генератори;

– мікрохвильові пристрої високої потужності, з яких найбільш сучасним є осцилятор з віртуальним катодом;

– SOS - генератори EMI.

Генератори зі стиском потоку за допомогою вибухівки (FC-генератор), рис. 2.13.

FC-генератор – це пристрій, здатний створити електромагнітну енергію порядку десятків МДж за сотні мікросекунд, пікова потужністю від одиниць до десятків ТВт.

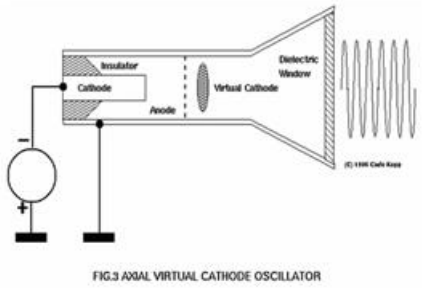


Рис. 2.13. FC-генератор
1 – електромагнітний резонатор; 2 – стояча хвиля; 3 – вибухова речовина;
4 – спрямоване електромагнітне випромінювання;
5 – продукти вибуху, що розлітаються

Основні технічні проблеми застосування FC-генераторів у військових цілях – це джерело стартового струму і спосіб “упакування” FC-генератора у бомбу або боєголовку. Остання проблема спрощується завдяки геометрії коаксіальної або конічної конструкції FC-генераторів.

Хоча FC-генератори є потенційною технологічною базою для генерації потужних електричних імпульсів, їхнє використання внаслідок фізики процесу обмежене смугою частот нижче від 1 МГц.

МГД генератори на вибухових речовинах. Принцип дії: провідник, що рухається у магнітному полі, виробляє електричний струм перпендикулярно напряму поля і руху провідника. У МГД генераторі провідником є плазма – іонізований газ від вибухової речовини – яка рухається поперек магнітного поля. Струм концентрується на електродах, які контактують з плазмовим

потоком. Їхня потенційна роль – генерація стартового струму для МГД генераторів.

Джерела мікрохвильового випромінювання високої потужності - релятивістські клістрони, магнетрони, рефлекс-тріоди, Spark Gap-пристрої й осцилятори з віртуальним катодом – віркатори тощо.

Віркатори (Рис. 2.14) – одноразові прилади, здатні виробити дуже потужний одиночний імпульс енергії. Вони конструктивно прості, невеликі за розмірами, здатні працювати у відносно широкій смузі частот мікрохвильового діапазону.

В основі роботи віркатора лежить принцип прискорення потужного потоку електронів сітчастим анодом. Частота осциляції залежить від параметрів електронного пучка; віркатори можна настроювати на частоту. Діапазон потужності, досягнутий в експериментах з віркаторами, становить від 170 кВт до 40 ГВт, діапазон довжин хвиль – від дециметрового до сантиметрового.

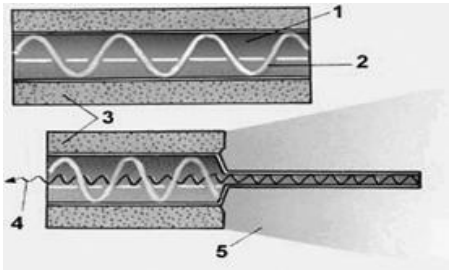


Рис. 2.14. Віркатор

Вченими Росії розроблені та практично апробовані багаторазові мобільні SOS-генератори EMI (рис. 2.15), проникаюча спроможність випромінювання яких суттєво перебільшує розглянуті вище технології. Принцип дії SOS - генераторів базується на ефекті наносекундної комутації щільних токів у напівпровідникових пристроях (SOS – Semiconductor Opening Switch).

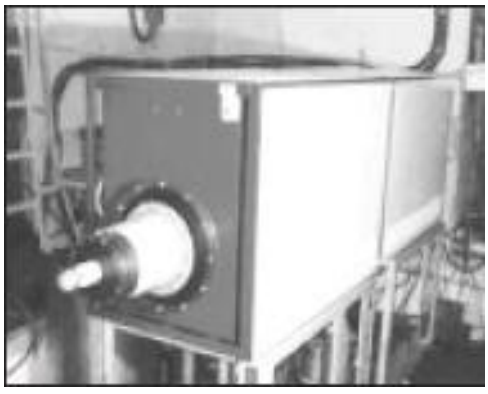


Рис. 2.14. Мобільни SOS-генератори EMI

Вражаюча дія електромагнітної зброї. Низькочастотна електромагнітна зброя може добре впливати на типову провідну інфраструктуру, таку, як більшість телефонних ліній, мережні і силові кабелі. Діапазон напруг пробою для кремнієвих високочастотних приладів, що використовуються в обладнанні зв'язку, як правило, становить 15-65 В. Арсенід-галієві польові транзистори звичайно мають напругу пробою 10 В [14-16].

Піддаються впливу електромагнітного імпульсу комп'ютерна техніка та мережі. Зокрема, мікросхеми динамічної пам'яті з довільним доступом, DRAM, мають напругу пробою до 7 В. Напруга пробою CMOS логіки лежить у діапазоні від 7 до 15 В, майже такий діапазон мають мікропроцесори з їх номінальною напругою в 3,3...5 В. Функціональні збої ПЕОМ у разі впливу електромагнітних імпульсів ультракороткої тривалості з різними граничними рівнями спектральної щільності напруженості поля Егр (f) наведено в табл. 2.1.

Мікрохвильова зброя високої потужності, що працює у сантиметровому і міліметровому діапазонах, має можливість впливати на обладнання через вентиляційні отвори, щілини між панелями і погано екранованими інтерфейсами.

Дослідження показали, що опромінення площі діаметром у 400-500 м електромагнітними мікрохвильовими боєприпасами з висотою підриву в 4 км (генератор високої потужності 10 ГВт, 5 ГГц) призведе до напруженості поля в декілька кіловольт на метр, що в свою чергу створить напругу від сотень вольт до кіловольт на опромінених проводах і кабелях. Це призведе до ураження радіоелектронної апаратури у зазначеному радіусі. Радіус ураження комп'ютерної техніки – 1000...1500 м [14-16].

Таблиця 2.1

Функціональні збої ПЕОМ у разі впливу електромагнітних імпульсів ультракороткої тривалості з різними граничними рівнями спектральної щільності напруженості поля Егр (f)

Характер збоїв ПЕОМ	Егр(f), В/м (f = 0.5...2 ГГц)
Збій клавіатури, пов'язаний з наведенням на інтерфейсний кабель	≥0, 025
Викривлення рядкової розгортки монітора. Зона викривлень 10-25%	≥0,8
При відкритому корпусі системного блоку фатальна помилка (повідомлення BIOS): немає доступу до жорсткого диску. Сильні викривлення рядкової розгортки монітора. Область викривлень 50-100% екрана	≥1
Збій (фатальний) у відеосистемі у разі подальшої експлуатації або у разі зупинки в роботі персонального обладнання	≥1,5

ЕМЗ – новий вид зброї РЕБ для впливу на особовий склад

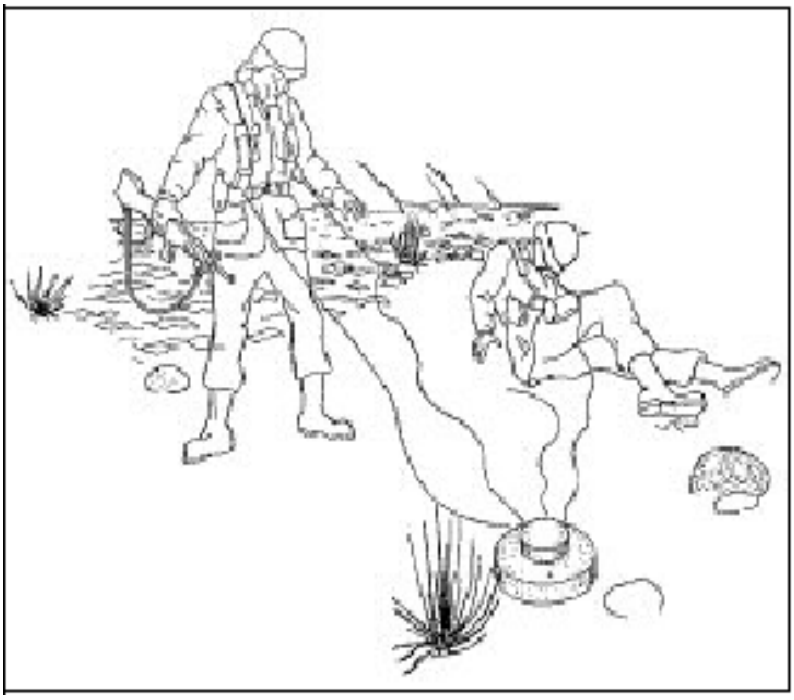


Рис. 2.16. Тейзерна міна у дії

Американська компанія HSV Technologies разом з Каліфорнійським університетом розробила новий тип електромагнітної зброї – так звані тетанайзери, або тетанизатори. Вони дозволяють тимчасово обезрушувати людину на видаленні до 100 м. Своєю назвою цей тип бойових засобів ЕМЗ зобов'язаний фізіологічному явищу тетанизації (м'язовим судорогам), що виникають у результаті впливу послідовності електричних імпульсів, що дублюють за формою невральні сигнали людини. Оптимальні параметри такої імпульсної послідовності, за яких обезрушування об'єкта впливу не супроводжується погіршенням його дихальної й серцевої активності й, як стверджується, майже не викликає ніяких хворобливих відчуттів, сила струму-25 мА, частота повторення-100 Гц. У загальному випадку для тетанизації тварин і людей можуть використовуватись струми в діапазоні 20-50 мА із частотою повторення імпульсів від 1 Гц до 10 кГц. Середня потужність електричного тетанизуючого впливу, при якому відбувається ще безопікове подолання опору м'язових тканин, регламентується значенням порядку 600 Вт. Для запобігання летальних наслідків силу струму тетанайзера обмежують величиною 250 мА. Крім сили струму й періоду проходження електричних імпульсів велике значення має їхня форма: найменша ефективність у неперервних синусоїдальних сигналів, найвища, у зростаючого по амплітуді за експоненційним законом імпульсу [14-16].

Ідея дистанційного нелетального впливу на особовий склад з використанням ЕМЗ знайшла свою реалізацію у новому типі мін – тетанайзерних мінах (патент США № 3803463). При спрацьовуванні ці міни викидають у радіусі декількох метрів множину проводів, наприклад, з фіксуючими голками для подачі електричного струму на об'єкт поразки (рис. 2.16).

Зараз отримані експериментальні підтвердження щодо створення струмопровідних шляхів за допомогою рідинних потоків, спрямованих у напрямку на ціль (патенти США №№ 3971292, 448687, 48460144, 5103366 й ін.). Але ці підходи істотно уступають лазерному методу формування повітряного токопроводу.

Вже зараз є дані що розроблені компанією HSV Technologies (США) тетанайзери застосовують промені лазера, що іонізують повітря по траєкторії свого поширення на дальності в кілька сотень метрів. Дальність дії таких тетанайзерів істотно залежить від ступеня поглинання лазерного випромінювання атмосферою й визначається як відстань від апертури лазера до точки зниження інтенсивності його імпульсу в визначену кількість разів щодо початкового значення. Розрахована протяжність токопроводячих каналів, що створені лазером з променем з довжиною хвилі 248 нм, складає біля 2 км.

Слід зазначити, що важливою перевагою короткохвильових лазерів є їх відносна біологічна безпека. При характерних для тетанайзерів інтенсивностях промінь із довжиною хвилі 193 нм безпечний для відкритих шкірних покривів і практично для органів зору. Існує лише невелика можливість ушкодження роговиці, коли лазер тетанайзера спрямований в око протягом декількох хвилин, причому хворобливі симптом звичайно зникають протягом 6-24 годин.

Подача тетанізуючого впливу до цілі може здійснюватися як по одному, так і по двох каналах іонізованого повітря. Один канал використовується за умови, якщо генератор тетанизируючих імпульсів має високу напругу і цілі заземлені (рис. 2.17). При цьому промінь лазера від джерела імпульсного когерентного випромінювання попадає на ціль або відбившись від струмопровідного дзеркала, або пройшовши через струмопровідну прозору пластину. І дзеркало, і пластина при використанні з’єднуються з виходом генератора ЕМІ через змінний резистор R, що обмежує тетанизируючий струм на несмертельному рівні й підтримує постійне його значення. Генератор синхросигналів забезпечує погоджену роботу лазера й генератора ЕМІ.

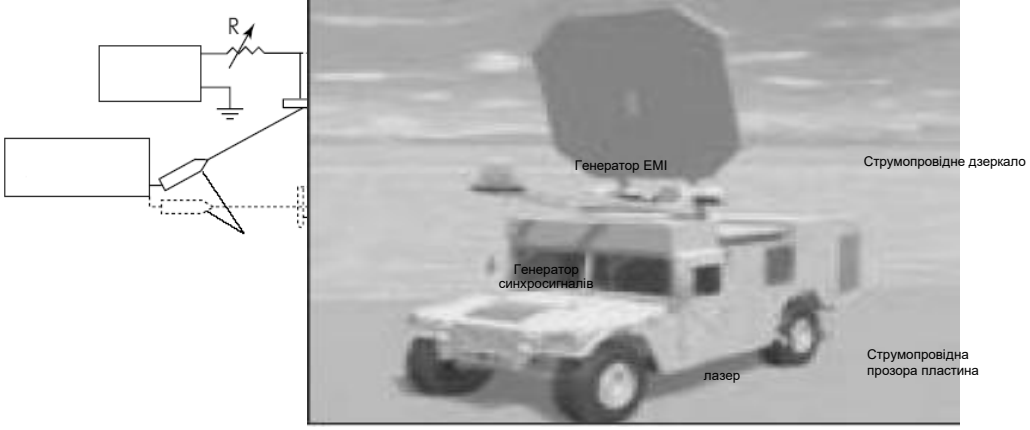


Рис. 2.18. VMADS

Рис. 2.17. Однопроменевий тетанайзер

Двоканальний варіант тетанайзера застосовується, якщо ціль електрично ізольована. Два його лазери формують іонізовані канали у повітрі, кожний з яких використовується для передачі тетанизуючого впливу від відповідного виходу генератора EMI й одночасно для повернення електричного струму від іншого його виходу. Принцип дії кожного каналу аналогічний одноканальному тетанайзеру. Як варіант може застосовуватися й один лазер із двопроменевою діаграмою випромінювання, сформованої за допомогою системи призм і дзеркал.

Окремим напрямком впливу на людину є використання ЕМЗ для створення больових відчуттів у особового складу. Логічним результатом розвитку цього напрямку у США є створення й випробування в 2001 р. Зразок нової зброї, що нагріває шкіру людей мікрохвильовими променями, одержав назву VMADS (Vehicle Mounted Active Denial System). Очікувана сфера його застосування – розгін демонстрацій, стихійних мітингів, блокування та роззброєння терористичних груп. У перспективі її можна буде застосовувати як невидиму зброю загородження. VMADS (рис. 2.18) має антену, схожу на супутникову тарілку, розміром 3х3 м, систему наведення й тепловизор, що дозволяє аналізувати ступінь нагрівання цілі. Представники американського дослідницького центру ВПС (шт.Нью-Мексико) заявляють, що установки VMADS можуть розміщуватись на кораблях і літаках. У період до 2009 року США планують приступити до закупівлі серійних зразків системи на транспортному засобі типу Humvee, або HMMWV (High Mobility Multi-purpose Wheeled Vehicle).

Науково-практичні аспекти тактики застосування ЕМЗ в операціях (бойових діях)

Засоби доставки ЕМЗ. На формування тактики застосування ЕМЗ істотний вплив має вибір засобів доставки. На сучасному етапі одним із способів вирішення проблеми доставки електромагнітної зброї є встановлення електромагнітних боєголовок на крилаті ракети, безпілотні літальні апарати (БПЛА) типу “Предейтор”, “Грант”, авіаційні бомби (рис. 2.19).

Електромагнітна боєголовка ракети включає електромагнітний пристрій, конвертер електричної енергії і бортове джерело живлення (рис.2.19).

Електромагнітний пристрій буде ініційовано за командою бортової системи підриву. Відношення маси боєголовки до загальної маси ракети становитиме 15... 30%. Застосування крилатих ракет як носіїв потребує обмеження маси електромагнітної зброї до 350 кг.

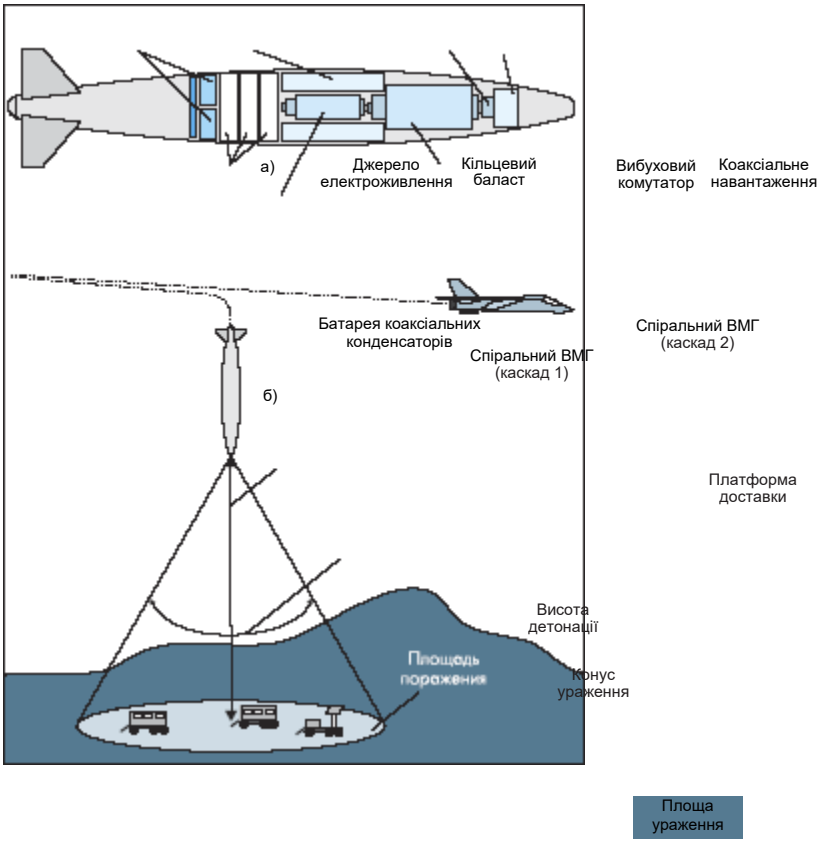


Рис. 2.19. Конструкція (а) і принцип бойового застосування (б) типового ЕМБ – Мк.84 (900 кг)

Боєголовка електромагнітної бомби складається з електромагнітного пристрою, конвертера електричної енергії і акумулятора енергії для накачування й підтримання заряду електромагнітного пристрою після відокремлення його від платформи-носія. Підірвати бомбу можна за допомогою радіовисотомірного пристрою для здійснення вибуху у повітрі (рис. 2.19), барометричного пристрою або навігаційної системи у GPS-керованих бомбах. Співвідношення корисного навантаження до загальної маси може досягати 85%.

Ведення операцій (бойових дій) із застосуванням ЕМЗ. Мета застосування ЕМЗ – дезорганізація управління основними системами життєзабезпечення держави і збройних сил, військами (силами) і зброєю противника шляхом деструктивного впливу на його радіоелектронні системи, комплекси і засоби.

Об’єкти впливу ЕМЗ (об’єкти ЕМП) [13, 14]**:**

комплекси (засоби) управління виробництвом, комунікаційні вузли, базові елементи економічної і політичної інфраструктури держави, теле- і радіоцентри;

– командні пункти об’єднань, з’єднань і частин противника, а також їхні вузли зв’язку;

– елементи підсистем управління загальновійськовими об’єднаннями, з’єднаннями і частинами;

– радіоелектронні комплекси та засоби управління зброєю противника;

– елементи глобальних, регіональних та локальних комп’ютерних мереж;

– елементи систем зв’язку комерційного призначення.

Під час ведення операції ураження об’єктів треба здійснювати масовані або високоточні електромагнітні удари, постійно координуючи дії з вогневого ураження, радіоелектронного подавлення радіомереж та радіолокаційних станцій управління зброєю противника, інформаційно-комп’ютерної боротьби та дезінформації, а також дії з прориву системи ППО противника для забезпечення ефективного застосування засобів доставки ЕМЗ.

Способами застосування ЕМЗ в операціях (бойових діях) є [29]**:**

– зосереджено-вибірковий;

– масований.

Формами застосування ЕМЗ в операціях (бойових діях) є:

– поодинокі електромагнітні впливі;

– групові електромагнітно-вогневі удари;

– масовані електромагнітно-вогневі удари;

– комбіновані форми застосування.

Основні оперативно-тактичні характеристики об’єктів ЕМП (ОЕМП) в операціях (бойових діях) можна охарактеризувати множиною:

$$C_{\text{об}} = \left\{ K_{\text{об}} , S_i, P_{\text{рд}}, Z, N \right\}, \tag{2.1}$$

де $K_{\text{об}}$ – ступінь важливості об’єкта ЕМП; S_i – площа i-го об’єкта ЕМП; $P_{\text{рд}}$ – розвіддосяжність об’єкту ЕМП; Z – ступінь захищеності об’єкта від ураження електромагнітним боєприпасом (ЕМБ); N – кількість радіоелектронних засобів (комплексів), або телефонних каналів та ліній радіозв’язку, електричних та кабельних мереж, які пов’язані з іншими органами управління або об’єктами.

Показник важливості об’єкта ЕМП визначається його пріоритетними властивостями, що визначаються станом системи управління противника, етапом (завданням) операції (бойових дій), в рамках якого організується ураження, рішенням відповідного командувача (командира) та ін. У загальному вигляді показник $K_{\text{об}}$ можна визначити виваженою сумою [14, 29]:

$$K_{\text{об}} = \nu_1 \cdot K_1 + \nu_1 \cdot K_2 + \text{L} \ + \nu_m \cdot K_m, \tag{2.2}$$

де, $K_1,...,K_m$ – відповідне значення часткового показника, що характеризує деяку властивість (характеристику) об’єкта ЕМП; $\nu_1,...,\nu_m$ – ваговий коефіцієнт, що враховує важливість конкретної властивості об’єкту ураження в умовах обстановки, що склалася.

Сутність показника розвіддоступності об’єктів ЕМП у (3.22) пояснює вираз:

$$P_{\text{рд}} = 1 - P_{\text{зпр}} \cdot P_{\text{рер}} \cdot P_{\text{кр}} \cdot P_{\text{звр}}, \tag{2.3}$$

де $P_{\text{зпр}}, P_{\text{рер}}, P_{\text{рлр}}, P_{кр}, P_{\text{звр}}$ – ймовірність помилки при виявленні об'єкта ЕМП засобами повітряної, радіоелектронної, космічної та загальновійськової розвідки відповідно.

Показник захищеності об'єкту ЕМП від ураження ЕМБ визначимо виразом:

$$Z = Z_{\text{форт}} + Z_{\text{тм}} + Z_{\text{ппо}} + Z_{\text{реа}}, \tag{2.4}$$

де, $Z_{\text{форт}}, Z_{\text{тм}}, Z_{\text{ппо}}, Z_{\text{реа}}$ – ступінь фортифікаційного обладнання, тактичного (оперативного) маскування, ураження силами ППО засобів доставки ЕМБ, захищеності радіоелектронної апаратури від ураження ЕМБ об'єкта ЕМП відповідно.

Кількість радіоелектронних засобів (комплексів, терміналів), або телефонних каналів та ліній радіозв'язку, електричних, кабельних та волоконно–оптичних мереж, які організовані з іншими органами управління або об'єктами ЕМП визначимо сумою:

$$N = N_{\text{рез}} + N_{\text{ел}} + N_{\text{каб}} + N_{\text{комп}} + N_{\text{вол-опт}}, \tag{2.5}$$

де, $N_{\text{рез}}$ – кількість радіоелектронних засобів (комплексів) на об'єкті ЕМП; $N_{\text{ел}}$ – кількість електричних мереж на об'єкті ЕМП; $N_{\text{каб}}$ – кількість кабельних мереж на об'єкті ЕМП; $N_{\text{комп}}$ – кількість комп'ютерних мереж; $N_{\text{вол-отп}}$ – кількість волоконно-оптичних мереж.

Основними оперативно-тактичними показниками ЕМП в операціях (бойових діях) слід вважати ступінь виконання завдань з ЕМП в операції (або за етапом (задачею)) та зону виконання завдань з електромагнітного подавлення в операції [14, 29].

Конкретизуємо введені показники.

Нехай розглядається кінцева множина M об'єктів впливу в операції (бою):

$$M = \left\{ m_i \,/\, K_{\text{об}_i} \geq K_{\text{кр}} \right\}, \; i = 1...n, \tag{2.6}$$

де n – кількість об'єктів ЕМП; $K_{\text{кр}}$ – критичне значення вагового коефіцієнта $K_{\text{об}}$ для зарахування радіоелектронного об'єкту до множини ОЕМП.

Множина M містить дві підмножини:

$$M_1 = \left\{ m_i \,/\, K_{\text{об}_i} \geq K_{\text{кр}}, r_i \leq R \right\}, i = 1...l; \tag{2.7}$$

$$M_2 = \left\{ m_i / K_{\text{об}_i} \geq K_{\text{кр}}, r_i > R \right\}, i = 1...k, \tag{2.8}$$

де $r_i = \sqrt{S_i / \pi}$ – приведений радіус ОЕМП; S_i – площа ОЕМП; R – радіус ураження електромагнітного боєприпасу; l, k – кількість об'єктів ЕМП, для яких виконується вимога $r_i \leq R$ та $r_i > R$ відповідно; $l + k = n.$

Основним показником ступеню виконання завдань з ЕМП можна вважати ймовірність ураження $P_{\text{ур}}$ сукупності n об'єктів, $n = l + k$. У першому наближенні:

$$P_{\text{ур}} = \prod_{i=1}^{l} (1 - P_{\text{збер}_i}(r_i \leq R)) \cdot \prod_{i=1}^{k} (1 - P_{\text{збер}_i}(r_i > R)), \tag{2.9}$$

$$P_{\text{збер}_i}(r_i \leq R) = \exp\left[\frac{-(R + r_i)^2}{2\delta^2} \right], \tag{2.10}$$

$$P_{\text{збер}_i}(r_i > R) = \exp\left[\frac{-m \cdot (R + r_i)^2}{2\delta^2} \right], m \geq 2, \tag{2.11}$$

де, $P_{\text{збер}_i}$ – ймовірність збереження об'єкту від ураження ЕМЗ; m – кількість ударів ЕМБ по об'єкту; δ – помилка системи наведення електромагнітного боєприпасу на об'єкт, який уражається.

Результати (3.30), (3.31) та (3.32) можуть бути конкретизовані на випадок врахування заходів з захисту об'єктів противника від ураження ЕМЗ. Так, наприклад, якщо для захисту об'єкту противником в рамках заходів з оперативного маскування створена хибна позиція з радіусом виносу $r_{\text{в}}$ від основного, то (3.31) перетворюється до вигляду:

$$P_{\text{ур}_i}(r_i \leq R) = \exp\left[\frac{-((R + r_i) - r_{\text{в}})^2}{2\delta^2} \right]. \tag{2.12}$$

Враховуючи (3.27...3.32), зона виконання завдань з електромагнітного подавлення в операції – це просторова область, яка обмежена умовами виконання критерію:

$$P_{\text{ур}} \geq P_{\text{ур}}^{\text{кр}}, \tag{2.13}$$

де $P_{\text{ур}}, P_{\text{ур}}^{\text{кр}}$ – те, що досягається та критичне значення ймовірності ураження угруповання об'єктів ЕМП в операції (зона ЕМП в операції) відповідно.

Основні оперативно-тактичні показники бойового застосування комплексів (засобів) ЕМП представимо множиною [29]:

$$C_{\text{бз}} = \left\{ R_{ij}, P_{\text{ур}_{ij}}, P_{\text{дост}_{ij}} \right\} \tag{2.14}$$

де, R_{ij} – зона електромагнітного ураження i-го об'єкта електромагнітним боєприпасом j-го типу, яка є частиною простору, де потужність електромагнітного випромінювання $P_{\text{емб}_{ij}}^{\text{реа}}$, що впливає на РЕ(А), призводить до наведення на її елементах електричних токів $I_{\text{нв}}^{\text{реа}}$ не менш критичних $I_{\text{нв}}^{\text{кр}}$. При цьому $I_{\text{нв}}^{\text{кр}}$ – мінімальна сила електричного току, при якій відбувається функціональне ураження елементної бази РЕА, що подавляється; $P_{\text{ур}_{ij}}$ – ймовірність електромагнітного ураження i-го об'єкта електромагнітним боєприпасом j-го типу. Визначення цього показника може бути проведено із застосуванням (3.31),(3. 32), вибираючи тип об'єкту ураження ($(r_i \le R)$ – точковий, $(r_i > R)$ – площинний); $P_{\text{дост}_{ij}}$ – ймовірність доставки ЕМБ до i-го об'єкта електромагнітного ураження j-го типу електромагнітного боєприпасу. Порядок визначення цього показника залежить від типу засобу доставки ЕМБ.

Зона електромагнітного ураження – це просторова область, яка обмежена умовами виконання критерію:

$$P_{\text{уро}} \ge P_{\text{уро}}^{\text{кр}}, \tag{2.15}$$

де, $P_{\text{уро}}, P_{\text{уро}}^{\text{кр}}$ – досяжне та критичне значення ймовірностей ураження ОЕМУ відповідно.

В загальному вигляді ймовірність $P_{\text{дост}_{ij}}$ може бути визначена з уточненням особливостей розрахунку до конкретного засобу доставки у вигляді [29]:

$$P_{\text{дост}_{ij}} = 1 - P_{\text{нз}}^{\text{ппо}} \cdot P_{\text{нз}}^{\text{нав}}, \tag{2.16}$$

де, $P_{\text{нз}}^{\text{ппо}}$ – ймовірність невирішення завдань з подолання відповідним засобом доставки ЕМБ системи ППО противника; $P_{\text{нз}}^{\text{нав}}$ – ймовірність невирішення завдань з навігаційного забезпечення наведення засобу доставки ЕМБ на об'єкт ураження.

Науково-практичні аспекти захисту об'єктів своїх військ (сил) від ураження ЕМЗ в операціях (бойових діях).

Однією з основних тенденцій розвитку концептуальних основ РЕБ є вдосконалення радіоелектронного захисту об’єктів від ЕМЗ.

Основними напрямками досліджень у цій області є:

– розробка методів протидії засобам доставці ЕМЗ;

– розробка технічних заходів щодо захисту радіоелектронної апаратури;

– розробка нормативно-адміністративних (організаційних) заходів захисту РЕА.

Найбільш ефективний спосіб захисту від ЕМЗ – заважання процесу доставки електромагнітних боєприпасів шляхом знищення комплексів (засобів) доставки. Однак активне застосування засобів доставки з малою радіолокаційною помітністю (БПЛА, крилатих ракет) ускладнює реалізацію цього способу на практиці.

Конкретизуємо **основні шляхи розвитку технічних аспектів захисту радіоелектронної апаратури від ЕМЗ** на сучасному етапі.

Найбільш ефективний метод захисту полягає у тому, щоб помістити обладнання в екрануючу електропровідну сітку, яка називається чарункою Фарадея [14].

На практиці використовують менш надійні засоби захисту, зокрема струмопровідні сітки або плівкові покриття для вікон, контактні пружинні прокладки, встановлені по периметру дверей і люків.

Радіоелектронне обладнання має комунікації із зовнішнім середовищем (із джерелами живлення, мережні з’єднання і т. п.). Це спричинює появу “точок входу” навіть в оптимально екранованому обладнанні, через які електричні перехідні процеси можуть викликати ушкодження. Тому у місцях входу на електропровідному каналі слід встановлювати мережні фільтри, а також іскрові розрядники, метало-окисні варистори [14] і високошвидкісні зенерівські діоди [29].

Найбільш раціональним підходом до проектування засобів захисту від ЕМЗ кабельних вводів є створення таких роз’ємів, у конструкції яких передбачено елементи фільтрів і заздалегідь вбудовані зенерівські діоди.

Складність вирішення завдання захисту від ЕМЗ і висока вартість розроблених для цього засобів і методів змушують на перших порах іти шляхом їхнього вибіркового застосування в особливо важливих системах зброї і військової техніки.

У комунікаційних мережах доцільно застосовувати топологію з достатнім надлишком і механізмами ліквідації збоїв, щоб забезпечити можливість роботи у разі виведення з ладу великої кількості вузлів і ліній зв’язку. Це не дозволить противникові вивести з ладу більшу частину мережі або навіть мережу в цілому шляхом знищення ключових вузлів або ліній зв’язку однією атакою або невеликою кількістю атак.

Для оцінки ефективності заходів з захисту радіоелектронних об’єктів від ураження ЕМЗ можуть бути трансформовані підходи (3.30 – 3.33).

Системи і засоби електромагнітної поразки за ефектом, що досягається при впливі на радіоелектронні об’єкти противника можуть бути прирівняні до

тактичної ядерної зброї. При цьому можливе нанесення і високоточних ударів по конкретних об'єктах.

Необхідно акцентувати увагу на важливому, в умовах загальної гуманізації збройної боротьби, факті – ЕМЗ не призводить до ураження особового складу. Ця властивість ЕМЗ визначає високу актуальність її застосування при вирішенні завдань по блокуванню і знищенню незаконно створених збройних формувань, терористичних сил в спеціальних та гуманітарних операціях, де втрати мирного населення неприпустимі.

Тому у сучасних поглядах на ведення збройної боротьби ЕМЗ необхідно розглядати як симбіоз узагальненої, сформованої на новому рівні абстрактного подання, сукупності властивостей зброї масового ураження, ВТЗ, традиційних вогневих засобів ураження. З таких позицій повинний відбуватися розвиток концептуальних основ тактики застосування ЕМЗ в операціях (бойових діях) сучасності й у майбутньому.

Поява нових видів зброї призвели до активної трансформації форм ведення РЕБ. Тому тут дамо визначення та стисло проаналізуємо деякі загальні особливості застосування нових форм РЕБ на прикладі радіоелектронного удару.

Радіоелектронний удар – нова форма ведення РЕБ у збройній боротьбі сучасності та у майбутньому.

У війнах четвертого покоління основною формою РЕБ був радіоелектронний вплив. Корінні зміни зброї РЕБ, поглядів на основи ведення РЕБ в операціях призвели до формування нових форм РЕБ [29]:

– радіоелектронний та радіоелектронно-вогневий удар; операція РЕБ.

Радіоелектронний удар (РЕУ) – сукупність узгоджених за метою, завданнями, місцем і часом потужних **короткочасних впливів**, що здійснюються угрупованнями сил та засобів **радіоелектронного, електромагнітного та програмно - комп'ютерного подавлення** за єдиним замислом і планом для порушення функціонування радіоелектронних засобів (комплексів) систем управління військами (силами) і зброєю та ураження особового складу противника в операціях (бойових діях).

Радіоелектронно-вогневий удар (РЕУ) – сукупність узгоджених за метою, завданнями, місцем і часом потужних короткочасних впливів, що здійснюються угрупованнями силам та засобів вогневого ураження, радіоелектронного, електромагнітного, програмно - комп'ютерного подавлення за єдиним замислом і планом для порушення функціонування радіоелектронних засобів (комплексів) систем управління військами (силами) і зброєю та ураження особового складу противника в операціях (бойових діях).

2.6. Аналіз досвіду ведення російсько-терористичними військами РЕБ в АТО та операції об'єднаних сил

Засоби РЕБ та РЕР армії РФ.

2.6.1. Літак дальнього радіолокаційного виявлення та управління А-50

А-50 призначений для виявлення і супроводу повітряних цілей і надводних кораблів, оповіщення командних пунктів автоматизованих систем управління видів Збройних Сил про повітряну і надводну обстановку, управління літаками винищувальної і ударної авіації при їх наведенні на повітряні, наземні і морські цілі, організації повітряного командного пункту (див. рис. 2.20).

Рис. 2.20. Літак А-50

Технічні характеристики	
Екіпаж льотний / тактичний, чол.	5/10
Двигуни Д-30КП	4
Тяга двигунів, кгс.	4 * 12000
Швидкість макс. / крейсерська, км. / год.	810/750
Тривалість патрулювання в повітрі без дозаправки на видаленні 10000 км від аеродрому зльоту, ч.	4
Дальність польоту максимальна без дозаправки в повітрі, км.	7500
Максимальна злітна маса, кг.	190000
Довжина пробігу, м.	500
Радіоелектронне озброєння	
Маса радіотехнічного комплексу, т.	20
Кількість одночасно супроводжуваних цілей, шт.	50-60
Кількість одночасно наводяться винищувачів, шт.	10-12
Дальність виявлення винищувачів з ЕПР = 3 м2, км.	220-240

Дальність оперативного радіозв'язку: - по каналу КВ діапазону; - по каналу УКХ діапазону; - по широкосмугового радіолінії.	 2000 400 400
Дальність передачі інформації на КП АСУ видів ЗС по радіолінії, км: - мет. і дециметрового діапазону; - короткохвильового діапазону; - супутникового зв'язку.	 350 2000 більше 2000

2.6.2. Комплекс радіоелектронної боротьби РП-377ЛА "Лоранд"

Лоранд – малогабаритний багатофункціональний комплекс радіоконтролю, пеленгування і придушення, який забезпечує оперативний пошук, визначення місця розташування і радіопридушення радіоелектронних засобів УКХ радіозв'язку незаконних збройних формувань, терористичних груп та джерел перешкод системам управління і зв'язку.

Комплекс РП-377ЛА "Лоранд" розміщується на автомобілі підвищеної прохідності і може застосовуватися в польових умовах.

Залежно від розв'язуваних завдань комплекси можуть об'єднуватися в систему з двох і більше комплексів РП 377Л або РП-377ЛА "Лоранд", один з яких виконує функцію пункту управління системою (див. рис. 2.21).

Рис. 2.21. Комплекс радіоелектронної боротьби (РЭБ) РП-377ЛА “Лорандит” на шасі УАЗ

Технічні характеристики	
Діаназон технічного аналізу частот, МГц	0,1-1800
Діапазон пеленгування джерел радіовипромінювання, МГц	20-1800
Діаназон радіорозвідки, радіоподавлення, МГц	20-2700
Точність пеленгування, °	2-3°
Швидкість пеленгування,МГц/с	2000
Смуга одночасного огляду, кГц	180-1200
Потужність передавача постановника навмисних завад, Вт	40-500

2.6.3. Автоматизована станція завад Р-330ж “Житель”

Р-330ж “Житель” – автоматизована станція перешкод. Прийнята на озброєння в 2000 році.

Автоматизоване визначення, пеленгування й аналіз сигналів джерел радіовипромінювання в діапазоні частот 100-2000 МГц.

Постановка радіоперешкод носимим і мобільним наземним станціям радіозв’язку, системам супутникового зв’язку “Інмарсат” і “Ірідіум”, навігаційній апаратурі GPS NAVSTAR, базовим станціям та терміналам стільникового зв’язку GSM-900/1800/1900.

Віддаленість подавлення виявлених засобів до 30 км.

Автоматизоване ведення телекодового обміну з аналогічною спряженою станцією перешкод для забезпечення синхронного пеленгу джерел радіовипромінювання з метою визначення їх координат (див. рис. 2.22).

Рис. 2.22. Р-330ж “Житель”

2.6.4. Комплекс РЕБ РБ-341в “Леер-3”

РБ-341в “Леер-3” – комплекс подавлення/імітації GSM-зв’язку за допомогою використання БПЛА (див. рис. 2.23). Можливості:

– Подавлення мобільного зв’язку.

– Імітація роботи базової станції стільникового зв’язку в діапазонах GSM 900 і GSM 1800 і відправлення помилкових сигналів (повідомлень).

– Ведення розвідки шляхом визначення місць випромінювання апаратів у мережах GSM.

– Виявлення абонентських терміналів (мобільні телефони, планшети й інші комплекси зв’язку).

– Нанесення місця розташування абонентських терміналів на цифрову карту.

– Передавання даних про місце абонентських терміналів артилерійським розрахункам для завдання вогневого удару.

– Повітряне спостереження за обстановкою на полі бою й пересуванням військ.

– Оцінка стану армійських і флотських об’єктів.

– Дослідження рельєфу місцевості.

Рис. 2.23. РБ-341в “Леер-3”

Технічні характеристики	
Діапазон частот каналу управління, МГц	902- 922
Стандарт контрольованої мережі	GSM 900, GSM 1800
Діапазон робочих частот, МГц	935 – 960 МГц, 1805 – 1880 МГц, 890 – 915 МГц, 1710 – 1785 МГц.
Радіус зони блокуємих терміналів стільникового зв’язку, км.	до 6
Кількість одночасно блокуємих абонентів стільникового зв’язку	2000
Кількість одночасно блокуємих операторів стільникового зв’язку	3
Кількість одночасно керованих БПЛА	2

Тип БПЛА	Орлан-10
Прийняття на озброєння	2015 рік

2.6.5. Комплекс радіорозвідки і радіоподавлення для підрозділів ВДВ РБ-5316 “Інфауна”

Призначення – забезпечення захисту авто- і бронетехніки, а також особового складу підрозділів десанту від радіокерованих мінно-вибухових пристроїв і забезпечення радіоподавлення засобів зв’язку противника в частинах РЕБ батальйонного рівня. До складу обладнання комплексу входять традиційні для комплексів РЕБ засоби радіоелектронного подавлення засобів зв’язку й управління, а також засоби оптико-електронної розвідки й подавлення. Прийнятий на озброєння в 2012 році (див. рис. 2.24).

Рис. 2.24. РБ-5316 “Інфауна”

2.6.6. Комплекс РЕБ Р-934УМ “Удар”

Призначення Р-934УМ “Удар” (див. рис. 2.25):

– автоматизоване виявлення, пеленгування й аналіз сигналів джерел радіовипромінювання у робочому діапазоні частот;

– постановка радіоперешкод УКХ радіотелефонного зв’язку й базових станцій транкінгових систем рухомого радіозв’язку;

– автоматизоване ведення телекодового інформаційного обміну з аналогічної сполученої АСП для забезпечення синхронного пеленгування джерел радіовипромінювань із метою розрахунки їхніх координат;

– автоматизоване ведення телекодового інформаційного обміну з вищим пунктом управління з метою одержання завдання на ведення бойової роботи й доповіді результатів роботи;

– ведення картографічних даних з відображенням інформації про розвіддані джерела радіовипромінювань на тлі електронної топографічної карти місцевості або в сітці прямокутних координат.

Рис. 2.25. Р-934УМ “Удар”

Технічні характеристики	
Діаназон робочих частот: - при веденні радіорозвідки, МГц; - при веденні радіоподавлення, МГц.	 100...2000 100...400
Середньоквадратична похибка виміру пеленгів на джерела радіовипромінювань, °	не більше 2°
Швидкість сканування частотного діапазону: - у режимі виявлення, МГц/с; - у режимі пеленгування, МГц/с.	 800 400
Вихідна потужність передавача, Вт.	не менше 100
Ширина діаграми спрямованості передавальної антени: - по азимуту, °; - по куту місця, °.	 120° 40°
Види сигналів перешкод: - частотно-модульована шумова перешкода; - частотна-маніпульована хаотичною імпульсною послідовністю несівна частота.	
Кількість одночасних випромінювань сигналів постановки перешкод	не більше 4.
Швидкість обміну телекодовою інформацією: - між сполученими АСП, кбіт/с; - між АСП і пунктом управління, кбіт/с.	 не менше 256 не менше 48
Прийняття на озброєння	2018 рік

2.6.7. Комплекс РЕБ СПР-2М (1Л262Э) “Ртуть-БМ”

СПР-2М (1Л262Э) “Ртуть-БМ” – постановник перешкод для радіопідривників боєприпасів/подавлення засобів УКХ радіозв’язку та радіолокації.

Виріб “Ртуть-БМ” призначений для зниження впливу уражаючи елементів артилерійських снарядів на дружні війська й бронетехніку шляхом впливу на режим роботи радіопідривників боєприпасів. Здатна, при успішній електронній атаці, забезпечити підрив снаряда на безпечній відстані (за 200 – 300 м до цілі) або перевести режим роботи радіопідривників в контактний. Основним місцем використання є війська першого ешелону, командні пункти, місця скупчення військ і пускові установки. Також може застосовуватися для прикриття рухомих об’єктів у місцях переправ та на марші (див. рис. 2.26).

Рис. 2.26. СПР-2М (1Л262Э) “Ртуть-БМ”

Зміна роботи радіопідривників снаряда досягається за рахунок застосування спеціального приймача, що визначає несучу частоту підривника й відтворює необхідні для підриву боєприпасів сигналів. Час визначення частоти становить кілька мікросекунд, а формування відповідного сигналу – до декількох млс., при цьому формується квазінеперервна перешкода.

Технічні характеристики	
Діапазон робочих частот, МГц	95-420
Час виявлення частоти радіопідривника та постановки перешкоди, мс	1,5-2
Потужність передавача перешкод, Вт	250-300
Кількість УКХ р/ліній, що подавляються	3-6
Захищена ділянка місцевості, га	20-50
Імовірність успішного подавлення	не менше 0,8
Прийняття на озброєння	2011 рік

2.6.8. Станція РЕБ “Шиповник-Аэро”

Станція РЕБ, шифр “Шиповник-Аэро” – комплекс радіомоніторингу і блокування/перехоплення каналів управління БПЛА (див. рис. 2.27).

Рис. 2.27. Станція РЕБ, шифр “Шиповник-Аэро”

Технічні характеристики	
Час на перехоплення управління БПЛА: - для моделей, які відомі, мс; - для невідомих моделей, с.	 умовно 700 умовно 25
Визначення координат БПЛА, °	2-3°
Визначення координат ПУ БПЛА	орієнтовно 100м (ГЛОНАС, GPS).
Віддаленість виявлення БПЛА, км	не менше 10
Типи безпровідних мереж, що придушуються	Wi-Fi, WiMAX DECT, GPS
Робочий діапазон радіомоніторингу БПЛА, МГц	25-2500, 400-500, 800-925 і 2400-2485.
Проходив польові випробування, в тому числі на Донбасі, починаючи з 2014 року та в ході навчань військ РЕБ ПівдВО та Чорноморського флоту РФ у серпні 2016 року.	

2.6.9. Станція РЕБ “Красуха-2”

Станція РЕБ, шифр “Красуха-2” – багатофункціональний комплекс активних перешкод для подавлення ліній зв’язку та бортових РЛС літаків, вертольотів, а також систем ДРЛВ (див. рис. 2.28).

Призначення: прикриття командних пунктів, угрупувань військ, засобів ППО, важливих промислових і адміністративно-політичних об’єктів

активними перешкодами. Здійснює подавлення радіоелектронного обладнання супутників, наземних РЛС і авіаційних систем AWACS.

Рис. 2.28. Станція РЕБ, шифр “Красуха-2”

Станція прийнята на озброєння у 2012 році.

2.6.10. Станція РЕБ “Красуха-4”

Багатофункціональний комплекс активних перешкод для подавлення ліній зв’язку та бортових РЛС літаків і вертольотів, а також систем ДРЛВ (див. рис. 2.29).

Рис. 2.29. Станція РЕБ, шифр “Красуха-4”

Призначення: прикриття командних пунктів, угрупувань військ, засобів ППО, важливих промислових і адміністративно-політичних об’єктів активними перешкодами. Здійснює подавлення радіоелектронного обладнання супутників, нахемних РЛС і авіаційних систем AWACS.

Віддаленість дії комплексу приблизно 150-300 км.

Прийняття на озброєння – 2012 році.

2.6.11. Комплекс РЕБ РБ-301Б “Борисоглебск-2”

РБ-301Б “Борисоглебск-2” – комплекс розвідки й подавлення засобів супутникового зв’язку та навігації інших засобів КХ/УКХ діапазону в тактичній ланці управління (див. рис. 2.30).

Склад: пункт управління Р-300КВМ та апаратні машини: Р-378БМВ, Р-330БМВ, Р-934 БМВ та Р-325УМВ. Прийняття на озброєння – 2013 рік.

Рис. 2.30. РБ-301Б “Борисоглебск-2”

2.7. Сили радіоелектронної боротьби Збройних Сил України. Склад, призначення та бойові можливості

Вивчення бойових можливостей та завдань що вирішують частин (підрозділи) РЕБ ЗСУ є надважливими для врахування під час організації взаємодії між підрозділами Держспецзв’язку та РЕБ ЗС України при виконанні завдань за призначенням.

Завдання радіоелектронної боротьби в мирний час та в операціях (бойових діях) виконуються силами та засобами, які організаційно зведені в спеціальні військові формування – частини і підрозділи РЕБ, розвідки і радіоелектронної боротьби (Р і РЕБ), радіоелектронної розвідки і РЕБ (РЕР і РЕБ) – або засобами РЕБ, які знаходяться на озброєнні об'єднань, з'єднань і частин видів Збройних Сил (індивідуальні і групові засоби постановки завад, що встановлені на літаках, вертольотах; корабельні засоби РЕБ; спеціальні пристрої (прилади) радіоелектронного захисту радіоелектронних засобів), а також об'єднаннями, з'єднаннями, частинами, підрозділами родів військ і спеціальних військ.

2.7.1. Частини (підрозділи) РЕБ Збройних Сил України

Завдання радіоелектронної боротьби в мирний час та в операціях (бойових діях) виконуються силами та засобами, які організаційно зведені в спеціальні військові формування – частини і підрозділи РЕБ, розвідки і радіоелектронної боротьби (Р і РЕБ), радіоелектронної розвідки і РЕБ (РЕР і РЕБ) – або засобами РЕБ, які знаходяться на озброєнні об'єднань, з'єднань і частин видів Збройних Сил (індивідуальні і групові засоби постановки завад, що встановлені на літаках, вертольотах; корабельні засоби РЕБ; спеціальні пристрої (прилади) радіоелектронного захисту радіоелектронних засобів), а також об'єднаннями, з'єднаннями, частинами, підрозділами родів військ і спеціальних військ.

Бойовий склад сил та засобів РЕБ об'єднання (з'єднання) – сукупність частин (підрозділів) РЕБ (Р і РЕБ), які залучаються до участі в операції (бойових діях). Він складається зі штатних та приданих сил та засобів РЕБ. З бойового складу частин (підрозділів) РЕБ з метою забезпечення дій військ (сил) на головному та інших напрямках створюються головне та інші угруповання сил і засобів РЕБ, а також резерв.

Організаційно частини та підрозділи РЕБ зведені в окремі полки (батальйони) РЕБ (з наземними, літаковими, космічними засобами), радіоелектронної розвідки і РЕБ, розвідки і РЕБ; ескадрильї (ланки) РЕБ; роти РЕБ; окремі вузли, центри РЕБ.

На частини та підрозділи РЕБ Сухопутних військ Збройних Сил України покладені такі завдання:

– на окремий полк РЕБ з наземними засобами (оп РЕБ-Н) командування Сухопутних військ – радіоподавлення короткохвильових засобів зв'язку в оперативно-стратегічній і оперативній ланках управління противника;

– на окремий полк РЕБ з літаковими засобами (оп РЕБ-Л) командування Сухопутних військ – прикриття від повітряної радіолокаційної розвідки і прицільних ударів з повітря (в тому числі від ураження ВТЗ з лазерними та оптико-електронними системами наведення) угруповань військ та об'єктів шляхом радіоелектронного подавлення бортових засобів

радіолокаційної розвідки (РЛР), управління зброєю, радіонавігації, лазерних і оптико-електронних засобів;

– на окремий батальйон РЕБ з літаковими засобами (об РЕБ-Л) командування Сухопутних військ – прикриття від повітряної радіолокаційної розвідки і прицільних ударів з повітря угруповань військ та об'єктів шляхом радіоелектронного подавлення бортових засобів РЛР, управління зброєю, радіонавігації;

– на окремий батальйон РЕБ з космічними засобами (об РЕБ-К) центрального підпорядкування (резерву) – радіоподавлення супутникових ліній зв'язку в оперативно-стратегічній, оперативно-тактичній і тактичній ланках управління противника;

– на частини розвідки і РЕБ об'єднань: окремі полки, батальйони Р і РЕБ, окремі батальйони РЕБ з наземними засобами (оп, об Р і РЕБ, об РЕБ-Н) – радіоподавлення короткохвильових та ультракороткохвильових засобів зв'язку в оперативно-тактичній і тактичній ланках управління противника;

– на частини Р і РЕБ тактичних груп (батальйони Р і РЕБ), підрозділи РЕБ механізованих бригад (роти РЕБ) – радіоподавлення короткохвильових та ультракороткохвильових засобів зв'язку управління частинами та підрозділами першого ешелону противника; прикриття пунктів управління і військ від ураження артилерійськими снарядами (бомбами) із радіопідривачами;

– на окремі вузли (ов РЕБ), спеціальні центри (СЦ) РЕБ командування СВ (об'єднань) центрального підпорядкування – контроль за проведенням штабами і військами заходів щодо радіоелектронного захисту РЕЗ в угрупованнях своїх військ, контроль радіоелектронної обстановки, забезпечення управління силами та засобами РЕБ.

Конкретизуємо бойові можливості та структуру частин та підрозділів РЕБ ЗС України. Бойові можливості частин (підрозділів) РЕБ визначаються показниками з радіорозвідки, радіоподавлення та маневру.

Окремий полк РЕБ-Н призначений для радіоподавлення короткохвильових (КХ) засобів зв'язку в оперативній та оперативно-стратегічній ланках управління противника (штабів видів ЗС, штабів об'єднань, армійських корпусів, розвідувально-ударних комплексів, з'єднань ВПС та ППО).

Полк в своєму складі може мати 2 батальйони радіозавад КХ - радіозв'язку, а також підрозділи забезпечення.

Полк спроможний:

– розвідати до 48 КХ- радіомереж противника: найважливіші КХ-радіомережі двох армій (армійських корпусів) на напрямку головного удару;

– за одну годину роботи визначити розташування до 30 КХ-радіостанцій пунктів управління оперативної та оперативно-стратегічної ланок управління противника;

– подавити до 32 станцій КХ - радіозв'язку (найважливіші КХ - радіомережі головних штабів 2-3 армій, ВПС, ППО, АК або 2-3 армій і двох армійських корпусів першого ешелону противника).

Глибина подавлення КХ – радіозасобів зв'язку – від 250 до 1500 км просторовою хвилею і до 80 км – поверхневою хвилею.

Термін розгортання (згортання) полку становить від 2,5 до 3 год., швидкість переміщення полку складає 30-40 км/год (при переміщенні на 100-150 км полк на маневр витрачає близько 9-12 год.).

Окремий батальйон РЕБ-Н призначений для радіоподавлення КХ- і УКХ – радіозасобів зв`язку СВ і авіації в оперативно-тактичній і тактичній ланках управління противника, радіоблокади вузлів зв'язку тактичної ланки управління та здійснення радіодезінформації.

Батальйон в своєму складі може мати: дві роти радіозавад КХ- та УКХ - радіозв'язку, взвод радіозавад УКХ - зв'язку авіації, взвод радіодезінформації і передавачів завад, що закидаються, підрозділи забезпечення.

Бойові можливості батальйону визначаються показниками з радіорозвідки, радіоподавлення радіозв'язку, радіоблокади вузлів зв'язку противника, радіодезінформації та маневру. Батальйон спроможний:

– вести періодичне спостереження за 24 КХ- радіомережами противника (найважливішими КХ - радіомережами армійського корпусу і двох дивізій першого ешелону противника);

– за одну годину роботи визначити місце розташування 20-30 КХ - радіостанцій на відстані до 40-60 км;

– вести періодичне спостереження в УКХ - діапазоні за 32 радіомережами (частотами) противника і визначати місцезнаходження 120 радіостанцій пунктів управління;

– подавити 48 КХ-, 48 УКХ- і до 16 авіаційних УКХ - радіомереж противника (найважливіші радіомережі пунктів управління корпусу і двох дивізій першого ешелону противника) на відстані 30-40 км;

– подавити такі радіомережі на дальності: КХ – радіозв'язку літеродрукуванням в ланці корпус - дивізія до 50 км, радіотелефоном на одній боковій смузі частот – до 40 км; УКХ - радіозв'язку радіотелефоном з частотною модуляцією в ланці дивізія - бригада до 30 км, бригада - батальйон – до 20 км і батальйон – рота до 5 км; УКХ – радіозв'язку авіації в ланці передовий авіанавідник – літак у повітрі – до 40 км при висоті польоту 100 м і в ланці літак-літак – до 80 км;

– одним комплектом ЗПП здійснити радіоблокаду 1 вузла зв'язку тактичної ланки;

– здійснити радіодезінформацію шляхом входження в три КХ- і три УКХ- радіомережі тактичної ланки управління противника.

Кількісними показниками батальйону по радіоподавленню вважаються можливості по глибині подавлення і кількості подавлених мереж радіо - і радіорелейного зв'язку. Батальйон має на озброєнні 12 станцій радіозавад КХ - радіозв'язку, 12 станцій завад УКХ - радіозв'язку та 4 станції завад авіаційному УКХ – радіозв'язку.

Можливості батальйону щодо радіоблокади вузлів зв'язку пунктів управління противника визначаються кількістю передавачів завад, нормативною кількістю ЗПП, необхідною для радіоблокади вузла зв'язку.

Можливості батальйону щодо радіодезінформації визначаються кількістю радіостанцій (засобів РЕБ), які можна застосувати для виконання завдання.

Час розгортання батальйону в бойовий порядок складає 2 год. 30 хв., згортання - 2,0 год. Швидкість переміщення батальйону складає до 20 км/год, в тиловому районі армійського корпусу - 30-40 км/год. Таким чином, загальний час маневру батальйону на відстань 100 км складає близько 8-10 год.

Окремий батальйон РЕБ-Л призначений для розвідки та радіоподавлення бортових радіоелектронних засобів з метою прикриття військ і об'єктів від повітряної радіолокаційної розвідки, прицільних ударів авіації противника з застосуванням РЛС та зриву радіонавігації тактичної і армійської авіації противника.

Об'єктами прикриття можуть бути райони зосередження з'єднань, позиційні райони ракетних з'єднань та частин, пункти управління, мостові переправи, залізничні станції, вузли доріг, аеродроми та інші об'єкти.

Батальйон у своєму складі може мати дві роти радіозавад, роту управління, роту зв'язку і підрозділи забезпечення.

Батальйон спроможний:

– виявити до 20 цілей за хвилину на відстані від 25 до 270 км залежно від висоти їх польоту, виявити за годину роботи до 60 цілей на відстані до 450 км;

– прикрити від радіолокаційної розвідки і прицільних ударів авіації і РУК противника позиції ракетної бригади, командний пункт армійського корпусу або головне угрупування армійського корпусу;

– прикрити типові об'єкти армійського корпусу (механізовану бригаду або командний пункт АК) зональним способом станціями радіозавад типу СПН-30 на дальностях 13-25 км, а СПН-40 – на дальностях 4-8 км;

– прикрити до 5 об'єктів з високою радіолокаційною контрастністю об'єктовим способом;

– зірвати радіонавігацію за допомогою радіонавігаційної системи ТАКАН і, тим самим, вихід в район цілей одночасно до 200 літаків двома станціями Р-388. Можливості батальйону по радіоподавленню радіонавігаційної системи ТАКАН визначаються кількістю станцій завад типу Р-388.

Переміщення на відстань 30-50 км батальйон здійснює за 5-6 год.

Рота РЕБ механізованого (танкового) з'єднання (батальйону Р і РЕБ) призначена для подавлення короткохвильового і ультракороткохвильового радіозв'язку в тактичній ланці управління противника, прикриття об'єктів бригади від ураження боєприпасами з радіопідривачами.

Для виконання завдань рота в своєму складі має взвод радіозавад КХ – радіозв'язку; два взводи радіозавад УКХ – радіозв'язку; взвод радіозавад радіопідривачам артилерійських снарядів, мін; взвод управління.

Можливості роти з радіоподавлення визначаються наявністю трьох станцій радіозавад КХ - радіозв'язку і 6 станцій радіозавад УКХ – радіозв'язку.

Бойові можливості роти визначаються показниками з радіорозвідки, радіоподавлення та маневру. Рота спроможна:

– вести періодичне спостереження за 8 радіомережами (частотами) КХ - радіозв'язку та за 12-16 радіомережами (частотами) УКХ – радіозв'язку противника;

– визначати місцезнаходження 20-30 УКХ - радіостанцій, 20-30 КХ – радіостанцій за годину;

– розвідувати радіостанції противника в УКХ - діапазоні на дальності – до 25-30 км, в КХ – діапазоні по наземній хвилі – до 50 км;

– подавити 8 КХ- і 16 УКХ- радіомереж противника (основна кількість радіомереж двох бригад першого ешелону дивізії противника).

Дальність радіоподавлення може становити при створенні радіозавад радіозв'язку літеродрукуванням в ланці бригада – батальйон до 20 км, радіотелефоном на одній боковій смузі частот – до 15 км; УКХ – радіозв'язку радіотелефоном з частотною модуляцією в ланці бригада - батальйон до 15 км і батальйон – рота до 7 км.

Можливості роти по прикриттю частин та підрозділів дивізії від боєприпасів з радіопідривачами визначаються наявністю 9 станцій завад СПР-2, якими рота здатна прикрити до 4-х об`єктів (типу артилерійський дивізіон, КП АК) на площі 150...200 га.

Час розгортання роти в бойовий порядок становить 40-60 хв., згортання – 20-50 хв. Швидкість переміщення роти в районі бойових дій може складати до 20 км/год (переміщення на відстань 10 км рота РЕБ здійснює за час від 2 до 2,5 годин).

2.7.2. Засоби і комплекси РЕБ видів Збройних Сил України

На озброєні Сухопутних сил, Повітряних Сил та Військово-Морських Сил Збройних Сил України знаходяться засоби, (комплекси) радіоелектронного подавлення та радіоелектронної розвідки які суттєво відрізняються як за своїми побудовою, завданнями які вони вирішують, місцем базування (наземне, літакове, корабельне) та інше. Так для Сухопутних сил є характерними засоби (комплекси), основною задачею яких є подавлення системи радіозв'язку противника. Для Повітряних Сил є характерними засоби (комплекси), основною задачею яких є подавлення систем радіолокації, наведення та радіонавігації які розміщаються на повітряних носіях та на земній поверхні. Для Військово-Морських Сил є характерними засоби (комплекси), які розміщаються на кораблях.

Розглянемо засоби, (комплекси) радіоелектронного подавлення у відповідності належності їх до видів Збройних Сил України.

2.7.2.1. Засоби та комплекси РЕБ Сухопутних військ

На озброєні частин РЕБ Сухопутних військ знаходяться засоби, комплекси радіоелектронного подавлення які забезпечують:

– своєчасне визначення параметрів сигналів і важливості цілей, що виявляються;

– масоване застосування радіозавад на обраному напрямку і контролю за їхньою ефективністю;

– швидке перенацілювання засобів радіозавад у ході бойових дій.

До складу засобів і комплексів РЕБ входять наступні основні підсистеми:

– радіорозвідки (окремі радіопеленгатори та апаратура безпосередньої розвідки станцій);

– управління (автоматизовані (неавтоматизовані) вузли, пункти управління, комплекси, командні пункти та підсистеми управління станцій завад);

– подавлення (станції завад та окремі передавачі завад).

2.7.2.1.1. Засоби радіорозвідки

Сучасні станції завад (Р-330У, Р-330Б, Р378А(Б), Р-325У) які є на озброєні частин (підрозділів) РЕБ Сухопутних військ (СВ) та Воєнно-Морських Сил (ВМС) у своєму складі мають пеленгаторну апаратуру, однак на озброєні цих частин (підрозділів) РЕБ є також неавтоматизовані станції завад (Р-330П, Р-378М, Р-325М), які працюють з автономним пеленгаторами Р-359 або Р-381-II. Основні ТТХ засобів РР надані в додатку 1.

Автомобільний короткохвильовий автоматичний радіопеленгатор Р-359 призначений для пеленгування радіостанцій з амплітудними і частотними модуляціями сигналів в зоні земних і пологих радіохвиль.

Інформаційні можливості Р-359: з пошуку – 5 радіомереж за годину; із спостереження – 2 радіомережі безперервно, 4 радіомережі періодично; 8 радіомереж в режимі контролю; з пеленгування – 30 пеленгів за годину.

Приймально-пеленгаторна машина Р-381-2 використовується у якості пеленгаторів УКХ діапазону (20...100 МГц) і призначена для пеленгування телеграфних і телефонних передач наземних радіостанцій з частотною і амплітудною модуляцією.

Радіопеленгатор Р-381-2 є складовою частиною комплексу засобів радіорозвідки Р-381Д, який призначений для ведення радіорозвідки в КХ і УКХ діапазоні.

Інформаційні можливості Р-381-2: з пошуку – 5 радіомереж за годину; із спостереження – 2 радіомережі безперервно, 4 радіомережі періодично; 8 радіомереж в режимі контролю; з пеленгування – 60 пеленгів за годину.

2.7.2.1.2. Засоби завад радіозв’язку

На озброєні частин (підрозділів) РЕБ СВ та ВМС можуть бути:

– засоби завад радіозв'язку КХ діапазону тактичної ланки управління противника (станції - Р-378М, Р-378А(Б), Р-325У);

– засоби завад радіозв'язку КХ діапазону оперативно-тактичної ланки управління противника (станції Р-325М2);

– засоби завад радіозв'язку УКХ діапазону тактичної ланки управління противника (станції завад - Р-330П, Р-330У, Р-330Б);

– засоби завад літакового радіозв'язку УКХ діапазону (станції Р-934, Р-934У).

Всі перераховані засоби подавлення працюють за двома алгоритмами.

Алгоритм роботи неавтоматизованих станцій завад (Р-378М, Р-325М2, Р-330П, Р-934):

– пошук і виявлення частот роботи радіоліній радіозв'язку в своєму робочому діапазоні частот;

– визначення належності ліній радіозв'язку, що розвідуються, до об'єкту РЕП шляхом слухового та візуального аналізу роботи виявленої лінії радіозв'язку;

– формування завад на одній частоті;

– ручний контроль роботи лінії радіозв'язку, що подавляється;

– ручне перенацілювання передавача завад на нову частоту.

Алгоритм роботи автоматизованих станцій завад (Р-378А(Б), Р-325У, Р-330Б, Р-934У):

– автоматичний пошук і виявлення ліній радіозв'язку;

– автоматичне пеленгування працюючих радіоелектронних засобів (РЕЗ) (за виключенням Р-934У у яких не передбачена апаратура пеленгації);

– відображення значень частоти і пеленгу виявлених РЕЗ на частотно-пеленгаційній панорамі (ЧПП) (за виключенням Р-934У);

– визначення належності виявлених ліній радіозв'язку до об'єктів радіоелектронного подавлення (РЕП) шляхом слухового та візуального аналізу сигналів та пеленгів (за виключенням Р-934У) на РЕЗ;

– записування і зберігання в запам'ятовуючих пристроях: значень частот, на яких заборонено створення завад; частот роботи РЕЗ, виявлених в процесі аналізу, що не являються об'єктами РЕП; частот роботи РЕЗ - об'єктів РЕП, що не мають пріоритету; частот роботи РЕЗ - об'єктів РЕП, що мають пріоритет; частот роботи РЕЗ, виділених для подавлення в даний момент часу;

– записування і зберігання в запам'ятовуючих пристроях значень меж завданого сектору розвідки (створення завад) (за виключенням Р-934У);

– автоматичне виключення із аналізу частот РЕЗ, які розташовані за межами завданого сектору розвідки (за виключенням Р-934У), а також частот, значення яких записані в запам'ятовуючих пристроях;

– відображення на блоці управління прийомом та передачею 10-и частот (20-и для Р-934У), що подавляються в першу чергу, їх пріоритету, а також вигляду вибраної завади;

– автоматичний контроль роботи ліній радіозв'язку, що подавляються;

– автоматичне перенацілювання передавача завад на частоти РЕЗ, виділених для подавлення.

Основні ТТХ засобів радіозавад надані в додатку 1.

Засоби завад радіозв'язку КХ діапазону тактичної ланки управління противника

Станції завад лініям КХ радіозв'язку призначені для створення радіозавад у радіомережах тактичної (взвод – рота – батальйон) і оперативно – тактичної (бригада – корпус) ланок управління противника.

Станція Р-378М є неавтоматизованою і працює в автономному або централізованому з ручним управлінням режимі, а станції Р-325У, Р-378А(Б) можуть працювати як в автономному так і в централізованому режимах роботи з автоматизованим управлінням від пункту управління тактичного (ПУ-Т) комплексу РЕП Р-330К (Мандат).

Ці станції забезпечують подавлення наступних видів зв`язку:

– слухового радіотелеграфного зв'язку з амплітудною маніпуляцією;

– слухового радіотелеграфного зв'язку з частотною маніпуляцією;

– слухового телеграфного радіозв`язку з амплітудно-тональною модуляцією;

– фототелеграфного зв'язку; букводрукуючого телеграфного зв`язку з частотною маніпуляцією (ЧТ бп і ДЧТ);

– радіотелефонного зв`язку з амплітудною і однополосною модуляцією (АМ і ОБП);

– радіотелефонного зв`язку з однополосною модуляцією з вторинним ущільненням декількома телефонними каналами;

– радіозв'язку з однополосною модуляцією при вторинному ущільненні декількома телефонними каналами частотною (ОМ-ЧТ) або фазовою (ОМ-ФТ) маніпуляцією.

Інформаційні можливості станції Р-378М: з пошуку – 5 радіомереж за годину; із спостереження – 2 радіомережі безперервно, 4 радіомережі періодично; 8 радіомереж в режимі контролю.

Інформаційні можливості станцій Р-378А(Б) та Р325У: з пошуку – 30 радіомереж за годину; із спостереження –10 радіомережі безперервно, 10 радіомережі періодично; 10 радіомереж в режимі контролю; із пеленгування – 120 пеленгів у годину.

Станції завад Р-378А і Р-378Б за своїми ТТХ і побудовою повністю ідентичні і відрізняються тільки тим, що Р-378А розміщується на шасі автомобіля ЗІЛ-131, а Р-378Б на шасі МТ-ЛБУ. Станція завад Р-325У аналогічна Р-378А, і відрізняється тільки передавачем (потужність передавача – 5кВт). Завдяки цьому дальність подавлення поверхневою хвилею збільшилась до 60км.

У склад станцій Р-378А(Б), Р-325У входять автоматичні пеленгуючі пристрої, які дозволяють пеленгувати ДРВ з середньоарифметичною інструментальною помилкою, що не перевищує – 4°.

Станції завад Р-378А(Б) забезпечують подавлення ліній радіозв`язку противника на відстанях:

а) до 30* км – із перевищенням дистанції завад над дистанцією зв`язку до 5 раз при одночасному випромінюванні завад на одній або двох частотах (Р-378М – одноканальна, тому подавляє тільки на одній частоті);

б) до 30* км – із перевищенням дистанції завад над дистанцією зв`язку в 2, 3 рази при одночасному випромінюванні завад на 3 частотах;

в) до 30* км – із перевищенням дистанції завад над дистанцією зв`язку в 1,5 рази при одночасному випромінюванні завад на 4 частотах. Для станцій Р-325У дальність 30* км змінюється на 60 км.

Засоби завад радіозв'язку КХ діапазону оперативної ланки управління противника

Станції завад лініям КХ радіозв'язку Р-325М2 входять у склад озброєння частин РЕБ СВ та ВМС і призначені для створення завад у радіомережах оперативно – тактичної (бригада - корпус) ланки управління противника.

Інформаційні можливості станції Р-325М2: з пошуку – 5 радіомереж за годину; із спостереження – 2 радіомережі безперервно, 4 радіомережі періодично; 8 радіомереж в режимі контролю.

Станції завад Р-325М2 за своєю побудовою та ТТХ подібна до Р-378М і відрізняється тільки потужністю передавача (5 кВт) та антеною системою (доповнена антенами які формують просторові хвилі).

Управління параметрами завад, що створюються станцією Р-325М2, можна здійснювати безпосередньо із апаратної машини або дистанційно з допомогою прийомного пункту Р-385, або дистанційно із машини «У» вузла управління Р-380М.

Час автоматичної перестройки передавача з моменту виявлення подавляємого сигналу приймачем станції складає не більше 10с при обслуговуванні станції двома операторами. Час ручної перестройки – 25с.

Засоби завад радіозв'язку УКХ діапазону тактичної ланки управління противника

Для створення завад у радіомережах УКХ діапазону тактичної (взвод – рота – батальйон) і оперативно – тактичної (бригада – корпус) ланок управління противника застосовуються неавтоматизовані станції завад Р-330П, та автоматизовані Р-330У, Р-330Б. Станції Р-330У можуть управляються від
Р-330ПУ, а Р-330Б - від пункту управління тактичного (ПУ-Т) комплексу РЕП Р-330К.

У склад станцій Р-330У, Р-330Б входять автоматичні пеленгуючі пристрої, які дозволяють пеленгувати джерела радіовипромінювання з середньоарифметичною інструментальною помилкою, що не перевищує – 3°.

Станції завад Р-330П, Р-330У та Р-330Б призначені для розвідки і подавлення наступних видів радіозв'язку:

– радіотелефонного зв’язку з частотною модуляцією; радіотелеграфного зв’язку з однополосною модуляцією;

– радіотелеграфного зв’язку з частотною маніпуляцією.

Інформаційні можливості Р-330П з пошуку – 5 радіомереж за годину; із спостереження – 4 радіомереж.

Інформаційні можливості Р-330У та Р-330Б: з пошуку – 30 радіомереж за годину; із спостереження – 10 радіомереж; з пеленгування – 120 пеленгів за годину.

Станції завад забезпечують подавлення ліній радіозв’язку противника на відстанях до 30 км з перевищенням дистанції завад над дистанцією зв’язку до 7 разів при безперервному випромінюванні завад на одній частоті (Р-330П – одноканальна, тому подавляє тільки на одній частоті), до 5 разів при квазіодночасному випромінюванні завад на двох частотах і до 3,5 разів при випромінювання на трьох (чотирьох) частотах.

Станція завад Р-330Б аналогічна Р-330У але відрізняється більш високою швидкодією та розширеним діапазоном. Середній час реакції станції завад (час від початку роботи лінії радіозв’язку на даній частоті до моменту створення завади на цій частоті) по одиночному випромінюванню складає: по невідомій частоті 0,3 с; по відомій частоті 20 мкс.

Станції Р-330П і Р-330Б можуть подавлять радіозв’язок як при русі (на плаву) так і на стоянці, а Р-330У тільки на стоянці.

Засоби завад лініям супутникового радіозв’язку СПС-1

Для забезпечення безперервного й стійкого управління в стратегічній і оперативно-тактичній ланках евентуального противника на найбільш важливих напрямках командування розвертає систему супутникової зв’язку між основними бойовими з’єднаннями й частинами армійського, корпусного і дивізійного підпорядкування та частинами ракетних військ і артилерії. Ця система містить у собі підсистему наземних станцій і ретранслятори зв’язкових ШСЗ.

Засоби супутникової зв’язку діапазону 225 – 400 МГц в армійських корпусах використаються для зв’язку повітряних КП із іншими ПУ й КП штабів артилерії дивізій, а також для зв’язку літаків розвідки з основними КП корпусів. Типовими засобами в цих лініях зв’язку є автомобільні й літакові станції *AN/TRC-157, AN/MSC-58, AN/WSC-3, AN/ARC-146*. Усередині дивізії використаються для зв’язку КП дивізії з підлеглими бригадами й дивізіонами станції типу *AT/MSC*-58, *AN/WSC-3*.

Загальне число станцій супутникового зв’язку діапазону 225 – 400 МГц які використовуються для організації зв’язку одного армійського корпуса складає порядку 30. Для організації супутникового зв’язку одного армійського корпуса використовуються до 10 каналів.

Загальна кількість станцій супутникової зв’язку діапазону 225 – 400 МГц у першому ешелоні що задіяні при проведенні стратегічної операцій, які є об’єктами РЕП, більше 200. При такій кількості станцій супутникової зв’язку

загальна кількість каналів окремого зв'язкового ИСЗ типу "Флитсатком", які необхідно подавляти, буде становити біля 70.

Для подавлення супутникового зв'язку діапазону 225-400 МГц на озброєні частин (підрозділів) РЕБ Сухопутних військ можуть бути станції завад СПС-1.

Автоматизована станція завад СПС-1 призначена для розвідки і подавлення ліній супутникового зв'язку противника, які працюють в дециметровому діапазоні хвиль через ретранслятори ШСЗ зв'язку с простим переносом частоти.

Приймально-аналізуюча апаратура станції завад дозволяє здійснити пошук, виявлення й аналіз частотно-модульованих, частотно-маніпульованих, фазоманіпульованих сигналів ліній СпЗ, працюючих через ретранслятори ШСЗ типу "Флитсат", "Марисат", СДС і через ретранслятори інших ШСЗ у діапазоні частот 225 – 400 Мгц.

Види випромінює мого завадового сигналу:

– безперервний на одній частоті;

– дискретизований (квазіодночасний) на 2 – 7 частот в відповідності о вибраною програмою.

Станція СПС-1 забезпечує подавлення ліній СпЗ:

– чотири однотипні лінії, які працюють у режимі ТЛГ при швидкості передачі 75-1200 біт/с у межах літера;

– дві однотипні лінії, які працюють у режимі цифрова ТЛФ при швидкості передачі 1600 біт/с у межах літера;

– три однотипні лінії, які працюють у режимі аналогової ТЛФ із енергопотенціалом абонентських станцій зв'язку до 34 дб/Вт у смузі частот до 2 Мгц;

– чотири однотипні лінії, які працюють у режимі аналогової ТЛФ із енергопотенціалом абонентських станцій зв'язку до 30 дб/Вт у смузі частот 2 Мгц;

– одну ТАТС - лінію, яка працює у режимі зі швидкістю 75 біт/с и с енергопотенціалом до 44 дб/Вт при відомій частотно-тимчасовій адресі й до 40 дб/Вт при невідомому частотно-тимчасовій адресі.

Засоби завад лініям літакового УКХ радіозв'язку

У частинах РЕБ Сухопутних військ та Повітряних Сил на озброєні є станції завад лініям літакового УКХ радіозв'язку – Р-934, Р-934У. Основні ТТХ цих станцій надані в додатку 1.2. Об'єктами подавлення для цих станцій завад є:

телефоні лінії радіозв'язку наведення літаків (вертольотів) тактичної і армійської авіації на наземні цілі в ланці " Передовий авіаційний навідник (ПАН) – літак (вертоліт)";

телефоні і телекодові лінії радіозв'язку наведення літаків тактичної авіації на наземні цілі в ланці " пунктів управління (ППУ) - літак".

Наземна станції активних завад Р-934, Р-934У призначені для створення прицільних за частотою завад лініям літакового УКХ радіозв'язку з метою:

– зриву наведення літаків тактичної авіації (ТА), армійської авіації (АА) і вертольотів армійської авіації, а також ПАН при безпосередній авіаційній підтримці сухопутних військ;

– зриву наведення літаків ТА із ППУ при нанесенні ударів по тиловим об'єктах;

– зриву наведення літаків винищувальної авіації на повітряні цілі із наземних і повітряних ПУ при забезпеченні дій своєї авіації;

– зрив передачі розвідувальної інформації із борту літака – розвідника на наземні ПУ противника.

Станції завад Р-934 можуть працювати в автономному або централізованому (управління від ротного ПУ "Банан") режимах, а станції Р-934У можуть управлятися від Р-934У, яка працює у режимі "диспетчерський напівкомплект"

Станції Р-934 можуть розвідувати і подавляти радіотелефоні зв'язки з АМ і ЧМ, а станції Р-934У – наступні види радіозв'язків:

– відкриті радіотелефоні зв'язки з АМ, ЧМ на фіксованих частотах і з ППРЧ;

– закриті лінії радіотелефонного зв'язку і передача даних з амплітудною, частотною, фазовою і відносно-фозовою маніпуляцією з використанням вокодерів;

– багатоканальні радіолінії зв'язку і управління.

Інформаційні можливості Р-934: з пошуку – 5 радіомереж за годину; із спостереження –2 радіомережі безперервно, 4 радіомережі періодично; 10 радіомереж в режимі контролю.

Інформаційні можливості Р-934У: з пошуку – 30 радіомереж за годину; із спостереження –10 радіомережі безперервно, 10 радіомережі періодично; 10 радіомереж в режимі контролю.

Середній час реакції станцій завад складає:

– Р-934 – 13 с – по невідомій частот, 2 с – по відомій частоті;

– Р-934У – 1с – по невідомій частот, 0,07 с – по відомій частоті.

Станції Р-934 і Р-934У можуть подавляти радіозв'язок тільки на стоянці.

Комплекси (вузли, пункти) управління засобами радіозавад

Наявність в частинах і підрозділах РЕБ автоматизованих станцій завад передбачає наявність автоматизованих систем управління завадами. Такими системами є: вузол управління Р-380М (об та оп РЕБ Сухопутних Військ); автоматизований пункт управління Р-330ПУ (ор РЕБ Сухопутних Військ); автоматизований пункт управління "Банан-2" (об РЕБ Сухопутних Військ і Повітряних Сил); автоматизований комплекс Р-330К (ор і об РЕБ Сухопутних Військ).

Основні бойові можливості вузлів управління, автоматизованих пунктів управління, автоматизований комплекс управління завадами приведені в додатку 1.

Автомобільний вузол управління Р-380М є складовою частиною комплексу радіозавад і призначений для централізованого дистанційного

управління групою станцій радіозавад Р-325М при створенні прицільних за частотою завад КХ радіозв'язку оперативно-тактичної ланки управління противника.

До складу вузла входять 12 машин п'яти типів: одна - центральна машина (ПУ) – "Ц"; три машини виявлення і цілевказівки – "О"; три машини управління - "У; три машини дистанційного управління передавачами завад – "Д"-; дві електростанції Э-351А (Э-349М2).

Вузол управління Р-380М забезпечує прийом і аналіз радіопередач, здійснює цілевказівки та контролює прицільність радіозавади за частотою при дистанційному керуванні станціями завад Р-325М2 .

Ротний пункт управління Р-330ПУ призначений для централізованого автоматизованого управління станціями завад Р-330У, дороблених для сумісної роботи з ПУ, а також неавтоматизованого управління станціями завад Р-330П, що входять до складу роти завад УКХ радіозв`язку об РЕБ і забезпечує рішення наступних задач:

– автоматизованого виявлення, пеленгування, визначення координат джерел радіовипромінювання в УКХ діапазоні та автоматичне відображення даних відносно радіоелектронної обстановки в районі дії роти; визначення належності ліній радіозв`язку до об'єктів РЕП шляхом їх слухового, візуального і просторово-часового аналізу та автоматизований цілерозподіл ліній УКХ радіозв'язку – об`єктів РЕП між станціями Р-330У (для Р-330П – ці операції здійснюються вручну);

– автоматизоване формування команд (цілевказівок) на станції завад Р-330У;

– запис і зберігання в запам'ятовуючих пристроях значень: частот на яких заборонено створення завад; частот роботи РЕС, виявлених в процесі аналізу, але які не є об'єктами РЕП; частоти роботи РЕС – об`єктів РЕП, які мають пріоритет; частоти роботи РЕС, які мають пріоритет але не виділені для першочергового подавлення; меж заданого сектору розвідки;

– формування в пам`яті ЕОМ і відображення на табло і планшеті даних по виявленим радіомережам.

Автоматизований пункт управління "Банан-2" ("Степ-О") – призначений для централізованого управління станціями завад літакового УКХ радіозв'язку (Р-934) і забезпечує рішення наступних задач:

– автоматичне виявлення, пеленгування, відображення та визначення належності виявлених радіостанцій;

– підтримка стійкого зв'язку з командиром частини, взаємодіючими підрозділами (частинами) ППО та станціями завад.

– Об'єм запам'ятовуючого пристрою – 40 кодів частоти радіоліній, які потрібно подавляти.

Автоматизований комплекс управління завадами Р-330-К – призначений для радіорозвідки і радіоподавлення засобів КХ і УКХ радіозв'язку в тактичній і оперативно-тактичній ланках управління військами та зброєю противника на основі автоматизації процесів радіорозвідки, цілерозподілу і радіоподавлення.

Автоматизований комплекс РЕП Р-330К представляє собою трьохрівневу систему:

– перший рівень – ПУ-ЗК (пункт управління засобами комплексу) у складі одного Р-330К, який є елементом КП об РЕБ;

– другий рівень – ПУ-Т (пункт управління тактичний) у складі одного або декількох Р-330К для управління одною, або декількома групами автоматизованих станцій завад. ПУ-Т є елементом ПУ роти РЕБ;

– третій рівень – станції завад у складі Р-330Б, Р-378А(Б), Р-325У.

Комплекс РЕП Р-330К може працювати в одному із трьох режимах:

1. Режим ПУ-ЗК (ПУ У2М) – режим 2 – виконання функцій управління одним або декількома ПУ-Т за допомогою телекодового зв'язку з ПУ У2М.

2. Режим ПУ-Т (ПУ У1М) –режим 1 – виконання функцій управління автоматизованими станціями завад і засобами пеленгації за допомогою телекодового зв'язку з ПУ У1М.

3. Режим ПУ-Т (ПУ У1М-ВГ) – режим 3 - виконання функцій управління автоматизованими станціями завад і засобами пеленгації без телекодового зв'язку з ПУ У2М (децентралізований режим-без ПУ-ЗК).

Як правило, у складі комплексу РЕП один Р-330К працює в режимі ПУ У2М, інші в режимі ПУ У1М.

Р-330К який працює в режимі ПУ-ЗК відрізняється за своїм складом від Р-330К – ПУ-Т тільки наявністю радіостанції Р-171 з блоком 101-12-00. Алгоритмічно будь який ПУ може виконувати функції У2М або У1М.

Пункт управління ПУ-ЗК призначений для управління роботою до 5 ПУ-Т, здійснення обміну інформацією з пунктами управління вищих ланок управління і забезпечує:

– обмін інформацією з ПУ вищих ланок;

– автоматизоване введення в обчислювальний комплекс інформації, яка приходить від ПУ-Т;

– формування і видача вихідної інформації на ПУ-Т у вигляді кодограм;

– накопичення і обробка інформації, що надходить від ПУ-Т;

– автоматизований цілерозподіл і видача цілевказівка між ПУ-Т;

– документування інформації.

Комплекс може виявити місцеположення до 120 радіостанцій УКХ діапазону при максимальному часі обробки пеленгів 30с і до 90 радіостанцій КХ діапазону при 40с. Час обробки задається при введенні вихідних даних в ЕОМ.

Пункт управління ПУ-Т призначений для управління 2...18 автоматизованими станціями завад КХ або УКХ радіозв'язку противника і забезпечує:

– автоматизований збір, накопичення і обробку інформації про РЕО в зоні відповідальності комплексу, які приходять від станцій завад, пеленгаторів і вищестоящих КП (ПУ);

– визначення належності ліній радіозв'язку противника;

– автоматизоване відображення даних РЕО в зоні відповідальності комплексу;

– автоматизований цілерозподіл виявлених ліній радіозв'язку (об'єктів подавлення) між станціями завад з наступним формування команд цілевказівок на станції завад;

– автоматичний контроль стану ліній радіозв'язку, що подавляються.

Автоматизований комплекс завад радіозв'язку "МАНДАТ-М" (за матеріалами рекламних проспектів *Виробника* та *UKRSPETSEXPORT*)

У найближчий час на озброєння частин РЕБ Збройних Сил України можуть поступити автоматизовані комплекси завад радіозв'язку "Мандат-М" або його окремі складові.

Автоматизований комплекс завад радіозв'язку "Мандат-М" призначений для подавлення наземних і повітряних засобів зв'язку шляхом постановки прицільних по частоті й напрямку завад, а також загороджувальних за частотою у КХ і УКХ діапазонах по джерелам радіовипромінювання, що працюють як на фіксованих так і на частотах які змінюються стрибкоподібно.

Комплекс завад є сучасним ефективним засобом, що дозволяє вирішувати завдання як радіорозвідки, так і радіоелектронного подавлення.

Комплекс завад радіозв'язку являє собою автоматизовану систему збору, обробки інформації щодо джерел радіовипромінювань в зоні обслуговування та випромінюваннь прицільних або загороджувальних завадових сигналів. Інформаційний обмін у комплексі здійснюється по телекодових каналах зв'язку з використанням формалізованих повідомлень, а також обміном мовної інформації між операторами пункту управління й автоматизованих станцій завад по службових радіоканалах.

Методи аналізу й обробки сигналу, закладені в комплексі "Мандат-М", дозволяють працювати не тільки із сучасними але й перспективними видами сигналів.

Комплекс завад "Мандат-М" пропонує модульний принцип побудови, що забезпечує його зручність в експлуатації.

До складу комплексу входять:

– пункт управління комплексом Р-330ПМ;

– станція радіорозвідки Р-330УК;

– автоматизовані станції розвідки й подавлення(АСРП):

– КХ діапазон (1,5 - 30 МГц) – три і більше станцій Р-330КМ2;

– УКХ діапазон (30 - 180 МГц) – три і більше станцій Р-330УМ2-1;

– УКХ діапазоні (400 - 1000 МГц) – три і більше станцій Р-330УМ2-2.

Кількість станцій завад в одному комплексі визначає Замовник, виходячи з конкретних бойових завдань, зони придушення, кількості одночасно працюючих каналів імовірного противника, структури підрозділів радіоелектронної боротьби Сухопутних військ, ВМС або Повітряних Сил.

Комплекс забезпечує виявлення, пеленгування, визначення координат джерел випромінювання та подавлення у діапазоні 1,5 - 1000 МГц.

Комплекс забезпечує в реальному масштабі часу:

– автоматичний пошук і виявлення ліній радіозв'язку;

– автоматичне пеленгування працюючих радіоелектронних засобів (РЕЗ);

– оцінку й відображення радіоелектронної обстановки;

– роботу з електронною картою місцевості;

– визначення належності виявлених ліній радіозв'язку до об'єктів радіоелектронного подавлення (РЕП) шляхом слухового та візуального аналізу сигналів та пеленгів на РЕЗ;

– призначення пріоритетів подавлення;

– цілерозподіл та видача цілевказівок на засоби подавлення;

– подавлення джерел радіовипромінювань;

– автоматичний контроль роботи ліній радіозв'язку, що подавляються;

– автоматичне перенацілювання передавача завад на частоти РЕЗ, виділених для подавлення;

– забезпечує накопичення, документування, зберігання добутої інформації й передачу по каналах телекодової зв'язку формалізованих повідомлень на АСУ та на командний пункт вищої ланки управління.

Станції завад, що входять у комплекс забезпечують постановку прицільних по частоті й часу або загороджувальних по раніше розвіданих частотах завад наземним засобам зв'язку, що унеможливлює прийняття інформації з відомими на теперішній час видами модуляції несучої радіочастоти.

Усі станції завад комплексу "Мандат-М" мають ідентичну побудову, аналогічне призначення і ТТД за окремими винятками. Тому відносно детально будуть розглянуті пункт управління Р-330ПМ, станція розвідки та одна із автоматизованих станцій розвідки і подавлення Р-330КМ2. Відносно інших станцій завад будуть відмічені тільки відмінності відносно Р-330КМ2.

На усіх засобах комплексу "Мандат-М" є системи прив'язки GPS NAVSTAR, GLONASS.

Пункт управління комплексом РЭБ Р-330ПМ призначений для аналізу й обробки отриманої від автоматизованих станції радіорозвідки та станцій розвідки і подавлення інформації, ефективного розподілу загального ресурсу станцій завад по подавляємим радіолініям, автоматизованого розрахунку поточної ефективності роботи комплексу, синхронізації режимів роботи станцій завад, забезпечення зв'язку з командним пунктом вищої ланки управління.

Пункт управління комплексом РЭБ Р-330ПМ забезпечує:

– видачу вихідних даних станціям завад;

– збір і накопичення в базі даних ПУ інформації про джерела радіовипромінювань;

– оцінку й відображення радіоелектронної обстановки на електронній карті;

– рішення завдань оптимізації розподілу частот для подавлення;

– інформаційний обмін зі станціями завад комплексу та пунктом управління вищих ланок управління;

– призначення пріоритетів подавлення;

– автоматичне виявлення радіомереж і вузлів зв’язку;

– дальність зв’язку з використанням радіорелейних станцій діапазону 320…645 МГц – до 60 км.

Пункт управління Р-330ПМ розташований на одному автомобілі високої прохідності типу КРАЗ з агрегатом живлення на двохвісному причепі.

Автоматизована станція радіорозвідки Р-330УК входить в автоматизований комплекс завад радіозв’язку “Мандат-М” і призначений для пошуку, виявлення, аналізу сучасних засобів радіозв’язку в діапазоні частот 1,5…2000 МГц із метою одержання відомостей про радіоелектронну обстановку контрольованого району.

Автоматизована станція радіорозвідки Р-330УК розташована на одному автомобілі високої прохідності типу КРАЗ з агрегатом живлення на двохвісному причепі.

Автоматизована станція розвідки й подавлення КХ діапазону Р-330КМ2 входить в автоматизований комплекс завад радіозв’язку «Мандат-М» і призначений для пошуку, виявлення, аналізу сучасних засобів радіозв’язку в діапазоні частот 1,5…30 МГц із метою одержання відомостей про радіоелектронну обстановку контрольованого району й здійснення радіоелектронного подавлення джерел радіовипромінювань, як безперервного, так і короткочасної дії, у тому числі систем, що використовують стрибкоподібну зміну частоти.

АСРП Р-330КМ2 забезпечує:

– цифрову реєстрацію сигналів;

– автоматичну класифікацію й вимір параметрів сигналів;

– слуховий і візуальний контроль;

– кількість видів завад - 9, у тому числі завада, яка формується з копії розвідуємого сигналу;

– потужність передавача завад не менш 1 кВт.

Кожна АСРП може функціонувати:

а) в автономному режимі;

б) у складі “сполученої пари”;

в) у складі комплексу.

АСРП Р-330КМ2 розташована на автомобілі високої прохідності, (машина розвідки й машина придушення) типу КРАЗ з агрегатом живлення на двохвісному причепі.

Комплекс, що складається із трьох АСРП Р-330КМ2, забезпечує розвідку й подавлення в зоні до 120 км по фронті й до 60 км у глибину.

Автоматизована станція розвідки й подавлення УКХ діапазону Р-330УМ2-1 має аналогічне призначення АСРП Р-330КМ2 але має наступні відмінності:

– станція працює у діапазоні частот 30…180 МГц;

– потужність передавача завад не менш 2,5 кВт.

Станція Р-330УМ2-1 розміщається в одному бронетранспортері типу “Вепр” на колісному ходу з агрегатом живлення на двохвісному причепі.

Автоматизована станція розвідки й подавлення УКХ діапазону Р-330УМ2-2 має аналогічне призначення АСРП Р-330КМ2 але має наступні відмінності:

– станція працює у діапазоні частот 180…1000 МГц;
– потужність передавача завад не менш 2,5 кВт.

АСРП Р-330УМ2-2 розташована на одному бронетранспортері типу “Вепр” на колісному ходу з агрегатом живлення на двохвісному причепі.

2.7.2.1.3. Комплект передавачів завад, що заносяться до наступних:

Комплект передавачів завад РП-377А – призначений для радіоподавлення засобів радіозв’язку оперативно-тактичної та тактичної ланки управління. Передавачі завад доставляються на територію противника розвідниками або розвідно-диверсійними групами. Для подавлення вузлів, окремих радіостанцій КХ, УКХ радіозв’язку застосовуються передавачі завад від першої до четвертої літери (20…120МГц). Для подавлення радіорелейного радіозв’язку застосовуються передавачі завад п’ятої і шостої літери (120…400МГц).

Передавачі завад формують загороджувальну за частотою, шумову заваду.

Один пульт управління НА-1 може дистанційно управляти шістьма передавачами завад НА-2. Пульт управління може дистанційно (до 15 км) включати в роботу по одному передавачу завад, або одночасно всі.

Діапазон робочих частот розбитий на 6 піддіапазонів (літерів): I літер – 20-30 МГц; II літер – 30-50 МГц; III літер – 50-80 МГц; IV літер – 80-120 МГц; V літер – 120-225 МГц; VI літер – 225-400 МГц.

Блоки електроживлення Н-4 – сім штук (по 20 батарей типу “елемент А343” у кожному, або акумулятори типу “10НКП-8” - по одному у кожному).

Вага комплекту живлення (для одного передавача завад) до 3кг. Вага передавача завад до 2кг. Вага комплекту передавачів завад – 27 кг.

Один розвідник може одночасно переносити три передавачі завад у спеціальному рюкзаку.

Комплект передавачів завад РП-377АМ є результатом модернізації комплекту РП-377А. Модернізація здійсненна в двох напрямках: розширення частотного діапазону з 20...400МГц до 20...500МГц; заміна блоків електроживлення Н-4 на Н-4М.

Технічні характеристики комплекту РП-377АМ ідентичні РП-377А і приведені в додатку 1.

Розширення частотного діапазону на 100МГц відбулося за рахунок до комплектації РП-377А передавачем завад літери 7 (частотний діапазон 400...500МГц).

Всі блоки електроживлення Н-4 замінені на блоки Н-4М (збільшені ємність блоків, та термін служби).

Комплект передавачів завад РП-377АМ можна застосовувати так як і РП-377А, але його можна використовувати також для подавлення систем дистанційного управління і зв’язку побутового призначення, які можуть,

виходячи з досвіду миротворчих операцій в Іраку, застосовуватися для радіоуправління вибуховими пристроями (фугасами).

У найближчий час на озброєння частин РЕБ Збройних Сил України можуть поступити комплект передавачів завад "Бакай" (за матеріалами рекламних проспектів виробника).

2.7.2.1.4. Засоби завад радіопідривачам

Наземні рухомі станції завад СПР-2 (станції входять у склад частин (підрозділів) РЕБ Сухопутних Військ) призначені для захисту живої сили і бойової техніки від ураження артилерійськими снарядами і мінами шляхом створення активних завад радіопідривачам (РП) цих боєприпасів з ціллю їх передчасного підриву на безпечній висоті або блокування (переведення на ударну дію).

Тактико-технічні дані СПР-2 приведені в додатку 1.

Об'єктами радіоелектронного подавлення для станції СПР-2 являються одночастотні автодинні РП, змонтовані у корпусі артилерійських снарядів і мін, з безперервним випромінюванням зондуючого сигналу, у тому числі і з спеціальними каналами захисту від завад.

Площа прикриття станції при веденні противником швидкого вогню боєприпасами з автодинними РП складає:

– не менше 50…60 га – при застосуванні тільки артилерійських снарядів з РП;

– не менше 25 га – при застосуванні тільки мін з РП;

– не менше 25 га – при сумісному застосуванні артилерійських снарядів і мін з РП.

Імовірність підриву (спрацювання) РП на висоті $H \geq 100$ м – не менше 0,8; при щільності потоку снарядів, що створюється при залповій стрільбі боєприпасами з РП шістьма батареями шестиорудійного (мінометного) складу, імовірність підриву (блокування) РП знижується на 20%.

2.7.2.2 Засоби та комплекси РЕБ Повітряних Сил

Задачі РЕБ у Повітряних Силах (ПС) вирішуються за допомогою як засобів та комплексів наземного базування (частини РЕБ ПС), так і засобів та комплексів РЕБ повітряного базування (вертолітні ланки РЕБ та літакові засоби і комплекси РЕБ).

За своїми завданнями, призначенням, побудовою ТТХ засоби та комплекси ПС суттєво відрізняються тому, розглянемо окремо засоби і комплекси РЕБ наземного та повітряного базування.

2.7.2.2.1. Засоби та комплекси РЕБ Повітряних Сил наземного базування

На озброєні частин РЕБ Повітряних Сил знаходяться засоби, комплекси радіоелектронного подавлення.

До складу засобів і комплексів РЕБ входять наступні основні підсистеми:

– радіоелектронної розвідки (окремі станції РТР, РЛС та апаратура безпосередньої розвідки станцій);

– управління (автоматизовані (неавтоматизовані) пункти управління, комплекси, командні пункти та підсистеми управління станцій завад);

– подавлення (станції завад, окремі передавачі завад, пристрої викидання (вистрілювання) витрачаємих засобів РЕБ та ракети класу "повітря – РЛС").

Засоби радіотехнічної розвідки

Наземні, рухомі, автоматизована станція РТР "Кольчуга" та неавтоматизована станція РТР ПОСТ-3М знаходяться на озброєні окремих батальйонів РЕБ Повітряних Сил (одна із них) і призначені для добування розвідувальної інформації про наземні (корабельні) і повітряні РЕС противника, що працюють в імпульсному і безперервному режимі з використанням дальнього тропосферного розповсюдження радіохвиль. Основні ТТХ засобів РЕР надані в додатку 1.

У станціях РТР реалізовані безпошуковий по частоті і пошуковий по напрямку методи виявлення, автоматизоване визначення частотно-часових параметрів сигналів та пеленгів РЕС. Крім того станція РТР "Кольчуга" проводить автоматичне визначення типів і екземплярів джерел радіовипромінювання та реєстрацію результатів обробки (є можливість збереження інформації щодо 50 типів і 300 екземплярів джерел радіовипромінювання) і передачу інформації на КП. Середній час розвідки одного ДРВ складає не більш 3 хвилин.

Розвідку наземних об'єктів станція "Кольчуга" веде в режимі "Земля", а повітряних об'єктів у режиму "Повітря". Діапазон частот станції, що розвідуються, складає: по наземним об'єктах від 915 до 11000 МГц, по повітряним об'єктах від 915 до 4000 МГц, від 8000 до 11000 МГц від 15000 до 18000 МГц.

Засоби радіолокаційної розвідки

На відміну від станцій завад засобам радіозв'язку, станції завад бортовим РЕС мають вузькоспрямовані антени. Тому для зменшення часу наведення антен на об'єкт подавлення на озброєні частин РЕБ Повітряних Сил є станція радіолокаційної розвідки П-18. Наземна, рухома РЛС П-18 сумісно з НРЗ-4П призначена для добування даних про координати (азимут і дальність) повітряних об'єктів та їх розпізнаванням за належністю ("свій" – "чужий"). Тактико-технічні характеристики РЛС П-18. Станція радіолокаційної розвідки П-18 може видавати інформацію в напівавтоматичному режимі на АКУП-22.

Засоби та комплекси подавлення Повітряних Сил наземного базування

Для постановки завад бортовим засобам радіолокації противника з метою порушення їх бойового застосування використовуються станції маскуючих (СПН-30, СПН-2,-3,-4), імітуючих (СПН-40, СПО-8М).

Основні ТТХ станцій СПН-30, СПН-2, СПН-3, СПН-4, СПН-40 та СПО-8М приведені в додатку 1.

Об'єктами радіоелектронного подавлення станцій є:

– бортові РЛС огляду земної поверхні;

– бортові РЛС управління зброєю класу "повітря – земля" та "повітря – повітря";

– бортові РЛС забезпечення польотів на малих висотах (ЗПМВ);

– розвідувальні бортові РЛС бокового огляду;

– інші РЕС, які працюють у діапазоні роботи станцій завад. Можливості.

Станції маскуючих завад

Наземні рухомі станції завад СПН-30, СПН-2, СПН-3, СПН-4 призначені для створення прицільних, або загороджувальних за частотою квазібезперервних прямошумових маскуючих завад у відповідь одиночним або груповим бортовим РЕС які працюють, як з поімпульсною перестройкою, так і на фіксованих частотах з метою виключення або суттєвого утруднення їх бойового використання (виявлення і прицільного ураження наземно-повітряних цілей).

Станція СПН-30 – одноканальна за напрямком і повинна назначатися для подавлення однієї БРЛС. Разом з тим частотно-енергетичні можливості станції дозволяють одночасно подавлять до 5 БРЛС, які працюють на фіксованих частотах, при умові знаходження їх у головному пелюстку ДН антени. При наявності перестройки частоти від імпульсу до імпульсу станція може подавляти тільки одну БРЛС.

Станції СПН-2, СПН-3, СПН-4, на відміну від СПН-30, можуть подавляти одночасно дві одиночні або одиночну і групу БРЛС, або дві групи БРЛС, без перестройки несучої частоти, що знаходяться під різними напрямками. Максимальна кількість одночасно подавляємих цими станціями БРЛС бокового огляду і БРЛС забезпечення польотів на малих висотах - дві. Причому вони можуть знаходитись, як на одному так і на двох напрямках. Максимальна кількість подавляємих РЛС управління зброєю - шість, до трьох БРЛС на кожному напрямку. Такі можливості СПН-2,-3,-4 можна пояснити наявністю спеціалізованої ЕОМ та фазованної решітки.

Середня ширина спектру завади станцій СПН-30 складає 30 МГц, а середня точність визначення частоти сигналу ±15 МГц.

Середня ширина спектру завади станцій СПН-2,-3,-4 складає 3…5 МГц, а середня точність визначення частоти сигналу ±1,5 МГц.

Станції можуть працювати, як автономно так і в режимі централізованого управління за даними цілевказівок від автоматизованих пунктів управління (СПН-30 від АКУП-22, а СПН-2,-3,-4 від АКУП-1).

Станції імітуючих завад

Завади, що імітують повинні вносити оманну інформацію в корисні сигнали БРЛС (РЛС). Тому такі завади можуть також називатися дезінформуючими. Характеристики активних імітуючих завад повинні достатньо повно відповідати всім або деяким характеристикам корисних сигналів і нести оманну інформацію відносно кількості цілей, їх координат та інше. Такі завади формують для БРЛС станції СПО-8М, СПН-40.

Рухомі автоматичні станції завад СПН-40 та СПО-8М призначені для створення імітуючих радіозавад у відповідь літаковим БРЛС, у 2-х і відповідно 3-х сантиметрових діапазонах довжин хвиль.

Станції можуть формувати наступні види завад - багатократні імпульсні завади – БІП-1 або БІП-2. В режимі БІП-1 станція формує пачку високочастотних імпульсів з частотою яка дорівнює частоті прийнятого сигналу від БРЛС. Тривалість пачки може бути 200, 400 або 800мкс (глибина прикриття 30, 60 або 120км відповідно), а в режимі БІП-2 – 200 або 400мкс (глибина прикриття 30 або 60км). В режимі БІП-2 забезпечується створення таких же імпульсів, як і при БІП-1, але щільність імпульсів в два рази більша (замість 8 імпульсів створюється 16 імпульсів). Станція може імітувати три розміри об’єктів: 0,7 … 1,2 км, 1 … 1,5 км, 1 … 2 км.

В обох режимах при опроміненні станції головною пелюсткою ДН антени БРЛС, що подавляється, у вказані групи імпульсів уводяться додатково 2...3 радіоімпульси у відповідь, які, на відміну від основних імпульсів, не змінюють своє положення і тривалість (формування нерухомих об’єктів потрібно для уведення в оману системи захисту з накопиченням).

Станції СПН-40 та СПО-8М мають режим БІП+ШП. Але в СПО-8М режим БІП+ШП використовується тільки в навчальних цілях, а в СПН-40 це бойовий режим. У цьому режимі сигнали завади являють собою суму шумових коливань і групи радіоімпульсів, що дозволяє збільшити ефект маскування. Тривалості шумових коливань і групи радіоімпульсів рівні між собою.

Завади, що запізнюються, у відповідь, формуються відразу після приходу зондуючого сигналу БРЛС.

Випромінення випереджуючих завад проходить з затримкою, визначеною періодом слідування зондуючих сигналів БРЛС. При цьому величина затримки змінюється в залежності від періоду слідування зондуючих сигналів таким чином, щоб час випередження був постійним і рівним 230, 460, 930мкс.

При сумісному виді формування завад проводиться одночасно, як з затримкою відносно прийнятих зондуючих сигналів, так і без них. Тривалість таких завад по зрівнянню із звичайним видом завад збільшується у два рази і складає 400, 800 або 1600мкс.

Середня ширина спектру завади в обох станціях складає 3 … 5 МГц, а середня точність визначення частоти сигналу ±1,5 МГц.

Комплекси управління засобами радіозавад

Наявність в частинах і підрозділах РЕБ автоматизованих станцій завад передбачає наявність автоматизованих систем управління завадами. Такими системами є: автоматизований комплекс управління завадами АКУП-22 (об РЕБ Повітряних Сил); автоматизований комплекс управління завадами АКУП-1 (об РЕБ Повітряних Сил).

Основні бойові можливості вузлів управління, автоматизованих пунктів управління, автоматизований комплекс управління завадами приведені в додатку.

Автоматизований комплекс управління завадами АКУП-22 призначений для автоматизованого управління угрупованням наземних засобів радіозавад бортовим РЕЗ (цілям) противника і може бути елементом пункту управління роти або командного пункту батальйону РЕБ повітряних сил який забезпечує управління бойовою роботою станцій завад: СПО-8м, СПН-30,
СПН-40.

Основними задачами, які вирішуються комплексом є:

– прийом і перетворення даних зовнішніх цілевказівок (АСУ ППО, П-18), відносно повітряної обстановки;

– вирішень задачі цілерозподілу засобів завади з урахуванням способу прикриття об’єктів, характеристик засобів завад і бортових РЛС;

– видачу команд управління на засоби завад, контроль за їх бойовою готовністю і бойовими діями;

– відображення повітряної та радіотехнічної обстановки і прийнятих по ним рішень;

– передача донесень щодо бойової готовності і бойових дій засобів завад на КП (АСУ).

Автоматизований комплекс управління завадами АКУП-1 призначений для управління бойовою роботою змішаного угрупування наземних засобів подавлення, яке може включати в себе як станції завад третього покоління (СПН-2,-3,-4) так і станції другого покоління (СПН-30, СПН-40, СПО-8М).

Автоматизований комплекс АКУП-1 являє собою трьохрівневу систему:

– перший рівень – АКПБ – автоматизований командний пункт батальйону в складі одного АКУП-1;

– другий рівень – АПУР – автоматизований пункт управління роти. До складу АКПБ може входити від одного до трьох АПУР або один, два АПУР і один АКУП-22;

– третій рівень – від однієї до трьох рот, які мають на озброєні до 27 автоматизованих станцій завад СПН-2,-3,-4 у будь якому співвідношенні і до 18 станцій завад СПН-30, СПН- 40, СПО-8М (12 станцій СПБ-7).

Комплекс забезпечує також неавтоматизоване управління АСУ “Банан-2” (“Степ-О”).

Основними задачами АКПБ є:

– автоматизований прийом, перетворення, і відображення даних від зовнішніх джерел інформації, а також інформації про бойову готовність (БГ) і хід бойових дій угрупування станцій завад (СП), які одержують від АПУР;

– автоматизований розподіл 50 цілей які повинні бути подавлені поміж трьома АПУР, або двома АПУР і одним АКУП-22 з наступним формуванням і автоматичною передачею інформації цілевказівок і управління на АПУР та АКУП-22;

– неавтоматизований розподіл секторів подавлення поміж трьома ротами та передачею команд на ПУ “Банан-2” наступним отриманням інформації зворотного контролю про бойову готовність, хід бойових дій угрупування станцій завад УКХ радіозв’язку і навігації;

– обмін командно оперативною інформацією з АПУР, АКУП-22, ПУ “Банан-2” по телефонним каналам зв’язку.

Основними задачами АПУР є:

– автоматизований прийом, перетворення, і відображення даних від зовнішніх джерел інформації, а також інформації про бойову готовність і хід бойових дій, які одержують від угрупування станцій завад ;

– автоматизований розподіл 20 цілей, які повинні бути подавлені, поміж дев’яти станцій завад;

– неавтоматизований розподіл секторів подавлення поміж станцій завад;

– формування і автоматичну передачу інформації цілевказівок і управління на станції завад, а також інформації щодо БГ і хід бойових дій роти станцій завад на АКПБ;

– обмін командно-оперативною інформацією (команди управління, розпорядження, донесення) з АПКБ і станціями завад.

Станція завад радіонавігаційним системам ближнього радіусу дії Р-388

Наземна рухома автоматизована станція завад Р-388 призначена для подавлення бортової апаратури системи ближньої радіонавігації “ТАКАН”. Станція створює прицільні за частотою активні завади імітуючого типу для каналів азимуту, дальності та передачі даних літакових навігаційних систем.

Дальність виявлення сигналів літакових бортових запитувачів – 300 км і залежить від висоти польоту літаків. Початок подавлення роботи літакових запитувачів станцією по дальномірному каналу проводиться при находженні літака на середині відстані між станцією завад і маяком на землі. По каналу азимуту та лінії передачі даних ця відстань збільшується приблизно на 25% у сторону противника (визначається енергетичним співвідношенням сигналу та завади).

Апаратура станції забезпечує автоматичний пошук сигналів літакових запитувачів у всьому діапазоні їх роботи і виводить передавач на подавлення не більш як через 30 секунд після початку роботи запитувача.

Кількість каналів формування завад (передавачів) – 2.

2.7.2.3. Засоби завад морського базування

Об'єктами радіоподавлення для корабельних засобів РЕП є радіолокаційні (РЛ) станції виявлення, розпізнавання та наведення, а також РЛ системи управління (самонаведення) зброї. Носіями об'єктів радіоподавлення можуть бути кораблі, літаки, підводні човни та засоби берегової оборони противника.

На кораблях ВМС ЗСУ на озброєні є як активні так і пасивні засоби завад.

До активних корабельних засобів відносяться (ті що є на озброєні) наступні станції завад: МП-401 (3см); МП-401С (3…3,5см); МП-405-1 (2см).

До пасивних корабельних засобів відносяться наступні:

– скидуємі надувні кутові відбивачі: А-1,0; А-1,3; А-1,6;

– відстрілюємі:82 мм для ПК-16 снаряди ТПС-60У ДС2,3,5,7,10; 100мм снаряди ПП/СМ-5; Б-34 (3…4см, 10см.), та 140 мм снаряди ТСП-41, ТСП-47 ДС2,3,5,7,10;

– радіолокаційні пастки СР-50, СО-50, СОБ-50.

На озброєні кораблів ВМС:

– клас фрегат – можуть бути наступні засоби РЕБ: станції активних завад МП-401 (401С), установки постанови пасивних завад ПК-10, ПК-16,

– клас корвет – можуть бути наступні засоби РЕБ: станції активних завад МП-405, установки постанови пасивних завад ПК-16, та у районі головного командного пункту корабля (ходової рубки) розміщується два лазерних приймачів випромінювань "Спектр-Ф", призначених для попереджувати щодо лазерного опромінення корабля противником (лазерним дальноміром або лазерними приборами цілевказівки/наведеня.

– клас десантні кораблі – можуть бути наступні засоби РЕБ: проект 773 – установки постанови пасивних завад ВМ-18.

2.7.2.3.1. Корабельні засоби та комплекси активних завад

Комплекси прицільно-загороджувальних завад МП-401 призначені для подавлення РЛС виявлення та управління зброєю, а також РЛ ГСН протикорабельних ракет (ПКР). Комплекс складається із підсистем: радіотехнічної розвідки; апаратура видачі цілевказування на засоби виявлення; збору, обробки та цілерозподілу; подавлення активними (МП-401) та пасивними завадами (ПК-10 або ПК-16); забезпечення корабельної електромагнітної сумісності (ЕМС) та автоматичного супроводження цілі.

Підсистема РТР працює в діапазоні 5,25…17,54 ГГц (5; 4; 3: 2 см) у круговому режимі огляду. Приймачі підсистеми мають достатньо високу

чутливість (-65…70 дБ/Вт), що дозволяє забезпечити великі дальності виявлення, але суттєво погіршує роботу комплексу при одночасній роботі з РЛС угрупування кораблів.

Підсистема подавлення формує у секторі 15˚х20˚ побортно (2 антенних поста у секторах 0-90-180˚, 0-270-180˚ відповідно курсу корабля) маскуючі прицільні (режим А) або загороджувальні (режим Б) за частотою завади в діапазоні 8,33…10,77 ГГц.

Мінімальна потужність передавача завад до 1000 Вт. Ширина спектру прицільної завади не менше 4 МГц при амплітудній і 10…15 МГц при фазовій модуляціях. У режимі прямошумової загороджувальної завади весь діапазон поділений на три нерівних частини. Найменша - шириною 500 МГц, найбільша – 1800 МГц. Вибір ширини спектру загороджувальної завади здійснює оператор за даними апаратури РТР, яка визначає частоти сигналів з точністю до ±3 МГц. Розвідка (дорозвідка) сигналів РЕС відбувається в паузи тривалістю 1; 2; 3 мс. При подавлені РЛС, які працюють на фіксованих частотах паузи можна скоротити до 20…200 мкс. Тривалість випромінювання завади можна встановлювати рівними 10, 20 або 40 мс.

Пропускна можливість комплексу з подавлення: режим А – чотири РЛС, які працюють у режимі огляду і одна РЛС – у режимі прицілювання; режим Б – пропускна можливість обмежується находженням сигналу цілі в межах частотного діапазону одної із трьох можливих частин загороджувальної завади і в межах відповідної ДН.

Підсистема подавлення має дві незалежних антенних системи, що дозволяє одночасно подавляти цілі на двох напрямках. Ширина ДН прийомних і передаючих антени складають: у горизонтальній площині - 15˚, у вертикальній площині – 30˚. Коефіцієнт підсилення антени дорівнює 50. Поворотом антен можна управляти, як у ручному режимі так і в режимі автосупроводження.

Підсистема ЕМС призначена для забезпечення беззавадової роботи підсистеми подавлення корабля сумісно з РЛС кораблів тактичного угрупування. Для цього використовується часова селекція.

Комплекс МП401 забезпечує управління чотирма пусковими пристроями комплексу ПК-16 (їх бойові можливості будуть розглянуті дальше). Вибір способу стрільби визначається за даними підсистеми РТР або РЛС.

Комплекс МП-401С є аналогом комплексу МП-401 і відрізняється тільки поліпшенням надійності та можливістю управління пусковим комплексом ПК-16. Чутливість прийомних пристроїв – 70 дБ. Середня потужність передавача завад 650 Вт. Станція може створювати завади у двох напрямках одночасно, ширина ДН антени в горизонтальній і вертикальній площині - 15˚х20˚, що забезпечує коефіцієнт підсилення антени – 110. На носових та кормових курсових кутах сектор завади може бути 30˚(сумарний).

На озброєні кораблів типу корвет є **комплекси радіозавад МП-405**. Вони призначені для автоматичного виявлення і подавлення випромінювань РЛС кораблів (літаків) противника та активних РЛ ГСН ПКР.

У склад комплексу МП-405 входять:

– підсистема РТР, яка дозволяє вести розвідку в діапазоні частот 4…17,54 ГГц.;

– підсистема збору, обробки та цілерозподілу;

– підсистема подавлення активним завадами (станція завад МП-405) – підсистема подавлення активним завадами працює в діапазонах частоти 4…8 ГГц, 8… 10 ГГц або 12…18 ГГц у залежності від комплектації (станція комплектується за модульним принципом);

– підсистема пасивних завад – комплекс пускових установок (ПК-16).

– Випромінювання РЛС противника виявляється із усіх напрямків у режимі "вузькі ДН" з середньоквадратичною помилкою 2,5˚, а в режимі "широкі ДН" - 15˚. Потужність передавача завад 500Вт, Др.-150 км, Дп-130 км.

Комплекс може подавлять маскуючою шумовою завадою одну ціль без перестройки несучої частоти і хаотично-імпульсною завадою одну ціль з перестройкою несучої частоти. Для угрупування кораблів, на озброєні яких є комплекси МП-405, передбачений режим роботи "мерехтіння".

2.7.2.3.2. Корабельні засоби пасивних завад.

На озброєнні надводних кораблях ВМС, є комплекси (установки), або артилерійські системи для стрільби снарядами пасивних завад. Вони є складовою частиною єдиного корабельного комплексу РЕБ. За допомогою цих комплексів формуються хибні (удавані) цілі (ХЦ), які вистрелюються для дезінформації противника та захисту кораблів від керованої зброї.

Корабельні пускові установки та засоби пасивних завад

Установки пасивних завад – ПК-10 можуть входить до складу комплексу МП401С. Вони призначені для постановки оманних увідних цілей. Забезпечує відведення ПРК від охороняємого корабля на етапі, коли головка самонаведення ПРК захопила та супроводжує корабель. Комплектується 4, 8 чи 12 пусковими установками (ПУ) в залежності від водотоннажності корабля (СКР-8, МПК-4). Кількість пускових труб в одній ПУ – 10. Використовуються снаряди калібру 120 мм які забезпечують викидання бойової частини зі швидкістю 100 м/с (АЗ-СР-50 – постановка оманних увідних радіолокаційних цілей проти ПКР типу "Екзосет", "Гарпун"; ОЕ / ІЧ пастки АЗ-СО-50).

Дальність постановки завади до 300 м від корабля.

Для комплексу ПК-10 призначені наступні види 120 мм снарядів завад:

– АЗ-СОМ-50 – постановка оманних увідних цілей проти ПКР з тепловою головкою самонаведення типу "Пінгвін";

– АЗ-СОБ-50 – прикриття кораблів від ПКР з оптико-електронною системою самонаведення типу "Уоллай" (в ВМС обмежена кількість).

Снаряди АС-СО-50 мають комбіноване спорядження, яке може імітувати нерухому оманну ціль з просторово-роподіленою структурою поля яскравості та температури. Для цього снаряд споряджають пластинчатими стікловолокновими елементами з нанесеним аерозольними та

тепловипромінюючими складовими (составом) та стіклянними кульками, що дозволяє створювати завади будь-яким ОЕС наведення та самонаведення зброї. Ці снаряди забезпечують оптичний контраст чорно-білого диму від -0,5 до +0,4, та коефіцієнт лазерного відбиття 0,2…0,3.На протязі 10…12с забезпечується потужне ІЧ випромінення.

Запас снарядів залежить від класу корабля (МЧ: СКР – 100, МПК – 40; ВЧ: СКР-180, МПК-80).

Установки пасивних завад – ПК-16 входять до складу комплексів МП401, МП-401С та МП-405, крім того, вони є на озброєні ракетних катерів. Вони призначені для постановки оманних теплових та радіолокаційних цілей. Комплектується 4 ПУ. Кількість пускових направляючих в одній ПУ – 16. Максимальна дальність стрільби до 5 км.

Для комплексу ПК-16 призначені наступні види 82 мм снарядів завад:

– турбореактивний снаряд ТСП-60У – радіолокаційний снаряд завад;

– турбореактивний снаряд ТСТ-60У – оптико електронний снаряд завад.

Установки пасивних завад – **ВМ-18** є на озброєні десантних кораблів (проект 773).

Вони призначені для постановки оманних теплових та радіолокаційних цілей. Комплектується 2 ПУ. Кількість пускових труб в одній ПУ – 10. Дальність постановки завад – до 7 км.

Час дії РЛ завіси – 6…7 хвилин (залежить від сили та напрямку вітру), ЕПР одного снаряда: 300 – 700 м², а час дії теплової цілі – 60 с.

Для комплексу ВМ-18 призначені наступні види 140 мм снарядів завад

Подавлення телевізійних засобів можна як за допомогою теплових снарядів завад так і за допомогою снарядів ТСТВ-47, які створюють імітаційні (маскуючі) чорно-білі аерозольні утворення. Ці утворення забезпечують також відбиття лазерного променю ($К_{відб} = 0,1$).

Для подавлення лазерних систем застосовуються також спеціальні снаряди спорядження яких складається із найдрібніших скляних кульок з коефіцієнтом лазерного відбиття на довжині хвилі 1,06 мкм приблизно рівним 0,3…0,5.

Розглянуті снаряди застосовуються для створення:

– оманних дезінформуючи цілей (РЛ);

– оманний відволікаючих цілей (РЛ, ОЕ);

– оманних відвідних цілей (ОЕ,ІЧ, РЛ).

Димові та аерозольні завіси.

Найбільш ефективним засобом захисту корабля від ОЕС зброї противника є димові та аерозольні завіси. Дими можуть створюватися за допомогою корабельної апаратури та димових шашок.

Основні характеристики димів:

– тривалість - від 4 (тип засобу МДШ-М) до 25 хвилин (ДА-2Б);

– довжина / висота димової завіси – 100 – 2400 м (БДШ-15 – ДШ-100-2) / 17 – 100 м (МДШ. - БДШ-15).

Крім димів застосовують аерозольні поглинаючі середовища (завіси, штучні тумани). Застосування аерозолів штучно порушує прозорість атмосфери, що приводить до ослаблення інфрачервоного та лазерного випромінювання (перевипромінювання). Ослаблення випромінювання відбувається за рахунок поглинання енергії парами і розсіюванням її зваженими в повітрі частками, коефіцієнт переломлення яких відмінний від переломлення середовища.

Існують наступні способи застосування аерозольних засобів:

– маскуючі аерозольні завіси, які прикривають свої сили від засобів спостереження і управління зброєю противника шляхом виключення спостереження ОЕС за значною територією;

– оманні аерозольні цілі для відволікання сил і зброї противника на оманні цілі шляхом створення аерозольних площин, розміри яких близькі до реальних кораблів;

– аерозольні цілі, що відводять для зниження імовірності наведення на кораблі управляємої зброї шляхом зміни геометричного центру цілі або її роздвоєння.

Димові шашки можуть застосовуватися, як із борту так і скиданням на воду, залпом або декількома серіями.

Параметри аерозольних утворень суттєво залежать від напрямку та швидкості вітру, ступеню вертикальної стійкості повітря та наявності опадів

Ведуться роботи по розробці аерозольних сумішей, за допомогою яких можуть бути створені оманні теплові цілі в результаті розпилювання в атмосфері речовин, здатних виділяти тепло в результаті хімічної взаємодії з киснем повітря, атмосферною вологою або спеціальними окислювачами.

Основні тактико-технічні характеристики комплексів РЕБ та РЕР частин (підрозділів) РЕБ ЗС України узагальнені у додатку 1.

Контрольні запитання до 2 розділу:

1. Які основі етапи історичного розвитку РЕБ?
2. Які основні тенденції розвитку РЕБ за досвідом локальних збройних конфліктів Ви знаєте? Як тенденції розвитку техніки РЕБ впливають на завадозахищеність систем зв’язку?
3. Які основні тенденції застосування РЕБ противника для порушення передачі інформації по каналах урядового зв’язку в операції об’єднаних сил, що проводиться на території Луганської та Донецької областей України?
4. Дайте визначення РЕБ, які складові РЕБ Ви знаєте?
5. Які основні форми РЕБ Ви знаєте? Дайте визначення та опишіть перспективи розвитку.

6. Що таке радіоелектронне подавлення? Вплив РЕП на завадозахищеність систем зв’язку?

7. Що таке радіоелектронний захист?

8. Що таке електромагнітне подавлення систем зв’язку?

9. Які основні оперативно-тактичні показники електромагнітного подавлення? Як чином впливає електромагнітна зброя на ефективність систем зв’язку?

10. Назвіть основні тактико-технічні характеристики комплексів РЕР та РЕБ Російсько-терористичних сил, що приймають участь у ГАнК на території Луганської та Донецької областей України?

11. Які частини (підрозділи) РЕБ Сухопутних військ Збройних Сил України Ви знаєте? Наведіть їх бойові можливості, зробить висновок що основних напрямків організації взаємодії між підрозділами Держспецзв’язку та РЕБ СВ ЗС України під час виконання завдань за призначенням в ході ООС.

12. Які частини (підрозділи) РЕБ Повітряних Сил Збройних Сил України Ви знаєте? Наведіть їх бойові можливості, зробить висновок що основних напрямків організації взаємодії між підрозділами Держспецзв’язку та РЕБ ПС ЗС України під час виконання завдань за призначенням в ході ООС.

13. Які частини (підрозділи) РЕБ Військово-Морських Сил Збройних Сил України Ви знаєте? Наведіть їх бойові можливості, зробить висновок що основних напрямків організації взаємодії між підрозділами Держспецзв’язку та РЕБ ВМС ЗС України під час виконання завдань за призначенням.

14. Які комплекси управління засобами радіозавад Збройних Сил України Вам відомі? Наведіть їх бойові можливості.

РОЗДІЛ 3
РАДІОЕЛЕКТРОННЕ ПОДАВЛЕННЯ ТА РАДІОЕЛЕКТРОННА РОЗВІДКА СИСТЕМ (КОМПЛЕКСІВ, ЗАСОБІВ) ЗВ'ЯЗКУ

3.1. Радіоелектронне подавлення. Визначення, мета, завдання та складові частини

Радіоелектронне подавлення (РЕП) – це сукупність узгоджених за метою, завданнями, простором і часом впливів радіоелектронними завадами та дезінформуючими повідомленнями (у перспективі, потужними електромагнітними імпульсами, деструктивними програмно - комп'ютерними засобами, що впроваджуються у комп'ютерні мережі), що здійснюються силами та засобами РЕБ, на радіоелектронні засоби систем управління військами (силами) та зброєю противника по єдиному замислу і плану відповідно з обстановкою, що склалася [18-21].

Для спрощеного розуміння можна визначити РЕП як навмисний вплив енергією електромагнітних (акустичних) коливань на РЕЗ та на середовище розповсюдження цих коливань, яке здійснюється практично у всіх діапазонах довжин хвиль.

Метою РЕП є зниження ефективності застосування радіоелектронних засобів управління військами (силами) і зброєю, розвідки та РЕБ противника в операціях (бойових діях) [18-19].

В ході ведення радіоелектронного подавлення здійснюється вплив електромагнітними (акустичними) хвилями на **радіоелектронні об'єкти** систем управління противника.

Радіоелектронний об'єкт (РЕОб) – наземний, повітряний, морський або космічний елемент (засіб) системи управління військами (силами) та зброєю, окремий бойовий засіб із сукупністю розташованих на ньому радіоелектронних засобів.

Радіоелектронні об'єкти противника, які підлягають радіоелектронному продавленню, є **об'єктами радіоелектронного подавлення** в операції (бойових діях).

Об'єкт радіоелектронного подавлення (Об РЕП) – це радіоелектронний об'єкт, який підлягає РЕП в умовах конкретної обстановки (операції, бойових дій чи їх етапу). Зокрема, Об РЕП в операціях (бойових діях) можуть бути КП (ПУ), вузли (центри) зв'язку або окремі засоби радіо-, радіорелейного, тропосферного, космічного зв'язку, радіолокації і радіонавігації, розвідки і РЕБ; літальні та космічні апарати, надводні кораблі та підводні човни.

Цілями радіоелектронного подавлення (Ц РЕП), цілями постановки завад є: приймачі засобів радіозв'язку і навігації; наземні, бортові та корабельні радіолокаційні системи та засоби виявлення, спостереження за цілями і управління зброєю; оптико-електронні і гідроакустичні системи і засоби розвідки, спостереження, зв'язку і управління, які розташовані на

об’єктах РЕП та на які може здійснюватися вплив радіоелектронними завадами.

Основними завданнями РЕП є [18-20]**:**

– створення активних радіозавад засобам радіозв’язку, передачі даних та радіонавігації противника;

– радіоелектронне прикриття військ (сил) і об’єктів від прицільних ударів систем (засобів) ураження противника, в тому числі високоточної зброї;

– запровадження дезінформуючих повідомлень в радіо- та комп’ютерні мережі противника.

Для виконання завдань радіоелектронної дезінформації залучаються сили та засоби частин РЕБ Збройних Сил, радіоелектронні засоби видів Збройних Сил, родів військ і спеціальних військ.

Прикриття об’єктів від прицільних ударів систем (засобів) ураження здійснюється шляхом створення маскуючих та імітуючих завад бортовим радіолокаційним засобам управління зброєю, радіолокаційним та оптико-електронним головкам самонаведення керованих снарядів і ракет; застосування хибних цілей і пасток, які можуть скидатися (відстрілюватися) з літаків, вертольотів, безпілотних і пілотованих літальних апаратів, кораблів, броньованих об’єктів, інших бойових засобів і військової техніки, а також встановлюватися на місцевості (у тому числі у воді).

В залежності від діапазону робочих довжин хвиль, у якому здійснюється РЕП, розрізняють наступні його види (рис. 3.1):

– радіоподавлення;

– оптико-електронне подавлення;

– гідроакустичне подавлення.

Радіоподавлення (РП) – це комплекс заходів з порушення (зриву) роботи радіоелектронних систем та засобів управління військами (силами) та зброєю, радіо, радіорелейного, тропосферного, супутникового зв’язку, радіолокації і радіонавігації противника шляхом [23-25]:

– впливу активними та пасивними радіозавадами;

– застосування хибних радіолокаційних цілей і пасток;

– передачі в радіомережах противника або своїх військ повідомлень, що дезінформують;

– демонстраційної (оманної) роботи своїх радіоелектронних засобів та імітації роботи РЕЗ противника;

– зміни умов розповсюдження радіохвиль.

Рис. 3.1. Складові частини радіоелектронного подавлення

Радіоподавлення ведеться з метою тимчасового ускладнення або неможливості застосування противником радіо-, радіорелейних, тропосферних та супутникових засобів зв'язку, радіолокації та радіонавігації для вирішення завдань управління військами (силами) та зброєю в операціях (бойових діях).

Радіоподавлення засноване на властивості радіоприймальних пристроїв приймати не тільки корисні сигнали, але й інші електромагнітні випромінювання, що співпадають з корисними за робочим діапазоном частот. В результаті цього, у залежності від енергетичного співвідношення корисного сигналу та завади, у кінцевих пристроях, що реєструють, прийом корисної інформації стає неможливим або відбуваються її викривлення, затримка, зменшення обсягу.

За результатами радіоподавлення у засобах радіо-, радіорелейного, тропосферного, супутникового зв'язку та радіонавігації під впливом завад відбувається повне або часткове викривлення інформації, а в радіолокаційних засобах – повне або часткове маскування відміток від цілей на екранах радіолокаторів або зрив автоматичного супроводження цілей.

Оптико-електронне подавлення (ОЕП) полягає у порушенні (зриві) роботи інфрачервоних, тепловізійних, телевізійних, лазерних і оптико-візуальних систем і засобів розвідки, спостереження, зв`язку і управління зброєю противника шляхом впливу на них активними і пасивними оптико-електронними завадами, застосуванням оманних оптичних цілей, пасток і аерозолів, а також виведенням з ладу електромагнітними випромінюваннями оптичних і фоточутливих елементів цих систем і засобів [18, 19].

Об'єктами ОЕП є радіоелектронні засоби, робота яких заснована на використанні теплового або оптичного випромінювання (оптичні, інфрачервоні, телевізійні і лазерні засоби розвідки, спостереження, зв'язку і управління зброєю) противника.

Роботу оптико – електронних засобів (ОЕЗ) можна порушити або суттєво ускладнити із застосуванням хибних цілей та пасток, активних та пасивних оптико-електронних завад, а також зниженням потужності теплового випромінювання військової техніки та об'єктів.

Хибна ціль уявляє собою пристрій, що імітує за відбиваючими або випромінюючими характеристиками реальний об'єкт.

Пастка – технічний засіб, що імітує об'єкт (ціль) для РЕЗ управління (наведення) зброї та застосовується для уведення від цілей керованих боєприпасів або зриву автоматичного супроводу цілі радіолокаційною станцією. При цьому пастка, на відміну від хибної цілі, призначена тільки для порушення роботи контурів наведення та самонаведення систем керування зброєю, тобто для зриву супроводження істинної цілі та переведення радіолокаційної станції або голівки самонаведення ракети на супроводження пастки.

Хибні оптичні цілі та пастки являють собою штучні джерела світлового випромінювання. До хибних цілей також належать макети бойової техніки.

Хибні цілі та пастки призначені також для ускладнення обстановки, введення в оману бойових розрахунків РЕС, ускладнення цілерозподілу, наведення та самонаведення засобів ураження противника.

Активні завади оптико-електронним засобам (ОЕЗ) створюються за допомогою оптичних квантових генераторів та джерел некогерентного випромінювання, що розташовані на об'єктах прикриття.

Пасивні завади ОЕЗ створюються шляхом постановки аерозольних або димових завіс. Створення аерозольних завіс, як правило, здійснюється частинами та підрозділами військ РХБз, а також із застосуванням спеціальних артилерійських боєприпасів, мін и авіабомб.

Активне застосування знаходять оптичні кутові відбивачі. Вони перевипромінюють потік енергії, що падає на них, у зворотному напрямку і тим самим порушують роботу ОЕЗ.

Оптико-електронне подавлення здійснюється за допомогою наземних, корабельних, авіаційних станцій оптико-електронних завад, спеціальних ракет, снарядів і патронів з інфрачервоними і плазмовими завадами, лазерних і інфрачервоних відбивачів (розсіювачів), спеціальних покрить, які зменшують помітність об'єктів, а також за допомогою оманних цілей, пасток, димів і аерозолів, а також виведенням з ладу електромагнітними випромінюваннями оптичних і фоточутливих елементів оптико-електронних систем та засобів.

Гідроакустичне подавлення (ГАП) полягає у порушенні (зриві) роботи засобів гідроакустичного виявлення і зв'язку, гідроакустичних систем самонаведення торпедної і протичовнової зброї, підривачів торпед, ракетоторпед і мін противника шляхом впливу на них гідроакустичними завадами, імітації підводних човнів і хибних цілей, зміни умов розповсюдження гідроакустичних хвиль [18-20].

Метою ГАП є порушення нормальної роботи стаціонарних, корабельних і авіаційних засобів гідроакустичного виявлення, зв'язку, а також систем самонаведення торпедної та протичовнової зброї шляхом створення гідроакустичних завад.

Об'єктами гідроакустичного подавлення є гідроакустичні засоби, робота яких заснована на використанні випромінюваннь і відповідному прийнятті (або тільки на прийнятті) гідроакустичних хвиль. Іншими словами, об'єктами ГАП є бортові гідролокатори і шумопеленгатори, засоби гідроакустичного зв'язку, гідроакустичні буї, а також стаціонарні гідроакустичні системи виявлення підводних човнів і надводних кораблів, головок самонаведення і підривачів торпед, ракетоторпед і мін.

Гідроакустичне подавлення здійснюється за допомогою самохідних і дрейфуючих приладів гідроакустичних завад, бортових станцій завад підводних човнів і надводних кораблів, вибухових джерел завад, самохідних і дрейфуючих імітаторів підводних човнів і хибних цілей.

Основні способи бойового застосування частин (підрозділів) РЕБ під час ведення РЕП

Основними способами бойового застосування частин (підрозділів) РЕБ під час вирішення завдань з РЕП радіоелектронних об'єктів систем управління військами (силами) та зброєю противника є **масований, вибірковий або їх комбінування** [18-20].

В ході ведення радіоподавлення частини РЕБ, що залучаються до виконання завдань з прикриття своїх військ та об'єктів від повітряної радіолокаційної розвідки та прицільних ударів з повітря (в т. ч. із застосуванням високоточної зброї), виконують їх **зональним, об'єктовим, бар'єрним способами або їх комбінуванням.** Кількість станцій завад, яка необхідна для прикриття об'єктів, визначається їх енергетичними та перепускними можливостями (щільністю нальоту), а також розмірами і радіолокаційною контрастністю об'єкту, якій прикривається.

Основні способи РЕП радіоелектронних об'єктів противника

Традиційним способом РЕП є **створення радіозавад** приймальним пристроям РЕЗ [23-25].

Для реалізації цього способу РЕП необхідно виконати частотну, енергетичну та часову умови.

Частотна умова: спектр радіозавади повинен попадати у смугу пропускання приймача РЕЗ, який подавляється.

Енергетична умова: потужність завади $Р_{п.вх}$ на вході приймача РЕЗ повинна бути більша за потужність корисного сигналу $Р_{с.вх}$ у $К_п$ разів, де $К_п$ – коефіцієнт подавлення – таке мінімально необхідне співвідношення цих потужностей, за якого ефективність функціонування РЕЗ противника буде не більше потрібного рівня. В якості показника ефективності функціонування РЕЗ може використовуватись, наприклад, ймовірність правильного виявлення сигналу в умовах фіксованого показника «ймовірність хибної тривоги», а для засобів зв'язку – ймовірність помилки на біт (на двійковий інформаційний символ) при прийомі повідомлення.

Енергетична умова визначає зону подавлення. Зона подавлення – це простір, у межах якого розташовані приймачі системи зв'язку, що подавляється, не зможуть ефективно (за потрібної якістю) приймати корисні сигнали.

Коли радіус зони подавлення радіоліній $R_п$ більше, ніж дальність прямого бачення $Д_{п.б.} \approx 4{,}12(\sqrt{h_1} + \sqrt{h_2})$, [км], де h_1[м] і h_2[м] – висоти антен, , станції радіозавад і приймальної станції, яка подавляється) відповідно, тоді потрібно брати $R_п = Д_{п.б.}$, бо розповсюдження радіохвиль завади не більш велику відстань обмежено прямолінійністю розповсюдження радіохвиль.

Часова умова: радіозавада повинна діяти у той час, коли приймач РЕЗ відкритий для прийому сигналів.

Реалізація зазначеного способу РЕП досягається**:**

– створенням активних і пасивних радіозавад комплексами та засобами РЕП, які знаходяться на озброєнні наземних, авіаційних частин і підрозділів РЕБ; комплексами й засобами (станції активних завад, засоби створення пасивних завад, імітатори, оманні цілі, пастки та ін.), що встановлюються на ракетах, літаках, вертольотах, безпілотних літальних апаратах, аеростатах, кораблях, наземних рухомих об'єктах, інших бойових засобах, в районах розташування угруповань військ і об'єктів, які прикриваються, а також за допомогою застосування передавачів завад одноразової дії;

– застосуванням оманних цілей і пасток. Вони можуть скидатися (відстрілюватися) з літаків, вертольотів, безпілотних і пілотованих літальних апаратів, кораблів, наземних рухомих об'єктів, інших бойових засобів і військової техніки, а також встановлюватися на місцевості (у воді) або створюватися станціями (комплексами).

Для створення пасивних радіозавад використовуються дипольні, ланцюгові, кутові та лінзові відбивачі; грати, що перевипромінюють. Пасивні завади створюються шляхом відбивання (розсіювання) електромагнітних хвиль від цих штучних об'єктів. Штучні відбивачі електромагнітних хвиль можуть створювати на окремих РЛС відмітки, які подібні до відміток від реальних цілей, або засвічувати ділянки екранів.

Дипольні відбивачі (ДВ) являють собою тонкі пасивні вібратори, які виготовляють із металізованих ниток скловолокна, нейлону, алюмінієвої фольги. Вони викидаються у простір за допомогою спеціальних пристроїв або вистрелюються за допомогою піропатронів. Недоліками ДВ є їх мала діапазонність, одноразовість їх використання і короткий час дії (швидкість зниження диполів у повітрі дорівнює 0,5÷3 м/хв.), а також можливість селекції таких завад за допплерівською частотою.

Кутові відбивачі (КВ) являють собою жорстку металеву конструкцію із взаємно перпендикулярних граней, що електрично з'єднані між собою. Навіть при малих розмірах граней вони мають великі ефективні площі розсіювання. Наприклад при довжині хвилі λ=3 см і стороні КВ a=50 см маємо, що його ЕПР ≈ 830 м^2, а ЕПР автомобілів, танків дорівнює всього 7...30 м^2; літаків – 3...100 м^2. Один із суттєвих недоліків КВ – вузька ширина діаграми розсіювання. У лінзових відбивачів ширина діаграми розсіювання більша.

Кутові та лінзові відбивачі використовуються для створення хибних цілей, радіолокаційних пасток, на які перенацілюються радіолокаційні головки самонаведення ракет, а також для зміни радіолокаційної контрастності місцевості. За їх допомогою можна імітувати на екранах РЛС залізничні мости, літаки, танки та інші об'єкти.

Важливим способом РЕП є **зниження радіолокаційної помітності**, яка характеризується ефективною площиною розсіювання σ. Дальність виявлення цілі пропорційна $\sqrt[4]{\sigma}$. Коли ЕПР зменшити в 16 разів, то дальність виявлення цілі зменшиться у 2 рази. Ефект зменшення ЕПР ще більше відчувається з позицій РЕП, через те, що необхідна потужність передавача завад, яка

потрібна для подавлення РЛС, пропорційна σ. При зменшенні ЕПР у 16 разів потрібна потужність передавача завад зменшиться також у 16 разів.

Основні способи зменшення ЕПР: вибір форми об'єкта та елементів його конструкції; використання радіопоглинаючих, композиційних матеріалів для деяких елементів конструкцій об'єкту; іонізація повітря, що призводить до поглинання електромагнітних хвиль; зниження кількості антен на об'єктах, які прикриваються.

Для зниження гідроакустичної помітності потрібно знизити рівень шумів двигунів підводних човнів та кораблів, а також інших джерел акустичних шумів на об'єкті.

Зміна умов розповсюдження електромагнітних хвиль досягається зміною електричних властивостей середовища, у якому вони розповсюджуються. Реалізація цього способу пов'язана з іонізацією локальних областей середовища.

Електромагнітні хвилі, які розповсюджуються через іонізовані області, можуть відбиватися від них, переломлюватися та поглинатися. Ці явища можуть призвести до засвічування екранів РЛС та маскування цілей за рахунок відбивання електромагнітних хвиль; до зменшення дальності дії за рахунок поглинання та через помилки вимірювання РЛС координат цілей за рахунок переломлення електромагнітних хвиль.

Протиракетний, **противинищувальний та протизенітний маневр** може розглядатись як окремий способів РЕП. Це обумовлено особливостями функціонування РЛС та голівок самонаведення ракет різних типів, які пов'язані з їх інерційністю супроводу цілей та іншими тактичними характеристиками. Спеціальні маневри цілі можуть призвести до нарощування динамічних помилок супроводу цілі і далі до зриву режиму супроводу. Використання спеціальних маневрів цілі, як одного з простих способів РЕП, стає актуальним у зв'язку з прийняттям на озброєння розвинутих країн надманеврових літаків.

Перспективним способом впливу на радіоелектронні об'єкти є створення потужних електромагнітних імпульсів (ЕМІ). Вплив ЕМІ може призвести або до фізичного руйнування (функціонального ураження) різних елементів РЕЗ, або до тимчасового порушення роботи ("осліплення") РЕЗ з наступним відновленням їх функцій (тимчасового функціонального подавлення). Існує можливість уражаючої дії потужних ЕМІ (ЕМІ – зброї) на вибухові речовини, неконтактні міни та на особовий склад. Вплив ЕМІ – зброї на особовий склад може викликати тимчасові порушення адекватної сенсомоторики людини, що призводить до його непрацездатності або до хибних дій (див. п.п 2.2.3).

Радіоелектронні удари із застосування ЕМІ – зброї стануть однією з основних форм ведення РЕБ у найближчому майбутньому.

Ще одним новим способом впливу на радіоелектронні об'єкти є впровадження деструктивних програмно-комп'ютерних засобів у комп'ютерні радіомережі противника.

Наприкінці розгляду способів ведення РЕП необхідно зазначити, що сучасний стан розвитку систем управління військами (силами) і зброєю противник буде комплексувати різні види РЕП під час вирішення завдань з зриву військового або державного управління. Тому при розробці методів завадозахисту необхідно оцінювати показники завадозахисту комплексно за умови одночасного застосування противником різних видів РЕП.

Ключовим поняттям, що виникає під час розгляду сутності та принципів РЕП та захисту від нього систем зв'язку є радіоелектронна завада. Розглянемо це поняття більш детально.

3.2. Радіоелектронні завади, їх класифікація. Оптимальна завада

Радіоелектронні завади – це неуражаючі електромагнітні або акустичні випромінювання, які виключають або погіршують якість функціонування радіоелектронних систем і засобів.

За своїм походження вони діляться на природні (завади природного походження) і штучні (завади, які створюються за допомогою штучних джерел). Останні в свою чергу діляться на навмисні і ненавмисні (які не призначаються для подавлення). Навмисні завади класифікуються, як правило, за способом їх створення, характеристиками завад, а також іншими ознаками (табл. 3.1) [8, 9, 23-25].

Об'єктами впливу навмисних завад можуть бути системи і засоби, які працюють з використанням різних фізичних полів (в першу чергу-електромагнітного (радіо і оптичного діапазонів), а також сейсмічного і т.п.).

Частіше використовуються: радіозавади- завади у діапазоні радіохвиль, оптико електронні завади – у діапазоні світлових хвиль і гідроакустичні завади, які створюються у водяному середовищі з використанням гідроакустичних хвиль.

В залежності від наявності джерела енергії в засобах РЕП, за допомогою яких створюються завади, вони розділяються на активні, пасивні, комбіновані.

Активні завади – це випромінювана електромагнітна, або гідроакустична енергія, створена засобами РЕП.

Вони можуть бути створені наземними, корабельними та літаковими станціями завад, імітаторами шумів підводних човнів і т.п. Активні завади (ті, що маскують або імітують) можуть бути створені у відповідь на кожний сигнал РЕС, що зондує, або бути загороджувальними за часом, табл. 3.1.

Пасивні завади створюються за рахунок зовнішньої для джерел завад енергії. Вони створюються перевипромінювачами (антенні ретрансляційні решітки; дипольні, кутові, діелектричні, лінзові перевипромінювачі), масками – екранами, протирадіолокаційними та протигідроакустичними покриттями і засобами, зміною електричних властивостей середовища (засоби, які іонізують зони атмосфери) та зміною прозорості атмосфери (димові та газові завіси) і т.п.

Комбіновані завади – це комплекс пасивних і активних завад. Дуже ефективними завадами є пасивні дипольні завади підсвічені широкосмуговою активною завадою.

За характером впливу на об'єкт подавлення розрізняють: завади, що маскують (подавляють) і імітують (дезінформують).

Завада, що маскує, сприймається як фон, що заважає виявленню і виділенню (селекції) сигналів, їх розпізнаванню і визначенню параметрів. Такі завади, впливаючи на приймальні пристрої РЕС, маскують сигнали в шумах, що аналогічні шумам підсилювачів. Така завада призводить до зменшення і затримки корисної інформації в системах управління противника. З підвищенням потужності завад їх властивості з маскування зростають.

Таблиця 3.1

Класифікація навмисних радіоелектронних завад

Ознака класифікації	Види завад
Вид випромінювання	Радіозавади, оптико-електронні, гідроакустичні завади.
Способи формування	Активні, пасивні, змішані.
Характер впливу на об'єкт.	Ті, що маскують (подавляють) або імітують (дезінформують).
Метод наведення параметрів завад.	Прицільні, загороджувальні.
Часова структура випромінювання.	Неперервна, квазінеперервна, імпульсна, імпульсні завади у відповідь (однократні, багатократні).
Способи взаємодії з корисними сигналами.	Адитивні, мультиплікативні (моделюючі)

Завади, що імітують, за своєю структурою аналогічні корисним сигналам, тому вони сприймаються в РЕС як сигнал від цілі. Таким чином, в систему управління вноситься хибна інформація. Така інформація створює в кінцевих пристроях (індикаторах) засобів, що подавляються, сигнали або відмітки від оманних цілей, подібні до реальних, знижує при цьому пропускну здатність системи, вводить в оману операторів, приводить до втрати частини корисної інформації, збільшує вірогідність оманної тривоги. Впливаючи на засоби управління військами, вона зриває автоматичне супроводження цілей по одному або декільком параметрам, перенацілює їх на імітовані цілі, викликає помилки при супроводженні цілі.

В залежності від методу наведення параметрів завади на аналогічні параметри сигналу подавляємих РЕС, навмисні завади можуть бути прицільними або загороджувальними.

Як правило ,створюються прицільні завади за частотою і за напрямком. Для подавлення КХ і УКХ зв'язку використовують прицільні по частоті завади (в цих діапазонах використовуються слабо спрямовані антени). А для подавлення РЕС в більш високочастотних діапазонах використовуються прицільні завади за напрямком. Завади вважаються: прицільними за частотою у випадках, якщо $\Delta fn \approx 1 \div 2 \Delta fnp$ (Δfn - ширина спектру завади, а Δfnp -

ширина пропускання приймача РЕС); загороджувальними, коли - $\Delta fn \approx 10 \div 20 \Delta fnp$; напівзагороджувальними якщо - $\Delta fn \approx \Delta Fрлс$, ($\Delta Fрлс$ - ширини смуги перестройки РЛС, що подавляється).

По часовій структурі випромінювання навмисні завади діляться на: неперервні, квазінеперервні (завади випромінюються з невеликими перервами на прийняття сигналу РЕС - $\Sigma \tau пі \approx t_{цп}$ (де $\Sigma \tau пі$ – сумарна тривалість випромінювання завад за $t_{цп}$ - час циклу постановки завад)) і імпульсні - $\Sigma \tau пі << t_{цп}$. Завади, що формуються у відповідь на прийнятий сигнал від РЕС, що подавлюється називаються завадами у відповідь. Такі завади для імпульсних РЕС можуть бути однократними або багатократними. В свою чергу в залежності від часу приймання імітованого сигналу і сигналу РЕС завада у відповідь може бути такою, що випереджає або запізнюється. В залежності від закону зміни затримки між прийняттям сигналу і випромінюванням завади можна формувати заваду, що відводить або за дальністю або за швидкістю.

Дуже важливим фактором при відокремлені сигналів від завад, є взаємодія їх на виході пристрою, що подавлюється. Так, наприклад, якщо завадовий сигнал поступає незалежно від корисного і додається в процесі обробки, то така завада називається адитивною. Завади, що впливають на фізичні поля, які використовуються для отримання інформації, і такі, що містять корисний сигнал, є мультиплікативними (моделюючими).

Вплив завад на радіоелектронні засоби призводить до втрати корисної інформації, отримання хибної інформації або отримання корисної інформації з підвищеними помилками. Часткова або повна втрата корисної інформації та отримання хибної є наслідком [23-25]:

– ослаблення корисного сигналу при його взаємодії з завадою в елементах радіоелектронного пристрою;

– маскування корисного сигналу, яка полягає у тому, що корисний сигнал, змішуючись з завадовим, втрачає властиві йому характеристики та не може бути виділений, хоча він також досягає вихідного пристрою, як і за відсутності завади;

– впливу завад, які несуть хибну інформацію.

Ослаблення та маскування корисного сигналу, які мають місце при його взаємодії з завадою в елементах радіоелектронного пристрою, визначаються видом сигналів та параметрами елементів радіоелектронного пристрою.

Всі елементи радіоелектронних пристроїв поділяються на лінійні та нелінійні. До лінійних звичайно відносяться: антенно-фідерна система, підсилювач високої частоти (ПВЧ), перші каскади підсилювача проміжної частоти (ППЧ) та відеопідсилювача (ВПЧ) або підсилювача низької частоти (ПНЧ), а також деякі системи кінцевих пристроїв.

Проходження завад та корисних сигналів через лінійні елементи радіоелектронних пристроїв може розглядатися незалежно. Тому ослаблення корисного сигналу в цих елементах радіоелектронних пристроїв відбуватися не буде. Втрата корисної інформації в лінійних ланцюгах радіоелектронних

пристроїв може мати місце тільки за рахунок маскування завадою тих параметрів сигналу, які несуть корисну інформацію.

Ослаблення корисного сигналу може спостерігатися тільки в нелінійних елементах радіоелектронних пристроїв. До таких елементів відносяться: останні каскади підсилювачів високої, проміжної, та низької частоти (при впливі потужних завад), детектори, інерційні системи АРП, пристрої з логарифмічною амплітудною характеристикою, обмежувачі та інші подібні елементи кінцевих пристроїв.

Ефект впливу хибних сигналів проявляється звичайно в кінцевих системах радіоелектронних пристроїв та визначається характером закладеної в них хибної інформації. Взаємодія завади з корисним сигналом в елементах радіоелектронного пристрою може бути при цьому повністю відсутня.

Умова гарантованого подавлення радіозв'язку. Відомо, що оптимальна завада для конкретного виду сигналу і відомого способу його прийому (обробки) повинна мати конкретно визначену структуру.

Взагалі, з точки зору теорії, однією з найбільш ефективних є завада, кожна складова структури якої цілком збігається з відповідною складовою структури корисного сигналу, але має протилежну фазу.

При одночасному надходженні такої завади і сигналу на вхід приймача сигнал буде повністю зкомпенсований, і на виході його не буде. Крім того, для подавлення дискретних видів зв'язку з пасивною паузою (наприклад, слуховий радіозв'язок з використанням коду Морзе) теоретично оптимальною буде дискретна завада, у якої імпульс збігається з паузою сигналу. У результаті впливу такої завади одержимо неперервний сумарний сигнал, що ніякої інформації не несе. Однак на практиці для створення такої завади необхідно, насамперед, заздалегідь знати, що буде передавати противник, а це неможливо.

Тому на практиці використовують завади, структура яких змінюється за випадковим законом. Загальний підхід до визначення необхідної спектральної структури таких завад полягає в наступному.

Усі параметри, що характеризують сигнал, що подавляється умовно можна розділити на розпізнавальні й інформаційні. До пізнавальних відносяться ті параметри, що служать для розпізнавання і виділення саме цього сигналу з множини інших сигналів. Ці параметри безпосередньо для передачі інформації не використовуються. Такими параметрами є номінал несівної частоти, тривалість імпульсу, довжина кодової комбінації, правила побудови сигналу і т.п., але тільки для випадку, коли ці параметри не модулюються повідомленням.

До інформаційних ж відносяться ті параметри, що характеризують саме повідомлення. Ці параметри змінюються відповідно до переданого повідомлення. Такими параметрами є миттєве значення частоти при частотній маніпуляції, тривалість імпульсу при імпульсно-широтній модуляції та інші.

Усі параметри сигналу в більшості випадків абоненту відомі і можуть використовуватися для виділення (селекції) сигналу з завад. Але на практиці

для селекції сигналу, як правило, використовуються лише розпізнавальні параметри.

Очевидно, що якщо який-небудь зазначений параметр завади буде збігатися з відповідним параметром сигналу, то селекція останнього по цьому параметру виявиться ускладненою або навіть неможливою.

Як відзначалося вище, практично створити заваду, усі параметри якої (частота, фаза, амплітуда, тривалість елементарних посилок) точно збігалися б з відповідними параметрами сигналу, неможна. Тому на практиці прагнуть досягти того, щоб розпізнавальні параметри завади збігалися б більш точно з відповідними параметрами сигналу, а характер зміни інформаційних параметрів завади був би подібним до характеру змін інформаційних параметрів сигналу. Іншими словами, статистична структура завади повинна бути подібна до структури сигналу, що подавляється.

3.3. Радіоподавлення засобів радіозв'язку

Для подавлення радіозв'язку використовується три способи РЕП, а саме:

– створення завад, що маскують;
– вплив на середовище розповсюдження електромагнітних хвиль;
– створення завад, що імітують.

Два перших способи дозволяють зменшити кількість, швидкість передачі інформації, а завади, що імітують, вносять хибну інформацію в повідомлення.

Для подавлення засобів радіозв'язку в теперішній час найбільше поширення знайшов спосіб створення активних завад, що маскують. Тому головну увагу доцільно звернути на цей спосіб РЕП.

В загальному випадку ефективність радіозавад залежить від багатьох факторів. До основних з них відносяться: відношення напруг завади і сигналу на вході приймача, що подавляється - (U_n/U_c), неточність (помилка) у суміщенні спектрів завади і сигналу (Δf), неспівпадіння виду завади з видом передачі повідомлення, тривалість радіопередачі, що підлягає подавленню та час реакції станції завад.

Ступінь викривлення, тобто ефективність подавлення повідомлення, у різній мірі залежить від зазначених факторів. Однак теоретичні дослідження і досвід радіоподавлення показують, що для того, щоб імовірність подавлення повідомлення була досить високою, необхідно, щоб усі приведені фактори були в межах визначених (граничних) значень.

Іншими словами можна сказати, що для забезпечення високого ступеню ймовірності подавлення радіозв'язку необхідно виконати наступні умови гарантованого подавлення: часову; частотну; енергетичну та умову щодо виду передачі.

3.3.1. Умови гарантованого подавлення радіозв'язку

Часова умова гарантованого подавлення радіозв'язку. Вихід в ефір (на зв'язок) радіостанцій – це імовірнісний процес. В залежності від умов підготовки або ведення бойових дій інтенсивність радіообміну може зростати або спадати, тому можна застосовувати прицільні або загороджувальні завади за часом. Загороджувальні завади за часом є менш ефективними за рахунок можливостей їх передчасної розвідки і переходу на інші запасні робочі частоти. Окрім того, вони не є ефективними з точки зору енергетичних витрат на подавлення. Тому більш доцільними є завади, прицільні за часом.

Такі завади застосовуються після попереднього визначення початку роботи радіолінії. У зв'язку з цим існує таке поняття, як час реакції станції завад [23-25].

Час реакції станції завад - це час від моменту визначення початку роботи каналу зв'язку до моменту початку його подавлення. Цей час ($t_{рп}$) характеризує швидкодію засобів розвідки і завад. Чим менше цей час, тим, при інших рівних умовах, вище імовірність подавлення повідомлення. Досвід створення радіозавад показує, що при впливі на змістовну частину радіограми повідомлення не можна розібрати, якщо завадами подавлено не менше половини тривалості передачі. Іншими словами, для надійного подавлення час реакції станції завад повинен бути не більше половини тривалості передачі повідомлення *(Т).* При впливі завад на адресну частину повідомлення або по іншим коротким службовим частинам радіограми час реакції станції завад повинен бути ще меншим. Ідеальна прицільна за часом завада - це та, яка подавляє адресну (службову) частину радіограми (наприклад, по сигналам автостопу, синхронізації та ін.)

Частотна умова гарантованого подавлення радіозв'язку. В залежності від співвідношення ширини спектру радіозавади і смуги пропускання лінії радіозв'язку, що подавляється, завади діляться на загороджувальні та прицільні. Загороджувальні завади мають ширину спектру, яка в десятки разів перевищує ширину смуги пропускання приймачів радіостанцій. Основним обмеженням при широкому застосуванні таких завад є мала спектральна щільність потужності завад (вона обернено пропорційна ширині спектру завади). Більш ефективною з точки зору енергії є прицільні за частотою завади. Вони можуть бути прицільними за несучою частотою, за шириною спектру, за частотою модуляції, за доплерівською частотою.

Помилка в суміщенні спектра прицільної завади зі спектром сигналу *(Δf),* якщо вона не перевищує допустимого значення, майже не впливає на імовірність подавлення. При значеннях, що більші за допустиму величину, для збереження тієї ж імовірності подавлення повідомлення, потрібно значне збільшення відношення потужності (амплітуди) завади і сигналу на вході приймача, що подавляється. Однак, це не завжди можна виконати.

Дослідженнями доведено, що допустима помилка в суміщенні спектрів завади і сигналу *(Δfпр)* на вході приймачів засобів радіозв'язку не повинна перевищувати 15—22% ширини спектра сигналу *(ΔFс)* тобто $\Delta f\ пр < (0{,}15—0{,}22)\ \Delta Fс$. Якщо помилка така, що частина спектра сигналу не накривається

завадою, то в ряді випадків, відфільтрувавши заваду, можна по залишку спектра сигналу забезпечить досить якісний прийом інформації.

Енергетична умова гарантованого подавлення радіозв'язку. У залежності від взаємного розташування передавальної, приймальної радіостанцій та станції радіозавад дуже важливою умовою є виконання енергетичної умови, сутність якої полягає в тому, щоб енергія сигналу завади на вході приймача $(E_{п.вх})$, що подавляється, була в k раз більшою за енергією корисного сигналу (або рівною) на вході того ж приймача $(E_{с.вх})$:

$$E_{п.вх} > k\, E_{с.вх}. \qquad (3.1)$$

Створення активних завад достатньої інтенсивності вимагає, як правило, великих енергетичних витрат. Тому на практиці створення завад прагнуть до нанесення противнику заданого інформаційного збитку при мінімальних енергетичних витратах. Для цих цілей служить енергетична характеристика завад, що маскують, - коефіцієнт подавлення $(K_п)$.

Коефіцієнтом подавлення називається мінімально необхідне відношення енергії сигналу завади до енергії сигналу, що подавляється, на вході приймального пристрою в смузі пропускання його лінійної частини, при якому забезпечується заданий інформаційний збиток (наприклад, задана ймовірність подавлення радіопередачі, задане скорочення дальності зв'язку та інше). Таким чином $k_п$ характеризує ступінь енергетичних витрат передавача завад, при якому досягається задана ефективність.

У багатьох випадках сигнали, що подавляються, і дискретні завади можна розглядати, як імпульси прямокутної форми. У цих випадках коефіцієнт подавлення виражається через відношення пікових потужностей, а для сигналів довільної форми- через середні значення потужностей:

$$k_{пP} = (P_п/P_с)_{вх.min}. \qquad (3.2)$$

При подавлені радіозв'язку коефіцієнт подавлення зручно виражати через напруги $(U_п, U_с)$ або напруженості $(E_п, E_с)$. Це пояснюється тим , що в діапазоні довгих, коротких та ультракоротких хвиль їх простіше виміряти:

$$k_{пU} = (U_п / U_с)_{вх.min,}, \; k_{пE} = (E_п/E_с)_{вх.min}. \qquad (3.3)$$

Коефіцієнт подавлення залежить від виду (спектральних структур) завади і сигналу, методу обробки сигналу в процесі його прийому, надлишковості кодів і деяких інших параметрів, що характеризують завадозахищеність РЕС.

Розглянемо методи визначення параметрів оптимальних завад (відносно виду передачі, коефіцієнту подавлення, допустимої помилки суміщення спектрів завади і сигналу) відповідно до двох видів радіозв'язку: букводрукування (дискретний частотно-маніпульований вид передачі) і радіотелефонії (неперервний вид передачі).

3.3.2. Радіоподавлення радіоприймачів частотно-маніпульованих сигналів

Одним із основних способів передачі інформації в радіозв'язку є двухпозиційна частотна телеграфія (ЧТ). При двухпозиційній радіотелеграфії «натиснення» ключа (посилці) відповідає випромінювання коливання на деякій частоті ω_1 а "відтиснення" (паузі) — випромінювання на іншій частоті ω_2. Це дозволяє розглядати частотно-маніпульований сигнал як сукупність двох амплітудно-маніпульованих сигналів: одного на частоті «натискання» ω_1, другого – на частоті паузи ω_2. Кожний із двох сигналів несе повну інформацію про передане повідомлення, і ідеальний приймач може здійснювати безпомилковий прийом, якщо на одній з частот завада відсутня. Звідси випливає, що у випадку ідеального приймача оптимальна завада для частотно-маніпульованого сигналу повинна в кожен момент часу мати складові на обох частотах випромінювання ω_1 і ω_2.

У реальних системах зв'язку приймальні пристрої не є ідеальними. Оскільки в кожен момент часу випромінюється тільки одна частота (або ω_1, або ω_2), то за відсутності завад напруга на вході або виході детектора приймача буде завжди більша на тій частоті, що у даний момент випромінюється.

Тому сутність звичайних методів прийому ЧТ сигналів полягає в порівнянні напруг на частотах ω_1 і ω_2 і реєстрації сигналу на тій частоті, де напруга більша. Звідси випливає, що можна здійснити ефективне подавлення радіозв'язку не шляхом випромінювання завад одночасно на двох частотах, а створювати заваду лише на одній частоті, саме на тій, на якій сигнал у даний момент відсутній. Якщо при цьому завада буде більш сильна, ніж сигнал, то приймач зреагує на заваду, а не на сигнал.

Таким чином, коефіцієнт подавлення сигналів повинен для ЧТ хоча б незначно перевищувати одиницю. У реальних умовах через наявність ненавмисних шумів на вході приймача і недосконаліть прийомних трактів подавлення повідомлення може мати місце вже при k_n = 0,8—0,9.

Допустиму помилку в суміщенні частот завади і сигналу для ефективного подавлення частотно-маніпульованих сигналів можна визначити із виразу:

$$\Delta f_0 \leq 1/2(\Delta f_{пр} - 3{,}9S f_0, \qquad (3.4)$$

де $\Delta f_{пр}$ – смуга пропускання приймача; Δf_0 – математичне очікування розстроювання частоти завади; $\sigma = S\ f_n \approx S\ f_0$ – середньоквадратичне відхилення частоти завади відносно частоти сигналу; S – відносна нестабільність частоти передавача завад.

Потрібно відзначити, що через нестабільність частоти передавача завад, що залежить від низки випадкових факторів (зміни температури, вологості, вібрації і т.д.), розстройка частоти завади щодо середніх частот каналів

прийому (ω_1, ω_2), також є випадковою величиною, щільність імовірності якої змінюється по нормальному закону.

Сучасні радіопередавачі сигналів зв'язку і завад мають відносну нестабільність частоти 10^{-6}–10^{-7}, а ширина смуги пропускання приймача при прийомі сигналів букводрукування зі звичайними швидкостями (45-50 бод) складає ($\Delta f_{пр}$= 400-750 Гц, тобто $2\Delta f_{пр}$= 0,8-1,5 кГц). Тоді відповідно з формулою (4.4), допустима помилка суміщення частот завади і сигналу складе:

$$\Delta f_0 \leq 0{,}5(400 \div 750)Гц, \; - 3{,}9(10^{-6} \div 10^{-7})3 \cdot 10^{6} Гц \approx 200 \div 300 Гц. \qquad (3.5)$$

Як бачимо, частота завади при подавлені частотно-маніпульованих сигналів (передач) може відрізнятися від основного розпізнавального параметра його несучої частоти на величину не більшу 200-300 Гц.

Кінцевий пристрій (у розглянутому випадку це найчастіше букводрукуючий апарат-телетайп) сконструйовано так, що знаки (букви, цифри) будуть видрукувані правильно, якщо тривалість елементарних посилок, що утворюють код цих знаків, буде відрізнятися від стандартної не більше, ніж на визначену частину, названу виправляючою здатністю апарата (μ).

Для збою посилок сигналів частіше за все використовуються завади з хаотичною зміною частоти маніпуляції. Основними характеристиками такої завади є:

– $F_{м0}$ – математичне очікування (середнє значення) частоти маніпуляції завади;

– – стандартне відхилення частоти маніпуляції завади.

Їх можна знайти із виразів:

$$F_{M0} \leq F_c / \mu - 3{,}9 \; \sigma_n \; ; \; \sigma_n \leq F_c / 7{,}8\mu. \qquad (3.6)$$

Як приклад, визначимо оптимальну частоту маніпуляції завади для подавлення букводрукувального каналу, швидкість передачі B в якому складає 50 бод, а виправляюча здатність телеграфного апарата μ = 37%.

Тривалість елементарної посилки τc і частота маніпуляції сигналу F_c у цьому випадку складають:

$$\tau_c = \frac{1000мс}{Вбод} = \frac{1000мс}{50бод} = 20 \; мс; \qquad (3.7)$$

$$F_c = \frac{1}{2c_c} = \frac{1}{2{,}2_c} = 25 \; Гц.$$

По формулі (3.7) стандарт відхилення:

$$\sigma_{\text{п}} \leq \frac{F_c}{7{,}8\mu} = \frac{25 Гц}{7{,}8 \cdot 0{,}37} \approx 8{,}7\ Гц. \tag{3.8}$$

Відповідно до (3.6) оптимальна частота маніпуляції дорівнює:

$$F_{мо} = \frac{25 Гц}{0{,}37} - 3{,}9 \cdot 8{,}7\ Гц \approx 33\ Гц. \tag{3.9}$$

Таким чином, при подавлені частотно-маніпульованого сигналу k_n = 0,8-0,9; оптимальна завада за структурою подібна до сигналу, що подавляється, а частота її маніпуляції перевищує на 20-25% частоту маніпуляції сигналу.

3.3.3. Радіоподавлення радіоприймачів радіотелефонного зв'язку

При радіотелефонному зв'язку кінцевим пристроєм, що реагує на прийнятий сигнал, є вухо людини. Тому при визначенні параметрів оптимальних завад для телефонних радіоканалів необхідно враховувати фізіологічні особливості слуху.

До таких особливостей відносяться, насамперед, експериментально встановлені властивості, що стосуються розбірливості мови. Так, дослідним шляхом встановлено, що якщо 70% слів нерозбірливі (мовна артикуляція менша за 30%), то мова в цілому також стає нерозбірливою. При цьому, як показують дослідження, акустична завада (при заданій середній потужності), яка більш за все знижує розбірливість мови, за своєю структурою близька до флуктуаційного шуму. Крім того, оскільки мовний сигнал несе в собі дуже велику надлишковість, для повного його подавлення потрібно, щоб потужність завади перевищувала потужність складного тексту приблизно в 5 разів. Якщо ж текст простий і передається повільно, то це перевищення повинно доходити до 25.

І нарешті, ефективність завад залежить від виду модуляції телефонного сигналу. Розглянемо параметри завади окремо для амплітудної, частотної й одно-смугової модуляції сигналу.

Амплітудна модуляція (АМ) є найбільш старим видом, але в силу простоти модуляції і детектування сигналу ще інколи знаходить застосування. При амплітудній модуляції спектр сигналу, як відомо, містить несівну частоту f_o і дві бокові смуги частот. При цьому несуча частота ніякої інформації не несе, а вся інформація міститься в огинаючій бокових смуг. Амплітудний детектор у результаті биття між несівною частотою і боковими смугами частот виділяє огинаючу прийнятого коливання.

Відомо, що навіть при 100% модуляції *(m* = 1) 2/3 усієї потужності зосереджено на несівній і тільки 1/3 приходиться на бокові смуги. При

середніх же значеннях індексу модуляції (m = 0,33) на частку бокових смуг приходиться усього лише 5% загальної потужності.

Але, як уже відзначалося, несівна частота ніякої інформації не має. Отже, і немає необхідності її подавляти. З викладеного випливає, що спектр завади, близький до оптимального, за своєю структурою повинен бути подібним до флуктуаційному шуму, збігатися з боковими смугами і не містити складових, що співпадаючих з несівною частотою сигналу, тому що така складова була б зайвою і на неї дарма витрачалася б потужність передавача завад.

Вище відзначалося, що для подавлення мови необхідно, щоб акустична потужність завади перевищувала акустичну потужність сигналу в 5—25 разів. Іншими словами, для подавлення телефонного сигналу потрібно забезпечити на виході приймача $P_п/P_с$ = 5-25. Звідси випливає, що і на вході приймача відношення потужностей завади і сигналу повинно бути таким же. Щоб визначити коефіцієнт подавлення, потрібно знайти залежність між відношенням завада/сигнал на виході і вході амплітудного детектора. Відношення потужностей завади і сигналу на виході і вході приймача можна записати, як:

$$(P_п/P_с)_{вих.} = \varphi\,(P_п/P_с)_{вх}. \qquad (3.10)$$

З (3.10) випливає, що якщо m = 0,33 і для подавлення зв'язку на виході приймача необхідно мати $P_{пвих}/P_{свих}$ = 5 - 10, то для цього на вході повинно бути $P_{пвх}/P_{свх}$ = 0,4—0,6. Якщо ж характер сигналу такий, що для його подавлення потрібно двадцятипятикратне перевищення потужності завади над потужністю сигналу (чітко озвучений і легкий для сприйняття текст), то на вході приймача потужність завади повинна перевищувати потужність сигналу на 15%.

Таким чином, для подавлення радіотелефонного зв'язку з амплітудною модуляцією потужність завади повинна бути приблизно такою ж, що і потужність сигналу.

Щодо точності суміщення спектрів завади і сигналу варто вказати, що, як показує досвід, разстройка не повинна перевищувати 5% ширини спектра сигналу, тобто, для звичайного телефонного сигналу допустима помилка Δf складає близько 300 Гц.

Що стосується структури оптимальної завади, то як було показано вище, її спектр повинен бути випадковим (нерегулярним) і подібним до спектра сигналу. На практиці оптимальну заваду одержують шляхом модуляції несівної частоти шумами.

Величина разстройки по частоті між сигналом і завадою в даному випадку великої ролі не грає, тому що при частотному детектуванні ефект впливу завади виникає не в результаті виникнення комбінаційних частот (як це має місце при амплітудному детектуванні), а внаслідок подавлення слабкого сигналу сильною завадою. Необхідно лише виконати умову попадання основної потужності завади в смугу пропускання приймача. Це

досягається, якщо розстройка складає не більш 10—20% від величини девіації сигналу.

При впливі частотно-модульованої завади на приймач за відсутності сигналу на виході приймача маємо звичайний шум. Якщо в цей час на вхід приймача починає надходити і сигнал, то на виході чути шум того ж характеру. Тому недосвідчений оператор може не помітити впливу завади. Таку заваду іноді називають “прихованою” [25].

У даний час для здійснення радіотелефонного зв’язку широке застосування знаходить односмуговий радіозв’язок. Це пояснюється головним чином економним використанням спектра частот і підвищеною завадозахищеністю ОС модуляції від навмисних завад. Висока завадозахищеність обумовлюється тим, що прийом сигналу ОС являє собою, власне кажучи, «лінійний» процес , а детектування, як виділення огинної сигналу відсутнє. Його роль виконує останнє перетворення частоти, що переносить спектр сигналу з зони проміжних частот в зону низьких частот.

Як показує аналіз, залежність між співвідношеннями потужностей завади і сигналу на вході і виході приймача при детектуванні сигналу ОС залишається практично без змін.

$$(P_п/P_с)_{вих.} \approx (P_п/P_с)_{вх}. \qquad (3.11)$$

Тому, якщо для подавлення радіотелефонного сигналу необхідно мати на виході приймача перевищення потужності шуму над потужністю сигналу в 5-25 разів то при одно смуговому сигналі приблизно таке ж співвідношення між потужностями завад і сигналу необхідно мати і на вході приймача. По напрузі ж завада повинна перевищувати сигнал на вході приймача, що подавляється, у 2-5 разів.

Структура завади повинна бути близька до структури флуктуаційного шуму, формування і підсилення якого має відомі труднощі. Експерименти показали, що завада, промодельована по частоті низькочастотним шумом, приблизно вдвічі менш ефективна, ніж нормальний шум. Але тому що пік-фактор частотно-модульованого коливання менше за пік-фактор флуктуаційного шуму більш ніж у 2 рази, то заміна останнього частотно-модульованою завадою при рівних середніх потужностях приводить до виграшу по піковій потужності приблизно в 4,5 рази. При цьому для подавлення сигналу ОС потрібно перевищення пікової потужності завади над піковою потужністю сигналу в 0,9—6,6 рази в залежності від характеру тексту, що переданий.

У випадку коли, для збільшення середньої потужності сигналу ОС (і, отже, для підвищення завадозахищеності) застосовується обмеження сигналу по амплітуді (кліпірування), то для подавлення такого сигналу потрібно визначене (незначне) збільшення потужності завади. Допустима неточність суміщення спектра завади зі спектром сигналу ОС складає 100 - 150 Гц.

Характеристика завад, близьких до оптимальних, для подавлення різних видів радіозв’язку приведена в табл. 3.2. Ці види завад реалізовані в більшості існуючих засобів радіозавад.

Основним завданням при організації подавлення радіозв’язку є визначення співвідношення потужностей (напруг) завадового і корисного сигналів на вході приймача, що подавляється. Це досягається в конкретній оперативно – тактичній ситуації. Тобто, треба дати відповідь на запитання: чи достатнє перевищення потужності завади над сигналом для подавлення даної радіолінії в залежності від розміщення (напрямків максимального випромінювання і прийому) та відстаней між приймачем та передавачами сигналу і завади.

При вирішені оперативно – тактичних задач, як правило, здійснюють розрахунки дальностей зв’язку і подавлення, які в подальшому використовуються для розрахунків зон подавлення радіозв’язку (зон простору, де виконуються енергетичні вимоги з подавлення).

3.4. Оптико-електронного подавлення як складова радіоелектронного подавлення систем і засобів зв'язку, розвідки та управління зброєю

Оптико-електронне подавлення полягає в зриві або порушенні нормальної роботи інфрачервоних, телевізійних, лазерних і оптико-візуальних систем і засобів розвідки, наведення, зв'язку і управління зброєю противника за рахунок завадового впливу, застосуванням оптичних цілей, пасток, аерозолів (димів), а також виведенням з ладу оптичних і фоточутливих елементів електронним випромінюванням.

Всю сукупність способів ОЕП можна умовно поділити на дві групи: способи, що забезпечують маскування, або імітацію. Вони в свою чергу, можуть поділятися на активне і пасивне ОЕП [18, 19].

Активне ОЕП ведеться з метою порушення роботи ОЕЗ розвідки і наведення (самонаведення) шляхом створення завад за допомогою потужних джерел випромінювання. До них відносяться лазерні і інфрачервоні (ІЧ) станції (комплекси) завад, а також станції (пристрої), що створюють потужні світлові потоки.

Пасивне ОЕП здійснюється з метою порушення роботи ОЕЗ розвідки і наведення (самонаведення) шляхом створення завад за допомогою аерозолів (димів), оманних цілей (пасток), застосуванням поглинаючих покриттів.

ОЕП відповідно до того, проти яких засобів воно здійснюється, поділяється на кілька видів: лазерне, інфрачервоне (теплове), телевізійне і візуально – оптичне.

Лазерне подавлення систем і засобів. Лазерні джерела випромінювання концентрують енергію у вузькому промені і можуть у залежності від інтенсивності або уражати фоточутливі елементи ОЕЗ, або тимчасово «засліплювати» їх. У першому випадку прийомний пристрій ОЕЗ остаточно виходить з ладу, у другому - відбувається тимчасова втрата його чутливості. При середній інтенсивності лазерного випромінювання знижується чутливість приймального пристрою, що призводить до зменшення дальності дії ОЕЗ. При збільшенні інтенсивності лазерного випромінювання відбувається руйнування приймального пристрою [18, 19].

При дії випромінювання рубінового лазера (λ = 0,69мкм) на передавальну трубку телевізійної апаратури при щільності енергії q_p = 0,5 Дж/см^2 (τi = 10^{-3} с) значно погіршується зображення на екрані приймача, а при 1 q_E = 1...2 Дж/см^2 відбувається повне засвічення триваліcтю до 10 с.

Потрібні значення щільності потужності (q_p, Вт/м^2) і енергії (q_E, Дж/м^2) для різних видів вражаючого впливу приведені в табл. 3.2.

Таблиця 3.2.

Потрібні значення щільностей потужності й енергії.

Вражаючий фактор		q_p.Дж /м^2	□. с	$q_{E,}$ Дж/м^2	Примітка
Екіпажу	Органів зору Опіки шкіри	$10^5/10^7$ 10^{10}	10^{-6} 10^{-4}	$10^{-1}/10$ 10^6	0,69/10,6 мкм
	Променева хвороба	10^5	1-10	10^5- 10^6	
Борт. ОЕЗ	Руйнування фотоприймача Осліплення	10^6 10^5	10^{-3} 10^{-3}	10^3 10^2	
	Руйнування	10^{10}- 10^{14}	10^{-3}	10^7- 10^{11}	
Носія	Нагрів	10^8- 10^{10}	10^{-2}- 10^{-4}	10^4- 10^8	$t_{нагр}=\frac{1}{2}t^0_{пл}$

Дальність дії лазерної зброї для досягнення заданого уражаючого впливу можна визначити по наступній формулі:

$$Д = \frac{1}{\theta_л}\sqrt{\frac{E_л}{q_E}}\,e^{-0,5\gamma_{\lambda,н}Д}, \qquad (3.12)$$

де θл – розходження (ширина) промінню лазера, град; $E_л$ – енергія випромінювання лазера, Дж; q_E – щільність енергії, яка необхідна для нанесення об'єкту необхідного збитку, Дж/м^2; $\gamma_{\lambda,н}$ – коефіцієнт загасання в атмосфері.

Ослаблення енергії лазерного випромінювання в атмосфері при різних метеоумовах може складати $\gamma_{\lambda,н}$ = *(0,005 ... 0,5) км*$^{-1}$.

Так, при досягнутій величині енергії 10^6 Дж і коефіцієнт загасання 0,3 км$^{-1}$ лазерний комплекс може здійснювати ураження органів зору на дальності 30—35 км, засвічування бортових ОЕЗ на 25—30 км, ураження ОЕЗ на 10—20 км, а руйнування конструкції носія на 3—5 км.

Основним фактором, що визначає можливість подавлення лазерних голівок самонаведення з напрямків поза полем зору їхньої оптичної системи, є багаторазове перевідбиття і розсіювання випромінюваннь конструктивними елементами їх приймальної системи. При збільшенні затуманення атмосфери певний внесок у сумарний ефект може давати також і розсіювання випромінювання атмосферою на трасі розповсюдження. Експериментально підтверджена можливість подавлення вузькосмугових лазерних головок самонаведення (ЛГСН) лазерним випромінюванням з напрямків, що на порядок перевищують миттєвий кут поля зору їхньої приймальної системи. При цьому відношення потужності завади до сигналу на вході оптичної системи повинно бути приблизно 40 дБ.

Таким чином, для подавлення лазерних систем і засобів розвідки, наведення (самонаведення), зв'язку і управління зброєю можна застосовувати потужні джерела лазерного випромінювання для безпосереднього

засвічування приймача або для створення оманних відволікаючих джерел – підсвічування водяної (наземної) поверхні лазерним променем.

До методів лазерного подавлення (пасивного) відноситься також, маскування за допомогою аерозолів (димів). Ослаблення димами лазерного випромінювання може бути визначене з рівняння:

$$T = \frac{1}{cb}, \tag{3.13}$$

де b — товщина шару диму; с — концентрація диму в шарі.

Експерименти показали, що маскуючі властивості диму для оптичних квантових генераторів виявилися в основному такими ж, як і для звичайних джерел випромінювання.

Подавлення інфрачервоних систем і засобів розвідки і управління

До методів інфрачервоного подавлення відносяться: теплове маскування об’єктів, створення оманних теплових цілей і активних теплових завад [18-21].

Теплове маскування здійснюється зменшенням теплового поля об’єктів, що прикриваються (танків, літаків, кораблів та ін.), і застосуванням поглинаючих матеріалів (покриттів).

Розглянемо зменшення теплової контрастності на прикладі найбільшого (контрастного) об’єкту – корабля.

Теплове поле цього об’єкта прикриття складається з двох компонентів: власного випромінювання об’єкта й відбитої складової. Для старих проектів кораблів, що відрізнялися великим ступенем нагрівання зовнішньої поверхні відносно навколишнього середовища, головним компонентом є складова власного випромінювання. Для сучасних і перспективних кораблів характерні невеликі відмінності температур випромінюючих зон від температур навколишнього середовища, тому зростає роль відбитої складової, а в денних умовах для більшої частини робочого діапазону спектра відбита складова практично визначає величину поля в цілому.

Власне теплове поле корабля є складною функцією великої кількості параметрів: температури і коефіцієнтів випромінювання зовнішньої поверхні корабля, навколишньої атмосфери, величини площ проекцій різних зон корабля в напрямку спостереження, а також відстані між ними.

Точний розрахунок теплового поля, в якому враховувалися б як власна, так і відбита складова об’єктів, представляє досить складне завдання.

Найбільш складний розподіл температур на зовнішній поверхні мають кораблі та літаки з високотемпературними зовнішніми поверхнями. Вони звичайно характеризуються декількома зонами з різною температурою. Найбільшу питому вагу у випромінюванні мають газовий факел, димові отвори і кожухи труб. Максимум випромінювання корпуса знаходиться в діапазоні довжин хвиль біля 10 мкм. Максимум випромінювання кожуху труб (для кораблів) зсунутий у короткохвильову частину спектра 3-7 мкм. На

теплове поле істотно впливає фон. За рахунок фона контрастне випромінювання кораблів, як правило, стає значно меншим абсолютного, крім того, просторово-часові зміни випромінювання фона є найбільш істотним фактором в утворенні завад роботі інфрачервоних приладів.

Випромінювання фону змінює спектральний розподіл контрастного випромінювання кораблів, зсуваючи їх максимум у короткохвильову частину спектру.

Визначення контрастного випромінювання кораблів за спектром показало, що воно в основному зосереджене в двох діапазонах довжин хвиль: від 2 мкм до 5 мкм і від 7,5 мкм до 14 мкм, причому максимуми лежать у діапазонах 4 мкм і 9 мкм. Короткохвильове випромінювання визначається в основному тепловим полем поверхні труб, довгохвильове - випромінюванням корпусу і надбудов.

Температура зовнішньої поверхні корабля, а отже, величина теплового поля в значній мірі залежить від температури навколишнього середовища, а контрастне випромінювання корабля визначається, головним чином, різницею значень температури морської поверхні й атмосфери.

Зменшення теплового поля корабля може здійснюватися такими способами:

– зменшенням температури поверхні корабля;
– застосуванням спеціальних покрить і фарб.

Для зниження температури корпусу використовуються: газоповітряне охолодження випускних газів шляхом природного підмішування атмосферного повітря; вприскування в потік випускних газів дрібно розпиленої забортної води; охолодження зовнішньої поверхні кожуху димаря шляхом циркуляції атмосферного повітря в просторі між кожухом димаря і змішувачем випускних газів; теплоізоляція стінок змішувача, орієнтація зрізів газовипускних пристроїв під «вухами», за яких сильно нагріті поверхні газоходів не попадають у поле зору інфрачервоних пристроїв засобів розвідки противника. Крім зазначених заходів для зменшення теплового поля корабля застосовують аерозольні поглинаючі середовища (завіси, штучні тумани). Застосування аерозолів штучно порушує прозорість атмосфери, що приводить до ослаблення інфрачервоного випромінювання. Ослаблення випромінювання відбувається за рахунок поглинання енергії парами і розсіюванням її зваженими в повітрі частками, коефіцієнт переломлення яких відмінний від коефіцієнту переломлення середовища [23-25].

Спеціальні покриття і фарби мають у інфрачервоній області коефіцієнт перевипромінювання не більший 0,2...0,3, у той час як звичайні фарби мають коефіцієнт 0,6...0,7.

Ведуться роботи з розробки аерозольних сумішей, за допомогою яких можуть бути створені оманні теплові цілі в результаті розпилювання в атмосфері речовин, здатних виділяти тепло в результаті хімічної взаємодії з киснем повітря, атмосферною вологою або спеціальними окислювачами.

Для створення активних теплових завад, що призводять до перевантаження інфрачервоних приймачів, повинні застосовуватися потужні

джерела інфрачервоного випромінювання. В якості таких джерел можуть бути використані оптичні квантові генератори. Однак поки що цей метод теплового подавлення практичного застосування не одержав.

Подавлення телевізійних і візуально-оптичних засобів. До методів телевізійного подавлення відносяться [18, 19, 23-25]:

– засвічування телевізійних приймачів потужним джерелом випромінювання;

– створення оманних дезінформуючих цілей;

– оптичне маскування об’єктів.

Подавлення телевізійних систем розвідки й управління зброєю можна шляхом їх засвічення некогерентними сітки на основі поліефірного волокна із сажовим просоченням.

Хибні (оманні) теплові цілі створюються шляхом спалювання спеціальних речовин, а також за допомогою електричних, хімічних чи інших джерел тепла.

Дальність подавлення телевізійних систем розвідки й управління зброєю може бути визначена по формулі, отриманої за експериментальними даними:

$$Dn = \sqrt{\frac{1}{Ел}}\, K \qquad (3.14)$$

де, I – сила світла джерела випромінювання завади, (кд); $Ел$ – освітленість на фотокатоді телевізійної камери (лк), що потрібно створити для заданого ефекту подавлення; K – коефіцієнт ослаблення світлового потоку; $Дп$ – дальність подавлення, (м).

Для оптичного маскування застосовують як аерозольні засоби (димозавіси), так і оманні оптичні цілі. Вони створюються з використанням макетів, що імітують кораблі, а також за допомогою диму. В останньому випадку дим під впливом потоків повітря розстеляється над поверхнею води і приймає контури, що на великих відстанях (15-20 км) можуть бути сприйняті за силует надводного корабля.

Засвічування телевізійних приймачів (ТП) та оптико-візуальних засобів (ОВЗ) потужними джерелами випромінювання практичного застосування поки ще не знайшло.

Пасивне подавлення ТП та ОВЗ полягає в застосуванні димів, аерозолів, екранів, масок, сіток і інших засобів для приховання своїх об’єктів.

3.5. Гідроакустичне подавлення як складова радіоелектронного подавлення систем і засобів розвідки і управління

Широке використання підводними човнами і протичовновими силами гідроакустичних засобів різного призначення (гідролокаторів, шумопеленгаторних станцій, станцій виявлення гідроакустичних сигналів, гідроакустичних буїв, тощо) обумовлює важливу роль гідроакустичного

подавлення (ГАП). Воно значно підвищує бойову стійкість і ударні можливості визначених сил.

Гідроакустичному подавленню як одному з видів радіоелектронного подавлення властива низка закономірностей, які є загальними для усіх видів РЕП. Це стосується насамперед, методів подавлення. Гідроакустичне подавлення може здійснюватися впливом на гідроакустичні засоби маскуючими завадами, зменшенням гідроакустичної помітності об'єктів, впливом на водяне середовище й імітацією гідроакустичних сигналів і шумів кораблів [18-20].

Поряд із загальними закономірностями гідроакустичне подавлення має і цілий перелік особливостей, обумовлених, насамперед, видом використовуваної енергії й умовами її поширення. Тому розглянемо більш докладно методи гідроакустичного подавлення, принципи їх реалізації при побудові засобів, а також основні види засобів ГАП, використані підводними човнами і надводними кораблями,

Активні методи ГАП. До активних методів ГАП відносяться методи створення активних і пасивних завад за допомогою станцій гідроакустичних завад, імітаційних патронів, а також використання оманних гідроакустичних цілей у вигляді буксированих, дрейфуючих і самохідних імітаторів.

Фактично сутність всіх активних методів зводиться до імітації гідроакустичних сигналів.

Активна імітація гідроакустичних сигналів. Імітація гідроакустичних сигналів здійснюється по вторинному і первинному гідроакустичних полях. У першому випадку імітуються зондуючі сигнали, а в другому - шуми кораблів. При цьому імітація здійснюється за всіми або тільки за деякими параметрами гідроакустичного сигналу в залежності від числа параметрів, які використовуються противником для класифікації.

Для імітації шумів кораблів можуть бути використані два способи:

спосіб фонограмування, заснований на магнітному записі і наступному відтворенні реального шуму об'єкту, що імітується;

спосіб фізичного моделювання, заснований на використанні шумових генераторів.

При використанні першого методу реальний шум з виходу шумопеленгатора записується на магнітний носій. При цьому об'єкт, шуми якого записуються, може за заздалегідь установленою програмою змінювати швидкість, курс, що впливає на структуру записаного шуму і забезпечує при відтворенні підвищення якості імітації.

Основна перевага методу магнітного запису полягає у високій ймовірності імітації даного об'єкта при даному варіанту його маневрування. При необхідності імітації іншого об'єкта й іншого варіанту необхідна заміна фонограми, що не завжди можна, якщо станція ГАП автономна.

Зазначений недолік не є характерним для методу фізичного моделювання. Шляхом застосування режимів роботи шумових генераторів можна здійснювати компонування шумів, характерних для кожного з імітованих об'єктів при будь-якому варіанті маневрування.

Для імітації відбитих сигналів активними засобами ГАП використовується ретрансляція сигналів, що зондують, гідролокаторів. Даний спосіб припускає магнітний запис прямого сигналу, що відповідає зміні його параметрів, наступне відтворення і перевипромінювання.

У залежності від виду імітатора знаходиться і кількість параметрів прямого сигналу, що підлягають зміні при ретрансляції. У самохідних імітаторах змінюється потужність з метою створення такого сигналу, який відповідав би потужності сигналу відбитого від імітованого об'єкта. Крім того, у самохідних імітаторів імітується зміна потужності і тривалості сигналу в залежності від зміни курсового кута. У дрейфуючих імітаторів з метою імітації руху додатково імітується ефект Доплера і зміна відстані у часі.

Пасивна імітація гідроакустичних сигналів. Для імітації відбитих сигналів пасивними засобами використовуються переважно завіси, що складаються з газових пухирців. Відбиваючи прямі сигнали гідролокаторів, завіси створюють відбиті сигнали, подібні до сигналів, відбитих від корпусу нерухомого корабля, оскільки при відбиванні від нерухомої завіси ефект Доплера не має місця.

Принцип дії газових завіс заснований на наступних фізичних явищах.

Газовий пухирець являє собою механічну коливальну систему з власною резонансною частотою. Як усяка коливальна система, при впливі енергії зовнішніх коливань (коливання несувної частоти гідролокатора) пухирець починає коливатися, частково розсіюючи і частково поглинаючи енергію, що падає на нього.

Якщо резонансна частота пухирців більше за частоту гідролокатора, що опромінює завісу ($fo > fглс$), більша частина енергії, що падає на завісу поглинається, а якщо $fo < fглс$ то більша частина енергії розсіюється.

Розсіюючі і поглинаючі властивості пухирців характеризуються кількісно ефективними площами поперечного перерізу розсіювання σs, і поглинання σa відповідно. Величини цих параметрів залежать від розмірів пухирців, частоти, виду використовуваного газу, тиску (глибини) і т.д.

Створення газових завіс може здійснюватися за допомогою механічного, електролітичного і хімічного способів.

При механічному способі завіса створюється шляхом продування газу через калібровані отвори і пористі матеріали. Запас газу зберігається в спеціальних балонах. Електролітичний спосіб заснований на розкладанні морської води електричним струмом і вимагає великих енергетичних витрат. Хімічний спосіб передбачає створення газових завіс за рахунок реакції спеціальної речовини з морською водою, що супроводжується виділенням досить великих кількостей газу. В даний час для цих цілей використовують гідриди лужних елементів і, головним чином, гідрид літію.

Зменшення гідроакустичної помітності. Зменшення гідроакустичної помітності об'єктів здійснюється по вторинному і первинному гідроакустичних полях. У першому випадку зменшується величина відбитих

сигналів за рахунок погіршення відбивної здатності маскованого об’єкта, а в другому зменшується його шумність.

3.6. Методика оцінки ефективності ведення радіоелектронного подавлення противником угруповання засобів зв’язку

Нехай СУ органами державної влади, що розглядається як учасник електронного конфлікту із засобами РЕП противника – це система масового обслуговування (СМО) з очікуванням, що містить n каналів обслуговування (передачі, приймання інформації).

На вхід цієї СУ в динаміці ведення гібридних воєнних дій впливає потік заявок (розпоряджень, повідомлень, команд, донесень) з пунктів державного управління усіх ланок. Потік заявок – найпростіший (відповідає вимогам стаціонарності, ординарності та відсутності післядії). Для вхідного потоку, який розглядається, число вимог k на деякому визначеному відрізку часу нехай буде розподілено за законом Пуассона (пуассонівський потік) з параметром λ [27]:

$$P_k(t) = \frac{(\lambda t)^k}{k!} e^{-\lambda t}. \tag{3.15}$$

Час обслуговування – випадкова величина, що розподілена за експоненційним законом:

$$f(t) = \begin{cases} \nu \cdot \exp^{-\nu t} \text{ при } t > 0, \\ 0, \text{ при } t \le 0 \end{cases} \tag{3.16}$$

з математичним очікуванням $M\{\Theta\} = 1/\nu$ [27].

Одним з основних параметрів, що характеризує здатність СУ державного управління виконувати свої функції в сучасних умовах особливого періоду є математичне очікування часу $M\{\gamma\}$, впродовж якого вимога (розпорядження, донесення), що надійшла у деякий час $t_{\text{нз}}$ очікує початку обслуговування (наприклад, початок доповіді по технічним засобам зв’язку).

СУ виконує свої функції у повному обсязі в умовах електронного конфлікту тоді та лише тоді, коли:

$$M\{\gamma\} \le \gamma_{\text{доп}}, \tag{3.17}$$

де $\gamma_{\text{доп}}$. – критичний час „старіння” інформації у системі управління, при якому виникають досягаються відповідні втрати своєчасності доставки інформації.

Параметр $\gamma_{\text{доп}}$ визначається інтенсивністю “старіння” інформації у загальному циклі державного управління, що розглядається. При цьому під терміном “старіння” інформації будемо розуміти часткову або повну втрату інформативності розввідданих, команд управління тими, кому вони призначені, з плином часу. Інтенсивність “старіння” інформації залежить від тактико-технічних характеристик кожної конкретної системи державного управління, характеру дій терористичних сил тощо.

Для визначення вимог до величини $\gamma_{\text{доп}}$ охарактеризуємо СУ військами (силами) і зброєю угруповання противника, що протистоїть, ймовірністю $P_{\text{су}}$ події, яка полягає в тому, що час розв’язання завдань з управління $t_{\text{упр}_{\text{ео}}}$ на конкретному етапі ведення операції (бою) не перевищує величини $t_{\text{в}}$ потрібного часу випередження [27]:

$$P_{\text{су}}(\gamma) = P\left\{t_{\text{упр}_{\text{ео}}}(\gamma) \langle t_{\text{в}}\right\} = \int_0^{t_{\text{в}}} F_{\text{упр}}(t_{\text{упр}_{\text{ео}}}(\gamma))dt, \qquad (3.18)$$

де

$$t_{\text{упр}_{\text{ео}}}(\gamma) = t_{\text{р}_{\text{сзв}}} + t_{\text{обр}} + t_{\text{вик}} + \gamma, \qquad (3.19)$$

$t_{\text{р}_{\text{сзв}}}$ – час добування розвід відомостей, формування доповідей про стан та положення справ у визначеному адміністративно-територіальному районі;

$t_{\text{обр}}$ – час, що витрачається керівниками державних органів управління на отримання, збирання, обробку даних, оцінку обстановки, прийняття рішення, постановку та доведення завдань до підлеглих (час обробки інформації командуванням);

$t_{\text{вик}}$ – час, необхідний підлеглим підрозділам на усвідомлення та виконання поставлених завдань;

$t_{\text{в}}$ – необхідний час випередження дій противника, зміни позиційного району, тощо;

$F_{\text{упр}}(t_{\text{упр}_{\text{ео}}}(\gamma))$ – функція розподілу часу управління на конкретному етапі проведення гібридних дій;

γ – час очікування початку обміну повідомленнями у СУ державного управління.

Не втрачаючи загальності викладення та беручи до уваги, що найбільш суттєвий вплив на процес „старіння” інформації у динаміці ведення операції (бою) має компонента $t_{\text{обр}}$, спростимо вираз (3.19) до вигляду:

$$t_{\text{упр}_{\text{ео}}} \approx t_{\text{обр}} + \gamma. \tag{3.20}$$

При проведенні оперативно-тактичних розрахунків визначимо $F_{\text{упр}}(t)$ у вигляді:

$$F(t_{\text{упр}_{\text{ео}}}(\gamma)) = 1 - \sum_{i=1}^{m} e^{-\alpha_i (t_{\text{обр}} + \gamma)} \prod_{j \neq 1}^{m} \frac{\alpha_j}{\alpha_j - \alpha_i}, \tag{3.21}$$

де $\alpha_i = м_i n_i - \lambda_{\text{вх}_i}$; $\lambda_{\text{вх}_i}$ – інтенсивність вхідного потоку даних на кожній з фаз етапу операції (бою), що надійшли на обробку командуванню; $м_i$ – інтенсивність обробки в i - й фазі етапу операції (бою); j – номер фази етапу обробки; m – кількість фаз етапу операції (бою).

Підставляючи вираз (3.20) у вираз (3.21), враховуючи умову (3.19) та вважаючи, що має місце розподіл часу „старіння” за експоненційним законом з інтенсивністю, шо дорівнює $1/t_{\text{в}}$, ймовірність $P_{\text{су}}$ визначимо у вигляді [27]:

$$P_{\text{су}}(t_{\text{упр}}(\gamma)) = \int_0^{t_{\text{в}}} e^{\frac{t_{\text{упр}}(\gamma)}{t_{\text{в}}}} \left[\sum_{i=1}^{m} \alpha_i e^{-\alpha_i} t_{\text{упр}}(\gamma) \prod_{\substack{j=1 \\ i \neq j}}^{m} \frac{\alpha_i}{\alpha_j - \alpha_i} \right] dt_{\text{упр}}(\gamma). \tag{3.22}$$

Як приклад розраховані типові величини параметра $\gamma_{\text{доп}}$ для різних ланок управління у системах управління військами (силами) і зброєю провідних країн світу, за яких досягається $P_{\text{су}} \leq 0,2$:

- тактична ланка управління – 10 : 20 хвилин;
- оперативно-тактична ланка управління – 20: 25 хвилин;
- оперативна ланка управління – 30: 40 хвилин;
- оперативно-стратегічна ланка управління – 40: 60 хвилин.

Вибір показника та формування критеріїв оцінки ефективності ведення РЕП СУ військами (силами) і зброєю противника. Вплив на СУ військами (силами) і зброєю противника шляхом вогневого ураження (ВУ) та РЕП її вузлів та ліній радіозв’язку, систем та засобів передачі інформації призводить до затримки кожного повідомлення в системі і, внаслідок цього, до часткових збоїв або повної втрати оперативної цінності інформації через переривання та, як наслідок, багатократне повторення повідомлень. Зрозуміло, невиконання вимоги (3.19) у складних умовах ведення сучасних операцій

(бойових дій) веде до ускладнення, зриву або повного порушення управління військами (силами) і зброєю противника. При цьому у запропонованій моделі СУ як СМО з очікуванням в умовах ведення РЕП кількість m каналів обслуговування визначимо у вигляді [27]:

$$m = n - n_{\text{РЕП}} - n_{\text{ВУ}}, \tag{3.23}$$

де $n_{\text{РЕП}}$ – кількість каналів передачі інформації, що подавлені за допомогою засобів РЕП; $n_{\text{ВУ}}$ – кількість каналів передачі інформації, що знищені під час ВУ вузлів зв'язку.

Тому, показником оцінки ефективності ведення РЕП в операції (бою) є математичне сподівання часу очікування обслуговування $M\{\gamma\}$ у СУ. Показником оцінки ефективності ведення РЕП також може бути пропускна здатність окремої лінії передачі інформації $N_{\text{лп}}$, напрямку радіозв'язку $N_{\text{нз}}$, системи зв'язку в цілому $N_{\text{су}}$ в умовах ведення РЕП.

Критерії оцінки ефективності ведення РЕП (3.17) можна конкретизувати стосовно до відомих ступенів дезорганізації СУ військами (силами) і зброєю противника, вибираючи $\gamma_{\text{доп}}$. із відповідних нерівностей:

Конкретизуємо порядок визначення параметра $M\{\gamma\}$ для визначеної моделі СУ військами (силами) і зброєю противника. Для цього визначимо закон розподілу $F_{\gamma}(z)$ випадкової величини γ.

Нехай $x(t)$ – число вимог, що знаходяться у системі у момент часу t. Тоді ймовірність $P(\gamma \geq z)$, $z > 0$ визначимо у вигляді множення двох ймовірностей:

$$P(\gamma \geq z) = \Pi \cdot \exp\left\{-n \cdot \nu \cdot z \cdot \left(1 - \frac{\lambda}{n \cdot \nu}\right)\right\}, \tag{3.24}$$

де

$$\Pi = \frac{1}{n!} \cdot p_0 \cdot \left(\frac{\lambda}{\nu}\right)^n \cdot \frac{1}{1 - \dfrac{\lambda}{n \cdot \nu}}; \tag{3.25}$$

$$p_0 = \frac{1}{\displaystyle\sum_{j=0}^{n-1} \frac{1}{j!} \cdot \left(\frac{\lambda}{\nu}\right)^j + \frac{1}{n!} \cdot \left(\frac{\lambda}{\nu}\right)^n \cdot \frac{1}{1 - \dfrac{\lambda}{n \cdot \nu}}}. \tag{3.26}$$

Враховуючи вирази (3.24), (3.25) та (3.26), після перетворень маємо [27]:

$$F_\gamma(z)=\begin{cases} 0 \quad \text{при } z<0; \\ 1-\Pi\cdot\exp\left\{-n\nu z\cdot\left(1-\dfrac{\lambda}{n\nu}\right)\right\} \quad \text{при} \quad z>0. \end{cases} \tag{3.27}$$

Враховуючи результат (1.17), вираз для визначення показника ефективності РЕП СУ $M\{\gamma\}$ одержуємо [27]:

$$M\{\gamma\}=\frac{\Pi}{n\cdot\nu-\lambda} \tag{3.28}$$

Показник (3.28) є функцією від кількості каналів, що підпадають під вплив, та середнього часу тривалості повідомлення у системі управління військами (силами) і зброєю противника. На рис. 3.2 наведені графічні залежності значення показника $M\{\gamma\}$ від співвідношення n/λ в умовах відсутності впливу (рис. 3.2) та при здійсненні РЕП та ВУ (рис. 3.3) елементів системи управління військами (силами) і зброєю у тактичній ланці управління, середній час обслуговування повідомлення у каналі радіозв'язку дорівнює відповідно 2, 3, 4, 5 хвилин.

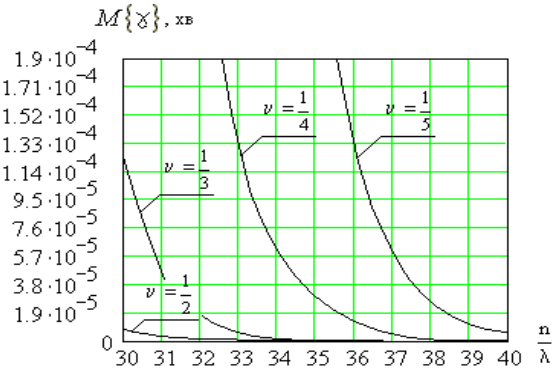


Рис. 3.2

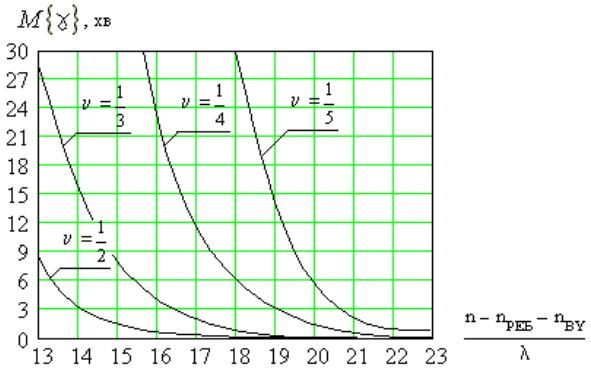


Рис. 3.3

Аналіз наведених графічних результатів свідчить, що у адміністративній ланці село – територіальна громада зрив управління виникає тоді, коли РЕП та ВУ зазнають не менше 77% каналів управління від загальної кількості каналів у СУ.

Таким чином, запропонована методика дозволяє проводити оцінку ефективності ведення РЕП в операціях (бойових діях). Зазначимо, що запропонована методика не заперечує відомих підходів, а дозволяє проводити уточнену оцінку ефективності ведення РЕП в операціях (бойових діях) з урахуванням особливостей функціонування СУ військами (силами) і зброєю противника та їх тактико-технічних характеристик. Отримані графічні результати нормовані та можуть застосовуватись в оперативно-тактичних

розрахунках, що проводять органи державного управління всіх рівнів під час реагування на кризові ситуації.

3.7. Методика розробки сценаріїв радіоелектронного та електромагнітного подавлення засобів зв'язку

Теперішній момент часу характеризується можливістю різкого загострення ситуації на Сході та Півдні України, переходом російсько-терористичних військ до широкомасштабної збройної агресії проти України або веденням масштабних терористичних дій.

В таких умовах першочерговими об'єктами (Об) РП та ЕМП противника [2] можуть стати як елементи радіосегмента ТП НТМ, що розташовані в зоні проведення операції об'єднаних сил (ООС), так і ті, що знаходяться на решті території України.

В цих нових, для системи Держспецзв'язку, умовах можливого створення противником складної сигнально-завадової обстановки (ССЗО), якісне виконання завдань за призначенням вимагає розробки та застосування у приймачах адаптивних до сценаріїв ССЗО алгоритмів завадозахисту. Це потребує автоматизованого розпізнавання станів ССЗО за апріорним словником нечітких сигнатур для подальшої обробки корисного сигналу.

Вирішення цього завдання можливо із розвитком галузі радіоелектронної боротьби (РЕБ) та теорії завадозахисту сценарного підходу [32-28]. Одним із завдань, що виникає при цьому, є розробка методики визначення сценаріїв РП та ЕМП (застосування новітніх засобів РП та ЕМП) Російською Федерацією ТП НТМ в реальних бойових ситуаціях та у гібридних діях на території України.

Поняття "сценарій РП та ЕМП" нове для теорії радіоелектронної боротьби та завадозахищеності.

Існує безліч різних визначень поняття "сценарій". Одне з них трактує сценарій як – послідовність прогнозованих подій у часі [33-39].

Загальними характеристиками сценаріїв є: гіпотетична природа сценарію; опис альтернативних варіантів майбутнього; опис майбутнього як кінцевого результату або ж як ланцюжка подій; причинно-наслідковий зв'язок і наявність внутрішньої узгодженості; можливість використовувати сценарій як базис для дій; описова природа; достовірність; пояснювальна природа; з'єднання минулого, сьогодення і майбутнього [4, 5].

В результаті узагальнення цих характеристик введемо в якості найбільш загального визначення сценарію радіо- та електромагнітного подавлення ТП НТМ наступне: сценарій РП та ЕМП ТП НТМ – це послідовний опис альтернативних гіпотетично можливих варіантів застосування засобів РП та ЕМП в майбутніх гібридних діях, який відображає різні можливі тактичні та оперативно-тактичні ситуації їх застосування, а також який може бути вихідними даними для розробки методів та способів протидії зриву інформаційного обміну у ТП НТМ в умовах РП та ЕМП противника. Визначення сценаріїв РП та ЕМП систем зв'язку є завданням проведення

сценарного дослідження. Кожне таке дослідження має свою специфіку і відрізняється від інших.

Аналіз останніх публікацій за проблематикою та визначення невирішених раніше частин загальної проблеми.

Питання оптимізації розподілу засобів РП за об'єктами впливу розглянуті в [35-36]. Однак, у відомій літературі можливі сценарії та способи радіо та електромагнітного подавлення ТП НТМ не досліджені. Постановки задачі раціонального розподілу ресурсу неоднорідних засобів радіоелектронної боротьби противника за елементами ТП НТМ для подальшої розробки методики визначення сценаріїв її РП в умовах ведення гібридних бойових та терористичних дій проведена в [36]. Методика оцінки показників якості порушення інформаційного обміну в ТП НТМ в умовах ведення РП розроблена в [27-28,32-33]. Однак, у відомій авторам літературі, методика визначення сценаріїв РП та ЕМП радіоканалів зв'язку ТП НТМ для синтезу адаптивних алгоритмів їх завадозахисту з урахуванням можливих сценаріїв складної сигнально-завадової обстановки не розроблена у повному обсязі.

Для подальшої розробки методів та способів завадозахисту систем зв'язку необхідно розробити методику визначення сценаріїв РП та ЕМП ТП НТМ та складної сигнально-завадової обстановки для синтезу адаптивних алгоритмів завадозахисту в умовах ведення гібридних дій на території України.

Це можливо зробити основі розвитку математичного апарату теорій вирішення багатоіндексних задач оптимального розподілу різнорідного ресурсу [35, 36], математичної статистики [5] та ідентифікації систем в практичну площину застосування сценарного підходу для визначення сценаріїв РП та ЕМП ТП НТМ та ССЗО під час ведення гібридних та терористичних дій.

Проведені дослідження показали, що методика містить п'ять етапів, рис. 3.4:

– I – формування множини вхідних даних;

– II – визначення множини гіпотетично можливих засобів деструктивного впливу противника на елементи ТП НТМ у гібридних діях;

– III – оптимізацію розподілу ресурсу різнорідних засобів РП та ЕМП противника, що можуть бути застосовані для визначення сценаріїв РП та ЕМП противника на ТП НТМ;

– IV – визначення послідовності застосування засобів РП та ЕМП противника у часі та просторі при виконанні підрозділами Держспецзв'язку завдань за призначенням в умовах РЕБ противника при веденні гібридних дій;

– V – визначення можливих сценаріїв СЗО та масивів їх сигнатур та ознак під час застосування підрозділів Держспецзв'язку в умовах РП та ЕМП противника, прогнозування її змін у часі. Розробка математичних моделей сценаріїв складної СЗО для формування апріорних масивів сигнатур та ознак для розпізнавання сценаріїв.

Перший етап методики труднощів не викликає. На цьому етапі проводиться формування множини вхідних даних шляхом аналізу гіпотетично

можливих засобів РП, ЕМП противника та загальної (РЕО). При цьому в доповнення до загальноприйнятих та визначених заходів необхідно [38, 39]:

– проаналізувати порядок комплексного застосування засобів радіозв'язку ТП НТМ (типи супутникових засобів передачі інформації, радіорелейних та УКХ засобів зв'язку, частотно-часові параметри їх сигналів та швидкості передачі даних у лініях, утворених ними, взаємозамінність, види модуляції (маніпуляції) тощо;

– проаналізувати можливості частин (підрозділів) радіоелектронної розвідки та РЕБ російсько-терористичних військ;

– окремої оцінки вимагають можливості засобів ЕМП противника та їх засоби доставки до об'єктів ураження під час гібридних дій та терористичної діяльності на території України.

На основі результатів оцінки радіоелектронної обстановки формується множина вихідних даних для визначення сценаріїв деструктивного радіоелектронного впливу на елементи ТП НТМ.

На другому етапі методики обґрунтовуються гіпотетично придатні для виконання завдань з РП, ЕМП засоби деструктивного впливу, що є (або можуть бути в перспективі) на озброєнні російсько-терористичних військ.

На третьому етапі методики проводиться оптимізація розподілу ресурсу існуючих та гіпотетично можливих засобів РП та ЕМП противника за об'єктами впливу ТП НТМ для формування визначення сценаріїв деструктивного впливу.

На четвертому етапі методики визначаються просторові, часові показники та порядок застосування засобів РП та ЕМП по елементах ТП НТМ. Це потребує детального врахування завдань, тактичних та оперативно-тактичних показників ведення гібридних дій та терористичної діяльності

У розробленій методиці наукового вдосконалення набули:

– постановка зворотної задачі векторної оптимізації розподілу ресурсу неоднорідних засобів РП та ЕМП за елементами ТП НТМ [7];

– пониження мірності векторної задачі оптимізації та перетворення її до виду однокритеріальної задачі розподілу різнорідних засобів РП та ЕМП по елементах ТП НТМ;

– порядок вирішення зворотної однокритеріальної задачі раціонального розподілу різнорідних засобів РП з врахуванням обмежень на ефективність зриву інформаційного обміну у ТП НТМ [6];

– порядок оцінки ефективності порушення інформаційного обміну у ТП НТМ та обґрунтування обмежень до неї [8].

Не гублячи загальності викладення, конкретизуємо порядок практичного застосування отриманих результатів при визначенні сценаріїв РП та ЕМП ТП НТМ.

Нехай, за результатами аналізу (РЕО) визначено що противник для вирішення завдань з РП та ЕМП ТП НТМ може гіпотетично застосувати засоби РП та ЕМП k типів, $k = 1, 2, ..., \nu$.

Противник під час підготовки та ведення гібридних дій (терористичної діяльності) ставить завдання зірвати обмін інформацією каналами державного

управління у певному територіальному районі України, що залежить від масштабів гібридних дій. При цьому, в залежності від масштабів гібридних дій, противник вирішує j часткових завдань $Z_1, Z_2, ..., Z_m$, $j = 1,2,..., m$, рис. 3.4. Зокрема, під час ведення гібридних бойових дій завданнями можуть полягати в наступному:

Наприклад, здійснення за єдиним замислом та планом РП та ЕМП засобів ТП НТМ в наступних просторових масштабах (рис. 3.4):

– ($j = 1$) – до 100 км від лінії розмежування;
– ($j = 2$) – до 250 км від лінії розмежування;
– ($j = 3$) – до 500 км від лінії розмежування;
– ($j = 4$) – на всю глибину території України.

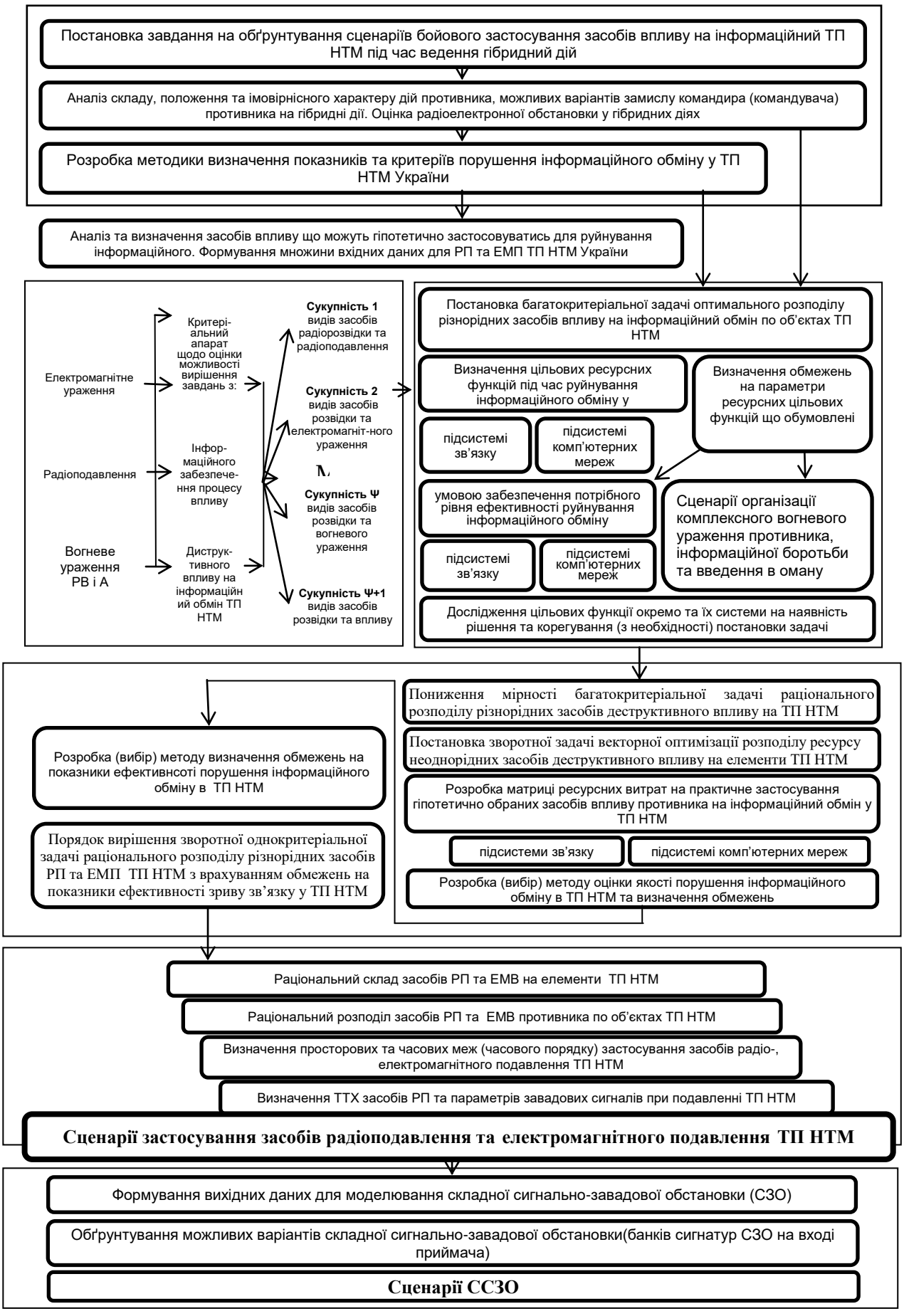


Рис. 3.4. Структура методики визначення сценаріїв РП, ЕМП ТП НТМ та складної сигнально-завадової обстановки

При цьому вважається, що завдання з подавлення інших видів зв'язку в інтересах державного управління повністю виконані окремими діями.

В рамках вирішення кожного j-го завдання за результатами попередньої РР противником викрито n_j типів функціонально незалежних елементів ТП НТМ – об'єктів (Об) РП та ЕМП. Q_{jz} – загальна кількість об'єктів z-го типу (терміналів ТП), $z = 1,2,...,n_j$, рис. 2. Кожен об'єкт організовує одну радіолінію ТП, яка за ТТХ терміналу є багатоканальною і, в залежності від ланки управління, включає в себе від одиниць до десятків радіоканалів.

На рис. 3.5 умовно схематично показані радіолінії ТП НТМ, які організовані об'єктами РП та ЕМП на глибину завдання Z_j , j=1, 2, 3 та 4 відповідно.

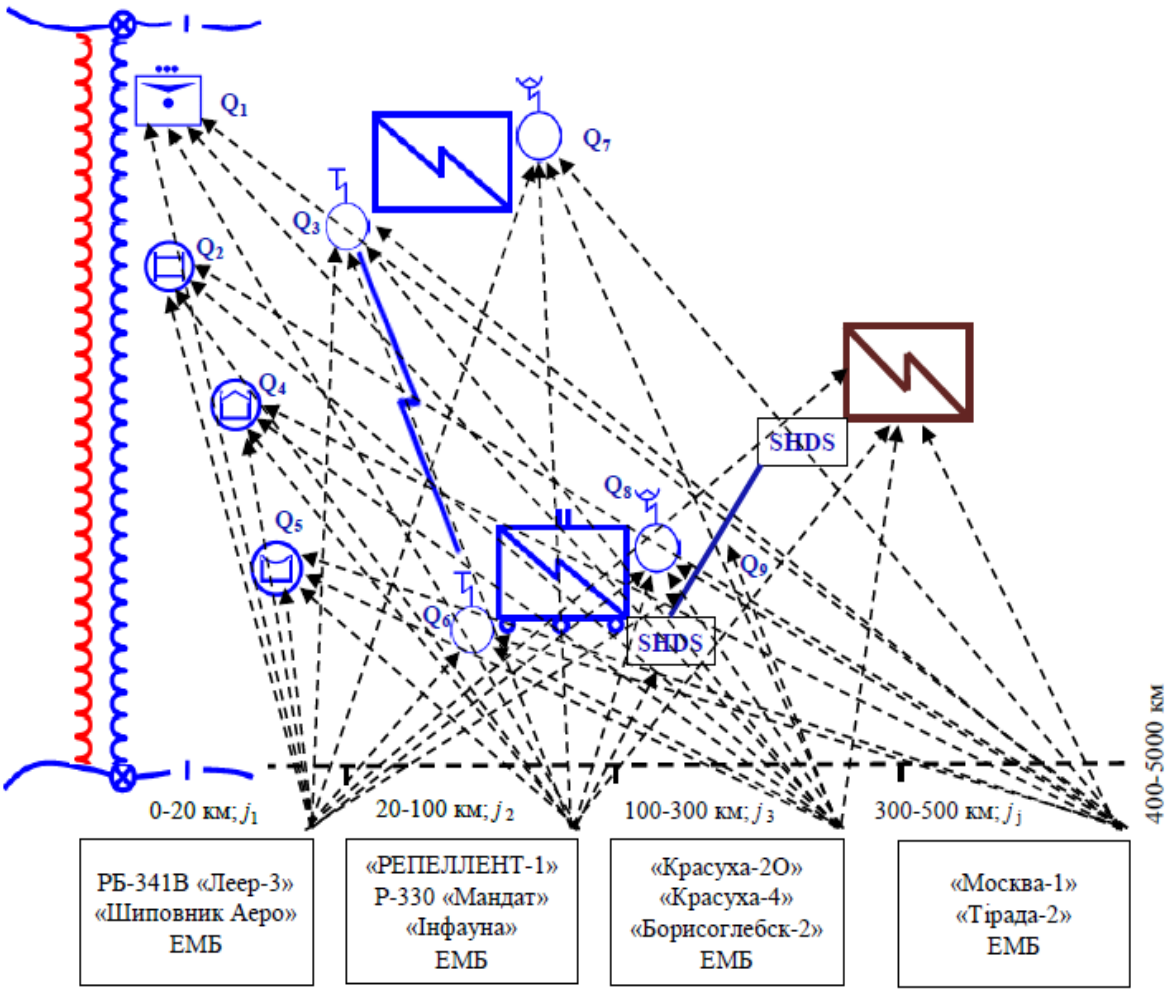


Рис. 3.5. Вихідні дані щодо постановки задачі оптимального розподілу неоднорідних засобів РП та ЕМП ТП НТМ для ведення гібридних дій

За результатами оцінки РЕО визначена загальна кількість радіоканалів Q_j, яка організована на всіх об'єктах z типів, що можуть бути об'єктами РП та ЕМП противника під час виконання j-го завдання. $Q_j = \sum_{z=1}^{n_j} Q_{jz} \cdot A_{jz}$, де A_{jz} – кількість радіоканалів, організованих однією радіолінією об'єкта z-го типу під час виконання противником j-го завдання.

Тоді, критерій для оцінки ефективності зриву інформаційного обміну в ТП НТМ шляхом РП та ЕМП противником її елементів при виконанні часткового завдання Z_j має вигляд:

$$Q_j^{\text{п}} \geq Q_j^{\text{кр}}, \tag{3.29}$$

де $Q_j^{\text{кр}}$ – критична кількість подавлених каналів ТП НТМ, за якої досягається потрібний рівень порушення інформаційного обміну у ТП НТМ [38].

$$Q_j^{\text{кр}} = Q_j^{\max} - \frac{\left(\frac{\frac{1}{Q_j^{\max}!} \cdot P_0 \cdot \left(\frac{\lambda_j}{\nu_j} \right)^{Q_j^{\max}} \cdot \frac{1}{1 - \frac{\lambda_j}{Q_j^{\max} \cdot \nu_j}}}{M\{t_{затр_j}^{кр}\}} - \lambda_j \right)}{\nu_j}, \tag{3.30}$$

$$P_0 = \frac{1}{\sum_{i=1}^{Q_j^{\max}-1} \frac{1}{i!} \cdot \left(\frac{\lambda_j}{\nu_j} \right)^i + \frac{1}{Q_j^{\max}!} \cdot \left(\frac{\lambda_j}{\nu_j} \right)^{Q_j^{\max}} \cdot \frac{1}{1 - \frac{\lambda_j}{Q_j^{\max} \cdot \nu_j}}}, \tag{3.31}$$

де $Q_j^{\max}, \lambda_j, \nu_j$ – кількість каналів ТП НТМ що розгорнуті, інтенсивність потоку повідомлень та середній час тривалості повідомлення у каналах ТП НТМ під час вирішення противником j-го завдання; $M\{t_{затр_j}^{кр}\}$ – математичне сподівання часу затримки передачі повідомлення в каналі ТП НТМ під час вирішення j-го завдання.

Для вирішення завдань $Z_1, Z_2, ..., Z_m$ в процесі ведення гібридних дій (терористичної діяльності) противник має сформувати оптимальний набір

$S_{\text{опт}} = \left\| Q^{\text{п}}_{jzk} \right\|$ каналів об'єктів ТП НТМ z-го типу, що подавляються відповідними засобами РП та ЕМП k-го типу під час вирішення j-го завдання, який забезпечує мінімізацію економічних витрат реалізації способу бойового застосування засобів РП та ЕМП ТП НТМ під час ведення гібридних дій (терористичної діяльності). При цьому необхідне одночасне виконання вимог до ефективності процесу РП та ЕМП (наприклад, оптимізація за критерієм "вартість – ефективність подавлення"). Критерій "вартість – ефективність подавлення" не є єдиним можливим підходом та обраний для прикладу, як найбільш простий для розуміння порядку застосування методики, рис. 3.4. На практиці необхідно визначити декілька можливих сценарії РП та ЕМП на основі застосування різних цільових функцій. Зокрема, доцільно застосовувати критерії "складність виконання бойового завдання – ефективність подавлення", або "вартість – складність виконання бойового завдання – ефективність подавлення".

Можливо поставити та вирішити задачу оптимального розподілу як багатокритеріальну та при визначенні сценаріїв обирати рівно ефективні варіанти призначення засобів РП та ЕМП з області Парето. Для цього в методиці, рис.3.4, додатково необхідно розробити:

- схему компромісів особи що приймає рішення (ОПР) під час вирішення багатокритеріальної задачі;
- метод визначення не гірших варіантів розподілу та відповідної номенклатури складу засобів РП та ЕМВ (визначення області Парето);
- матрицю ресурсних витрат на практичне застосування гіпотетично обраних засобів впливу противника на інформаційний обмін у ТП НТМ тощо.

Однак формалізація постановки задачі багатокритеріальної оптимізації із застосуванням цільових функцій "вартість подавлення – складність виконання бойового завдання – ефективність подавлення" виходить за рамки роботи та буде вирішена авторами в окремій публікації.

Не гублячи загальності доповіді, в процесі подальшого викладу порядку практичного застосування методики, рис. 3.4, етап 3, в якості прикладу будемо розглядати однокритеріальну задачу за критерієм "вартість подавлення" при переведенні показника "ефективності подавлення" в режим обмежень. На разі врахуємо, що перехід від багатьох цільових функцій до однокритеріального варіанту можливий шляхом застосування методу переведення деяких з них у режим обмежень. Наприклад, ефективність зриву інформаційного обміну у ТП НТМ доцільно розглядати як обмеження мінімізуючи цільову функцію вартості.

Математична постановка задачі оптимального розподілу неоднорідних засобів РП та ЕМП противника за елементами ТП НТМ в гібридних діях (терористичній діяльності) має вигляд [34, 37]:

$$S_{\text{опт}}(Q^{\text{п}}_{jzk}) = \min \left\{ \sum_{j=1}^{m} \sum_{z=1}^{n_j} \sum_{k=1}^{\nu} C_{jzk} \cdot Q^{\text{п}}_{jzk} \right\}, \qquad (3.32)$$

у разі обмежень на параметри цільової функції (3.34)

$$\sum_{z=1}^{n_j}\sum_{k=1}^{\nu} A_{jz}\cdot Q_{jzk}^{\text{п}} \geq Q_j^{\text{кр}},\ j=1,2,...,m,\ z=1,2,...,n_j, \tag{3.33}$$

$$Q_{jzk}^{\text{п}} = 1,2,...,Q_{jzk}, \tag{3.34}$$

$$C_{jzk} \geq 0, k=1,2,...\nu, \tag{3.35}$$

де, A_{jz} – кількість радіоканалів, організованих однією радіолінією об'єкта z-го типу j-ї ланки управління.

Об'єкти РП та ЕМП ТП НТМ складаються з сукупності приймальних або передаючих (при здійснення противником ЕМП) засобів СпЗ, РрЗ та УКХ радіозв'язку.

Кожний із засобів охарактеризований ймовірністю . $P_{yp_{jzk}}$. ураження (подавлення) його каналів, (перехід від ліній зв'язку до окремого каналу обумовлений врахування багатокальнальності ліній зв'язку) яка є функцією характеристик радіовпливу на Об РП z-го типу відповідним k-м типом засобів РП [5-7]. Визначена кількість каналів Q_{jz} та максимальна кількість каналів $Q^{\max}{}_{jz}$ засобів ТП НТМ, що розгорнуті на окремому та сукупності однотипних об'єктів z-го типу під час вирішення j-го завдання відповідно.

За результатами воєнно-економічного аналізу необхідно сформувати матрицю $\|C_{jzk}\|$ економічних витрат РП та ЕМП на кожен канал ТП НТМ об'єкту z-го типу засобами РП k-го типу, таблиця 1. Елементи матриці формуються із врахуванням захисних властивостей кожного типу Об РП, ЕМП та живучості засобів РП кожного типу, де – $C_{jzk} = \dfrac{C_k \cdot M_{jzk}}{Q_{jz}\cdot G_{jzk}^{\partial}}$; $C_k \cdot M_{jzk}(P_{yp_{jzk}})$ – відповідно вартість застосування засобу РП та ЕМП k-го типу противника та їх кількість, яка необхідна для ураження (подавлення) Об РП z-го типу засобом РП k-го типу під час вирішення j-го завдання; G_{jzk}^{∂} – коефіцієнт, що характеризує ступінь виконання завдання з доставки засобів РП, ЕМП k-го типу до Об РП z-го типу під час вирішення j-го завдання $\left(0 < G_{jzk}^{\text{д}} \leq 1\right)$. Ця процедура труднощів не викликає.

Таблиця 3.3

Приклад результатів формування матриці $\|C_{jzk}\|$ економічних витрат РП та ЕМП на кожен канал ТП НТМ об'єкту z-го типу засобами подавлення k-го типу

Об'єкти РП та ЕМП ТП НТМ / Засоби РП та ЕМП противника			Номер завдання (в залежності від просторових меж виконання завдань противником) з подавлення елементів ТП НТМ, j та номер типового Об РП та ЕМП (від 1 до 8)							
			$j=1$			$j=2$				$j=3$
			Танк (засіб «Либідь К-2РБ»)	БТР (засіб «Либідь К-2РБ»)	Автомобіль (засіб «Либідь К-2РБ» ,»Харріс»)	Станція РРЛ (засоби Р-414МУ, СРЩ-5000)	Станція супут., троп. звязку (Р-423)	Підрозділ зв'язку (ССЗ, СМЗ, КШМ)	Польовий вузол зв'язку (Дон-14)	Стаціонарний вузол зв'язку
Тип засобу РП та ЕМП	Тип засобу РП та ЕМП	Спосіб доставки	1	2	3	4	5	6	7	8
ЕМП	1	БПЛА	300	300	300	700	700	2000	10000	100000
	2	АБП	3230	3230	3230	–	–	–	–	–
	3	АБ	30000	30000	30000	30000	50000	50000	50000	100000
	4	ДРГ	1100	1200	1200	1500	2200	2500	3000	10000
РП – БПЛА - ПЗ	5	БПЛА	200	200	300	500	1000	1000	5000	5000
РП – 377 ЛА "Лорандит" УКХ: 30-300 МГц	6	НВП	771	771	771	771	–	–	–	–
РП - "Репеллент-1" (200-6000 МГц)	7	НВП	1748	1748	1748	1748	–	–	–	–
РП - Р-330Ж "Житель" GSM-900/1800	8	НВП	1748	1748	1748	1748	–	–	–	–
РП - "Борисоглебск -2" КХ (1,5-30 МГц); УКХ (30-100 МГц)	9	НВП	3178	3178	3178	3178	3178	–	–	–
РП - Р-934У УКХ (30-300 МГц); GSM-900/1800	10	НВП	1748	1748	1748	–	–	–	–	–
РП - "ТОРН" КХ (3-30МГц);	11	НВП	1748	1748	1748	–	–	–	–	–

УКХ (до 3000 МГц);										
РП - РБ-109А “Былина” Супутниковий, мобільний, РРЛ, транкінговий зв’язок	12	НВП	8770	8770	8770	8770	8770	8770	8770	8770
РП - ЗПЗ - ДРГ	13	ДРГ	1500	1500	1500	2000	2000	3000	4000	5000

Таблиця 3.4

Приклад результатів приведення матриці економічних витрат $\|C_{jzk}\|$ до матриці-строки C_z

	Номер типового Об РП та ЕМП (див. табл.3.3)							
z	1	2	3	4	5	6	7	8
k	3	3	3	6	6	4	4	2
C_z^k	200	200	300	500	500	500	1000	1000

Примітка. Умовні позначення: БПЛА ПЗ – безпілотний літальний апарат постановник завад; АБП – артилерійський боєприпас; АБ – авіаційна бомба; НВП – направлений випромінюючий пристрій; ДРГ – диверсійна розвідувальна група, ЗПЗ – передавач завад, що заносять.

Аналіз (3.29-3.35) дозволяє зробити висновок, що на третьому етапі методики задача розподілу засобів РП и ЕМП по ОРб при розробці можливих сценаріїв РП та ЕМП противником ТП НТМ за критерієм “вартість подавлення – ефективність подавлення” може бути зведена до вирішення багатоіндексної двоякої цілочисельної зворотної задачі лінійного програмування.

Метод мінімізації (3.32) суттєво визначається її мірністю та характером сукупності обмежень типу (5–7). Підходи до вирішення зворотних двояких задач досліджені в [8, 9]. Однак результати отримані або в умовах розподілу однорідного ресурсу, або невисокої індексності (не більш 2) цільової функції та їх використання для отримання однозначного рішення задачі (3.32–3.35) утруднено.

Іншим підходом до зняття виникаючих протиріч на третьому етапі методики є багаторівневий процес вирішення (3.32-3.35) з пониженням мірності цільової функції (3.32) задачі за рахунок перетворення матриці економічних витрат $\|C_{jzk}\|$. В результаті чого, формується матриця економічних витрат, яка приводиться до матриці-строки C_z, табл. 3.4, шляхом згортання за правилом, згідно з яким, з елементів кожного z-го стовпця матриці $\|C_{jzk}\|$ обирається мінімальний та його значення присвоюється відповідному елементу матриці-строки C_z^k зі збереженням індексу z, де верхній індекс k є

типом засобу РЕП, що чисельно дорівнює номеру строки в якій знаходився мінімальний для z-го стовпця елемент матриці $\left\| C_{jzk} \right\|$.

В результаті запропонованого підходу, задача (3.32-3.35) спрощується до вигляду [37]:

$$S_{\text{опт}}(Q_z^{\text{п}}) = \min\left\{ \sum_{z=1}^{n_j} C_z^k \cdot Q_z^{\text{п}} \right\}, \tag{3.36}$$

у разі обмежень [37]:

$$\sum_{z=1}^{n_j} Q_z \geq Q_j^{\text{кр}},\ j = 1,2,...,m,\ z = 1,2,...,n_j, \tag{3.37}$$

$$Q_{jz} = 1,2,...,Q_{jz}^{\max}, \tag{3.38}$$

$$C_{jz}^k \geq 0,\ k = 1,2,...,\nu. \tag{3.39}$$

Фізична трактовка (3.36)…(3.39) може бути наступною [6]. До кожного завдання $Z_1, Z_2, ..., Z_m$, $j = 1,2,...,m$, необхідно надати (створити під час гібридних дій) різнорідний ресурс каналів ТП НТМ що подавлені або уражені n_j типів, у разі обмежень зверху на їх сукупну кількість $Q_{jz}^{\max}$ за типами об’єктів та знизу на сукупну кількість подавлених каналів в межах кожного завдання, що вирішується (3.39).

Для вирішення задачі виду (3.36-3.39), виникає необхідність пошуку методу розв’язання. Проведений аналіз меж застосування відомого методичного апарату [6-7, 9-10] дозволили побудувати алгоритм оптимізації (3.36-3.39) на основі методу нормованих функцій, який детально розроблений авторами в [7].

В якості прикладу застосуємо підхід (3.29-3.39), рис. 3,4 та результати табл. 3.3 для виконання етапу ІІІ методики при розробці сценаріїв РП та ЕМП ТП НТМ під час зриву державного управління в гібридних діях (терористичній діяльності) на глибину до 300 км.

Нехай, при цьому необхідно вирішити три часткових завдання – зірвати інформаційний обмін у мережах державного управління відповідно на глибину до 20 км ($j = 1$), від 20 до 100 км ($j = 2$) та від 100 до 300 км ($j = 3$), табл. 3.4

За результатами ведення радіоелектронної, космічної, агентурної розвідки противником визначені у складі ТП НТМ типи об’єктів РП та ЕМП ($z = 8$). В табл. 3.4 наведена загальна кількість ліній зв’язку розгорнутих на всіх об’єктах кожного z-го типу.

Для РП та ЕМП противником гіпотетично може бути сформована сукупність із $k=13$ типів засобів РП та ЕМП.

В матриці-стовпці Q наведена, визначена на основі методики (2-3), необхідна кількість каналів ТП НТМ ($Q_j^{кр}$), що подавлені (ураженні), при якій забезпечується зрив інформаційного обміну у ТП НТМ при вирішенні кожного часткового завдання відповідно.

Таблиця 3.5

Формування матриці загальної кількості ліній зв'язку розгорнутих на всіх об'єктах кожного z-го типу

Номер часткового завдання	Типи об'єктів РП та ЕМП							
	1	2	3	4	5	6	7	8
1	10	10	20	-	-	-	-	-
2	-	-	-	20	10	10	15	-
3	-	-	-	-	-	-	-	35

Таблиця 3.6

Необхідна кількість каналів ТП НТМ ($Q_j^{кр}$), що подавлені (ураженні) при якій забезпечується зрив інформаційного обміну у ТП НТМ при вирішенні кожного часткового завдання

Номер завдання (в залежності від просторових меж виконання завдань противником) з подавлення елементів ТП НТМ, j	$Q_j^{кр}$
J=1	$Q_1^{кр}=12$
J=2	$Q_j^{кр}=9$
J=3	$Q_j^{кр}=19$

Результати оптимального розподілу кількості каналів ТП НТМ об'єктів z типів, k типів засобів РП та ЕМП по типовим Об для зриву інформаційного обміну у ТП НТМ у проміжок часу 4 години наведені в табл. 5 W ($Q_z^{п}$). При цьому, мінімальне значення цільової функції (3.38) за обмежень (3.39-3.41) S_{opt} дорівнює$1{,}17\cdot 10^5$, дол. США.

Таблиця 3.7

Результати оптимального розподілу кількості каналів ТП НТМ об'єктів z типів, k типів засобів РП та ЕМП по типовим Об для зриву інформаційного обміну у ТП НТМ у проміжок часу 4 години

Номер завдання (в залежності від просторових меж виконання завдань противником) з подавлення елементів ТП НТМ, j та номер типового Об РП та ЕМП (від 1 до 8)		
$j=1$	$j=2$	$j=3$

Танк (засіб «Либідь К-2РБ»)	БТР (засіб «Либідь К-2РБ»)	Автомобіль (засіб «Либідь К-2РБ» ,»Харріс»)	Станція РРЛ (засоби Р-414МУ, СРШ-5000)	супутникового, тропосферного звязку (Р-423)	Підрозділ зв'язку (ССЗ, СМЗ, КШМ)	Польовий вузол зв'язку (Дон-14)	Стаціонарний вузол зв'язку
2	1	9	2	3	4	3	19
Тип засобу РП та ЕМП що може бути застосований для завдання з порушення інформаційного обміну ТП НТМ (див. табл.1) та кількість (наведена у дужках)							
5 (2)	5 (2); 13(1)	5 (2); 3(2)	5 (2); 13(2)	12 (1);5 (2)	5(3); 12 (1)	5 (4);12 (2);	5(5); 12(2); 13 (2)

Результати таблиця 3.7 дозоляють визначити сценарій РП та ЕМП ТП НТМ за цільовою функцією пониженої мірності (8) при виконанні противником завдань у відповідних територіальних межах за умови гарантованого зриву інформаційного обміну. При цьому економічні витрати противника – мінімальні.

Для визначення сценарію необхідно щоб ураження (подавлення) відповідних об'єктів РП було узгоджено за просторовими та часовими вимогами їх виконання.

Інший варіант сценарію може бути отриманий варіаціями множини обмежень, оперативно-тактичних умов або зміною сутності та виду цільової функції.

На п'ятому етапі методики за результатами розробки сценарію РП та ЕМП ТП НТМ формуються данні щодо видів завадових сигналів противника, їх кількості, параметрів та порядку випромінювання, дій станцій зв'язку тощо [38-39]. Це дає змогу статистично описати можливі варіанти ССЗО за якої гіпотетично буде здійснюватися застосування підрозділів Держспецзв'язку за призначенням в умовах реалізації противником визначених сценаріїв РП та ЕМП ТП НТМ. Для цього шляхом математичного та імітаційного моделювання формуються вибірки можливих значень амплітуди суперпозиції спектрів корисних сигналів, адитивних шумів та завад різних типів (структурних, подібних та гармонічних вузькосмугових завад), що можуть випромінюватись обраними за результатами етапу ІІІ засобами РП противника. Моделюються реальні дистанції зв'язку, тактико-технічні характеристики засобів РП противника та своїх засобів зв'язку, реальні види завадових сигналів.

За результатами моделювання формуються вибірки розрахованих амплітуд суміші корисного сигналу та завад на фоні власних шумів приймача для різних сценаріїв РП та ЕМП ТП НТМ противником. Далі будуються гістограми вибіркового розподілу сумарної амплітуди спектру на вході приймача та вирішуються задачі статистичної перевірки гіпотез, що є підставою для вибору типу закону розподілу амплітуди спектру суміші "сигнал – гаусів шум – завада". Таким чином, створюється апріорний словник сигнатур випадкових процесів на вході приймача.

Задача з перевірки гіпотези про закон розподілу вибірки випадкової величини може бути вирішена із застосуванням відомих критеріїв, наприклад Пірсона (критерій χ^2) і Колмогорова [11].

У разі застосування критерію χ^2 дискретизується функція, що описує зміни амплітуди спектру суміші сигналу, завади та шуму на вході приймача. Далі формується вибірка обсягу n, яка розбивається на k інтервалів (від 8 до 20). Кількість елементів вибірки, що потрапили в i-інтервал, позначимо через n_j. Побудована за цими даними гістограма вибіркового розподілу амплітуди сигнала служить підставою для вибору типу закону розподілу. Параметри цього розподілу можуть бути знайдені або з теоретичних міркувань, або знаходженням їх оцінок за вибіркою. На підставі прийнятого закону розподілу обчислюються ймовірності p_i попадання випадкової величини в i-інтервал. Величина, що характеризує відхилення вибіркового розподілу від передбачуваного, визначається формулою [39]:

$$\chi^2 = \sum_{i=1}^{k} \frac{(n_i - np_i)^2}{np_i} \qquad (3.40)$$

де, k – кількість інтервалів; n – обсяг вибірки.

Сума (3.40) має наближено χ^2 – розподілення з $f = (k-1-c)$ ступенями вільності, де c – кількість параметрів гіпотетичного закону розподілу, що визначаються за вибіркою. Для нормального розподілу $c = 2$, якщо і $\bar{x}$, і s визначаються за даною вибіркою.

Гіпотеза про прийнятий тип закону розподілу приймається на обраному рівні значущості α, якщо $\chi^2 \le \chi^2_{1-\alpha}$, де $\chi^2_{1-\alpha}$ кванти розподілу Пірсона для даного α і кількості ступенів вільності f. В іншому випадку робиться висновок про те, що гіпотеза не узгоджується з вибірковим розподілом.

При використанні критерію χ^2 бажано, щоб обсяг вибірки був достатньо великим: $n \ge 50 \div 150$, а кількість елементів $n_j \ge 5 \div 8$.

При підрахунку теоретичних ймовірностей p_i вважається, що крайній лівий інтервал простягається до – ∞; крайній правий до + ∞.

Для застосування критерію згоди Колмогорова необхідно визначити найбільше абсолютне відхилення вибіркової функції розподілу $F_n(x)$ від генеральної $F(x)$ [39]:

$$D = \max \left| F_n(x) - F(x) \right|. \qquad (3.41)$$

Потім необхідно обчислити величину $\lambda = D\sqrt{n}$, $\lambda_{1-\alpha}$ – кванти розподілу Колмогорова.

Якщо $\lambda > \lambda_{1-\alpha}$, то гіпотеза про збіг теоретичного закону розподілу $F(x)$ з вибірковим $F_n(x)$ не відхиляється. При $\lambda > \lambda_{1-\alpha}$ гіпотеза відхиляється (або вважається сумнівною). Рівень значущості при застосуванні критерію Колмогорова обирають зазвичай в діапазоні (0,2 … 0,3).

У разі вибірок невеликого обсягу ($n < 50$) для перевірки гіпотези про закон розподілу можна використовувати прості критерії, засновані на порівнянні генеральних параметрів розподілу і їх оцінок, отриманих за вибіркою. В якості оцінок параметрів найзручніше обрати моменти.

Для опису різних моделей завад з можливістю оцінки їх майбутньої поведінки можливо застосувати ймовірнісні конструкції та підхід (9-12). Негаусівські завади можливо описати кінцевою послідовністю кумулянтів. Однак на практиці для поточного моменту t доцільно мати представлення про поведінку завади в момент $t+\kappa, \quad k \geq 1$. Для вирішення цього завдання потрібно знати мати умовну сумісну щільність ймовірності значень амплітуди суміші сигналу, шуму та завад $(t+\kappa), \quad k \geq 1$ при заданому наборі попередніх значень амплітуди. Однак у більшості практичних випадків реалізація цієї ідеї потребує великої кількості обчислень. В такий ситуації, розвиваючи підхід [10] у галузь моделювання завадової обстановки можливо формалізувати заваду співвідношенням [39]:

$$v(t) = \sum_{k=0}^{\infty} h(k) \cdot e(t-k), \tag{3.42}$$

де $e(t)$ – послідовність взаємно незалежних однаково розподілених випадкових величин з деякою функцією щільності ймовірності. Такий підхід дозволяє в подальшому здійснювати визначення сценаріїв та формування статистичних гіпотез про майбутню поведінку завади. Новизна такого підходу полягає у можливості апроксимації складних по формі завад шляхом визначення (підбору) різних функцій щільності ймовірності для послідовності $e(t)$ може моделювати (імітувати по формі) завади практично любого характеру складності. Цей практичний висновок відіграє важливу роль у створенні при подальших дослідженнях словника сигнатур ознак станів випадкових процесів на вході приймача у складній СЗО, дозволяє проводити дослідження з розпізнавання стану ССЗО за сформованими у процесі навчання.

Запропонований підхід дозволяє вирішувати завдання з визначення сценаріїв:

РП та ЕМП ТП НТМ на основі розподілу неоднорідних засобів РП та ЕМП противника за елементами ТП НТМ у гібридних діях (терористичній діяльності);

ССЗО що може скластися у інформаційному конфлікті засобів зв’язку та РЕБ противника.

В подальшому доцільно створити методику розробки апріорного словника сигнатур станів випадкових процесів на вході приймального засобу спецзв’язку. Це надасть можливості в подальшому синтезувати автоматизовані непараметричні статистичні та нейромережеві алгоритми розпізнавання станів ССЗО. Розроблені алгоритмі розпізнавання станів ССЗО дозволяють в подальшому розробити адаптивні до стану ССЗО алгоритмів завадозахисту.

3.8. Електронне забезпечення радіоелектронного подавлення засобів зв’язку

Особливою складовою РЕБ є **електронне забезпечення**, що включає електронну розвідку, управління силами та засобами РЕБ, попередження (оповіщення) екіпажів бойових засобів та військової техніки про опромінювання, застосування противником засобів постановки завад та керованої зброї, рис. 3.6.

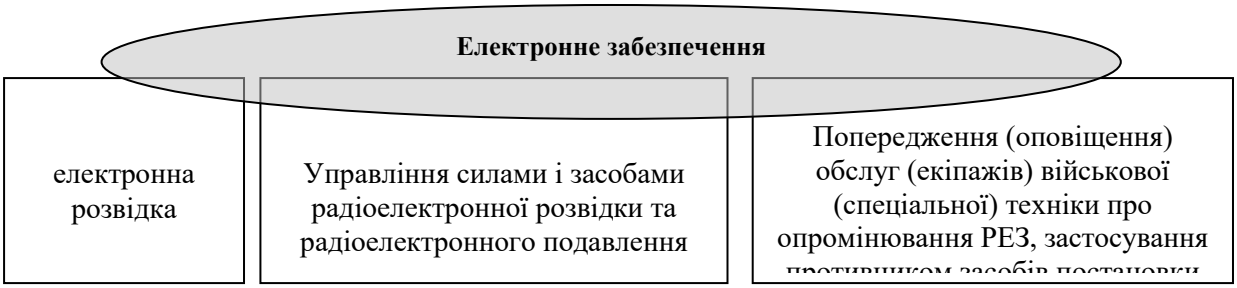


Рис. 3.6. Складові електронного забезпечення

Електронна розвідка включає: радіоелектронну (РЕР), оптико-електронну, гідроакустичну розвідки.

Оптико-електронна розвідка – добуває розвідувальну інформацію про противника за допомогою пасивних та активних оптико-електронних засобів шляхом виявлення та аналізу випромінювань радіоелектронних систем, засобів та об’єктів у оптичному діапазоні довжин хвиль.

Гідроакустична розвідка – добуває розвідувальну інформацію про противника за допомогою пасивних та активних гідроакустичних засобів шляхом виявлення та аналізу випромінюваннь об’єктів у діапазоні гідроакустичних хвиль.

Сутністю РЕР є добування за допомогою різних пасивних і активних радіоелектронних засобів розвідувальної інформації про противника шляхом виявлення та аналізу випромінюваннь його радіоелектронних систем, засобів та об’єктів, у радіодіапазоні довжин хвиль [18-20].

Радіоелектронна розвідка забезпечує добування інформації про радіоелектронну й оперативну обстановку, яка містить зведення та данні про

функціонуючі радіоелектронні засоби противника, їх тактико-технічні характеристики (ТТХ), оперативну приналежність, місце розташування, органи й об'єкти управління, а також про характер бойової діяльності противника [18].

Радіоелектронна розвідка принципово відрізняється від інших видів розвідки (агентурної, військової та ін.). Специфічними особливостями РЕР є не тільки способи добування інформації, але й технічні та оперативні можливості, зокрема:

– охоплює великі простори, межі яких визначаються умовами поширення електромагнітних хвиль і характеристиками активних і пасивних засобів локації;

– добуває інформацію в найкоротші терміни й у багатьох випадках у реальному масштабі часу;

– забезпечує одержання достовірних даних;

– функціонує безупинно протягом доби і за будь-якої погоді;

– діє потайно, тому що противник не в змозі установити факт ведення розвідки при застосуванні пасивних засобів;

– добуває розвідувальну інформацію, яку неможна одержати іншими видами розвідки.

Технічну основу РЕР складають [18-20]:

– пасивні пристрої пошуку, перехоплення й аналізу сигналів і пеленгування джерел електромагнітних випромінювань;

– радіолокаційні та інші активні засоби спостереження і виявлення;

– засоби автоматизованої обробки розвідувальної інформації;

– засоби реєстрації (індикації) і передачі інформації, яка добувається.

З метою інформаційного забезпечення процесу радіоподавлення у частинах (підрозділах) РЕБ на даний час активно застосовуються в основному **радіо** (РР), **радіотехнічна** (РТР) та **радіолокаційна** (РЛР) розвідки, які є складовими радіоелектронної розвідки, рис. 3.7.

Радіорозвідка (РР) ведеться шляхом пошуку, виявлення і перехоплення передач, здійснюваних засобами радіо-, радіорелейного, тропосферного і супутникового зв'язку, а також шляхом пеленгування засобів, що передають з метою визначення їх місцерозташування. Радіорозвідка ведеться розвідприймачами і засобами радіопеленгації [18].

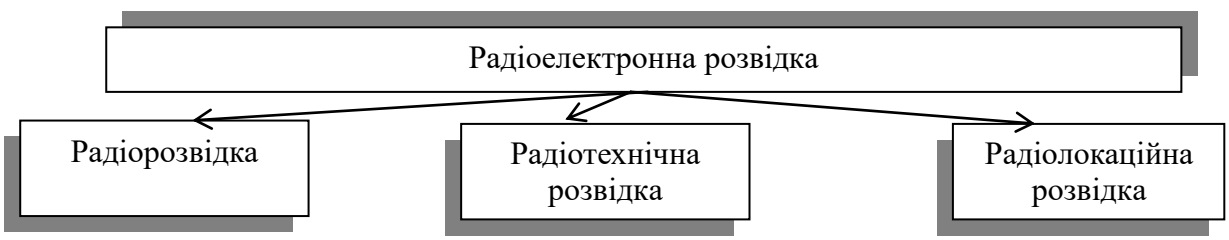


Рис. 3.7. Складові радіоелектронної розвідки

Розвіддані, добуті за допомогою засобів РР дозволяють: виявляти, розпізнавати, визначати ТТХ і місцерозташування засобів радіозв'язку, радіотелеметрії і передачі даних, виявляти склад систем зв'язку, дешифрувати перехоплені кодовані і формалізовані повідомлення, виявляти, розпізнавати і визначати місце розташування військових об'єктів, визначати характер діяльності військ [18-19].

Радіотехнічна розвідка ведеться шляхом пошуку, виявлення, перехоплення й аналізу радіовипромінювань засобів радіолокації і радіонавігації, що використовуються противником для керування військами і зброєю, а також шляхом пеленгування станцій даних засобів, що передають, із метою визначення їх місця розташування. Радіотехнічна розвідка ведеться станціями радіотехнічної розвідки. Крім того, радіо і радіотехнічна розвідка в частинах РЭБ ведеться станціями завад із використанням вбудованих засобів розвідки.

Радіолокаційна розвідка ведеться шляхом пошуку, виявлення і спостереження за космічними, повітряними, наземними і морськими радіолокаційно-контрастними об'єктами противника. Радіолокаційна розвідка ведеться радіолокаційними станціями.

Стосовно організації та ведення РЕБ електронна розвідка може вирішувати наступні завдання [18-20].

Завдання 1. Одержання інформації про противника в інтересах **організації РЕБ** при підготовці до операції (бойових дій). Наприклад, для ефективної організації бойового застосування частин РЕБ-С необхідна інформація про можливі варіанти дії повітряного противника, склад ударних груп його авіації при знищенні об'єктів, що захищаються, озброєння і радіоелектронне обладнання літаків, системи управління і радіонавігаційного забезпечення.

Для ефективної організації бойового застосування частин РЭБ-Н необхідна інформація про порядок організації системи зв'язку в угрупованні, що протистоїть, (про склад і розміщення ПУ об'єднань, з'єднань, частин і підрозділів противника, засоби зв'язку, їх ТТХ, розгорнуті противником радіомережі і радіонапрямки, сили та засоби РЕБ, організацію своїх систем управління та ін.). Електронна розвідка, що добуває інформацію в інтересах організації РЕБ називають **попередньою,** рис. 3.8.

В мирний час частини та підрозділи РЕБ ведуть попередню електронну розвідку з метою вивчення радіоелектронної обстановки (РЕО) та розвідувальних ознак РЕОб (цілей РЕП), спостереженням за цілями РЕП. Ці завдання виконуються силами та засобами радіо-, радіотехнічної, радіолокаційної, оптико-електронної, гідроакустичної розвідки та радіоелектронного подавлення під час несення бойового чергування (чергування по вивченню РЕО) з пунктів постійної дислокації, районів навчань. Попередня розвідка в інтересах РЕБ ведеться до початку операції (бойових дій), а також у ході операції (бойових дій) із метою виявлення змін у радіоелектронній та оперативній обстановці.

Завдання 2. Одержання інформації про дії противника в інтересах **ведення РЭБ** у ході операції (бойових дій). При цьому здійснюється:

– виявлення радіовипромінювань противника, що працюють, визначення у реальному масштабі часу їх оперативно-тактичної приналежності, класу (типу), визначення пріоритету на радіоподавлення;

– аналіз параметрів випромінюваннь радіоелектронних засобів противника, що є об'єктами РЕП з метою вибору оптимальних (по виду модуляції, частоті випромінювання та часовим параметрам) завад;

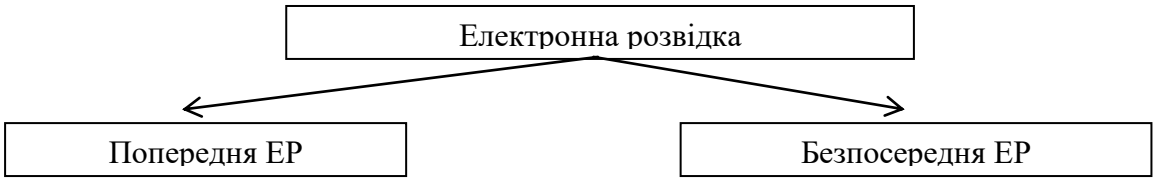
– виявлення радіоелектронних засобів противника, що здійснили маневр частотами, із метою перенацілення станцій завад;

– виявлення факту порушення радіодісципліни своїми частинами (підрозділами).

Розвідку в інтересах РЭБ, що добуває інформацію для ефективного ведення РЕБ, називають **безпосередньою,** рис. 3.8. Головна мета безпосередньої радіоелектронної розвідки полягає у визначенні належності випромінюваннь конкретним радіоелектронним об'єктам, цілям РЕП (розпізнавання цілей), які призначені для радіоелектронного подавлення і своєчасного наведення на них засобів завад.

Безпосередня розвідка в інтересах РЕБ ведеться в ході операції (бойових дій) в умовах, коли противник почав активно використовувати радіоелектронні засоби для управління військами і зброєю, а частини (підрозділи) РЕБ проводять заходи з РЕП та РЕЗт.

Рис. 3.8.



Типи електронної розвідки

Основними принципами ведення електронної розвідки в частинах РЕБ є: **неперервність, своєчасність і оперативність, вірогідність,** активність [8, 18-19, 25].

Неперервність – полягає в постійному спостереженні за роботою радіоелектронних засобів, що мають розвідувальну цінність або є важливі цілями для радіозавад, у неперервному контролі за місцезнаходженням і режимами роботи РЕЗ противника, безупинній обробці розвідувальних зведень на відповідних командних пунктах.

Своєчасність і оперативність полягає в добуванні розвідувальних зведень і одержанні оброблених розвідувальних даних до встановленого терміну. Цей термін обумовлений: при веденні попередньої розвідки - часом готовності до ведення РЕБ, під час ведення безпосередньої розвідки – тривалістю переданих по каналах зв'язку повідомлень, часом нанесення удару заобами ураження противника та ін.

Вірогідність даних розвідки полягає у правильності висновків про противника на підставі оцінці добитих свідок та даних.

Активність полягає в постійному і цілеспрямованому проведенні заходів щодо викриття системи управління військами (силами) і зброєю противника, прагненні в будь-яких умовах і всіх можливих способах добути необхідні розвідувальні дані про противника з метою подальшого радіоелектронного подавлення його найбільш важливих об'єктів.

Управління силами та засобами радіоелектронної розвідки і радіоелектронного подавлення, наведення засобів РЕП на цілі радіозавад здійснюється засобами управління комплексів РЕП, командними пунктами (ПУ) частин та підрозділів РЕБ. При цьому безумовно виконуються алгоритми ведення бойової роботи (застосування) сил та засобів розвідки і РЕП у відповідності до покладених завдань, змін оперативної і радіоелектронної обстановки.

Контроль ефективності радіоелектронного подавлення здійснюється на КП (ПУ) органів управління, частин та підрозділів РЕБ (розвідки і РЕБ), а також операторами постів управління, радіоелектронної розвідки і станцій завад. Начальник РЕБ, командир частини (підрозділу) РЕБ, посадові особи чергових змін відповідних пунктів управління зобов'язані приймати необхідні заходи для забезпечення ефективного радіоелектронного подавлення у ході операції (бойових дій).

Попередження (оповіщення) обслуг (екіпажів) спеціальної техніки частин (підрозділів) РЕБ про застосування противником засобів завад та керованої зброї (моменту пуску ракет, торпед, скидання бомб, мін) здійснюється в радіомережах оповіщення командира частини (підрозділу) про загальну повітряну обстановку.

Попередження (оповіщення) екіпажів літаків (вертольотів, кораблів, ЗРК) про опромінювання РЕЗ, моменту пуску ракет здійснюється спеціальними бортовими засобами (комплексами оборони) літальних апаратів, засобами розвідки і спостереження кораблів, засобами РТВ.

Оповіщення про повітряного противника здійснюється шляхом прийому даних в радіомережах оповіщення про загальну повітряну обстановку, централізованого бойового управління, начальника служби РЕБ об'єднання (з'єднання), командира частини (підрозділу) радіоелектронної боротьби, а також за допомогою сигнальних засобів.

Управління силами та засобами РЕБ, наведення засобів РЕП на цілі завад здійснюється засобами управління комплексів РЕП, командними пунктами (ПУ) частин та підрозділів РЕБ.

Попередження (оповіщення) обслуг (екіпажів) про опромінення РЕЗ і застосування противником керованої зброї здійснюється спеціальними комплексами (засобами РЕБ та розвідки), які встановлені на літаках (вертольотах), кораблях, бойових засобах і воєнній техніці [18-20, 26].

3.9. Методика оцінки ефективності ведення радіоелектронної розвідки частинами (підрозділами) РЕП противника в гібридних діях

Постановка задачі. Нехай угруповання засобів РЕП в складі k_m засобів завад, веде радіорозвідку у визначеній смузі дій об'єднання, при цьому [28]

$$k_m = \sum_{i=1}^{m} k_i, \tag{3.43}$$

де m - кількість комплексів РЕП, що вирішують завдання з РЕБ у операції (бойових діях); k_i - кількість засобів завад із i-ого комплекту РЕП, яка виділена для вирішення завдань з РЕР. В ході радіорозвідки проводиться оперативна обробка добутих розвідувальних відомостей, в результаті якої на засоби РЕП видаються дані, необхідні для подавлення. Тривалість процесу отримання, систематизації, вибору розвідувальних відомостей, представлення їх у вигляді розвідувальних ознак, встановлення місцеположення РЕЗ, розпізнавання джерел та об'єктів розвідки, прийняття рішення на зарахування їх до об'єктів і цілей РЕП повинні проходити до початку часу мінімально необхідного для радіоподавлення.

Тому у якості показника оцінки ефективності ведення РЕР i-им комплексом РЕБ введемо ймовірність своєчасної обробки розвідувальних відомостей $P_{соі}$ на пунктах управління та станціях завад [28]:

$$P_{соі} = 1 - P_{нсоі},\ i = 1...m, \tag{3.44}$$

де $P_{нсоі}$ - ймовірність несвоєчасної обробки розвідувальних відомостей на пункті управління. Зауважимо, що показник $P_{соі}$ по суті є ймовірністю того, що час обробки інформації $t_{обр}$, не перевищить величини t_y, яка задана вимогою випередження. Тоді,

$$P_{со}(t) = P(t_{обр} < t_y) = \int_0^{t_y} dF(t_{обр}), \tag{3.46}$$

де $P_{со}$ – ймовірність своєчасної обробки; $F(t_{обр})$ – функція розподілу часу обробки; $t_{обр}$ – час повного циклу оперативної обробки; $t_в$ – час, заданий вимогою випередження.

Враховуючи (3.44) та (3.45), ймовірність своєчасної обробки розвідувальних відомостей угрупованням засобів РЕП в операції, у складі m комплексів РЕБ визначимо у вигляді [28]:

$$P_{соуг} = 1 - \prod_{i=1}^{m} P_{нсоі} \qquad (3.47)$$

Процес обробки розвідувальних відомостей на пунктах управління, станціях завад носить стохастичний характер. Це визначається імовірнісним характером вхідного потоку розвідувальних відомостей, випадковими моментами часу вибірки, розпізнавання, прийняття рішення. Тому, у загальному вигляді, ймовірність своєчасної обробки $P_{со}(t)$ є функцією $P_{со}(t) = \int(\lambda, S, m, n, \mu, T_{обр})$, від інтенсивності вхідного потоку розвідувальних відомостей λ, старіння розвідувальних відомостей *S*, побудови структури обробки (*m* числа фаз та *n* каналів обробки), організаційно-технічних можливостей(інтенсивності обробки μ) і середнього часу обробки $T_{обр}$.

Закон розподілу допустимого часу обробки розвідувальних відомостей при веденні операцій (бойових дій) має вигляд:

$$F(t_{обр}) = 1 - \sum_{i=1}^{m} e^{-\alpha_i t_{обр}} \prod_{j \neq i}^{m} \frac{\alpha_j}{\alpha_j - \alpha_i}, \qquad (3.48)$$

де, $\alpha_i = \mu_i n_i - \lambda_{вхі}$, $\lambda_{вхі}$ - інтенсивність вхідного потоку розвідувальних відомостей на кожну з фаз обробки; μ_i - інтенсивність обробки в *і-й* фазі; *j* – номер фази обробки.

В ході обробки розвідувальних відомостей старіння виникає об’єктивно, а інтенсивність старіння є величиною, обернено пропорційною часу випередження. При експоненційному законі старіння розвідувальних відомостей з інтенсивністю *S* ймовірність своєчасної обробки:

$$P_{со}(t) = \int_{0}^{\infty} e^{-S t_{обр}} dF(t_{обр}) \qquad (3.49)$$

.

Підставляючи (3.46) у (3.47), маємо:

$$P_{со}(t) = \int_{0}^{\infty} e^{-S t_{обр}} \left[\sum_{i=1}^{m} \alpha_i e^{-\alpha_i t_{обр}} \prod_{\substack{j=1 \\ i \neq j}}^{m} \frac{\alpha_j}{\alpha_j - \alpha_i} \right] d t_{обр} \qquad (3.50)$$

.

Після перетворення вираз (6) має вигляд:

$$P_{co} = \prod_{i=1}^{m} \alpha_i \sum_{i=1}^{m} \frac{1}{(\alpha_i + S) \prod\limits_{\substack{j=1 \\ j \neq i}}^{m} (\alpha_j - \alpha_i)} \qquad (3.51)$$

.

Розглянемо порядок застосування запропонованого підходу на важливому, з практичної точки зору, прикладі оцінки ефективності ведення РР при дорозвідці в ході етапу радіоподавлення комплексом Р-330 К, який знаходиться на озброєнні окремого батальйону РЕБ-Н АК ОСШР в смузі його дій. Режими роботи комплекса – централізований автоматизований, почергово в КХ- та УКХ-діапазонах. Необхідність роздільної оцінки в КХ- та УКХ-діапазонах обумовлюється різною кількістю працюючих радіоліній в них і різною кількістю засобів завад, призначених для подавлення в цих діапазонах. При цьому будемо вважати, що умови енергетичної доступності виконані.

3.10. Порядок оцінки ефективності вирішення завдань з РЕР комплексом типу Р-330 К при радіоподавленні засобів КХ та УКХ радіозв'язку

Формування множини вихідних даних.

а) інтенсивність вхідного потоку розвідувальних відомостей $\lambda_{вх1}$ у першій фазі, тобто кількість радіовипромінювань, які надходять на вхід панорамних пристроїв виявлення АСП типу Р-378 А(Б) (КХ-діапазону), Р-330Б (УКХ-діапазону), що працюють режимах виявлення і пеленгування, за годину.

Припустимо найважчий для системи радіорозвідки варіант, коли всі радіолінії противника працюють одночасно. У реальній радіоелектронній обстановці на вхід панорамного пристрою виявлення автоматизованої станції завад будуть надходити сигнали не тільки передавачів противника, а й випромінювання своїх радіозасобів, об'єктів промисловості та природного походження. З урахуванням цих факторів до інформаційних можливостей противника в КХ-діапазоні, УКХ-діапазоні необхідно додати приблизно таку ж кількість радіовипромінювань своїх радіозасобів та до 20% від отриманої кількості – радіовипромінювання промислового та природного походження. Таким чином, оцінимо для КХ-діапазону $\lambda_{вх1}$=500, для УКХ-діапазону $\lambda_{вх1}$ =400.

б) інтенсивність обробки розвідувальних відомостей у першій фазі μ_1, тобто кількість радіовипромінювань, які можуть прийматися панорамними пристроями виявлення АСП Р-378 А(Б), Р-330Б за годину.

При створенні завад лініям радіозв'язку в централізованому автоматизованому режимі управління станції завад працюють циклічно; кожний цикл містить: подавлення ліній радіозв'язку – 1,5 сек., контроль роботи ліній радіозв'язку та дорозвідка – 0,5 сек. При швидкості перестройки

панорамних пристроїв виявлення до 100 МГц/сек. час, який витрачається на виявлення сигналу, визначення частоти, пеленгу, передачі розвідувальних відомостей у формалізованому вигляді на ПУ-Т, становить 0,5 сек. інтенсивність обробки розвідувальних відомостей $\mu_1 = 1800$.

в) кількість каналів обробки розвідувальних відомостей у першій фазі n_1, тобто кількість станцій завад Р-378 А(Б), Р-330Б, які працюють в режимі виявлення і пеленгування (ведуть дорозвідку).

Виходячи з рекомендацій інструкції по бойовому застосуванню ПУ Р-330К для дорозвідки призначаються: по одній АСП Р-378 А(Б) і Р330 Б в режимі виявлення та пеленгування; по одній АСП Р-378 А(Б) і Р-330 Б в режимі виконавчого пеленгування. Таким чином, в кожному діапазоні в режимі виявлення і пеленгування будуть працювати по одному засобу радіорозвідки, тоді для КХ- і УКХ-діапазонів $n_1 = 1$.

г) інтенсивність вхідного потоку розвідувальних відомостей $\lambda_{вх2}$ у другій фазі, тобто кількість виявлених в межах робочого сектору ДРВ, відправлених через ПУ-Т на ПУ-СК розвідувальних відомостей про виявлені ДРВ та, відповідно, команд на сполучені станції, які працюють в режимі пеленгування, на пеленгування і отримання від них відповідних пеленгів за годину.

У першій фазі на станції завад здійснюється селекція виявлених ДРВ по належності до робочого сектору, неналежності до частот, заборонених для радіоподавлення. При цьому із загальної кількості виявлених ДРВ вираховуються свої радіозасоби та загалом до 50 % випромінюваннь промислового та природного походження. Тому будемо вважати для КХ-діапазону $\lambda_{вх2} = 250$, для УКХ-діапазону $\lambda_{вх2} = 200$.

д) інтенсивність обробки розвідувальних відомостей у другій фазі μ_2, тобто кількість пеленгувань, які можуть бути виконані сполученими АСП Р-378 А(Б), Р-330 Б, що працюють в режимі пеленгування, за годину.

З урахуванням викладеного в п. б) будемо вважати для КХ- та УКХ-діапазонів $\mu_2 = 1800$.

е) кількість каналів обробки розвідувальних відомостей у другій фазі n_2, тобто кількість станцій завад Р-378 А(Б), Р-330 Б, які здійснюють пеленгування.

З урахуванням викладеного в п. в) будемо вважати для КХ- та УКХ-діапазонів $n_2 = 1$.

ж) інтенсивність вхідного потоку розвідувальних відомостей $\lambda_{вх3}$ у третій фазі, тобто кількість виконаних пеленгувань сполученими АСП Р-378 А(Б), Р-330 Б за годину.

У ідеальному випадку, коли кожна команда на виконавче пеленгування була виконана, для КХ-діапазону $\lambda_{вх3} = \lambda_{вх2} = 250$, для УКХ-діапазону $\lambda_{вх3} = \lambda_{вх2} = 200$.

з) інтенсивність обробки розвідувальних відомостей у третій фазі μ_3, тобто, кількість проведених на ПУ-СК розрахунків координат ДРВ по знятим пеленгам, порівнянь їх із зоною обслуговування, прийняття рішень на зарахування виявлених ДРВ до об'єктів РЕП та цілерозподілів за годину.

Будемо вважати для КХ- та УКХ-діапазонів $\mu_3 = 600$.

и) кількість каналів обробки розвідувальних відомостей у третій фазі n_3, тобто кількість ПУ-СК.

Згідно принципів бойового застосування комплексу Р-330 К один комплект ПУ Р-330 К призначається для роботи в режимі ПУ-СК, у якому здійснюються розрахунки координат ДРВ і цілерозподіл в КХ- та УКХ-діапазонах, тому для КХ- та УКХ-діапазонів $n_3 = 1$.

к) інтенсивність старіння розвідувальної інформації *S*.

Як відомо, лінія зв'язку вважається подавленою, якщо не прийнято більше 50 % переданої інформації. Приймемо, що середня тривалість роботи лінії радіозв'язку в телефонному та телеграфному режимах без програмної перестройки робочої частоти при передачі радіограм складає до 1 хв., тому час випередження буде складати 0,5 хв. Інтенсивність старіння розвідувальної інформації є величина, обернено пропорційна часу випередження:

$$S = \frac{1}{t_в}, \qquad (3.52)$$

З (9) отримуємо: *S*=120 1/год.

Порядок проведення оцінки ефективності ведення РР.

1. Враховуючи вищевикладене, для КХ-діапазону [28]:

$\lambda_{вх1}$=500 1/год; $\mu_1 n_1$=1800×1=1800 1/год;

$\lambda_{вх2}$=250 1/год; $\mu_2 n_2$=1800×1=1800 1/год;

$\lambda_{вх3}$=250 1/год; $\mu_3 n_3$=600×1=600 1/год;

α_1=1300; α_2=1550; α_3= 350 (1/год), *S*=120 (1/год).

2. Розрахуємо своєчасність обробки за формулою:

$$P_{co} = 1300 \times 1550 \times 350 \times \left[\begin{array}{l} \dfrac{1}{(1300+120)\times(1550-1300)\times(350-1300)} + \\ + \dfrac{1}{(1550+120)\times(1300-1550)\times(350-1550)} + \\ + \dfrac{1}{(350+120)\times(1300-350)\times(1550-350)} \end{array} \right] = 0{,}633$$

Таким чином, втрати в обробці розвідувальних відомостей в КХ-діапазоні становлять 36,7 %, а ймовірність несвоєчасної обробки розвідувальних відомостей складає 0,367.

3. Для УКХ-діапазону [28]:

$\lambda_{вх1}$=400 1/год; $\mu_1 n_1$=1800×1=1800 1/год;

$\lambda_{вх2}$=200 1/год; $\mu_2 n_2$=1800×1=1800 1/год;

$\lambda_{вх3}$=200 1/год; $\mu_3 n_3$=600×1=600 1/год;

α_1=1400; α_2=1600; α_3= 400 (1/год), *S*=120 (1/год).

4. Розрахуємо своєчасність обробки за формулою:

$$P_{co} = 1400 \times 1600 \times 400 \times \left[\begin{array}{l} \dfrac{1}{(1400+120)\times(1600-1400)\times(400-1400)} + \\ + \dfrac{1}{(1600+120)\times(1400-1600)\times(400-1600)} + \\ + \dfrac{1}{(400+120)\times(1400-400)\times(1600-400)} \end{array} \right] = 0{,}659$$

Таким чином, втрати в обробці розвідувальних відомостей в УКХ - діапазоні складають 34,1 %, а ймовірність несвоєчасної обробки розвідувальних відомостей складає 0,341 [28].

Контрольні запитання до 3 розділу:

1.Що таке радіоелектронне подавлення. Який зміст та складові?

2.Яка мета радіоелектронного подавлення систем зв’язку?

3.Що таке радіоподавлення. Які методи радіоподавлення систем зв’язку Вам відомі?

3.Які основні завдання радіоподавлення систем зв’язку?

4.Які комплекси радіоподавлення Російської Федерації вам відомі? Наведіть основні тактико-технічні характеристики.

5.Що таке оптико-електронне подавлення? Наведіть методи оптико-електронного подавлення.

6.Який зміст гідро - акустичного подавлення систем передачі інформації?

7.Які основні способи бойового застосування частин (підрозділів) РЕБ під час ведення РЕП систем зв’язку та управління?

8.Які умови радіоподавлення систем зв’язку?

9. Що таке радіоелектронна завада? Наведіть класифікацію радіоелектронних завад.

10. Що таке коефіцієнт подавлення, як його визначити, як визначити зону радіоподавлення засобів зв’язку під час ведення бойових дій?

11. Як визначити ефективність радіоподавлення системи зв’язку?

12.В чому зміст методики визначення ефективності радіоподавлення системи зв’язку?

13. В чому зміст методики розробки сценаріїв радіоелектронного та електромагнітного подавлення засобів зв’язку для розробки методів їх завадозахисту?

14. Що таке радіоелектронне забезпечення процесів РЕБ? Що таке радіоелектронна розвідка, її зміст та складові?

15. Які показники ефективності радіоелектронної розвідки Вам відомі? Сутність методики оцінки ефективності ведення радіорозвідки частинами (підрозділами) РЕБ в гібридних діях?

РОЗДІЛ 4
РАДІОЕЛЕКТРОННИЙ ЗАХИСТ ПІДРОЗДІЛІВ ТА ЗАСОБІВ ЗВ'ЯЗКУ

Радіоелектронний захист (РЕЗт) своїх систем і засобів – це комплекс організаційно-технічних заходів, спрямований на забезпечення зниження ефективності ведення противником РЕР, РЕП, застосування ВТЗ та радіокерованої зброї і забезпечення стійкої роботи своїх радіоелектронних засобів.

Радіоелектронний захист організовується і здійснюється з метою забезпечення стійкої роботи своїх систем і засобів управління військами і зброєю [18-21]. Він включає: захист від РЕР противника; захист радіоелектронних засобів від ураження високоточною зброєю; захист своїх РЕЗ від радіоелектронних завад противника; захист від взаємних завад; захист від іонізуючого та електромагнітного випромінювання; управління радіочастотним ресурсом (РЧР) військової підсистеми користувачів (рис. 4.1) [18-21].

Основними завданнями радіоелектронного захисту є [18-21]:

– забезпечення стійкої роботи своїх систем управління військами (силами) та зброєю;

– радіоелектронне прикриття військ і об'єктів від прицільних ударів авіації, високоточної зброї та зброї, що наводиться на випромінювання [26];

– зниження ефективності ведення противником технічної розвідки.

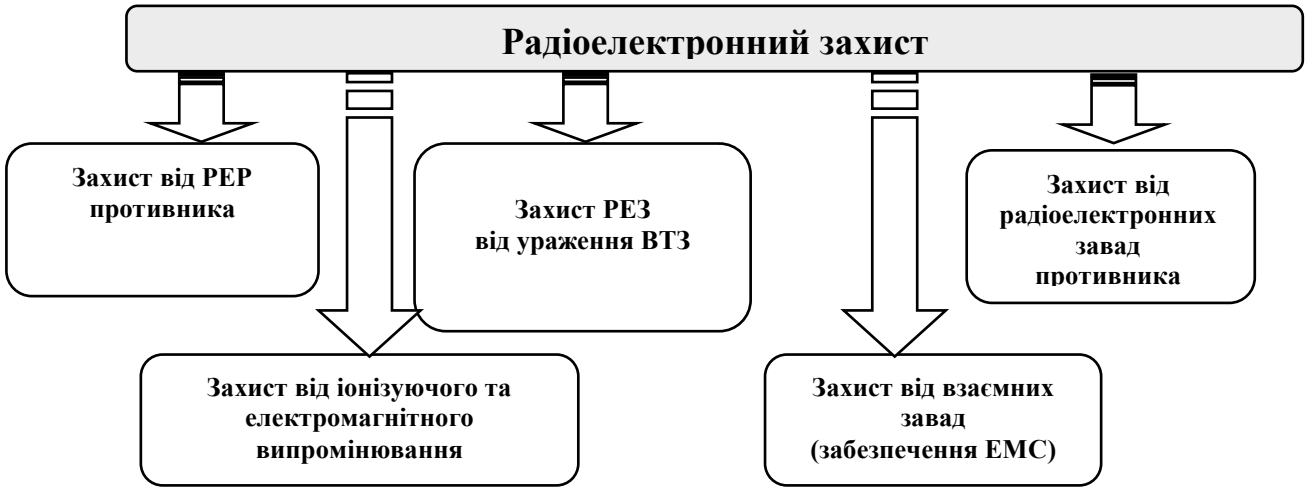


Рис. 4.1. Складові радіоелектронного захисту

Радіоелектронний захист систем і засобів управління своїми військами і зброєю спрямований на забезпечення стійкої роботи цих систем і засобів в умовах ведення противником радіоелектронної боротьби і взаємного впливу радіоелектронних засобів в зоні розташування угруповання військ.

Загальне керівництво усіма діями по організації і забезпеченню РЕЗт в військах здійснює Центральне управління РЕБ Головного командування Сил

Підтримки ЗС України. Управління РЕБ здійснює координацію заходів по РЕЗт РЕЗ між видами і родами військ.

Відповідальність за РЕЗт систем і засобів управління, об'єктів в оперативно-стратегічних угрупованнях військ (сил), об'єднаннях, з'єднаннях та частинах ЗСУ несуть відповідні командувачі (командири).

Начальники штабів об'єднань (з'єднань) є організаторами радіоелектронного захисту. Вони керують роботою служби РЕБ, та іншими службами штабів по підготовці військ для виконання бойових завдань в умовах ведення противником РЕБ і здійснюють контроль за проведенням заходів по РЕЗт в підпорядкованих військах.

4.1. Загальна характеристика організаційних методів радіоелектронного захисту

Організаційні методи захисту РЕЗ від засобів РЕБ противника дозволяють вирішити завдання РЕЗт за рахунок раціонального використання РЕЗ, організації взаємодії між ними, підготовки особового складу і матеріальної частини до роботи в умовах РЕБ [18-21, 26].

До основних організаційних заходів захисту радіоелектронних засобів відносяться:

– створення розгорнутої мережі КП і систем управління;

– комплексне використання радіоелектронних засобів різних принципів та тих, що працюють у різних діапазонах частот;

– створення хибних угруповань, РЕЗ і радіомереж, необхідних резервів;

– правильне розташування радіоелектронних засобів в угрупуваннях і їх уміле використання;

– підготовка військ до ведення бойових дій в умовах РЕБ.

Розглянемо більш детально визначені заходи РЕЗт.

Розгорнута мережа КП і ПУ є обов'язковою умовою ефективного управління військами (силами) і зброєю в умовах ведення противником РЕБ. Поряд із стаціонарними основними і запасними командними пунктами (КП) та центрами (КЦ) системи управління повинні включати наземні рухомі і повітряні КП (КЦ). Вони повинні бути автоматизованими і мати швидкодіючі ЕОМ, які здатні в реальному масштабі часу забезпечити адаптацію угруповання РЕЗ в цілому і його окремих елементів до умов РЕО, що складається.

Комплексне використання РЕЗ з різними принципами дії і частотними діапазонами передбачає створення угруповань, до складу яких входять наступні засоби:

– активних, пасивних і активно-пасивних комплексів;

– командного активного, напівактивного і пасивного наведення (самонаведення) ЗРК і ЗАК;

– радіо-, радіорелейного, тропосферного і супутникового радіозв'язку;

– багаточастотних і тих, що перестроюються по частоті;

– засоби, що працюють в різних ділянках радіо- і оптичного діапазонів частот;

– засоби, що використовують як імпульсне, так і неперервне випромінювання, різні види модуляції (маніпуляції) сигналів і методи передачі інформації.

Таке використання РЕЗ виключає, по-перше, надійне подавлення завадами всіх РЕЗ угруповання, заважає застосуванню самонавідної зброї, зменшує вплив на роботу РЕЗ іонізуючих утворень ядерних вибухів. По-друге, воно дозволяє вирішувати завдання боротьби із засобами повітряного нападу на основі використання сигналів завад або сигналів, які випромінюють самі об'єкти, що сприяє першочерговому (упереджуючому) ураженню джерел завад. В результаті цього можливості отримання інформації про противника і дії по ньому активними засобами ППО значно підвищуються.

Створенням хибних угруповань, прихованих (скритих) РЕЗ і радіомереж, дублюючих і обхідних напрямків зв'язку, необхідних резервів вирішується в основному перше завдання. Так, наприклад, хибне РЛ поле, яке створено на базі РЕЗ старого парку, примушує противника задіяти частину сил і засобів на його подавлення і знищення. Це призводить до їх розпорошення і, як наслідок, до полегшення умов роботи РЕЗ основного радіолокаційного поля. Використання дублюючих і обхідних напрямків зв'язку, окрім розпорошення засобів противника дозволяє збільшити надійність зв'язку в умовах іонізації визначених просторових зон тактичними ядерними вибухами. Разом із проведенням цих заходів досягається і ряд нових результатів. Так, створення "прихованих" РЕЗ і радіомереж, які включаються тільки в крайньому випадку, виключає попередню підготовку противника до їх подавлення і знищення. В результаті цього подавлення завадами таких РЕЗ (знищення самонавідною зброєю) може виявитись неможливим або малоефективним, особливо у таких випадках, коли вони працюють в нових частотних діапазонах або на нових принципах.

Правильне розташування РЕЗ в угрупованнях військ, їх уміле використання і організація взаємодії є заходами захисту, які здійснюються як в період підготовки, так і в ході бойових дій. Ці заходи забезпечують найбільш доцільне використання в інтересах бою всієї різноманітності РЕ засобів всіх родів військ, засобів АСУ і зв'язку створених угрупувань військ, особливо на напрямку головного удару.

Вирішення цього завдання в значній мірі визначається:

– вибором та інженерним обладнанням позицій РЕЗ із врахуванням їх захисту від самонавідної на випромінювання зброї, а також електромагнітних і іонізуючих випромінюваннь ядерних вибухів;

– виконанням вимог прихованого (скритного) управління військами, встановлених режимів роботи РЕЗ і правил їх експлуатації;

– безперервною оцінкою на КП всіх систем управління РЕО, що склалася, і визначенням найбільш доцільних способів бойового застосування РЕЗ, своєчасним маневром силами і засобами, використанням резервів, прихованих РЕЗ і радіомереж;

– зосередженням зусиль на першочерговому знищенні носіїв засобів РЕБ, пошуку і знищенню передавачів завад, що закидаються;

– раціональним призначенням і маневром РЕЗ, оперативним вибором робочих частот відповідно до РЕО, що склалася, а для засобів радіозв'язку – з урахуванням характеристик трас з найбільшим часом їх надійного зв'язку;

– своєчасним отриманням інформації по каналам взаємодії і рівнем організації спільних дій по виявленню і знищенню противника.

– Ефективність захисту РЕЗ є одним із вирішальних чинників підготовки військ для ведення бойових дій в умовах РЕБ. Вона є основною складовою частиною бойової підготовки і виховної роботи військ і передбачає:

– постійне вивчення можливостей противника по порушенню нормального функціонування РЕЗ управління військами і зброєю угрупувань військ, способів застосування ним засобів РЕБ;

– тверде засвоєння найбільш доцільних прийомів управління військами в складній РЕО, методів і апаратури захисту своїх РЕЗ від засобів РЕБ противника;

– морально – психологічну підготовку особового складу розрахунків РЕЗ для роботи в складних умовах РЕБ.

Визначальну роль у вирішенні цих завдань мають тренування особового складу, навчання військ і бойове застосування зброї в реальних умовах РЕО.

4.2. Загальна характеристика технічних методів радіоелектронного захисту

Захист РЕЗ від активних і пасивних завад технічними методами здійснюється [18-21]:

– створенням умов, які виключають порушення нормального режиму приймальних пристроїв РЕЗ при дії завад;

– виділенням інформативних сигналів із суміші з завадами;

– врахуванням особливостей формування імітуючих завад і їх впливу на системи протирадіолокаційних цілей за дальністю, швидкістю і кутовим координатам;

– використанням сигналів завад для отримання інформації про координати носіїв завад і наведення на них засобів ураження.

Порушення нормального режиму роботи приймачів РЕЗ спостерігається при прийомі потужних сигналів завад (перевантаженні) через обмежений динамічний діапазон. Для розширення динамічного діапазону приймачів РЕЗ здійснюють наступне:

– у вихідних каскадах підсилювача проміжної частоти і протирадіолокації використовують потужні підсилюючі пристрої, які працюють при підвищених напругах;

– вводять ручне і різноманітне автоматичне регулювання підсилення; особливо ефективним в умовах маскуючої завади є ШАРП (шумове автоматичне регулювання підсилення), яке дозволяє підтримувати постійний

рівень умовної ймовірності хибної тривоги незалежно від інтенсивності завади;

– використовують підсилюючі пристрої з логарифмічними амплітудними характеристиками.

Виділення інформативних сигналів із суміші з завадами базується на використанні відмінностей між інформативними сигналами і сигналами завади. Підвищення ефективності цієї властивості засобів прийму та обробки інформації може бути досягнуто за рахунок:

– збільшення енергії корисних сигналів (метод “силової боротьби” з завадою, або енергетична селекція);

– зменшення рівня бокових пелюсток ДСА, або підвищення коефіцієнту підсилення антени (просторова селекція);

– використання частотної, часової та поляризаційної селекції.

Підвищення завадозахищеності РЕЗ на основі врахування особливостей формування імітуючих завад і їх впливу (дії) на систему автосупроводження досягається:

– ускладненням створення ефективних імітуючих завад;

– своєчасним виявленням впливу імітуючих завад;

– компенсацією складових завади, що несуть хибну інформацію про кутові координати цілі.

Використання завад для отримання інформації про координати і параметри руху їх постановників, наведення на них засобів ураження здійснюється методами пасивної локації.

4.3. Радіоелектронний захист від активних радіозавад

Розглянемо більш детально можливі методи селекції (виділення) корисного сигналу радіоелектронного засобу на фоні активних радіозавад.

Енергетична (амплітудна) селекція. Енергетична селекція в умовах РЕП досягається підвищенням енергетичного потенціалу РЕЗ, тобто “силовим” подоланням завади.

Збільшення енергетичного потенціалу РЕЗ здійснюється безпосередньо, або раціональним розподілом енергії в просторі.

Безпосереднє збільшення енергетичного потенціалу досягається:

– використанням потужних генераторних пристроїв;

– застосуванням багатогенераторних передавальних систем;

– використанням сигналів великої тривалості.

В результаті розвитку електровакуумної техніки потужність окремих генераторних приладів на сьогодні досягає 50 МВт в імпульсному і декілька сотень кіловат в неперервному режимах. Найближчим часом ці показники можуть збільшитися в два рази. Але треба мати на увазі, що збільшення потужності веде до збільшення габаритів, вартості генераторів і джерел живлення, пред`являє жорсткі вимоги до енергетичної міцності фідерного тракту і потребує прийняття спеціальних заходів для захисту обслуговуючого персоналу. Тому при конструюванні сучасних РЕЗ здійснюється розумний

компроміс між потрібною енергетикою РЕЗ і вимогами до його мобільності, вартості і т.п.

Можливості підвищення енергетичного потенціалу РЕЗ за рахунок застосування зондуючих сигналів великої тривалості особливо збільшилися у зв`язку з розробкою і використанням методів оптимальної обробки широкосмугових сигналів. При цьому, як відомо, можна мати добру розрізняльну здатність, зберігаючи велику енергію в імпульсі.

Раціональний розподіл енергії у просторі допускає, як правило, підвищення енергії, що випромінюється в загрозливих напрямках (секторах) за рахунок більш тривалого зондування цих напрямків, або зміни параметрів сигналів, наприклад, збільшення тривалості імпульсів. Він базується на комплексному використанні РЕЗ з оглядом простору по програмі, яка змінюється в залежності від завадової обстановки.

Просторова селекція. Під просторовою селекцією розуміють підвищення завадозахищеності РЕЗ за рахунок використання відмінностей в напрямках прийому корисних сигналів і завад.

Основними заходами просторової селекції є:

– звуженням головного пелюстка діаграми спрямованості антени (збільшенням коефіцієнта підсилення);

– зменшенням рівня бокових пелюстків ДСА;

– ослабленням завад, що приймаються по боковим пелюсткам, за рахунок багатоканальної обробки.

Звуження головної пелюстки ДСА РЕЗ може бути досягнуте за рахунок скорочення довжини хвилі або збільшення геометричної площі антени. При цьому треба вирішувати протиріччя і знаходити компроміси, щоб досягти балансу всіх ТТХ РЕЗ.

Рівень бокових пелюсток можна зменшити за рахунок раціональної побудови антен, а саме:

– вибором оптимального співвідношення між параметрами характеристики спрямованості опромінювача і геометричними розмірами антени;

– зменшенням екрануючої дії опромінювача;

– створенням оптимального розподілу амплітуд і фаз електромагнітного поля в апертурі антени;

– застосуванням додаткових екранів і поглинаючих покриттів на елементах антени, що найбільш сильно розсіюють електромагнітну енергію;

– раціональним розміщенням антенних систем на місцевості, що виключає вплив сигналів завад, відбитих від місцевих предметів.

Поряд з розробкою зазначених методів зниження рівня бокових пелюстків розробляються схемні методи захисту РЕЗ від завад, які засновані на застосуванні додаткових каналів прийому зі своїми антенами (звичайно слабо спрямованими) і пристроями компенсації.

Поляризаційна селекція – метод захисту РЕЗ від завад з регулярною поляризацією. При цьому методі використовуються відмінності між поляризаціями сигналу і завади. Для реалізації методу поляризаційної селекції

необхідно щоб поляризація корисного сигналу змінювалася за відповідним законом (наприклад, кругова або еліптична) і щоб в будь-який момент часу вектор поляризації сигналу був близьким до ортогонального вектору поляризації завади, що досягається відповідними технічними рішеннями в радіоелектронних системах. Перевагою методу є можливість значного послаблення завад по головному пелюстку ДСА.

Для реалізації методу використовують поляризаційні селектори на базі кореляційних автокомпенсаторів завад, в яких коливання корисного сигналу можна розкласти на дві складові: одну має поляризацію завади, а друга – їй ортогональна. Складова сигналу, що співпадає по поляризації з завадою, подавляється автокомпенсатором. Корисний вихідний ефект створюється лише складовою, поляризація якої ортогональна до поляризації завади.

Частотно-часова селекція. Всі методи частотно-часової селекції умовно підрозділяються на дві групи:

– методи раціонального розподілу енергії зондуючих сигналів по спектру частот;

– методи селекції сигналів із суміші з завадами на основі розбіжностей в їх частотно-часових характеристиках.

Раціональний розподіл енергії зондуючих сигналів по спектру частот досягається:

– застосуванням РЕЗ, що перестроюються по частоті;

– використанням широкосмугових зондуючих сигналів;

– освоєнням нових діапазонів довжин хвиль.

Перелаштування робочої частоти може бути ручною або автоматичною. Як ручна так і автоматична перестройка може здійснюватись під впливом завад, або оператором. При цьому вона може виконуватись дискретно (стрибком) або неперервно. Закон перелаштування може задаватися програмою або бути випадковим (сигнали з програмним перелаштування робочої частоти (ППРЧ)). При цьому розрізняють повільну (до 100 стрибків за секунду) та швидку (близько 500 стрибків за секунду) ППРЧ. Існує перелаштування частоти від імпульсу до імпульсу, при якій неможливе подавлення прицільними завадами тих об`єктів (цілей), дальність яких від РЕЗ менша дальності до постановника завад.

Методи селекції сигналів із суміші з завадами на основі їх частотно-часових розбіжностей дуже різноманітні. Проте, для виділення сигналу із суміші з завадами найбільш частіше використовують:

– вузькосмуговість завади у порівнянні з сигналом;

– вузькосмуговість модулюючої завади шумової напруги, або так звану “недосконалість” частотно-модульованих (амплітудно-частотно-модульованих) шумових завад;

– відмінності в амплітудах, тривалостях і частотах слідування сигналів і завад.

Широке застосування в практиці виділення корисного сигналу на фоні імпульсних завад отримали селектори за тривалістю сигналів і їх періоду слідування, а також за амплітудою.

Захист від імітуючих радіозавад. Відомо, що вид і характеристика імітуючої завади (ІП) залежить від призначення РЕЗ, яка подавляється, і від характеристик його сигналу. Тому, з великої різноманітності ІП можна виділити дві основні групи: ІП, що призначені для порушення роботи РЛС виявлення цілей, а також ІП, що подавляють РЛС супроводження.

Захист РЛС виявлення цілей від імітуючих завад. Імітуючі завади для РЛС виявлення цілей представляють собою імпульсні однократні або багатократні завади у відповідь. Тобто, вони імітують оманну ціль, що має дальність, яка відрізняється від дальності до істинної цілі.

Багатократні ІП імітують велику кількість цілей на різних дальностях і, в основному, вирішують завдання перевантаження прийомних каналів. Ці радіозавади створюються за рахунок ретрансляції зондуючого сигналу РЛС спеціальним пристроєм, який затримує сигнал РЛС, а потім випромінює у відповідь.

Для захисту від таких завад можна застосовувати перемінний запуск в РЛС, а для захисту від завад, що діють по боковим пелюсткам ДСА, використовують методи когерентної або некогерентної компенсації з додатковою слабо спрямованою антеною.

Захист РЛС супроводження цілей від імітуючих завад. Головне практичне застосування ІП знайшли для протидії РЛ системам, в яких застосовується режим автоматичного супроводження цілей з метою: ускладнити вибір істинної цілі для супроводження; збільшити помилки супроводження; викликати зрив автоматичного супроводження цілі.

Імітуючі завади, що призначені для зриву автоматичного супроводження, називають завадами у відповідь. Вони відводять (порушують супроводження) за дальністю або кутовим координатам.

Для захисту від завад, що здійснюють зрив супроводження за дальністю застосовують:

– складні (широкосмугові) сигнали, що ускладнюють створення ІП;
– багатоканальні схеми з різними сигналами.

Схемні методи дозволяють своєчасно виявляти “відведення” стробів супроводження завадою і повернути їх на дальність істинної цілі.

Для захисту від ІП, що відводять по куту місця, застосовують метод некогерентної компенсації завад, що впливають на бокові пелюстки ДСА. Найбільш досконалим методом захисту від таких завад є застосування багатоімпульсних вимірювачів, де інформація про кутові координати цілі визначається по одному імпульсу.

4.4. Радіоелектронний захист від високоточної зброї

Високоточна зброя являє собою комплекс функціонально зв`язаних елементів засобів розвідки, цілевказання та наведення на ціль засобів ураження, високоточних засобів ураження і засобів доставки. До високоточної зброї (ВТЗ) відносять без’ядерні боєприпаси, які в сукупності з системою наведення дозволяють знищити задані об`єкти з імовірністю не нижче 0,9 за

будь-яких метаумов, часу доби, при активній протидії з боку противника [18-21, 26].

Для масового ураження цілей на всю глибину оперативної побудови військ необхідна достовірна, повна, в реальному масштабі часу інформація про характеристики об`єктів ударів.

Найбільш широкого розповсюдження в системах ВТЗ отримали засоби розвідки наземного, повітряного і космічного базування.

Всі засоби розвідки наземного, повітряного і космічного базування являють собою складну комплексну сукупність датчиків, розташованих на одному чи декількох носіях. Можуть також використовуватися різні класи носіїв.

Ведуться роботи по створенню спеціалізованої системи розвідки і цілевказання для систем ВТЗ (програма MTS). Така система розвідки повинна забезпечити знаходження, класифікацію, розпізнавання, супроводження рухомих цілей на території противника.

Основною ланкою високоточної зброї, що забезпечує якісний стрибок її бойового потенціалу, є розробка нового покоління систем наведення на ціль, які реалізують концепцію “постріл-ураження”. Залежно від характеру апаратури управління боєприпасом, місця її розташування, особливостей енергетичного контакту з об`єктом ураження розділяють 4 типи управління: телеуправління; автономне; самонаведення; змішане або комбіноване [21, 26].

Самонаведення ВТЗ здійснюється за допомогою головок самонаведення (ГСН), які приймають енергію, що випромінює об`єкт, або яка відбивається від нього.

За призначенням високоточна зброя підрозділяється на ВТЗ тактичного призначення (глибина зони бойового застосування до 30 км); оперативно-тактичного призначення (до 200 км); оперативного призначення (понад 200 км).

Високоточна зброя тактичного призначення використовується з метою знищення танків, БМП, БТР, самохідної артилерії, зенітних комплексів, бойових машин ПТУР та інших броньованих об`єктів.

Високоточна зброя оперативно-тактичного призначення використовується для нанесення ударів по районах зосередження колон бронетанкової техніки та найбільш важливих об`єктах другого ешелону об`єднання з метою їх ізоляції від зв`язаних бойовими діями з`єднань і частин першого ешелону.

Високоточна зброя оперативного призначення використовується для нанесення ударів по районах зосередження бойової техніки, мостах, тунелях та інших цілях для затримання висування резервів, а також для знищення найбільш важливих об`єктів військового і економічного потенціалу країни у глибині її території.

Засобами доставки ВТЗ тактичного призначення є: наземні протитанкові комплекси; ствольна артилерія та реактивні системи залпового вогню; вертольоти армійської авіації, безпілотні літальні апарати; літаки штурмової авіації.

До засобів доставки ВТЗ оперативно-тактичного призначення відносять: літаки тактичної авіації, тактичні і оперативно - тактичні ракети.

Доставка ВТЗ оперативного призначення може здійснюватися літаками тактичної і стратегічної авіації, крилатими ракетами наземного і повітряного (морського) базування.

Більшість типів ВТЗ є багатоцільовою зброєю, що застосовується для ураження різноманітних об`єктів. Найбільш масовими системами ВТЗ є протитанкові ракетні комплекси (ПТРК), які складають основу протитанкової оборони сухопутних військ армій економічно розвинутих країн світу.

В умовах застосування противником ВТЗ складовою частиною живучості ТВУЗ є їх захищеність від неї.

Основні технічні характеристики різних сучасних ГСН приведені в табл. 4.1.

Таблиця 4.1

Тактико-технічні характеристики головок самонаведення

Тип ГСН	**Дальність дії, км**	**Діапазон частот, ГГц**	**Поле зору, град**	**Точність наведення, м**	**Потужність випромінювання, Вт**	**Типові цілі для ураження**	**Зразки озброєння**	**Переваги**
Тепловізійна	До 20	$3\text{-}8x10^4$	Скануюча ІЧ грата	2-2	-	Танки, БМП, автомобілі	ПТРК, КАБ, КР Мейверік - Е”	Використання у будь-який час доби у диму і тумані
Лазерна: активна напів-активна	До 15 До 10	$4\text{-}6x10^5$	Скануюча грата до 0,5	1,5-8	До 100 До 1000	Танки, БМП, автомо-білі	“Халфайр”,“ Мейверік - Е”	Наведення на маловисотні цілі
Радіолокаційна: активна напівактив-на пасивна	До 2 До 3 0,5 - 0,6	30 – 40 - -	4	0,5 –1,5 - -	1	БТТ	КР “УОСП”	Наведення у тумані, диму, пилу, вночі, малі габарити ГСН
Радіометрична, кореля-ційна	200 - 400	3 – 20	-	10	До 10^3	Площадна ціль	КР GLAM МКАБМ	Використання за будь-якої погоди, висока захищеність
Пасивна з випромінюванням цілі	70 – 100	3 – 20	2	9	10	Працюючі РЛС	ППР “Харм” та інш.	Використання за будь-якої погоди
Випромінювання ТВ-командна	30 – 40	$4\text{-}6x10^5$	-	3	-	ОВТ	КАБ	Використання по неконтрастних цілях в ІЧ діапазоні
Різнодально-мірна (радіо)	50 – 70	3 – 10	-	9 – 15	1000	ОВТ з відомими корди-натами	РВК ПЛСО, КАБ GBU--20	Багаторазове використання апаратури

Захист військ від ВТЗ – комплекс організаційних, спеціальних і технічних заходів, що здійснюються з метою виключення раптового удару високоточними засобами, зниження ефективності його ударів по своїм

військам, створення частинами та підрозділами сприятливих умов для вступу в бій, успішного його ведення.

Розглянемо більш детально захист РЕЗ від ВТЗ, а саме захист від самонавідної на випромінювання зброї (снарядів).

Основними елементами головки самонаведення є координатор, який вимірює кутові відхилення напрямку на РЛС від повздовжньої вісі ракети по азимуту і куту місця. Координатор виробляє напруги, що пропорційні цим кутовим відхиленням. Ці напруги використовуються для управління кермами ракети таким чином, щоб її вісь була орієнтована на джерело випромінювання (ціль).

Визначення кута місця і азимуту РЛС здійснюється моноімпульсним методом.

Всі відомі методи захисту РЕЗ від самонавідної на випромінювання зброї можна умовно поділити на пасивні, активні і комбіновані. Розглянемо їх більш детально.

Активні методи захисту

До активних методів відносяться такі, за яких захист РЕЗ здійснюється знищенням самонавідної зброї або порушенням нормального функціонування її системи самонаведення за допомогою заважаючих випромінювань [18-21, 26].

Основними методами захисту РЕЗ від СНЗ є:

– знищення СНЗ або її носіїв;

– завчасний підрив снарядів під впливом випромінюваннь, що діють на неконтактні радіопідривачі снарядів;

– використання заважаючих випромінюваннь.

Ці способи захисту не потребують зміни режимів функціонування РЕЗ і не призводять до зниження їх ефективності. Разом з тим їх реалізація пов’язана з певними труднощами і значними економічними витратами. Так, наприклад, знищення самонавідного засобу ускладнене через великі швидкості руху. Штучний підрив неконтактних радіопідривачів ускладнений через відсутність відомостей про принципи їх дії і основні характеристики.

Тому, широке розповсюдження мають методи захисту, що просто реалізуються за рахунок використання заважаючих випромінюваннь.

Заважаючи випромінювання можуть бути маскуючими, імітуючими і відволікаючими. Маскуючі випромінювання в принципі можливі, але вони неекономічні, тому що середня потужність доповнюючого випромінювача повинна перевищувати середню потужність РЕЗ, який захищається. Імітуюче випромінювання потребує великої кількості додаткових випромінювачів, що по потужності близькі до РЕЗ, яка захищається, і тому економічно недоцільне. У зв`язку з цим найбільше розповсюдження отримало відволікаюче випромінювання; воно може бути когерентним і некогерентним.

За наявності некогерентного додаткового випромінювача (ДВ) снаряд орієнтується на так званий енергетичний центр пари (або більшої кількості) випромінювачів і здійснюється зсув точки наведення на величину помилки.

Пасивні методи захисту

Пасивні методи мають за мету зниження ефективності самонавідної зброї шляхом удосконалення РЕЗ і способів їх бойового застосування [18-21, 26].

Захист РЕЗ від самонавідної зброї пасивними методами здійснюється:

– підвищенням стійкості РЕЗ до уразливих факторів самонавідної зброї;

– збільшенням енергетичної і просторової прихованості;

– змінами часових режимів функціонування і параметрів випромінювання РЕЗ, що захищаються.

Підвищення стійкості РЕЗ до уразливих факторів самонавідної зброї забезпечується розробкою спеціальних конструкцій антенних систем, їх виносом на відповідну відстань від основної апаратури і інженерним обладнанням позицій РЕЗ.

Збільшення енергетичної і просторової прихованості досягається:

– використанням мінімально необхідних потужностей випромінюваннь;

– зменшенням рівня головного і бокових пелюсток ДСА;

– застосуванням широкосмугових сигналів, що виключає при неоптимальній обробці випромінювань по бокових пелюстках отримання необхідного для самонаведення відношення сигнал/шум;

– компенсацією сигналів РЕЗ, що випромінюються по бокових пелюстках в спектрах найбільш ймовірного застосування самонавідної зброї;

– виключенням паразитного випромінювання РЕЗ.

Методи захисту, що базуються на змінах часових режимів функціонування РЕЗ, мають на меті зменшення кількості інформації, яка надходить від РЕЗ в пасивну систему самонаведення, і, як наслідок, збільшення помилок самонаведення.

Основними з цих методів є [18-19, 26]:

– максимальне скорочення часу роботи РЕЗ на випромінювання, в тому числі використання випромінювання РЕЗ, що мерехтить по відповідній програмі, з метою накопичення помилки наведення, коли її збільшення за час мовчання не усувається за час випромінювання;

– повне виключення РЕЗ, що атакується, наприклад, після відділення на екрані індикатора РЕЗ мітки від літака-носія і самонавідного засобу;

– виключення РЕЗ в секторі, що відповідає орієнтації головної пелюстки її ДСА в напрямку на засіб ураження, який наводиться тільки по головній пелюстці діаграми спрямованості антени РЕЗ;

– повільне розвертання антени РЕЗ з наступним переключенням передавача на еквівалент антени, в результаті чого можливе перенацілення самонавідної зброї, наприклад, на місцевий предмет;

– позмінна робота двох однотипних РЕЗ, що рознесені на одній позиції на певну базу.

Використання цих способів супроводжується деяким зниженням ефективності РЕЗ, що може бути скомпенсоване частково лише при роботі РЕЗ в складі угрупування з єдиною системою управління. Ця система на основі даних про застосування СНЗ повинна визначати найбільш доцільні режими функціонування РЕЗ і управляти їх роботою.

Одним із важливих моментів, що визначають виконання цих завдань, є своєчасне виявлення СНЗ. У зв`язку з цим особливо актуальним стає широке застосування телевізійних, оптико-візуальних та інших пасивних засобів розвідки, по яких застосування СНЗ ускладнюється.

Комбіновані методи захисту

Комбіновані методи захисту РЕЗ від СНЗ являють собою у загальному випадку конкретні поєднання різних методів пасивного або активного захисту, а також різні їх комбінації.

На практиці використовуються, наприклад, такі комбіновані методи [18-21, 26]:

– метод періодичних включень і виключень РЕЗ з забороною випромінювання у відповідному секторі або на час польоту СНЗ на кінцевій ділянці траєкторії, з періодичною зміною робочих частот або періодів випромінювання сигналів;

– метод відволікаючого випромінювання з включенням РЕЗ на випромінювання тільки у відповідному секторі, і т.п.

Основною перевагою комбінованих методів є можливість підвищення ефективності захисту РЕЗ при менших сумарних економічних витратах. У зв`язку з цим вони можуть включати також такі методи захисту, які самостійно широкого використання не мають.

Так, наприклад, доцільне поєднання імітуючого випромінювання з випромінюванням РЕЗ, що мерехтить по відповідній програмі, або з перевлаштуванням їх робочих частот. Такий метод захисту РЕЗ значно підвищує ймовірність захвату ГСН СНЗ сигналів імітуючих джерел, в якості яких можуть використовуватись передавачі, що відпрацювали встановлений ресурс.

Заходи захисту РЕЗ, військ і об`єктів від ураження системами ВТЗ

Заходи захисту РЕЗ від СНЗ спрямовані на використання спланованих і добре відпрацьованих на тренуваннях методів захисту. З фізичної точки зору методи захисту зручно класифікувати за їх цільовим призначенням:

– методи, що спрямовані на зменшення інформаційної спроможності РЕЗ (виключення РЕЗ в секторі, робота РЕЗ, яка переривається і т.п.);

– методи, що забезпечують зсув точки наведення снаряду (додаткові випромінювачі, перевипромінювання енергії сигналу штучними або природними відбивачами);

– постановка завад засобам СНЗ;

– підвищення живучості РЕЗ (відділення активних систем від основної апаратури, зниження рівня бокових пелюсток ДСА, підвищення енергетичної скритності;

– знищення СНЗ (застосування спеціальних ЗУР, або завчасний неконтактний підрив радіопідривача).

4.5. Захист радіоелектронних засобів від електромагнітного і іонізуючого випромінюваннь

В умовах застосування тактичної ядерної та електромагнітної зброї (ЕМЗ) в сучасних збройних конфліктах важливого значення набуває захист РЕЗ від випромінюваннь ядерних вибухів. До основних чинників ядерного вибуху, що впливають на працездатність РЕЗ, відносять електромагнітний імпульс (ЕМІ) і проникну радіацію [18-21].

Захист РЕЗ від іонізуючих випромінюваннь здійснюється в основному організаційними методами і базується на використанні тих РЕЗ, вплив на які по частотних діапазонах, або за просторовим розташуванням є мінімальним.

Методи захисту РЕЗ від електромагнітних випромінюваннь зводяться, в основному, до виключення впливу на роботу РЕЗ високих напруг і струмів наведених ЕМІ. Вони є як технічними, так і організаційними.

Основними технічними методами захисту РЕЗ від ЕМІ є:

– екранування апаратури і якісне з`єднання екранів, оболонок кабелів з контуром заземлення;

– оптимальний монтаж схем, вузлів і блоків апаратури;

– використання комплектуючих елементів з підвищеною стійкістю до дії ЕМІ;

– застосування схем або пристроїв, що обмежують величину сигналів або блокують апаратуру на час дії ЕМІ;

– використання симетричних кабельних ліній, зменшення відстаней між підсилюючими пунктами, відключення зовнішніх ліній і перехід на автономне електроживлення.

Однією з основних тенденцій розвитку концептуальних основ РЕБ є вдосконалювання радіоелектронного захисту об’єктів від ЕМЗ.

Основними напрямками досліджень у цій галузі є:

– розробка методів протидії засобам доставки ЕМЗ;

– розробка технічних заходів щодо захисту радіоелектронної апаратури (РЕА);

– розробка нормативно-адміністративних (організаційних) заходів захисту РЕА.

Перший і найбільш ефективний напрямок у захисті від ЕМЗ – заваджання доставці електромагнітних боєприпасів шляхом знищення комплексів (засобів) доставки. Однак активне застосування засобів доставки з малою радіолокаційною помітністю (БПЛА, крилаті ракети) ускладнює реалізацію даного напрямку на практиці.

Конкретизуємо основні шляхи розвитку технічних аспектів захисту радіоелектронних апаратур від ЕМЗ на сучасному етапі.

Найбільш ефективний метод реалізації даного напрямку полягає у тому, щоб помістити обладнання цілком в електропровідну клітку, яка називається ячейкою Фарадея. На практиці використовуються менш надійні засоби захисту, такі як струмопровідні сітки або плівкові покриття для вікон, контактні пружинні прокладки, розташовувані по периметрам дверей і люків.

Радіоелектронне обладнання має комунікації із зовнішнім світом (наприклад, із джерелами живлення, мережеві з'єднання й т.п.). Це призводить до появи "точок входу" навіть у дуже добре екранованому обладнанні, через які електричні перехідні процеси можуть викликати ушкодження. Тому у місцях входу електропровідних каналів повинні бути встановлені мережеві фільтри, а також іскрові розрядники, металоокісні варистори і високошвидкісні зенеровські діоди.

Найбільш раціональним підходом до проектування засобів захисту від ЕМЗ кабельних вводів є створення таких роз'ємів, у конструкції яких передбачені спеціальні заходи, що забезпечують формування елементів фільтрів і установку вбудованих зенеровських діодів.

Складність рішення завдання захисту від ЕМЗ і висока вартість розроблених для цих цілей засобів і методів змушують піти на перших кроках по шляху їхнього вибіркового застосування в особливо важливих системах зброї і військової техніки.

Комунікаційні мережі повинні застосовувати топологію з достатньою надлишковістю і механізмами ліквідації збоїв для реалізації можливості роботи при виході з ладу великої кількості вузлів і ліній зв'язку. Це не дозволить противникові вивести з ладу більшу частину мережі або навіть мережу в цілому шляхом знищення ключових вузлів або ліній зв'язку однією атакою або невеликою кількістю атак.

4.6. Забезпечення ЕМС

Електромагнітна сумісність (ЕМС) РЕС – це спроможність РЕС одночасно функціонувати в реальних умовах в експлуатації з потрібною якістю при дії на них ненавмисних радіозавад і не створювати неприпустимих радіозавад іншим РЕС [3].

До ненавмисних радіозавад слід віднести радіозавади, що створюються джерелами штучного і природного походження і не призначені для порушення функціонування РЕС.

Основним змістом проблеми ЕМС РЕС є зниження або виключення ненавмисних радіозавад, які залежно від джерела походження можна розділити на три групи.

До першої групи відносяться радіозавади від випромінювання РЕС, до другої – індустріальні, до третьої – радіозавади природного походження.

Найбільш поширеними ненавмисними радіозавадами, з якими найбільш часто зустрічаються при вирішенні питань забезпечення ЕМС РЕС, є випромінювання у передавачів різного призначення.

До індустріальних завад відносять випромінювання, що створюються будь-якими електричними і електронними пристроями, за винятком високочастотних трактів передавальних пристроїв. До індустріальних завад відносять також випромінювання передавальних пристроїв поза антенами (через стінки кожухів передавачів, від допоміжного обладнання), випромінювання, гетеродинів, генераторів селекторних імпульсів та інших частин радіоприймачів. При цьому радіозавади від приймального пристрою можуть розповсюджуватися по ланцюгах живлення або комутації і навіть випромінюватися антеною.

Спетр і інтенсивність індустріальних радіозавад залежать від характеру їх джерела. Найбільше індустріальні завади впливають на роботу РЕС в діапазоні радіочастот до 100 МГц.

Радіозавади природного походження виникають в результаті теплового випромінювання Землі, її атмосфери, включаючи випромінювання молекулярного кисню і водяної пари, а також в результаті випромінюваннь Сонця і Галактики.

В цілому ненавмисні завади дуже негативно впливають на роботу приймального пристрою, який поряд з сигналом, що несе корисну інформацію, одночасно приймає інші сигнали. У зв’язку з цим і виникла проблема забезпечення ЕМС РЕС. Забезпечення ЕМС РЕС є одним із заходів радіоелектронного захисту. Для успішного вирішення цієї проблеми необхідно знати основні причини взаємного впливу РЕС.

Основними причинами, що приводять до взаємного впливу радіоелектронних засобів, є наступні:

1. Висока насиченість угрупувань військ радіоелектронними засобами, що приводить до об’єктивної необхідності розташовувати їх на невеликих відстанях один від одного. Найбільш несприятливі умови створюються при розміщенні великої кількості РЕЗ на одному радіоелектронному об’єкті (літаку, кораблі, вузлі зв’язку, командному пункті, позиції ЗРК і т.п.). На вузлах зв’язку оперативного угруповання військ може знаходитись до 120 і більше РЕЗ. В районах адміністративно-промислових центрів і воєнно-морських баз може бути зосереджено до 10-12 тис. РЕЗ. На сучасному літаку може бути встановлено до 30-40 різних РЕЗ, а на надводному кораблі – до 50 і більше. В цей час спостерігається тенденція зростання щільності угруповань РЕЗ як у військах, так і в народному господарстві. Рівні ненавмисних завад в цих умовах настільки високі, що виникає реальна загроза порушення нормального функціонування РЕЗ.

2. Обмеження освоєної частини радіочастотного спектру і нерівномірність її використання міжнародним Регламентом радіозв’язку радіочастотний спектр розподілений в діапазоні від 3 кГц до 3 ТГц. Проте в ньому практично використовується ділянка до 40 ГГц, в якій найбільш інтенсивно “завантажено” діапазон від 3 МГц до 12 ГГц., табл.4.2.

Нерівномірність використання спектру склалася історично і обумовлена технічним прогресом в області радіоелектроніки і особливостями використання різних діапазонів радіохвиль в практичних цілях. Так, наприклад, використання міліметрових і субміліметрових хвиль, які мають дуже велику кількість частотних каналів, ускладнюється через їх інтенсивне поглинання в атмосфері і технічні труднощі створення відповідної радіоелектронної апаратури.

Таблиця 4.2

Розподіл електромагнітного спектру по піддіапазонах і їх умовні позначення

Найменування хвиль	**Діапазон довжин хвиль (м)**	**Позначення і найменування частот**	**Діапазон частот (Гц)**
Радіодіапазон			
	Тисячі км – 100 000 км	*ELF* – наднизькі	Частки Гц – 3 кГц
Міріаметрові (наддовгі)	10-100 км (10^4-10^5)	*VLF* – дуже низькі частоти	3-30 кГц ($3\cdot10^3$ - $3\cdot10^4$)
Кілометрові (довгі)	1-10 км (10^3-10^4)	*LF* – низькі	3-300 кГц ($3\cdot10^4$ - $3\cdot10^5$)
Гектометрові (середні)	100-1000 м (10^2-10^3)	*MF* - середні	300-3000 кГц ($3\cdot10^5$ - $3\cdot10^6$)
Декаметрові (короткі)	10-100 м (10-10^2)	*HF* - високі	3-30 МГц ($3\cdot10^6$ - $3\cdot10^7$)
Метрові	1-10 м	*VHE* – дуже високі	30-300 МГц ($3\cdot10^7$ - $3\cdot10^8$)
Дециметрові	10-100 см (10-10^2)	*UHF* - ультрависокі	300-3000 МГц ($3\cdot10^8$ - $3\cdot10^9$)
Сантиметрові	1-10 см (10^{-2}-10^{-1})	*SHF* - надвисокі	3-300 ГГц ($3\cdot10^9$ - $3\cdot10^{10}$)
Міліметрові	1-10 мм (10^{-3}-10^{-2})	*EHF* – крайньо високі	30-300 ГГц ($3\cdot10^{10}$ - $3\cdot10^{11}$)
Дециміліметрові (субміліметрові)	0,1-1 мм (10^{-4}-10^{-3})	-	300-3000 ГГц ($3\cdot10^{11}$ - $3\cdot10^{12}$)
Світловий (оптичний) діапазон			
Інфрачервоні	0,75-100 мкм ($7{,}5\cdot10^{-7}$-10^{-4})	-	3-400 ТГц ($3\cdot10^{12}$ - $4\cdot10^{14}$)
Видимі	0,4-0,75 мкм ($4\cdot10^{-7}$-$7{,}5\cdot10^{-7}$)	-	400-750 ТГц ($4\cdot10^{14}$ – $7{,}5\cdot10^{14}$)
Ультрафіолетові	0,1-0,4 мкм (10^{-7}-$4\cdot10^{-7}$)	-	750-3000 ТГц ($7{,}5\cdot10^{14}$ – $3\cdot10^{15}$)

В той же час необхідність у виділенні частот для РЕЗ, які щойно створюються, безперервно зростає. Тільки для засобів радіолокації, радіонавігації, радіомовлення, телебачення і радіозв’язку потреби в радіочастотах за останні 15-20 років зросли більше, ніж в 10 разів.

Обмеженість спектру, що використовується, призводить до багатократного використання деяких його ділянок великою кількістю різноманітних за призначенням РЕЗ.

Все це призводить до необхідності роботи РЕЗ на співпадаючих частотах, що є одним із значних чинників виникнення взаємного впливу РЕЗ.

Потужності сучасних передавачів досягають десятків – сотень кіловат в неперервному режимі і десятків – сотень мегават в імпульсному режимі.

Чутливість приймачів РЕЗ сягає величин 10^{-14} – 10^{-16} Вт, а в окремих типів приймачів вона наближується до 10^{-21} – 10^{-22} Вт.

Поряд з корисним ефектом збільшення дальності дії і підвищення надійності прийому і передачі інформації, що особливо важливо в умовах завад, це призводить до збільшення зон взаємного впливу РЕЗ.

До основних недоліків трактів формування і прийому радіосигналів можна віднести:

– наявність у передавальних пристроїв небажаних радіовипромінювань за межами смуги частот радіовипромінювання, необхідного для передачі і отримання корисної інформації. Небажані радіовипромінювання підрозділяються на позасмугові і побічні. Позасмугові – це небажані радіовипромінювання в смузі частот, що примикає до необхідної смуги пропускання приймача; вони виникають за рахунок модуляції сигналу. Побічні – це небажані радіовипромінювання, що виникають в результаті будь-яких нелінійних процесів в передавачеві або паразитних зв’язків в передавальних пристроях або в його каскадах;

– високий рівень бокових і задніх пелюсток діаграм спрямованості антен відносно основної, що призводить до зниження ефекту просторової селекції (рівень бойових пелюсток у сучасних РЕЗ складає: для РЕЗ см діапазону хвиль 20-40 дБ; для РЕЗ дм діапазону хвиль – 15-25 дБ; для РЕЗ м діапазону хвиль – 10-20 дБ);

– наявність побічних каналів прийому, тобто можливість прийому сигналів на частотах, що знаходяться за межами смуги основного каналу прийому, яка необхідна для прийому корисного сигналу. До побічних каналів прийому відносять канали, що включають проміжну, дзеркальну, комбінаційну частоти і субгармоніки частоти налаштування радіоприймача. Комбінаційні канали виникають в результаті взаємодії у змішувачеві частот гетеродину і завади. Наявність небажаних випромінювань у передавачів і побічних каналів прийому у приймачів є однією з причин взаємного впливу РЕЗ, що працюють на значних частотних віддаленнях;

– недосконалість організаційних і технічних заходів, спрямованих на забезпечення ЕМС РЕЗ.

Забезпечення ЕМС РЕЗ є складною комплексною науково-технічною і організаційною проблемою, яка потребує вирішення питань розподілу і призначення частот, технічного удосконалення апаратури, організації роботи штабів усіх рівнів і військ.

Забезпечення ЕМС РЕЗ угруповання – це сукупність узгоджених по цілі, завданням, місцю і часу організаційних і технічних заходів, що проводяться командирами і штабами всіх рівнів по запобіганню і виключенню взаємного впливу поміж РЕЗ з метою надійного і неперервного управління військами і зброєю.

Аналіз і узагальнення досвіду боротьби з ненавмисними завадами показує, що для вирішення цієї проблеми можна виділити наступні напрямки:

раціональний розподіл, а за необхідності і перерозподіл діапазонів частот між РЕЗ різних типів з урахуванням їх відносної важливості їх завдань і реальних або очікуваних умов сумісної роботи;

– опанування новими ділянками радіочастотного діапазону;

– розробка технічних заходів, які спрямовані на запобігання причин виникнення ненавмисних завад, і реалізація їх в радіоелектронній апаратурі;

– розробка організаційних заходів, які спрямовані на забезпечення ЕМС РЕЗ, і практична їх реалізації у військах;

– проведення кількісної оцінки взаємного впливу РЕЗ для різних типових угруповань військ з метою виявлення найбільш небезпечних каналів взаємного впливу, типів РЕЗ, які піддаються ненавмисним завадам, і типів РЕЗ, які є найбільш небезпечними джерелами ненавмисних завад;

– відпрацювання методів забезпечення ЕМС РЕЗ в практиці оперативної і бойової підготовки військ.

Основною ціллю розподілу і призначення частот РЕЗ є максимальне задоволення потреб військ в частотах і забезпечення роботи РЕЗ без ненавмисних завад. Процес розподілу частот полягає у виділенні набору частот всім споживачам, а призначення частот – у виділенні частот конкретним РЕЗ, радіомережам і радіонапрямкам.

Правильний розподіл і призначення є одним із найбільш ефективних і оперативних способів забезпечення ЕМС РЕЗ, що проводяться у військах.

Властивість РЕЗ виконувати поставлені завдання в реальній ЕМО закладають при висуненні відповідних вимог на етапах проектування, розробки, експлуатації і модернізації РЕЗ. До найбільш важливих напрямків забезпечення ЕМС РЕЗ угруповання військ в результаті удосконалення якості функціонування РЕЗ в реальній ЕМО можна віднести [18-21]:

1. Розробку адаптивних РЕЗ, які автоматично пристосовуються до змін ЕМО і забезпечують при цьому необхідну якість функціонування за рахунок зміни структури і параметрів сигналу. До основних технічних заходів, що дозволяють реалізувати даний напрямок, можна віднести:

– реалізація принципу вільного доступу до радіочастотного спектру;

– регламентація часових режимів роботи РЕЗ в угрупованні військ;

– зміна потужності сигналів, що випромінюються, і чутливості приймачів в залежності від умов роботи.

2. Розробку схемних рішень, які спрямовані на підвищення якості селекції корисних сигналів із суміші з завадами, а також підвищення інформаційної ємності сигналів, що використовуються в РЕЗ.

До основних технічних заходів, що дозволяють реалізувати даний напрямок, можна віднести:

– застосування в передавачах складних (широкосмугових) сигналів;

– використання модуляції робочих сигналів по декількох параметрів;

– підвищення точності вимірів і розрізняльної спроможності по кутовим координатам;

– застосування спеціальних пристроїв захисту від ненавмисних завад в прийомному і передаючому трактах РЕЗ.

3. Удосконалення неосновних технічних характеристик передавальних і прийомних пристроїв, які впливають на ЕМС.

До заходів, що реалізують даний напрямок, можна віднести наступні:

– стандартизацію технічних характеристик передавачів і приймачів, що впливають на ЕМС РЕЗ;

– зниження рівня бокових і задніх пелюсток ДСА;

– підвищення стабільності частоти передавачів і гетеродинів приймачів РЕЗ.

Реалізація основних напрямків удосконалення якості функціонування РЕЗ в складній ЕМО потребує проведення комплексних досліджень і підготовки технічної основи для їх реалізації в зразках РЕЗ.

Важливе місце в забезпеченні ЕМС РЕЗ відводиться організаційним заходам. Ці заходи спрямовані на організацію роботи РЕЗ в угрупуваннях шляхом встановлення режимів, що регламентують роботу в просторі, часі і за частотою, виконання норм частотно-територіального рознесення.

Основними з цих заходів є:

– управління радіочастотним ресурсом (РЧР) в угрупованні військ, тобто забезпечення необхідного частотного рознесення РЕЗ шляхом раціонального визначення робочих і запасних частот для деяких РЕЗ з урахуванням їх взаємного розташування на місцевості (в просторі) і умов розповсюдження радіохвиль;

– встановлення і суворе дотримання узгодженого порядку використання радіочастот при наявності завад;

– введення обмежень (заборони) на використання тих чи інших частот і ділянок діапазонів частот;

– забезпечення територіального (просторового) рознесення РЕЗ шляхом розташування їх на таких взаємних відстанях, які в сукупності з величинами частотного рознесення і умовами розповсюдження радіохвиль на трасі поміж РЕЗ забезпечують повну відсутність або дуже малу ймовірність взаємного впливу; в деяких випадках можуть вводитися обмеження на райони розташування тих чи інших РЕЗ;

– вибір і обладнання позицій РЕЗ з урахуванням екрануючих властивостей місцевості в напрямках на потенційні джерела завад і узгодженість роботи РЕЗ по режимам;

– розподіл і узгодженість роботи РЕЗ по режимам функціонування, по часу і просторових секторах.

Висока ефективність організаційних заходів, спрямованих на забезпечення ЕМС РЕЗ, досягається узгодженою роботою управлінь (відділів) штабів родів військ і служб, чітким виконанням військами поставлених перед ними завдань по організації бойового застосування РЕЗ.

До розробки організаційних заходів по забезпеченню ЕМС РЕЗ треба підходити творчо, враховуючи конкретні особливості ЕМО і пам’ятаючи, що угруповання військ будується, виходячи із поставлених завдань, замислу і плану ведення бойових дій. Завдання раціонального розташування РЕЗ в угрупуванні військ вимагає великої кількості обчислень, тому що його

вирішення, як правило, пов'язане з аналізом ряду варіантів і вибором найбільш раціонального з них.

Основні принципи організації заходів по забезпеченню ЕМС РЕЗ в угрупованнях можуть бути сформульовані наступними положеннями:

– заходи по забезпеченню ЕМС РЕЗ повинні відповідати замислу і плану операції (бою);

– відповідальність за своєчасну організацію і проведення в повному обсязі заходів по забезпеченню ЕМС РЕЗ несуть ті командири і начальники, які планують застосування РЕЗ за призначенням;

– умови нормальної роботи забезпечуються першочергово для тих РЕЗ, які використовуються для вирішення найважливіших завдань;

– забезпечення ЕМС РЕЗ повинно проводитись в комплексі з вирішенням завдань по їх захисту від ненавмисних завад і від технічних засобів іноземних розвідок.

При цьому, відповідно з замислом командування, зусилля штабів по забезпеченню ЕМС РЕЗ спрямовуються в першу чергу на виключення ненавмисних радіозавад в тих угрупуваннях, які діють на головних, найбільш відповідальних напрямках і вирішують найважливіші завдання на основних рубежах військ.

4.7. Радіоелектронний захист у ході повсякденної діяльності

У ході повсякденної діяльності радіоелектронний захист розглядається як система взаємозв'язаних за метою, завданнями, місцем і часом організаційних та технічних заходів і дій, спрямованих на забезпечення стійкої і надійної роботи своїх РЕЗ систем управління військами (силами) та зброєю в мирний час, а також в умовах раптового застосування противником засобів РЕБ.

Радіоелектронний захист в умовах повсякденної діяльності військ (сил) організується і здійснюється з метою захисту своїх РЕЗ і систем від радіоелектронної розвідки противника, від взаємних завад, а в загрозливий період та в окремих раптово виникаючих ситуаціях – і від вогневого та радіоелектронного впливу противника.

Радіоелектронний захист при цьому організується і здійснюється у тісному поєднанні, перш за все, з організацією та виконанням заходів щодо протидії технічним засобам розвідки противника, безпеки зв'язку, тощо.

Сутність радіоелектронного захисту полягає у здійсненні комплексу конкретних, що відповідають радіоелектронній обстановці, заходів і дій, які проводяться командирами і штабами всіх ланок управління, відповідними управліннями, службами (відділами) РЕБ, іншими службами, а також безпосередньо формуваннями військ (сил).

Специфіка заходів щодо радіоелектронного захисту, що проводяться у ході повсякденної діяльності військ (сил), полягає у тому, що вони організуються і здійснюються в процесі підготовки військ (сил) до бойових дій і, перш за все, до бойових дій в умовах РЕБ.

Цей процес передбачає планування і проведення заходів, що підвищують завадозахищеність і захищеність від самонавідної на випромінювання зброї угруповань військ, а також підготовку всіх категорій особового складу до бойової роботи в зазначених умовах. Одночасно розробляються і здійснюються заходи щодо електромагнітної сумісності і ПД ТЗР.

Основні заходи радіоелектронного захисту, що проводяться у повсякденній діяльності військ (сил), такі [18-21]:

– виявлення джерел ненавмисних (взаємних) завад та прийняття заходів для зняття (зниження) їх впливу;

– встановлення часових, частотних, просторових та енергетичних обмежень у роботі радіоелектронних систем;

– захист від радіоелектронного подавлення, ураження самонавідною зброєю, впливу іонізуючих і електромагнітних випромінюваннь;

– застосування різноманітних режимів роботи засобів, що забезпечують роботу в умовах завад;

– здійснення взаємодії з питань забезпечення електромагнітної сумісності радіоелектронних засобів (захист від взаємних завад);

– прогнозування радіоелектронної обстановки з переходом на частоти воєнного часу.

У ході бойової підготовки на заняттях з тактичної (тактико-спеціальної), спеціальної і технічної підготовки здійснюються заходи щодо навчання особового складу та бойового злагодження з'єднань, частин (підрозділів) для ведення бойових дій. При цьому досягається мета: отримання знань, набуття (удосконалення) умінь і навичок у всіх категорій тих, хто навчається, здійснення бойового злагодження всіх формувань, підготовка їх до виконання бойових завдань в умовах РЕБ.

Навчання і тренування доцільно планувати і проводити в умовах, максимально наближених до реальних бойових дій. При цьому необхідно добиватися:

– прийняття посадовими особами доцільних (раціональних) рішень у складній загальній, частковій, у тому числі і радіоелектронній обстановці;

– накопичення досвіду бойової роботи в складних, іноді непередбачуваних ситуаціях в умовах впливу радіоелектронних завад і СНЗ;

– постійного поглиблення і розширення знань, удосконалення вмінь та практичних навичок особовим складом бойових розрахунків у зазначених умовах;

– постійного скорочення часу виконання операцій бойовими розрахунками, зменшення кількості помилок при роботі на апаратурі;

– удосконалення засобів і методів пошуку джерел завад, у тому числі закидних передавачів завад;

– набору статистики впливу різноманітних завад на свої РЕЗ;

– підвищення якості взаємодії між номерами бойових розрахунків, а також між бойовими розрахунками в підрозділах, частинах, з'єднаннях.

Кожне навчання (тренування) повине бути спрямоване на виконання певного кола завдань, що відпрацьовуються в умовах ведення противником активної радіоелектронної боротьби.

Контрольні запитання до 4 розділу:

1.Що таке радіоелектронний захист. Який його зміст та складові?

2.Яка мета радіоелектронного захисту систем зв’язку?

3.Які основні завдання радіоелектронного захисту систем зв’язку?

4.Що таке захист від радіоелектронних завад противника. Які методи захисту від радіоелектронних завад Вам відомі?

5. Що таке захист від радіоелектронної розвідки противника. Які методи захисту від радіоелектронної розвідки противника Вам відомі?

6.Що таке захист від іонізуючого та електромагнітного випромінювання противника. Які методи захисту іонізуючого та електромагнітного випромінювання противника від Вам відомі?

7. Що таке захист від взаємних завад? Які методи радіоелектронного захисту від високоточної зброї Вам відомі?

8. В чому зміст радіоелектронного захисту від високоточної зброї? Які методи захисту від взаємних завад Вам відомі?

9.Які основні заходи з радіоелектронного захисту у ході повсякденної діяльності Вам відомі?

ЗАКЛЮЧЕННЯ

Досвід усіх без винятку локальних війн та збройних конфліктів останніх десятиліть підтвердив пріоритетне значення РЕБ при виконанні завдань дезорганізації управління сухопутними військами противника, його системою ППО, іншими системами та створення сприятливих умов для успішного ведення бойових дій. Тому актуальним завданням сучасної теорії і практики РЕБ є аналіз тенденцій розвитку РЕБ за досвідом організації і ведення РЕБ у локальних війнах і збройних конфліктах, виділення проблемних питань підготовки органів управління і частин РЕБ Збройних Сил України до застосування за призначенням та визначення шляхів їх вирішення в сучасних економічних реаліях.

Об'єктивний розгляд перспективних напрямків розвитку РЕБ в ЗС України неможливий без детального аналізу основних тенденцій розвитку РЕБ у арміях провідних країн світу. Загальна тенденція розвитку РЕБ у світі, яка історично склалася з початку її зародження, полягає в тому, що у відповідь на появу кожного нового радіоелектронного засобу (або системи), що з'являвся у противника і був призначений для забезпечення функцій управління, створювався "антизасіб", тобто станція завад, яка за технологічним рівнем не поступалася, а, як правило, випереджала сам "засіб". Тобто, між потенційними противниками відмічалася, своєрідна "гонка технологій". Очевидно, протягом деякого часу це було виправдано.

Однак сьогодні такий підхід має суттєвий недолік – не кожна країна може собі дозволити величезні асигнування на подібну "гонку" в умовах інтенсивного розвитку систем зв'язку, телекомунікацій та новітніх інформаційних технологій.

Тому, крім традиційної техніки РЕБ, у розвинених країнах інтенсивно розвивається перспективна техніка і зброя РЕБ, яка вже знайшла своє застосування в локальних війнах та збройних конфліктах, починаючи з операції "Буря в пустелі" (1991 р.), а також визначає нові напрямки розвитку форм і способів збройної боротьби у війнах майбутнього.

Пріоритетними завданнями ЗС України в напрямку розробки і озброєння частин РЕБ новою технікою визначено:

– завершення ДКР "Сокіл" – розробка автоматизованого комплексу РЕП ліній управління авіації;

– завершення ДКР "Сполох" – розробка комплексу індивідуального захисту об'єктів від ВТЗ;

– проведення ДКР "Мікрометр" – розробка портативних передавачів завад для подавлення УКХ ліній зв'язку та РЛС ППО метрового і дециметрового діапазону;

– модернізація станцій завад бортовим РЛС, комплексу РЕП "Мандат", станцій завад супутниковим лініям зв'язку.

До головних завдань в інших напрямках розвитку РЕБ в ЗС України віднесено:

– подальшу розробку форм і способів ведення РЕБ та бойового застосування частин РЕБ в операціях та бойових діях, а також в інтересах інформаційної боротьби;

– удосконалення системи управління силами та засобами РЕБ Збройних Сил України з чітким розподілом функцій та повноважень між органами управління всіх рівнів;

– підвищення бойових можливостейчастин РЕБ нового виду Збройних Сил – Повітряних Сил;

– підвищення рівня бойової та мобілізаційної готовності частин РЕБ, створення частин (підрозділів) РЕБ постійної бойової готовності;

– удосконалення організаційно-штатних структур частин РЕБ Збройних Сил України.

На закінчення можна зазначити наступне:

– по-перше, можливість реалізації перспективних напрямків розвитку РЕБ в ЗС України тісно пов’язана із розв’язанням існуючих проблем в галузі РЕБ і в значній мірі залежить від економічних можливостей держави;

– по-друге, сили та засоби РЕБ в Збройних Силах України розвиваються за традиційною для колишнього СРСР тенденцією “гонки технологій”, тоді як досвід армій провідних країн світу свідчить про необхідність упереджувального розвитку з орієнтуванням на ведення війн майбутнього;

– по-третє, для широкого кола науковців і практиків в галузі РЕБ є широке поле творчої діяльності та реалізації творчих ідей в напрямку розвитку і впровадження у Збройних Силах України нових форм і способів ведення РЕБ.

Необхідно акцентувати, що дійсний момент часу характеризується переломом в ідеології ведення сучасної війни. Одна з основних причин цього – глобальна інформатизація суспільства й збройних сил. На зміну застарілим підходам ведення війн 4 й 5-го поколінь приходить ідеологія збройної боротьби шостого та сьомого поколінь, невід’ємними компонентами якої є широкомасштабні інформаційні операції, операції РЕБ, інтелектуальний тероризм, масоване застосування несмертельної зброї.

СПИСОК ЛІТЕРАТУРИ

1. ДСТУ 3265-95. Зв’язок військовий. Терміни та визначення.
2. Котельников В.А. Теория потенциальной помехоустойчивости. – М.: Госэнергоиздат, 1956. – 152 с.
3. Зюко А.Г., А.И.Фалько, И.П. Панфилов, В.Л. Банкет, Л.В. Иващенко Помехоустойчивость и эффективность систем передачи информации; Под.ред. Зюко А.Г. – М.: Радио и связь, 1985. – 272 с.
4. Варакин Л. Е. Теория систем сигналов. М., “Сов. Радио”, – 1978, 304 с.
5. Финк Л.М. Теория передачи дискретных сообщений. – М.: Сов. радио, 1983. – 320 с.
6. Теплов Н.Л. Помехоустойчивость систем передачи дискретной информации. – М.: Связь, 1964. – 359 с.
7. Игнатов В.А. Теория информации и передачи сигналов. Учебник для ВУЗов, Изд-во Советское радио, 1979. – 280 с.
8. Вакин С. А., Шустов Л. Н. Основы радиопротиводействия и радиотехнической разведки. М. “Сов. Радио”,1968. – 285 с.
9. Палий А. И. Радиоэлектронная борьба. – М.:Воениздат, 1989. – 350с.
10. О. Черниш. Основи формування нової ідеології ведення радіоелектронної боротьби у війнах і збройних конфліктах майбутнього / О. М. Черниш, С. О. Тищук, С. М. Шолохов // Наука і оборона. – 2006. – № 4. – С. 48–51.
11. Тищук С.О., Шолохов С.М., Лучук Е.В., Завацький О.Б. Радіоелектронна боротьба: військово-аналітичні аспекти розвитку та трансформації. Напрямки розвитку РЕБ у Збройних Силах України// Зб. наук. праць “Труди академії”, К.: НАОУ, № 57. – 2005. – С. 114...120.
12. Шолохов С.М., Лучук Е.В., Завацький О.Б. Тенденції та перспективні напрямки розвитку радіоелектронної боротьби // К.: Арсенал-ХХІ». – 2006. – № 12 (38). С. 39-45.
13. Шолохов С.М., Лучук Е.В., Завацький О.Б. Программно – компьютерное подавление – наступательная компонента вооруженной борьбы современности и будущего // К.: Арсенал-ХХІ».- 2007. – № 18 (42). С. 45-55.
14. С. Тищук. Електромагнітна зброя / С. О. Тищук, С. М. Шолохов // Волонтер. – 2005. – № 5 (37). – С. 18–21.
15. Шолохов С.Н., Сидченко С.А. Информационное оружие – новый класс вооружения для дезорганизации автоматизированных систем управления войсками и оружием при проведении информационных наступательных операций // Сб. научн. трудов ХВУ, Х.: ХВУ. – № 1(39), – 2002. С.10...14.
16. Основы теории радиоэлектронной борьбы. Под ред. Н.Ф. Николенко. М.: Воениздат, 1987, – 352 с.
17. В. В. Змиевский, С. Л. Емельянов. Теория радиоэлектронного подавления, техника РЭП и ее эксплуатация. Часть 1. МО СССР, 1991. – 239 с.
18. Певцов Г.В., Шолохов С.Н. Обоснование величины пороговой

чувствительности при оптимизации панорамных приемных устройств на основе Фурье – процессоров. К.:КПІ.- Известия Вузов. Радиоэлек-троника. – 1999. – № 3. – С. 62-68.

19. Перунов Ю. М., Фомичев К. И., Юдин Л. М. Радиоэлектронное подавление информационных каналов систем управления оружием. – М.: Радиотехника, 2003. – 415 с.

20. Куприянов А. И., Сахаров А.В. Радиоэлектронные системы в информационном конфликте. – М.: Вузовская книга, 2003. – 527 с.

21. Довідник з протиповітряної оборони. – К.: МО України; Х.: ХВУ, 2003. – 368 с.

22. Високоточна зброя та основи захисту військ від неї. Навч. посібник. К.: НАОУ, – 2010, 186 с.

23. Шолохов С.М., Завацький О-др.Б., Павленко І.А., Дубинін В.В. Методика оцінки ефективності ведення РЕП в операціях (бойових діях) на основі математичного апарату терії масового обслуговування // Зб. наук. праць “Труди академії”, К.: НАОУ, № 50 . – 2004. – С. 148...154

24. Шолохов С.М., Лучук Е.В., Сесік В.П. Методика оцінки ефективність ведення радіоелектронної розвідки частинами (підрозділами) РЕБ в операціях (бойових діях) // Зб. наук. праць “Труди академії”, К.: НАОУ, № 50. – 2004. – С. 148...152.

25. Шолохов С.М., Тищук С.О., Завацький О. Б., Лучук Е. В. Електромагнітна зброя: сутність, принципи застосування та перспективи використання в операціях (бойових діях) // Вісник воєнної розвідки. К.: в/ч 2659, № 10. – 2005. – С. 94…104.

26. Шолохов С. М., Завацький О. Б., Лучук Е.В., Міроненко П.О. Оперативно - тактичні показники застосування електромагнітної зброї при обґрунтуванні оптимального бойового складу угруповання частин (підрозділів) РЕБ в операціях (бойових діях) // Зб. наук. праць “Труди академії”, К: НАОУ, № 60. – 2005. – С. 134...139.

27. Шолохов С.М., Тищук С.О., Лучук Е. В. Програмно-комп’ютерне подавлення комп’ютерної транспортної мережі передачи даних тактичної ланки в операціях (бойових діях) // Зб. наук. праць “Труди академії”, К: НАОУ, № 59. – 2005.

28. Шолохов С.М., Лучук Е.В., Завацький О.Б. Оцінка ефективності програмно-комп’ютерного подавлення при обґрунтуванні оптимального бойового складу угруповання частин (підрозділів) РЕБ в операціях (бойових діях)) // Зб. наук. праць “Труди академії”, К: НАОУ, № 61. – 2005.

29. Г.М.Тіхонов, С.М.Шолохов, Б.А.Ніколаєнко, В.М.Тютюнник Modern Information Technologies in the Sphere of Security and Defence № 2(41)/2021.

30. Г.Певцов. Наукові основи обґрунтування способів бойового застосування сил та засобів радіоелектронного подавлення в операціях / Г. В. Певцов, С. М. Шолохов, Г. М. Тіхонов, І. М. Тіхонов // Системи управління, навігації та зв’язку. – 2008. – № 3(7). – С. 120–125.

31. В. Космодемьянский. Математические методы оптимизации /

В. А. Космодемьянский– М.: 1967. – 96 с. – (МО СССР).

32. Е. Берзин. Оптимальное распределение ресурсов и элементы синтеза систем / Е. А. Берзин; под ред. Е. В. Золотова – М.: Сов. радио, 1974. – 303 с.

33. Шолохов С.М., Гордієнко Ю.В. Постановка зворотної задачі раціонального розподілу ресурсу неоднорідних засобів радіоелектронної боротьби противника по елементах транспортної платформи національної телекомунікаційної мережі для визначенні сценаріїв її радіоелектронного подавлення // Спеціальні телекомунікаційні системи та захист інформації. К.: 2020. № 1(7). С. 34 – 40.

34. Шолохов С.М., Гордієнко Ю.В. Оцінка ефективності радіоелектронного та програмно-комп’ютерного подавлення телекомунікаційних систем урядового зв’язку при обґрунтуванні перспективних способів їх радіоелектронного захисту в умовах ведення гібридної війни // Спеціальні телекомунікаційні системи та захист інформації. 2019. № 2(6). С. 59 – 65

35. Шолохов С.М., Гордієнко Ю.В. Методика розробки сценаріїв радіоелектронного та електромагнітного подавлення національної телекомунікаційної мережі та складної сигнально-завадової обстановки для синтезу адаптивних алгоритмів завадозахисту К.: НАОУ. – “Труди академії”. 2020. № 17 (167). – С.127 – 139.

Додаток

Основні тактико-технічні характеристики комплексів РЕБ та РЕР ЗС України

Станції розвідки частин (підрозділів) РЕБ

Станція розвідки	**Призначення засобу**	**Діапазон (МГц)**	**Точність Пеленгації (СКП)**	**Д розвідки (км)**	**Точності визначення**			**База К-сть шасі**	**Час розгор. Час згорт.**	**Об'єкт подавлення**
					F (МГц)	**τ (мкс)**	**Тп (мкс)**			
Р-359	Радіопеленгатор	1,5…25	4°	1500	-	-	-	ЗІЛ-131 1 причіп	3 г/3 г	наземні РЕС
Р-381-2	Радіопеленгатор	20...100	4,5°	40	-	-	-	ГАЗ-66	5 хв/8 хв	наземні РЕС
ПОСТ-3М	Станція РТР	2,5…37,5 ГГц	4°	До 400	±500	0,1		ЗІЛ-131 2 причіпи	1 г/1 г	Бортові та наземні РЕС
Кольчуга	Станція РТР	0,915…11 ГГц	4°	190	0,4	0,1	0,1	Урал-43203/ 1 причіп	35 хв/35 хв	Бортові та наземні РЕС
		11…18 ГГц	12,5°	450	4,8	0,2	0,2			
П-18	радіолокаційна станція	Метровий діапазон хвиль	Точність визначення азимуту ± 1.5°	190км на висоті10км 230км-20км Точність визнач. дальності ± 1,8 км	-	-	-	Урал-43203 2 шт/ 2 причіп	1,5 г/1,5 г	Повітряні цілі

Станції перешкод частин (підрозділів) РЕБ Сухопутних військ

Станції перешкод	Вид управління	Діапазон (МГц)	Потужність (Вт)	Час реакції (с)	Наявність пеленгатора Точність пеленгування	Час розгорт (хв) Згорт (хв)	База Кількість шасі	Дальність розвідки (км) Д подавл. (КМ)	Можливість з подавлення
Р-330П	Автономне	30...100	1000	>10	–/–	50/30	МТ-ЛБу/1	40/30	На 1-й частоті
Р-330У	Автомат. від Р-330ПУ	30...60	1000	>0,3	+/3°	70/50	Урал 355/2	40/30	На 4-х частотах
Р-330Б	Автомат. від Р-330К	30...100	1000	0,3<	+/3°	40/20	МТ-ЛБу/1	40/30	На 3-х частотах
Р-378М	Ручний	1,5...25,5	1000	>10	–/–	60/60	Зіл-131/2	40/30	На 1-й частоті
Р-378А(Б)	Автомат. від Р-330К	1,5...30	1000	0,3<	+/4°	60/*60	“А”Зіл-131/2, ”Б”МТ- ЛБу/1	40/30	На 4-х частотах
Р-325У	Автомат. від Р-330К	1,5...30	5000	>10	+/4°	60/60	Зіл-131/2	80/60	На 4-х частотах
Р-325М	Ручний від Р-380	1,5...25,5	5000	>10	–/–	60/6-	Зіл-131/3	1000/від 250 до 1000	На 1-й частоті
Р-934	Автомат. від „Банан” («Степ-О»)	220...400	1000	11	–/–	30/25	Зіл-131/1	350/250	На 1-й частоті
Р-934У	Автом. від ведучої Р-934У	100...400	1000	1	–/–	30/25	Урал 375/1	350/250	На 4-х частотах
Р-934Б	Автом. від ведучої Р-934Б	100...400	700	0,072	–/–	10/10	МТ-ЛБу/1	350/250	На 3-х частотах
РП1-377АМ	За програмою або від дист. пульта управл.	20...500 (7-м автоном. прд перешкод)	3	-	–/–	1	1 солдат заносить 3 шт. передавачів, або на БТР-70	Площина кола з радіусом менше 1 км.	Загородж. по частоті
СПР-2	Автономне	95...420	25	-	-/-	4/4	БТР-70	Площ. не менше 25 га	До 2-х носіїв одночасно

Станції перешкод частин (підрозділів) РЕБ

Станції перешкод	Вид управління	Діапазон (МГц)	Потужність (Вт)	Час реакції (с)	Наявність пеленга-тора Точ-ність пеленгу-вання	Час розгорт (хв) Згорт (хв)	База Кількість шасі	Дал. розвідки, км Дал. подав., км	Можливість з подавлення
СПС-1	Автомат. від ПУ	225…400	1000	0,4мс<	–/–	90/110	2-а Урал 355/+2причіпи		До 4-х
Комплекс «Мандат-М» (за матеріалами рекламних проспектів *Виробника* та *UKRSPETSEXPORT*)									
Р-330КМ	Автомат. від ПУ Р-330ПМ	1,5…30	1000	0,3мс<	+/2°	-	2-а КРАЗ	70/60	ФРЧ-8, ППРЧ-2
Р-330УМ1	Автомат. від ПУ Р-330ПМ	30…180	2500	0,3мс<	+/2	-	БТР-3У	70/60	ФРЧ-8, ППРЧ-2
Р-330УМ2	Автомат. від ПУ Р-330ПМ	180…1000	2500	0,3мс<	+/2	-	БТР-3У	70/60	ФРЧ-8, ППРЧ-2
«Лиман-П1»	Автомат. від ПУ	225…400	50000	0,3мс<	+/2	-	КРАЗ (Урал або БТР) / 1 причеп.	250/200	-
«Лиман-П2»	Автомат. від ПУ	960…1215	100000	0,3мс<	+/2	-	КРАЗ / 1 причеп	250/200	-

Станції радіоперешкод частин (підрозділів) РЕБ-Л

Станція перешкод	Вид управління	Діапазон (ГГц)	Потужність (Вт)	Час реакції	Вид перешкод	$Д_{розвід}/Д_{под}$	Пропускна здатність	База/Кількість шасі	Час розг./Ча	Об’єкт подавл.

									с згор.	
СПН-30	Автомат. з АКУП-22	8,3…10	800±150	10 мкс	Квазібезпе-рервна прямошумова	400/250	До 5 цілей	Урал-375/3 шт.	40/25 (хв)	Бортові (літакові) РЕС
СПН-40	Автомат. з АКУП-22	13,5…17,5	300	4…40 мкс	Імітація до 16 об’єктів	350/180	До 3 цілей	Урал-375/1 причіп	40/30 (хв)	БРЕС
СПО-8М	Автомат. з АКУП-22	8,3…10	250	40 мкс	Імітація до 16 об’єктів	350/180	До 2 цілей	Урал-375/1 причіп	40/30 (хв)	БРЕС
СПН-2	Автомат. з АКУП-1	10…13,45	750…1300	10 мкс	Квазібезпе-рервна прямошумова	350/180	До 6 цілей із 2-х напрямків	Урал-375/3 шт.	15/15 (хв)	БРЕС
СПН-3	Автомат. з АКУП-1	13,45…17,54	750…1300	10 мкс	Квазібезпе-рервна прямошумова	350/180	До 6 цілей із 2-х напрямків	Урал-375/3 шт.	15/15 (хв)	БРЕС
СПН-4	Автомат. з АКУП-1	8…10	750…1300	10 мкс	Квазібезпе-рервна прямошумова	350/180	До 6 цілей із 2-х напрямків	Урал-375/3 шт.	15/15 (хв)	БРЕС
Р-388	Автомат.	0,962…1,024 1,151…1,213	200	30 с<	Імітаційно - відвідна	300/180	100	Зіл-157	30/30 (хв)	РНС «Такан»

Автоматизовані вузли, пункти управління та комплекси РЕБ

АПУ		**Об'єкт керування**	**Кількість об'єктів управління**	**Зона обслуговування**	**$Д_{макс.}$ управл. СП**	**База**
Автоматизований пункт управління Р-330ПУ		В автомат. реж. Р-330У, в ручн. режимі Р-330П	До 4-х Р-330У, та до 6-и Р-330П	30х30 км	до 30 км	Урал-375/1 причіп
Автоматизований комплекс управління Р-330К у складі ПУ-тактичний (ПУ-Т), та ПУ-засобами комплексу (ПУ-ЗК)	ПУ-Т	Станц. перешк. УКХ і КХ діапаз.	до 10-и (Р-378А(Б), Р-325У) або Р-330Б	30х60 км 30х30 км	до 30 км	Урал-375/1 причіп
	ПУ-ЗК	ПУ-Т	до 5-и ПУ-Т	30х60 км	о 30 км	Урал-375/1 причіп
Вузол управління Р-380		Р-325М (М2)	до 12-и Р-325М	$Д_{розв.}$ – більше 1000 км $Д_{под}$ – до 1000 км	до 30 км	9 шт.Зіл131 3 шт.ГАЗ-66
Автоматизований пункт управління „Банан-2"(„Степ-0")		Р-934	до 6-и Р-934	$Д_{под}$ – до 250 км	до 30 км	2 шт. Зіл-131
Автоматизований комплекс управл.перешкод АКУП-22		СПН-30, СПН-40, СПО-8М	До 18-и СП у різному співвідношенні	$Д_{розв}$ – до 400 км $Д_{под}$ – до 230 км	до 40 км	2шт. Урал-375
Автомат компл упр. перешк. АКУП-1 у складі автомат. ПУ роти (АПУР) та авт. КП б (АКПБ)	АКПБ	АПУР, та АКУП-22	До 3-х АПУР, або до 2-х АПУР і 1-го АКУП-22	$Д_{розв}$ – до 400 км $Д_{под}$ – до 230 км	до 40 км	3 шт Урал-375
	АПУР	СПН-2, СПН-3, СПН-4.	До 9 шт. СПН-2, -3,-4 у будь якому співвідношенні	$Д_{розв}$ – до 400 км $Д_{под}$ – до 230 км	до 40 км	3 шт. Урал-375

ПРИМІТКИ