

ЗАСТОСУВАННЯ ЗАВАД ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ РАДІОКАНАЛОМ

Складність вирішення проблем захисту інформації обумовлена необхідністю створення систем захисту інформації в умовах обмежених в рамках проектів фінансових, матеріальних, людських та часових ресурсів, використовуючи доступні технології захисту. Тому питання захисту інформації, захисту інформації від витоку радіоканалом за допомогою завад є актуальним науковим завданням, вирішенню якого і присвячена дана стаття. У статті розглядається питання адаптації методів використання завад для запобігання витоку інформації по радіоканалу. Наведені рекомендації по застосуванню завад для захисту інформації яка може бути передана по радіоканалу засобами негласного отримання інформації.

Ключові слова: засоби негласного отримання інформації, завада, корисний сигнал, захист інформації, канал витоку даних, радіозакладка.

Ч

Вступ

Широке використання в процесі інформатизації суспільства сучасних технологій автоматизованої обробки інформації та управління технологічними процесами створило не тільки об'єктивні передумови підвищення ефективності всіх видів діяльності особи, суспільства та держави, але і ряд проблем захисту інформації. Спроби отримати доступ до конфіденційної інформації не обмежуються діями інсайдерів та прихованим підключенням до телекомунікаційних каналів зв'язку. Непоодинокі випадки встановлення заставних пристроїв, що перехоплюють акустичні сигнали. Вони використовуються організаціями, що спеціалізуються на конкурентній розвідці, а їх пошук утруднений малодоступністю спеціального обладнання. Радіоканали витоку інформації залишаються актуальною проблемою інформаційної безпеки. При розгляді радіоканалів витоку інформації об'єкт виглядає як акустичні дані у вигляді промови, телефонних переговорів (пристрій зняття даних часто встановлюється в стаціонарному або мобільному телефонному апараті) або відеоінформації про дії людей, що цікавлять замовника, у певному приміщенні. використовуються пристрої різних типів.

Ідеального захисту немає. Всі заходи безпеки лише знижують ризик витоку інформації та ускладнюють доступ до даних. Чим краще ви захищаєте свою інформацію, тим дорожчим і складнішим стає процес її отримання для зловмисників. Використовуйте всі доступні засоби для підвищення рівня захисту даних та мінімізації ризиків.

Одним з напрямом захисту інформації від витоку радіоканалом є застосування завад. Тому завдання по застосуванню завад для захисту інформації від витоку радіоканалом є актуальним. Вирішенню цього завдання і присвячена дана робота

Аналіз літературних джерел та формулювання проблеми.

Швидкий розвиток інформаційних систем, несе в собі цілий ряд загроз пов'язаних з порушеннями конфіденційності, цілісності та доступності інформації, які, в свою чергу, приводять до різних втрат (в тому числі - фінансових) і інколи - значних. Тому питанню захисту інформації, захисту інформації від витоку радіоканалом за допомогою завад присвячено багато публікацій. Так у роботі [1] надана оцінка завадо захищеності існуючих систем радіолокаційної ідентифікації. Доведено, що використання прямокутних радіосигналів з часово-імпульсною модуляцією у якості сигналів запиту та відповіді, які випромінюють повітряні об'єкти, має низьку завадо захищеність та виключає енергетичну прихованість. І, як наслідок, надає можливість здійснювати несанкціоноване отримання інформації. Але методи запобігання витоку інформації залишилися без розгляду.

У роботах [2, 3] наведено приклади застосування цифрових методів модуляції та завадостійкого кодування в сучасних інформаційно-комунікаційних технологіях з односторонньою радіопередачею. Показані результати аналізу ефективності використання

цифрових методів модуляції. Та завадостійкого кодування за критерієм мінімуму значення ймовірності помилки. Розглянуто особливості застосування комбінованого випадкового кодування, яке передбачає використання поєднання завадостійкого та стохастичного кодування. Але методи блокування радіосигналів не розглядаються.

У роботах [4-6] наведено аналіз задачі захисту систем радіозв'язку від навмисних завад. Головним завданням є забезпечення завадостійкого радіозв'язку на більшій площі розміщення своїх засобів радіозв'язку. Вплив на систему управління шляхом ведення радіоелектронної боротьби є невід'ємною частиною сучасного протистояння будь-якого масштабу. Але методики захисту від умисних завад не наведено.

У роботах [7, 8] система радіолокаційного розпізнавання приналежності виявлених радіосигналів є важливою системою і зобов'язана органічно входити в єдину інформаційну систему. Вона повинна вирішувати завдання розпізнавання як в інтересах визначення ступеня небезпеки. Нажаль системи блокування радіосигналів залишились без розгляду.

Таким чином, у результаті вивчення наукових публікацій за темою статті, дисертацій, патентів, монографій та практичних доробок встановлено, що на сьогодні невирішеним залишається питання запобігання несанкціонованого витоку інформації за радіоканалом. Тому наукове завдання по застосуванню завад для захисту інформації від витоку радіоканалом є актуальним. Вирішенню цього завдання і присвячена дана робота.

Мета роботи та цілі дослідження

Метою статті є аналіз існуючих завад. Адаптація методів використання завад для запобігання витоку інформації по радіоканалу. Видача рекомендацій по застосуванню завад для захисту інформації яка може бути передана по радіоканалу засобами негласного отримання інформації.

Виклад основного матеріалу

Впливаючи на приймальні пристрої, завади імітують або спотворюють спостережувані і реєстровані кінцевою апаратурою сигнали або зображення, затрудняють або виключають виділення корисної інформації, ведення радіопередачі, знижують їх дальність. Під дією завад засоби негласного отримання інформації, які передають інформації по радіоканалу, можуть припинити передачу інформації, незважаючи на їх повну справність і працездатність.

Для запобігання витоку інформації за допомогою радіозакладних пристроїв одного і того ж класу, але з використанням різних видів сигналів і способів їх обробки, застосовуються різні види завад.

Треба мати на увазі, що завади, в залежності від джерела їх створення, можуть бути природні (грозові розряди, індустриальні завади, вплив сусідніх радіозасобів) та навмисні. Все різноманіття завад, за частотно-часовими характеристиками, можна звести до шести основних різновидів [9, 12]: шумові, імпульсні, вузькосмугові (в граничному наближенні – синусоїдальні), внутрішньо системні, ретрансльовані, імітаційні.

Внутрішньо системні завади можна віднести тільки до ненавмисних (природних). Вони є характерними для асинхронно-адресних систем зв'язку, що працюють в одній смузі частот. Завади виникають, перш за все, за рахунок не ідеальності взаємкореляційних функцій адресних кодів.

Шумову заваду представляють у вигляді зовнішнього флуктуаційного шуму, що збільшує інтенсивність шуму приймача.

Імпульсні завади діють протягом обмеженого часу; в залежності від форми імпульса розрізняють шумові (обмежений у часі шум), відео- та синусоїдальні (вузькосмугові) імпульсні завади. Імпульс завади може бути одиночним, але при створенні навмисних завад частіше застосовують пакет імпульсної завади, який вражає елементи сигналу, спотворюючи його часові характеристики. Вузькосмугова завада перебиває частину спектра сигналу, що передається. При цьому спотворюється спектр та погіршуються як спектральні, так і кореляційні властивості сигналу.

Імпульсні завади представляють собою серію немодульованих або модульованих високочастотних імпульсів. Модуляцією за амплітудою, частотою слідування, тривалості радіоімпульсів завад або за декількома цими параметрами підвищується їх ефективність. Можна так підібрати амплітуду і тривалість випромінюваних імпульсів, що відрізнити їх від корисного сигналу буде практично неможливо. Оскільки при створенні імпульсної завади передавач випромінює електромагнітну енергію короткочасно, при незначній його середній потужності можна отримати високу імпульсну потужність.

При великому різноманітті імпульсних завад, немає, однак, єдиної універсальної моделі, що описує ці завади. Як правило, рівні та тривалості таких завад приймають розподіленими за експоненційним законом, а ймовірність появи m імпульсів на інтервалі часу T_{13} (у відповідності до розподілу Пуассона) [10]:

$$P_{13}(m) = (LT_{13})^m \exp(-LT_{13}) / m!, \quad (1)$$

де L – середнє число імпульсів на інтервалі T_{13} .

Імпульсні завади можуть генеруватися постановниками завад або ретрансляторами сигналів, прийнятих від станції, що підлягає подавленню (завади у відповідь).

Таблиця 1.6

Класифікація навмисних радіоелектронних завад

Класифікаційна ознака	Характеристика завад
За способом формування (реалізації)	Активні – завади, що створюються енергією джерел завад (генераторів або ретрансляторів)
	Пасивні – завади, що створюються розсіюванням енергії електромагнітних хвиль об'єктами або середовищами
За ефектом (характером) впливу на РЕЗ	Маскувальні – завади, що затрудняють виявлення, розпізнавання та визначення параметрів корисних сигналів засобів радіозв'язку
	Імітаційні (дезінформуючі) – завади, що створюють невірну інформацію (сигнали) в засобах радіозв'язку
За співвідношенням спектра завад і корисних сигналів	Прицільні – завади, що випромінюються на робочій частоті засобів радіозв'язку, що подавляється
	Загороджувальні – завади з шириною спектра, що перевищує смугу частот сигналу засобів радіозв'язку
	Прицільно-загороджувальні – завади (скануючі, ковзаючі) зі змінною частотою випромінювання в діапазоні роботи радіозакладних пристроїв
За структурою випромінювання	Неперервні – завади, модульовані за амплітудою, частотою (фазою) або шумовою напругою
	Імпульсні – завади у вигляді серій не модульованих або модульованих радіоімпульсів
За інтенсивністю	Слабкі – завади, що не перевищують за рівнем корисний сигнал. Можуть визвати втрату до 25% переданої інформації, при цьому не знижують можливостей передачі перехопленої інформації
	Середні – завади, які за рівнем співрозмірні з сигналами засобів радіозв'язку. Викликають втрату не менше 50% інформації
	Сильні – завади, що значно перевищують корисний сигнал за рівнем. Призводять до втрати не менше 75% інформації і виключають можливість отримання корисної інформації

Найскладніше моделювати навмисні завади, якість яких тим вища, чим менше визначена їх статистика. Однак кожна завада характеризується декількома параметрами, які при моделюванні можуть бути задані в апріорно вибраному діапазоні значень у вигляді, наприклад, випадкових чисел.

Ретрансльована завада створюється в результаті підсилення та перевідбиття переданого сигналу однією-двома сусідніми станціями. Перевідбитий та затриманий сигнал, потрапляючи

до приймача істинної станції (адресата), створює специфічну заваду, вплив якої тим більший, чим гірші кореляційні властивості сигналів, що передаються.

Загальну класифікацію навмисних радіоелектронних завад подано в табл. 1.6.

За ефектом (характером) впливу навмисні завади розділяють на імітаційні та маскувальні.

Імітаційні (дезінформуючі) завади – це сигнали, що випромінюються приладами завад для внесення неправдивої інформації, що підлягають подавленню. За структурою вони близькі до корисних сигналів і тому створюють в кінцевому пристрої сигнали, подібні до реальних, зменшують пропускну спроможність системи, призводять до втрати частини інформації. При впливі імітаційних завад характеристики приймального пристрою не погіршуються.

Часто імітаційну заваду називають структурною або прицільною. Термін „прицільна завада” стає виправданим при співпаданні в приймачі фази або середньої частоти завади з фазою переданого сигналу або з середньою частотою одного або декількох частотних підканалів. В останньому випадку заваду іноді називають зосередженою.

За структурою і способом застосування такі завади можна розділити на два типи.

Перший слід віднести до завад, що впливають на радіоканали чергового прийому. Їх основним призначенням є запуск апаратури і введення неправдивої інформаційної вставки, або блокування радіоканалу зв'язку з метою його зриву. За характером застосування такі імітозавади переважно носять попереджувальний характер (варіант загороджувальних завад). Ця особливість дозволяє ефективно застосовувати загороджувальні по частоті завади. Причому, враховуючи можливість звуження діапазону частот (за даними радіо перехвату і прогнозованими особливостями розповсюдження радіохвиль), можливе застосування напівзагороджувальних завад з перестройкою (скануванням) параметрів випромінювання по області невизначеності.

Необхідний час блокування визначається тривалістю і іншими особливостями диверсійних операцій, а також можливостями засобів виявлення і часом реакцій упереджувальних сил, який може складати від десятків хвилин до десятків годин.

До другого типу відносяться імітаційні завади, що діють в процесі радіозв'язку (варіант завади у відповідь), основною ціллю яких є недопущення прийому корисної інформації, і, як більш складний варіант – з метою введення неправдивої інформації. Завади цього типу можуть викликати хибні режими роботи засобів зв'язку за рахунок впливу на системи тактової і циклової синхронізації приймача.

Маскувальні завади погіршують характеристики приймального пристрою, створюють фон, на якому затрудняється або повністю виключається виявлення, розпізнавання, виділення корисних сигналів. Із збільшенням потужності завад їх маскувальний вплив зростає.

В залежності від способу наведення завад, співвідношення ширини спектрів завад і корисних сигналів маскувальні завади розділяють на загороджувальні і прицільні. Загороджувальні завади мають ширину спектра частот, що значно перевищує смугу, яку займає корисний сигнал, що дозволяє подавлювати одночасно декілька засобів радіозв'язку без точного наведення передавача завад на по частоті. Їх можна створювати, не володіючи повними даними про параметри сигналів подавлюваних засобів радіозв'язку. Особливістю загороджувальних завад є те, що при незмінній потужності передавача станції завад їх спектральна щільність потужності G_z (Вт/МГц) зменшується з розширенням спектра випромінювання.

Прицільні завади мають ширину спектра, рівну або в 1,5-2 рази більшу за ширину спектра корисного сигналу. Ефективність їх впливу залежить від точності співпадання частоти з сигналом, спектральної щільності потужності та способів обробки сигналів в приймачі засобу радіозв'язку. Прицільні завади характеризуються високою спектральною щільністю потужності. Оскільки вони випромінюються у вузькій смузі частот, то можуть бути реалізовані малопотужними передавачами.

Одним із способів формування загороджувальних завад є швидка перестройка передавача вузькосмугових завад в широкій смузі частот. Завдяки цьому в певній частині діапазону роботи засобу радіозв'язку послідовно зосереджується достатньо висока щільність потужності, необхідна для їх подавлення. Однак при наявності схем захисту ефективність цих завад може виявитися нижчою, ніж загороджувальних, які створюються передавачем без перестроювання по частоті.

Недоліком прицільних завад є те, що вони одночасно можуть подавляти тільки один засіб радіозв'язку, який працює в даному діапазоні.

Для розв'язання великої кількості задач у теорії електрозв'язку широко використовується поняття білий гауссівський шум, під яким розуміють ідеалізований гауссівський випадковий процес, спектральна щільність потужності якого рівномірна в нескінченній смузі частот. Спектральна щільність потужності білого шуму рівномірно розподілена в нескінченній смузі частот:

$$G(f) = G_0; \quad 0 < f < \infty. \quad (2)$$

Найбільш універсальною і стійкою до різних способів підвищення завадостійкості є шумова загороджувальна завада (рис. 1.5), моделлю якої є обмежений у смузі білий гауссівський шум зі спектральною щільністю потужності G_3 :

$$G_3 = P_3 / \Delta f_c, \quad (3)$$

де Δf_c – ширина спектра сигналу.

Загороджувальна завада повинна перекривати частотний діапазон і при відповідній потужності бути в змозі подавити радіосигнал при будь-яких способах перестройки частоти. Оскільки частотний діапазон може бути досить значним, потужність передавача завад повинна бути достатньо великою. В зв'язку з цим завади загороджувального виду представляють велику небезпеку з точки зору забезпечення електромагнітної сумісності (ЕМС) для інших радіоелектронних засобів, що працюють в тому ж діапазоні частот. При цьому сама завада стає радіопомітною. Відмічені недоліки звужують можливості застосування завад загороджувального виду.

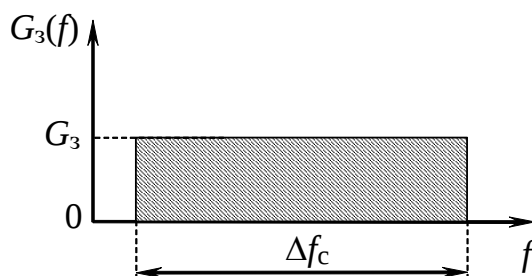


Рис. 1.5. Шумова загороджувальна завада

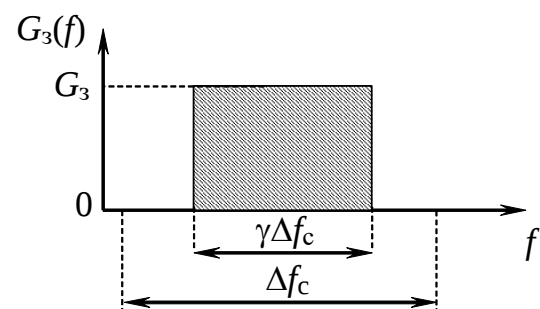


Рис. 1.6. Шумова завада в частині смуги

Потужність шумової завади може бути використана ефективніше за рахунок зосередження її в обмеженій смузі частот, значно меншій, ніж діапазон частот радіозакладки. Таку заваду прийнято називати шумовою завадою в частині смуги (зосередженою по спектру завадою, завадою з частковим перекриттям спектру сигналів радіозакладок) (рис. 1.6). Спектральна щільність потужності шумової завади в частині смуги G_3 , може бути представлена у вигляді двох рівнів [11, 12]:

$$G_3 = \begin{cases} \frac{P_3}{\gamma \Delta f_c} & \text{в смузі } \gamma \Delta f_c; \\ 0 & \text{в смузі } (1 - \gamma \Delta f_c), \end{cases} \quad (4)$$

де γ – коефіцієнт, що характеризує частину смуги сигналу, яку займає завада, $0 \leq \gamma \leq 1$.

Як видно з виразу (4), спектральна щільність потужності шумової завади в частині смуги зростає в $1/\gamma$ разів у порівнянні зі спектральною щільністю потужності шумової загороджувальної завади (3). Станція шумових завад з рівномірно розподіленою потужністю в межах смуги $\gamma \Delta f_c$ подавляє частотні елементи сигналу.

З метою підвищення ефективності системи захисту, спектр шумової завади в частині смуги може стрибкоподібно за випадковим законом переміщуватися по всьому діапазону частот. При даній моделі завади для будь-якого співвідношення сигнал/завада P_c/P_3 має місце оптимальне значення частини подавлюваної смуги γ_{opt} , при якій завадостійкість буде мінімальною. Завада з такими параметрами є найгіршою. З метою поточної оптимізації ширини спектру завади в частині смуги і потужності завади необхідно мати апаратуру для вимірювання параметрів сигналів, що підлягають подавленню.

Для радіозакладних пристроїв ефективною завадою, за певних умов, є полігармонійна завада (багатотональна завада) [9-11], що представляє собою набір із l немодульованих гармонійних коливань рівної потужності, розподілених по діапазону частот f_c відповідно до заданої постановником завад стратегії (рис. 1.7):

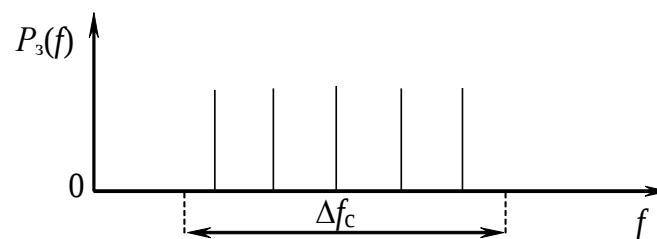


Рис. 1.7. Полігармонійна завада

Наприклад, для радіозакладних пристроїв з псевдовипадковим перестроюванням робочої частоти (ППРЧ) для створення ефективною полігармонійної завади потрібне достатньо точне наведення вузькосмугових завад на центральні частоти каналів, а також забезпечення на вході i -го каналу приймача певного співвідношення потужності завади P_3 і потужності сигналу P_c

$$\frac{P_3}{l} = \frac{P_c}{\alpha}; \quad (5)$$

де α – деяке позитивне число (параметр розподілу потужності), що вибирається постановником завад відповідно до заданої стратегії так, щоб оптимізувати ефективність завади. Ефективність полігармонійної завади, що діє в тому ж каналі, в якому знаходиться і сигнал, залежить від різниці фаз між завадою і сигналом. При несприятливих фазових співвідношеннях і рівності $P_3 = P_c$ завада може повністю подавити корисний сигнал.

Основними методами постановки багатотональних завад для радіозакладних пристроїв (рис. 1.8):

1. Метод “смугового подавлення”, суть якого полягає в розподілі m немодульованих сигналів в кожній M -ічній смузі, $m \in [1, M]$. При цьому кожна M -ічна смуга містить або точно m тонів, або не містить жодного тону.

2. Метод “незалежного багатотонального подавлення” полягає у випадковому розподілі немодульованих сигналів по сегментах широкосмугового сигналу в смузі Δf_c , при якому постановник завад не управляє їх числом в окремих каналах СРЗ.

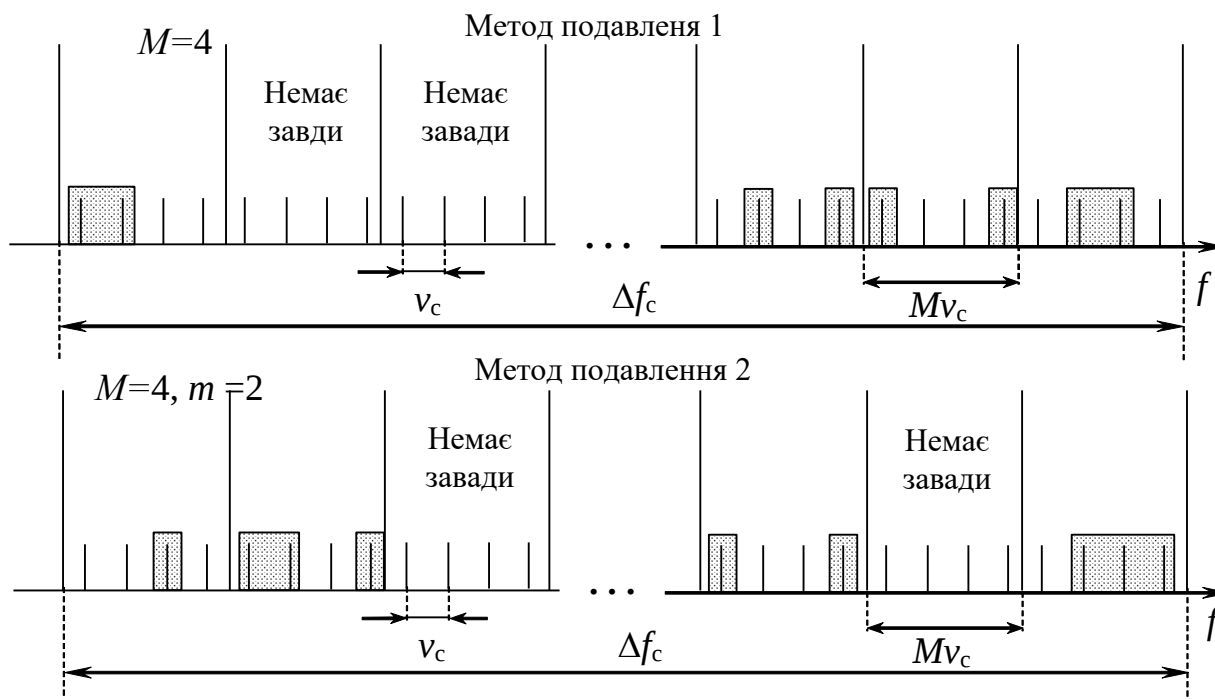


Рис. 1.8. Методи багатотонального подавлення

Ефективність методів подавлення 1 і 2 залежить від апріорної інформації про характеристики сигналів M -їчної СРЗ. Так, метод “смугового подавлення” застосовується у разі, коли постановнику завад відома частота M -їчного сегменту та є можливість розмістити заваду в сегмент, що вражається.

Оскільки стратегія методу “смугового подавлення” вимагає, щоб M -їчна смуга містила або точно n тонів, або жодного, то M -їчна смуга подавлюватиметься з ймовірністю $P = \frac{M\gamma}{n}$. Метод “смугового подавлення” найбільш ефективний при $n = 1$. Метод “незалежного багатоканального подавлення” не вимагає таких допущень (як метод 1), тому при $l \gg M$ ймовірність подавлення M -їчної смуги $P = 1 - (1 - \gamma)^M$ або при великих відношеннях E_c/G_3 ймовірність подавлення $P \approx \gamma M$ [8].

Внаслідок того, що однієї гармонійної завади достатньо, щоб викликати помилку в M -їчному символі, а постановнику завад невідома послідовність переключення частот, то він спробує охопити завадами якомога більше M -їчних смуг, максимізувавши тим самим ймовірність подавлення p .

Наявну потужність станції завад (СЗ) найбільш раціонально можна використовувати при створенні завад у відповідь (ретрансльованих завад) [2, 12]. Потужність передавача завад в цьому випадку концентрується лише в смузі частот основного або додаткового (або основного і додаткового) каналів, що подавлюється, і лише під час її роботи. У якості завади у відповідь можуть застосовуватися шумова і вузькосмугова (гармонійна) завада (рис. 1.9), а також комбінація шумової і вузькосмугової завад.

Завади у відповідь певною мірою є копією частотних елементів радіосигналу, що подавлюється. Це може привести до того, що на приймальній стороні такі завади можуть бути сприйняті як корисні сигнали свого кореспондента. Загалом же випадку завади у відповідь

можуть бути модульовані шумом перехоплені частотні елементи сигналу. Моделлю таких завад є стаціонарний вузькосмуговий гаусівський процес.

Завади у відповідь з погляду енергетичних можливостей є одними з найбільш ефективних для подавлення радіосигналу.

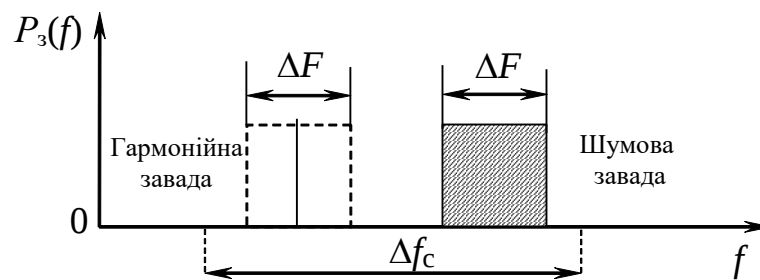


Рис. 1.9. Комбінована завада

Висновки

Аналіз показав, що основними видами завад, які порівняно просто реалізуються в системах радіоелектронного подавлення, є: шумова загороджувальна завада; шумова завада в частині смуги; полігармонійна завада.

Проведені дослідження довели, що найбільш універсальною і стійкою до різних способів підвищення завадостійкості, є шумова загороджувальна завада. Потужність шумової завади може бути використана ефективніше за рахунок зосередження її в обмеженій смузі частот, значно меншій, ніж діапазон частот радіозакладок, тобто за рахунок створення шумової завади в частині смуги. Для ефективного радіоелектронного подавлення сигналу радіозакладок з ППРЧ доцільно використовувати прицільну за частотою заваду у відповідь (ретрансльовану заваду). Найбільш ефективною завадою з точки зору подавлення корисного сигналу для радіозакладок з цифровою модуляцією представляють імітаційні (дезінформуючі) завади, при впливі яких система залишається працездатною, однак, не забезпечує передачі корисної інформації. В деяких випадках дезінформуючі завади можуть призводити до введення неправдивої інформації в радіосигнал, викликати хибні режими роботи за рахунок впливу на системи тактової і циклової синхронізації приймача.

Перелік посилань

1. Дробик О. В., Лаптев О. А., Пархоменко І. І., Богуславська О. В., Пепа Ю. В., Пономаренко В. В. Розпізнавання радіосигналів на основі апроксимації спектральної функції у базисі передатних функцій резонансних ланок другого порядку. Сучасний захист інформації. 2024. №2. С.13-23.
2. S.Yevseiev, O. Laptiev, O.Korol, S.Pohasii, S.Milevskyi, R. Khmelevsky. Analysis of information security threat assessment of the objects of information activity. International independent scientific journal. Poland. Vol. 1, №34, 2021, pp.33 – 39. ISSN 3547-2340
3. Лаптев О.А., Бучик С.С., Савченко В.А., Наконечний В.С., Михальчук І.І., Шестак Я.В., Виявлення та блокування повільних ddos-атак за допомогою прогнозування поведінки користувача. Наукоємні технології. Інформаційні технології, кібербезпека. Том 55 № 3 .2022. С.184-192. DOI: 10.18372/2310-5461.55.16908
4. Serhii Yevseiev, Khazail Rzayev, Oleksandr Laptiev, Ruslan Hasanov, Oleksandr Milov, Bahar Asgarova, Jale Camalova, Serhii Pohasii. Development of a hardware cryptosystem based on a random number generator with two types of entropy sources. Eastern-European journal of enterprise technologies. Vol.5№9 (119), 2022 P. 6–16. ISSN (print) 1729 - 3774. ISSN (on-line) 1729-4061. <https://doi.org/10.15587/1729-4061.2022.265774> Scopus.
5. Barabash O.V., Open'ko P.V., Kopiika O.V., Shevchenko H.V. and Dakhno N.B. Target Programming with Multicriterial Restrictions Application to the Defense Budget Optimization. Advances in Military Technology. 2019. Vol. 14, No. 2, pp. 213 – 229.
6. Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., ...Laptieva, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, P. 67–70
7. Yevseiev, S., Laptiev, O., Lazarenko, S., Korchenko, A., & Manzhul, I. (2021). Modeling the protection of personal data from trust and the amount of information on social networks. eureka: Physics and Engineering, (1), 24-31. <https://doi.org/10.21303/2461-4262.2021.001615>

8. Lukova-Chuiko, N., Herasymenko, O., Toliupa, S., Laptiev A, T., Laptiev, O. The method detection of radio signals by estimating the parameters signals of eversible Gaussian propagation. Conference Paper. 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory, ATIT 2021 - Proceedings, 2021, pp. 67–70.
9. Barabash O., Laptiev O., Grushina O. The conceptual model of the intelligent network. Сучасний захист інформації, №4 (56), 2023, Р. 1-9. [https://doi.org/ 10.31673/2409-7292.2023.030202](https://doi.org/10.31673/2409-7292.2023.030202)
10. Король О.Г., Лаптева Т.О., Метод використання кіберрозвідки для виявлення індикаторів компрометації на базі матриці Mitre Att&ck. Сучасний захист інформації. 2024. No 3(59). С.69-74. DOI: 10.31673/2409-7292.2024.030007
11. Sobchuk V., Laptiev S., Laptieva T., Barabash O., Drobyk O., Sobchuk A. A modified method of spectral analysis of radio signals using the operator approach for the fourier transform. 2024. *IT, Automation, Measurements in Economy and Environmental Protection*. Vol. 14, No 2, P.56–61. <https://doi.org/10.35784/iapgos.5783> Scopus

Надійшла 31.01.2025