УДК 621.391.827

С. О. Сєрих

СКРИТНІСТЬ ПОВІДОМЛЕНЬ В МЕРЕЖАХ ІЗ РАДІОДОСТУПОМ ТА НАПРЯМКИ ЇЇ ПІДВИЩЕННЯ

В статі проведено аналіз видів скритності передавання повідомлень, факторів, що на неї впливають та визначені напрямки підвищення з метою формулювання рекомендацій до застосування при проектуванні нового обладнання систем радіозв'язку чи його удосконалення. Запропоновано підвищувати скритність передавання повідомлень за рахунок використання складних сигналів із зазначенням такого виду, який забезпечить необхідну скритність і завадостійкість передавання. Порівняльну оцінку сигналів проведено за узагальненим показником структурної та енергетичної ентропійною скритності із визначенням раціональних параметрів сигналів. Визначені напрямки подальших досліджень.

Ключові слова: повідомлення, радіодоступ, скритність, шумоподібні сигнали.

Вступ

В мережах із радіодоступом однією з невирішених остаточно проблем залишається проблема конфіденційності обміну повідомленнями.

В першу чергу це пояснюється: необмеженим доступом до загального середовища розповсюдження радіосигналів, який можливо контролювати тільки на передачу; значним підвищенням їх широкосмуговісті пропорційної до пропускної спроможності сучасних радіосистем; стрімким збільшенням кількості радіоелектронного обладнання (РЕО) при загальній тенденції його удосконалення, як за напрямком покращення технічних характеристик (наприклад, чутливості приймачів, збільшення їх діапазону), так і якісних показників радіоелектронних компонентів (РЕК).

По друге низьким рівнем ефективності систем аутентифікації і авторизації РЕО користувачів за рахунок спрощення програмного забезпечення, здешевлення обладнання у наслідок виключення спеціального обладнання захисту даних.

В трете намаганнями виробників РЕО застосовувати уніфіковані методи модуляції, які з одного боку забезпечують якість обміну, що вимагається, а з іншого підтримують стандартність у показнику ціна-ефективність обладнання.

Це перешкоджає більш активному просуванню систем радіозв'язку (СРЗ) на ринку сучасних технологій. До того ж використання засобів радіовипромінювання умовно контролюємої потужності при підвищенні їх щільності суттєво погіршують електромагнітну сумісність. Складність надійного обміну повідомленнями зростає у разі, коли РЕО стають об'єктом навмисного пригнічення із використанням спеціалізованих засобів постановників завад [1], із широким цільовим діапазоном впливу завдяки різноманітності арсеналу завад [2], що застосовується після розвідки параметрів цілі придушення [3]. Енергетична адаптація СРЗ до завадових умов, як напрямок протидії впливу, технічно обмежена, локальна в застосуванні, тимчасова, а тому малоефективна.

Інший напрямок, за яким останнім часом вдосконалюються СРЗ для підвищення завадостійкості та конфіденційності [4], базується на використанні складних сигналів із змінними параметрами, які завдяки своїм властивостям мають підвищену скритність, тобто маскують сам факт випромінювання, бо енергетично та структурно нагадують шум, тому мають назву [5] – шумоподібні сигнали (ШПС). Природно, що саме процес їх використання впливає на безпеку передачі даних, бо одночасно є додатком до змін в модуляції, кодуванні, спрощує реалізацію адаптації до рівня та виду завад, ускладнює розвідку параметрів і протидіє різноманітним видам загроз СРЗ.

Особливістю є те, що на рівні моделі взаємодії відкритих систем місце їх застосування відповідає фізичному (бо має апаратне рішення) і частково канальному рівню (при адаптації можуть змінюватись параметри каналів взаємодіючих засобів). На вищі рівні де зазвичай зосереджуються основні зусилля по захисту інформації вони не впливають, хоча загальну задачу розв'язують частково попередньо.

Постановка задачі

Проведення аналізу видів скритності передавання повідомлень, факторів, що на неї впливають та визначення напрямків підвищення з метою формулювання рекомендацій до застосування при проектуванні нового обладнання СРЗ чи його удосконалення.

Основна частина

Для розв'язання поставленої задачі необхідно виконати аналіз загроз для безпеки СРЗ, що дозволить висунути вимоги до параметрів ШПС і визначити їх ефективність за властивостями. Розподіл загроз, як на найгірший випадок, диктується намірами систем протидії згідно прийнятих концепцій застосування [6] і поділяється на :

• порушення фізичної цілісності системи;

• перехоплення повідомлення, що передавалось;

• несанкціоноване проникнення в систему.

Кожна з перерахованих загроз має свою специфіку і потребує індивідуального розгляду для визначення шляхів її усунення. При цьому об'єкт, який створює дані загрози, доцільно у загальному випадку зазначити як джерело загроз (ДЗ).

Порушення фізичної цілісності системи

Цілісність СРЗ може бути порушена як умисно (дія навмисних завад), так і ненавмисно (дія випадкових завад: природних, промислових тощо). Для боротьби із ДЗ застосовуються підрозділи служби радіоконтролю за частотними ресурсами, які крім контролю вживають адміністративні заходи, щодо припинення випромінювань як для зареєстрованих засобів порушників, так і для не санкціонованих, не ліцензованих радіо засобів. А для покращення електромагнітного стану і при розв'язанні суперечливих питань, згідно із рекомендаціями МСЕ пропонують [3]:

• погодження на зміну частоти СРЗ;

• використання спрямованих антен відповідних апертур;

• коригування часового розподілу, розкладів або складання експлуатаційних угод;

• зміна класу випромінювання, виду модуляції;

• просторове переміщення СРЗ чи частотне переміщення окремих каналів для багатоканальних систем передачі;

• перенесення тимчасового навантаження на інші частоти;

• припинення роботи засобу, що є постійним порушником - ДЗ, для інших.

Такі міри є організаційними і зазвичай не розв'язують термінових проблем.

Необхідні заходи технічного характеру до підвищення завадостійкості радіозасобів, реалізовані в РЕО, які повинні мати високу ступень адаптації за реакцією на вплив і алгоритми протидії зорієнтовані на поширений діапазон можливостей ДЗ. Це не енергетичні методи зміни характеристик РЕО, а параметричний метод адаптації сигналу, заснований на просторовій, частотній, поляризаційній селекції сигналів, використання сигналів змінного виду та структур.

Перехоплення повідомлення

На сьогодні технічні можливості засобів перехоплення радіосигналу в мережах із радіодоступом такі, що ускладнити їм роботу важко. Виключаючи напрямок закриття змісту повідомлення спеціалізованими засобами захисту слід розглянути ті напрямки, що зменшують демаскуючи признаки випромінювання та забезпечують підвищену скритність радіосигналу. Це такі, які ускладнюють розвідку параметрів сигналу та зменшують імовірність вибору його в якості об'єкта пригнічення. Крім таких заходів можливе використання організаційних, наприклад, вибір місць розташування СРЗ, скритих режимів роботи, використання у якості екранів місцевість, робота гостро направленими антенами.

Несанкціоноване проникнення в систему

Для проникнення в СРЗ необхідно виконання декілька вимог, які, зазвичай, визначаються ймовірностями дій, можливостей і підтвердження мети [3], серед яких принциповими стають

такі: - імовірності прийняття рішення ДЗ на проникнення в систему – $Q_{пр}$, імовірності енергетичної спроможності розвідки параметрів сигналів СРЗ - $Q_{ер}$ та імовірності часового контакту засобу ДЗ та РЕО – Q_t і визначають коефіцієнт проникнення - $К_п$ порівняння значень якого дозволяє здійснювати оцінку ефективності чи неефективності загрози:

$$К_п = Q_{пр}\ Q_{ер}\ Q_t\ .$$

Аналіз розглянутих загроз безпеки СРЗ показує, що практично у всіх випадках (крім ненавмисних завад) для ДЗ в порушенні безпеки необхідні апріорні відомості про стан, режими роботи, характеристики РЕО, параметри сигналів. Отримання такої інформації здійснюється шляхом радіомоніторингу, який за підвищенням скритності сигналів перевищуватиме відведений термін часу, зменшуючи тим самим $К_п$.

Таким чином головною властивістю СРЗ для подолання наміру загроз стає скритність, яку доцільно визначати як здатність протистояти діям ДЗ, що спрямовані на виявлення наявності вимірювання радіосигналів, їхніх параметрів, розкриття особливостей їхнього застосування в умовах адоптації до завад.

Розрізняють такі [7] види скритності сигналів СРЗ, що підвищуються застосуванням ШПС:

- енергетична скритність радіосигналу та модулюючого ШПС;
- структурна скритність виду і параметрів ШПС;
- інформаційна скритність повідомлення завдяки сигналу ШПС;
- тимчасова і просторова скритності сигналів.

Аналіз рівня загроз і можливостей РЕО показує [3] що для забезпечення підвищеної енергетичної скритності повинні виконуватись комплексні організаційно-технічні заходи, спрямовані на виключення або істотне ускладнення пошуку сигналів СРЗ, визначення параметрів ШПС в останньому випадку це параметрична скритність, що є складовою енергетичної і структурної скритності ШПС, яка пов’язана із ентропійною невизначеністю сигналу.

Для радіосигналів показовим стає кордонна відстань R між ДЗ і РЕО, необхідна для прийняття рішення про сигнал, що враховує не структурні його особливості, а тільки впливові на енергетичний потенціал, показники дуальної, розвідувальної радіолінії:

$$R=(\lambda/4\pi)[P_{пд}\ G_{пд}\ G_{пм} / (W_{пл}W_{ф}W_{ср}P_{пм}\ q^2)]^{1/2},$$

де: λ – довжина хвилі передавача РЕО; $P_{пд}$ – його потужність; $G_{пд}$ – коефіцієнт підсилення його антени в напрямку ДЗ; $P_{пм}$ – чутливість приймального пристрою ДЗ; $G_{пм}$ - коефіцієнт підсилення його антени в напрямку РЕО; q^2 – відношення сигнал/шум на вході приймального пристрою ДЗ, при якому досягається задана якість виявлення сигналу СРЗ;

$W_{пл}$ – втрати за рахунок розбіжності в поляризації ПД-ПМ;

$Wф$ – стандартизовані втрати у антенно-фідерного тракті ДЗ;

$W_{ср}$ – втрати, що визначаються R, властивостями та умовами розповсюдження сигналів.

Аналіз виразу дозволяє зробити висновки про недоцільність підвищення енергетичного потенціалу СРЗ для підвищення скритності, бо зменшення R примусово потребує просторового наближення ДЗ до об’єкту розвідки. Рівень енергетичної скритності є визначальним для оцінки інших видів скритності, так як вони розглядаються за обов'язкової умови, що сигнал РЕО виявлений ДЗ і $Q_{пр}\rightarrow 1$.

Структурна скритність передбачає виключення або істотне утруднення розкриття структури і параметрів сигналів СРЗ. Структура радіосигналу визначається видом модуляції, що використовується системою і типом кодування сигналів. Показником ефективності структурної скритності є ймовірність розкриття структури сигналу за умови, що він виявлений. Кількісним параметром, що оцінює структурну скритність зазвичай число вимірювань [8], які необхідно провести, щоб розкрити структуру сигналу. Так, наприклад, для різновиду складного сигналу, що має назву – сигнал із псевдовипадковою перебудовою робочої частоти (ППРЧ) скритність [9] визначається так:

$$S_{\text{ппрч}} = 0.693\ Б_c \log_2 (Б_c),$$

де $Б_c$- база складного сигнала.

Але такій підхід до кількісного визначення скритності недосконалий, має суттєві недоліки. По-перше він спрощений і зазвичай використовується для прискореної загальної оцінки, бо не враховує різницю в ефективності видів складних сигналів у боротьбі із завадами [1] при $Б_c$=*const.*

По-друге ускладнює загальну оцінку видів скритності за рахунок індивідуалізації показника $S_{\text{ппрч}}$.

Більш прийнятним вважатимемо інший підхід, коли застосовується узагальнений показник ентропійної скритності [10] радіопередачі складного сигналу - H_Σ.

При такому розгляданні структурна скритність H_A, що є скритністю множини змінних параметрів сигналу визначається як:

$$H_A = -\sum_{i=1}^{N} Q(a_i)\log(a_i)\ , \qquad (1)$$

де - $Q(a_i)$ імовірність вибору для передачі деякого значення параметра a_i, із повної множини $\{a_i\}$, i=1,2…N.

До того ж величину (1) можна розглядати як мінімально необхідне середнє число двійкових вимірювань чи проб з рівно імовірними наслідками для розкриття невизначеності H_A, тобто структури сигналу з ансамблю складних сигналів [11], що використовують. Чим більше $Б_c$ тим об'ємніше ансамбль сигналів. Але не всі структури мають однакову ефективність і тому потребують розробки методики [12] пошуку оптимальних із загальної кількості – $N = 2^{Бc}$.

У свою чергу енергетична скритність H_E - характеризує ступень невизначеності параметрів сигналу при ведені розвідки структури його в умовах застосування маскуючих сигналів одної чи декількох сусідніх радіостанцій:

$$H_E = -\sum_{i=1}^{N} Q(a_i)\sum_{j=1}^{N} Q(a_j/a_i)\bullet loq(a_j/a_i)\ , \qquad (2)$$

де $Q(a_j/a_i)$ - умовна імовірність регістрації структури складного сигналу a_j з ансамблю N, при передачі a_i.

Тоді загальна ентопійна скритність радіопередачі при сумісній оцінці:

$$H_\Sigma = H_A H_E. \qquad (3)$$

Методика розрахунку H_Σ із (3) зводиться до визначенню N сигналів, що порівнюються і знаходженню імовірності $Q(a_j/a_i)$ для (2) при однакових значеннях інших параметрів радіолінії. При цьому слідує враховувати, що не всі сигнали з N будуть рівно імовірно використовуватись для передавання, а тільки ті, які мають хороші взаємокореляційні властивості [12].

Аналіз ефективності видів складних сигналів проведений в [12] на основі розрахунку введеного [13] показника – мінімального коефіцієнту пригнічення завади за рахунок згортки сигналу - β_{min} показав, що найбільшою завадостійкістю володіють ФМ ШПС. У найгіршому випадку - збігу багатьох параметрів сигналу і завади він дорівнює β_{min}=0,5$Б_c$.

Для такого виду сигналів як ППРЧ і при дії найнебезпечнішою багаточастотної завади він складає - $\beta_{min} = Б_c^2/2$, тобто при $Б_c$=*const* програє ФМ ШПС за показником в $\sqrt{Б_c}$ разів. Для ФМ ШПС-ППРЧ цей програш становить від $\sqrt{Б_c}$ - до одиниці разів, що пояснюється можливістю зменшення числа частотних позицій сигналу M_f, складової частини ППРЧ і водночас збільшенням числа елементів N_e, складової частини ФМ ШПС і тим самим наближенням ФМ ШПС-ППРЧ до ФМ ШПС аж до миті переродження, коли M_f=1.

Результати розрахунків ентропійною скритності сигналів, що найбільш застосовуються в РЕО отриманих за (3) із допомогою (1) та (2) зведені в таблицю 1.

Аналіз результатів показує, що найбільшою скритністю володіють ФМ ШПС-ППРЧ. Це пояснюється необхідністю розвідки не одного, як для інших, а декількох структурних параметрів цього сигналу із різних складових ансамблів N={1,N_e} і N'={1,M_f}, що збільшує ступінь невизначеності ФМ ШПС-ППРЧ і значно ускладнює розвідку його параметрів.

З метою поліпшення оцінки скритності сигналів в таблиці 1 наведені результати розрахунків N для сигналів, що досліджуються за рекомендованою в [13] методикою.

Таблиця 1

Порівняльна характеристика складних сигналів за скритністю передавання

Вид сигналу Параметри	**ФМ ШПС**		**ППРЧ**		**ФМ ШПС-ППРЧ**		
$Б_c$	$N=\varphi^*(Б_c)/\kappa$	H_Σ	$M_f=f(Б_c^{1/2})$	H_Σ	$M_f=f(N_f^{1/2})$	N_e/N $N=\varphi^*(Ne)/\kappa$	H_Σ
511	**48**	**5,5934**	**23**	**4,5275**	**5**	**21 / 6**	**1,4385**
2047	**176**	**7,4910**	**45**	**5,4997**	**7**	**41 / 6**	**1,7469**
8191	**630**	**9,4127**	**91**	**6,5240**	**9**	**101 / 18**	**2,7340**
32768	**1800**	**11,1383**	**181**	**7,5323**	**13**	**194 / 16**	**3,51507**
65535	**2048**	**11,3692**	**256**	**8,0460**	**16**	**256 / 16**	**2,91684**
131071	**7710**	**14,2997**	**362**	**8,5650**	**19**	**362 / 16**	**4,18452**
262143	**7776**	**14,3239**	**512**	**9,0922**	**23**	**496 / 48**	**10,60287**
524287	**27594**	**19,6724**	**724**	**9,6303**	**27**	**719 / 60**	**13,06043**
1048575	**31396**	**20,5258**	**1024**	**10,1846**	**32**	**1024 / 60**	**17,87742**

* $\varphi(Б_c)$ функція Ейлера

В якості кодової послідовності розглянуті М-послідовності максимальної довжини. Застосування функції Ейлера - $\varphi(N_e)$ дозволило визначити кількість М-послідовностей для формування сигналів [5] з гарними взаємокореляційними властивостями. Це попередня загальна оцінка N без визначення структури сигналу, яка потребує подальшого дослідження і розробки методики визначення оптимального об'єму ансамблю сигналів з загальним N. Але є

достатньою для визначення ефективного виду складного сигналу, яким залишається ФМ ШПС.

Інформаційна скритність визначається здатністю СРЗ протистояти заходам, спрямованим на розкриття змісту повідомлення. У якості кількісного показника інформаційної скритності використовують імовірність розкриття повідомлення $Q_{рп}$, значення якого залежить від складності кодів, частоти їх зміни і методів кодування [8]. При застосуванні складних сигналів у спосіб накладення псевдо випадкових послідовностей (ПВП) на інформаційний елемент скритність зростає пропорційно значенню $Б_с$, а за рахунок великого об'єму N при аперіодичній зміні структури ПВП підвищується додатково.

Напрямками подальшого підвищення інформаційної скритності при застосуванні складних сигналів слід вважати:

- блоковість кодування [14] при застосуванні ФМ ШПС;
- прискорення зміни параметрів та структур ПВП для ФМ ШПС чи ППРЧ;
- застосування комбінованих ФМ ШПС із ППРЧ, та реалізацією адаптивної можливості перерозподілу параметрів складових при загальній $Б_с$=*const*.

У якості додаткових мір, що носять більш організаційний характер, для підвищення інформаційної скритності знаходять застосування – формалізація повідомлень; використання спеціалізованих таблиць із змінним кодом розкриття змісту повідомлення.

Тимчасова скритність сигналів, що визначається часом реакції ДЗ відведеної на розвідку його параметрів, просторова скритність, яка приховує місце знаходження РЕО, напрямки їх підвищення докладно розглянуті в [3].

Висновки

Таким чином, завадостійкість, що необхідна для збереження цілісності СРЗ в умовах впливу завад і скритність сигналів, їх характеристик та параметрів є обґрунтовано важливими властивостями РЕО, що забезпечують інформаційну безпеку мереж із радіодоступом.

Зазначені властивості в повній мірі та комплексно реалізуються використанням складних сигналів. Проте в залежності від виду складного сигналу, що застосовується, досягаються різні значення властивостей. Так при використанні ФМ ШПС раціональної структурі та параметрів для передачі повідомлень досягається максимальний рівень захисту від широкого класу завад, а застосування ППРЧ в більший мірі забезпечує номінальну скритність.

Тоді доцільно, з метою уніфікації обладнання, запропонувати використовувати складений сигнал ФМ ШПС-ППРЧ із змінними параметрами та структурою, який гарантовано забезпечить:

• ефективну протидію впливу навмисних завад, боротьбу із інтерференційними та взаємними завадами в СРЗ завдяки збільшенню значення $Б_с$ для складової ФМ ШПС;

• підвищену скритність сигналу завдяки збільшенню частотної невизначеності за рахунок перерозподілу $Б_с$ до складової ППРЧ;

• покращену електромагнітну сумісність засобів СРЗ за рахунок оптимізації параметрів ФМ ШПС-ППРЧ до умов функціонування.

Напрямки подальших досліджень

Головним напрямком в протидії РЕО завадам обґрунтовано обрано структурний, а не енергетичний спосіб, що базується на зміні видів, параметрів та структур складних сигналів. Саме цими змінами досягається висока ступень адаптованості до завадової обстановки. Проте швидкість зміни суттєво залежить від часу реакції комплексу ДЗ, особливо навмисних завад, які постійно удосконалюються як за кількісними так і якісними показниками. Це потребує додаткового дослідження з метою визначення вимог до сучасного РЕО.

Підвищення $Б_с$ при використанні складних сигналів має обмеження, що визначаються наданою РЕО смугою частот і реалізаційними можливостями пристроїв їх формування та обробки. Застосування складених сигналів дозволяє досягати максимальних $Б_с$ меншими затратами, але при цьому погіршуються взаємокореляційні властивості сигналів. Вибором раціональних структур сигналів з загального ансамблю N цей недолік можна усунути, для чого необхідно розробити методику пошуку такого об'єму ансамблю сигналів.

Література

1. Сєрих С.О. Проблеми завадостійкості радіоліній з складними сигналами в умовах активних завад. // ЗВ'ЯЗОК.—2013.-- № 4.- С. 32-37.

2. Серых С.А. К вопросу о влияниях радиоэлектронных помех на современные и перспективные радиоэлектронные системы связи/ Серых С.А., Соловьев В.Р., Богуш В.В. // ЗВ'ЯЗОК.— 2008.— № 2.- С. 69–73.

3. Серых С.А. Оценка безопасности систем радиосвязи с расширеным спектром/ С.А. Серых, Г.И. Гайдур, О.В. Кокотов// Вісник ДУІКТ.- 2008. – Т. 2 № 6. С. 92-97.

4. Ю. Писарев. Безопасность беспроводных сетей // PC Magazine / Russian Edition.1999.№12.

5. Варакин Л. Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин.-М.: Радио и связь, 1985.- 384 с.

6. Харкевич А.А. Борьба с помехами / А.А. Харкевич.-М.: Книжный дом «ЛИБРОКОМ», 2009.-280с.

7. Сєрих С.О. Аналіз методів широкосмугової модуляції для безпроводових технологій./ С.О. Сєрих, Г.І. Гайдур, Міжнарожна НТК «Проблеми інформатизації». 2014. - С. 26-27.

8. Витерби А.Д., Омура Д.К. Принципы цифровой связи и кодирования. -- М.: Радио и связь, 1982 -- 536с.

9. Борисов В.И. и др. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты.-М.: Радио и связь, 2000.-354с.

10. Каневский З.М. Энтропийная оценка скрытности радиопередачи – Радиотехника, т.35 №4, 1980. – С. 30-35.

9. Серых С.А. Анализ спектров составных фазоманипулированных сигналов и условия их применения в телекоммуникационных системах/ С.А. Серых, В.Р. Соловьев, О.В. Кокотов, П.М. Скачков // ЗВ'ЯЗОК.- 2002.- № 6.- С. 48-51.

12. Серых С.А. Методика выбора составного фазоманипулированного ШПС для мобильных систем CDMA/ С.А. Серых, В.Р. Соловьев, М.В. Соловьева, А.И. Остапук // ЗВ'ЯЗОК. – 2003. – №2.– С. 60-62.

13. Барлабанов В.В. Эффективность применения сложных сигналов в условиях помех/ В.В. Барлабанов, С.А. Серых, А.И. Звягин // Радиоэлектроника, Изв. вузов МВ и ССО СССР.- 1989. –Т.34, №4.- С. 82-84.

14. Вишнівський В.В. Підвищення завадостійкості радіоліній за рахунок блочності кодування складних сигналів в умовах активізації навмисних завад/ В.В. Вишнівський, С.О. Сєрих // ЗВ'ЯЗОК.—2013.-- № 6.- С. 31-36.

Надійшла 03.06.2015 р. Рецензент: д.т.н., проф. Єрохін В.Ф.