

## ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ КАНАЛІВ ЗВ'ЯЗКУ НА ОСНОВІ ТЕХНОЛОГІЇ РОЗШИРЕННЯ СПЕКТРУ / RESEARCH SECURITY OF COMMUNICATION CHANNELS BASED ON SPREAD-SPECTRUM TECHNOLOGY

© С.Родін, 2015

This paper is dedicated to research security of communication channels based on spread-spectrum technology. A brief description of types of intentional interference and their impact on the signal transmitter were given. Effect of various intentional interference, such as broadband, narrowband, tone, impulsive and repeat-back on security of communication channels based on spread-spectrum technology was researched.

**Keywords** – spread-spectrum, communication channel, security, signal, interference, noise.

Статтю присвячено дослідженню захищеності каналів зв'язку на основі технології розширення спектру. Дано короткий опис типів навмисних завад та їх вплив на передавач. Досліджено вплив навмисних завад, таких як: широкосмугові, вузькосмугові, тонові, імпульсні, ретрансляційні на захист каналів зв'язку на основі технології розширення спектру.

**Ключові слова** – розширення спектру, канал зв'язку, захищеність, сигнал, завада, шум.

### Вступ

Спочатку методи *розширення спектру (РС) (spread-spectrum — SS)* застосовувалися при розробці військових систем керування й зв'язку. Методи розширення спектру застосовуються створення завадостійких систем зв'язку, зокрема для боротьби з навмисними завадами. У процесі досліджень, розширеному спектру знайшлося й інше застосування — зниження щільності енергії, високоточна локація й використання при множинному доступі. Методи розширення спектру одержали свою назву завдяки тому, що смуга, використовувана для передачі сигналу, набагато ширша за мінімальну, яка необхідна для передачі даних.

Система зв'язку називається системою із розширеним спектром у таких випадках:

1. Використовувана смуга значно ширше мінімально-необхідної для передачі даних.
2. Розширення спектра проводиться за допомогою так званого *розширювального (або кодового) сигналу*, який не залежить від переданої інформації.
3. Відновлення вихідних даних приймачем ("звуження спектра") здійснюється шляхом зіставлення отриманого сигналу й синхронізованої копії розширювального сигналу.

Слід зазначити, що розширення спектра сигналу також відбувається при використанні деяких стандартних схем модуляції, таких як частотна й імпульсно-кодова модуляція. Однак ці схеми не відносяться до методів розширеного спектра, оскільки не задовольняють усім наведеним вище умовам.

Існують такі методи розширення спектра:

*Метод прямої послідовності (direct sequencing — DS)* і *метод стрибкоподібного переналаштування частоти (frequency hopping — FH)* — є найпоширенішими.

Перший метод розширення спектра DSSS заснований на використанні псевдовипадкових послідовностей (ПВП). Другий метод широкосмугової передачі заснований на псевдовипадковому переналаштуванні робочої частоти сигналу (ППРЧ).

Відрізняються ці методи тим, що в другому розширення спектра здійснюється не за рахунок перемножування кодової інформації із ПВП, а за рахунок синтезованої синтезатором робочої (несучої) частоти модулятора, що й переналаштовує її за псевдовипадковим законом.

На приймальній стороні проводиться зворотне перетворення, що приводить до стиску спектра перед демодуляцією.

Третій метод, *перемикання часових інтервалів (time hopping — TH)*, використовується за наявності навмисних завад, оскільки він дозволяє приховувати координати сигналу від потенційного супротивника. Крім того, існують змішані методи, такі як DS/FH, FH/TH або DS/FH/TH.

### Вплив та типи навмисних завад

При постановці навмисних завад основне завдання полягає в тому, щоб позбавити супротивника надійного зв'язку й при цьому звести матеріальні витрати до мінімуму. Завдання приймача й передавача — створити систему зв'язку, стійку до завад, ґрунтуючись на наступних припущеннях:

- абсолютна стійкість до завад неможлива;
- станція-постановник навмисних завад забезпечена інформацією про основні параметри системи (частотний діапазон, час сеансів зв'язку, обсяг переданої інформації і т.д.);
- станція-постановник навмисних завад не має апіорної інформації про послідовність стрибків частоти або псевдовипадкових кодах.

Сигнал передавача повинен бути сформований таким чином, щоб єдиною можливістю для придушення сигналу було створення широкосмугового гаусівського шуму. Інакше кажучи, необхідно, щоб застосування ускладнених методів придушення сигналу не давало ніяких переваг. Основне правило при створенні завадостійкої системи зв'язку — зробити процес придушення сигналу максимально дорогим.

Наведемо рисунок з різними типами завад [1]:

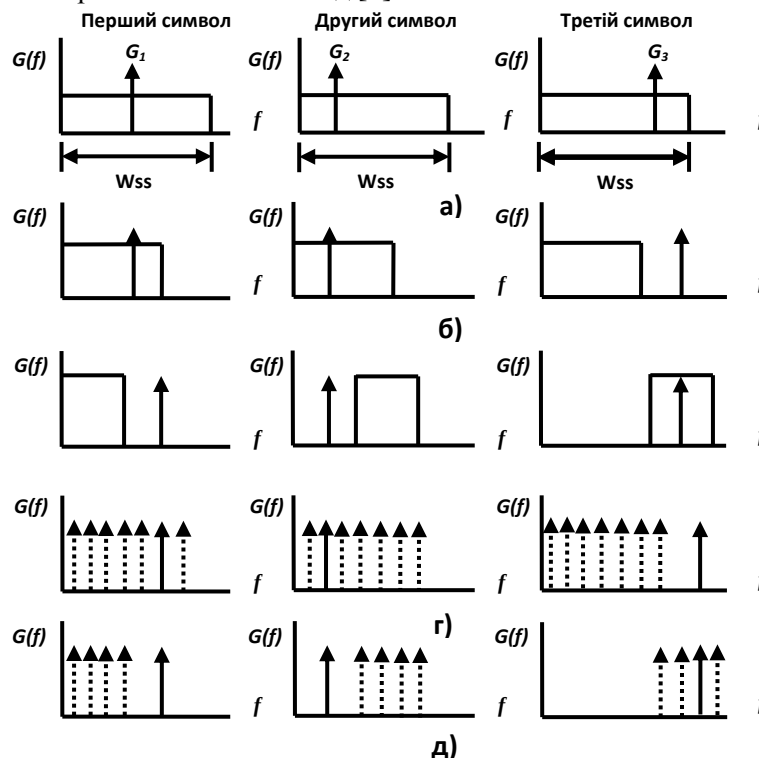


Рис. 1. Типи навмисних завад: а) широкосмуговий шум; б) вузькосмуговий шум; в) східчастий шум; г) вузькосмугові тонові завади; д) східчасті тонові завади;  $W_{ss}$  — смуга розширеного спектру

Для придушення зв'язку можливе використання різних сигналів [1]. Вибір залежить від системи зв'язку, сигнал якої потрібно придушити. На Рис. 1. зображені графіки спектральної щільності потужності різних типів навмисних завад, накладених на тонові сигнали системи зв'язку з *M*-арною частотною маніпуляцією й стрибкоподібним переналаштуванням частоти (FH/MFSK). Область по осі абсцис являє собою смугу розширеного спектру  $W_{ss}$ . Три стовпці графіків відповідають трьом моментам часу передачі символів (трибкам частоти), у які відбувається передача символів зі спектрами  $G_1, G_2$  і  $G_3$ . Рис. 1, а ілюструє роботу станції навмисних завад порівняно малої потужності, що створює шуми по всій області розширеного спектра. На рис. 1,б ширина покриття діапазону навмисними завадами зменшується, але при цьому збільшується потужність самих завад (при цьому площа, яку обмежує крива потужності шумів, залишається сталою). У цьому випадку область шумів не завжди співпадає із сигналом. Однак якщо це все-таки відбувається, негативний вплив на сигнал може бути значним. На рис. 1, в завади створюються в окремих частинах діапазону у випадково обрані відрізки часу. Використання такого методу не дозволяє системі зв'язку адаптуватися до наявності завад. У двох випадках, що залишилися, для придушення зв'язку використовується вже не безперервна смуга частот, а набір тонових сигналів, переданих у певних точках діапазону (рис. 1, г), які можуть розміщатися з певним кроком (рис. 1, д). Останній метод звичайно застосовується для придушення зв'язку в системах зі стрибкоподібним переналаштуванням частоти. Ще один метод, не представлений на рис. 1 - створення імпульсно-модульованого шуму з обмеженою шириною смуги.

Надалі будемо вважати (якщо не обговорено протилежне), то для придушення зв'язку використовується широкосмуговий шум, який постійно покриває всю смугу  $W_{ss}$ .

#### Дослідження захищеності каналів зв'язку на основі технології розширення спектру до різних типів навмисних завад

##### Широкосмугові

Розглянемо створення навмисних завад, які можуть бути змодельовані за допомогою стаціонарного гаусівського шуму з нульовим середнім і рівномірним розподілом спектральної щільності потужності (принаймні, у розглянутій області частот). Якщо генератор, використовуючи всю свою потужність, створює завади у всьому діапазоні розширеного спектра, його називають **широкосмуговим постановником завад (broadband jammer)**.

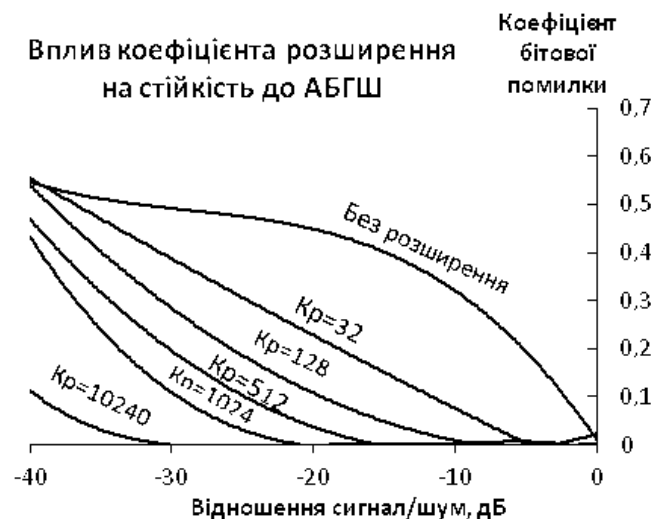


Рис. 2. Вплив коефіцієнта розширення спектру на стійкість до адитивного білого гаусівського шуму (АБГШ)

Єдина можливість зменшити вплив завад полягає в збільшенні коефіцієнта розширення спектру сигналу.

## Вузькосмугові

Негативний вплив постановника завад на систему зв'язку зі стрибкоподібним переналаштуванням частоти найчастіше може бути збільшений за рахунок використання **вузькосмугових завад**. Покриваючи меншу частину діапазону, генератор має можливість збільшувати в ній потужність завад.

Негативний вплив на сигнал значно вищий при використанні вузькосмугових шумів порівняно із широкосмуговими. Зменшити цей вплив можна за допомогою методу **прямого виправлення помилок (forward error correction — FEC)** шляхом чергування [2]. Фактично для кодів з досить низькою інтенсивністю (метод FEC) може привести до того, що постановник вузькосмугових завад буде завдавати максимальної шкоди тільки при роботі в широкосмуговому режимі [3,4].

## Різнотонові

При створенні різнотонових завад станція-постановник ділить повну отриману потужність  $J$  між безперервними тонами, що мають випадкову фазу й рівними по потужності. Ці сигнали розподіляються в діапазоні розширеного спектру  $W_{SS}$  у певному порядку. Аналіз впливу тонових завад на сигнал значно складніше, чим у випадку шумів, особливо для систем DS. Часто тонові завади розглядають як гаусівський шум. Продуктивність некогерентної системи зв'язку FH/FSK уважається однаковою як при вузькосмугових тонових завадах, так і при вузькосмуговому шумі. Однак застосування вузькосмугових тонових завад для придушення сигналу FH/FSK більш ефективне. Причина в тому, що використання безперервних тонових завад дозволяє більш ефективно ввести енергію в некогерентні детектори.

На рис. 3, а і б представлено вісімкову схему FSK зі стрибкоподібним переналаштуванням частоти й без рознесення сигналу, а також система зі швидким стрибкоподібним переналаштуванням частоти з використанням багаторазової ( $N = 4$ ) передачі даних і обмеження елементарних сигналів [1]. Сигнал, який надійшов у накопичувач позначається вектором. Як видно з рис. 3, а, при окремому стрибку частоти смуга даних зайнята отриманим символом з потужністю  $S$ . Якщо тонова завада з отриманою потужністю  $J$  ( $J > S$ ) випадково потрапить у діапазон даних, детектор буде не в змозі правильно визначити отриманий символ.

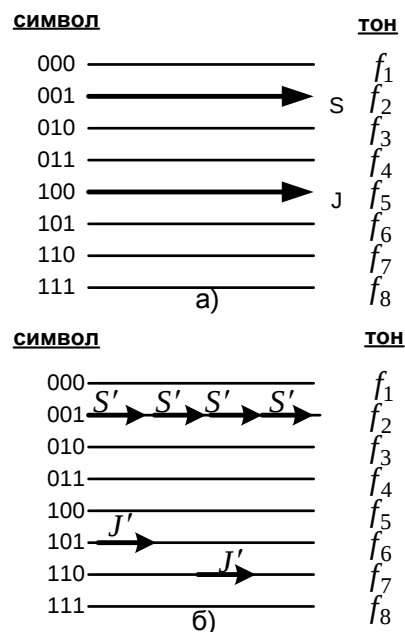


Рис. 3. Багаторазова передача символів зі швидкими стрибками при наявності тонових завад: а) окремий стрибок частоти; б) чотири стрибки частоти

На рис. 3, б чотири елементарні сигнали (довжина кожного вектора є мірою потужності обмеженого елементарного сигналу  $S'$ ) підсумуються й повністю заповнюють накопичувач. Якщо тонові завади випадково потрапляють у спектральну область сигналу, це не вплине на роботу детектора, оскільки потужність завад обмежується до одного рівня з елементарними сигналами зв'язку ( $J'=S'$ ). У прикладі, наведеному на рис. 3, б два сигнали тонових завад потрапляють у діапазон даних. Однак завдяки обмеженню потужності ніяких сумнівів при визначенні отриманого символу не виникає.

## Імпульсні

Розглянемо роботу системи зв'язку DS/BPSK (з прямим розширенням спектру та двійковою фазовою маніпуляцією) при придушенні сигналу імпульсними завадами. Станція навмисних завад генерує імпульси білого гаусівського шуму у вузькій смузі частот. Припустимо, що генератор шумів може визначити центральну частоту й смугу, які використовуються для передачі даних. Припустимо також, що потужність завад може бути збільшена за рахунок зменшення часу передачі. Тоді протягом використовуваного часу спектральна щільність потужності постановника зростає.

Отже, негативний вплив на систему DS/BPSK (без застосування кодування) при однаковій вихідній потужності буде значно відчутнішим при використанні імпульсних завад. Результат такого впливу аналогічний впливу вузькосмугових завад на систему зв'язку FH/BFSK (зі стрибкоподібним переналаштуванням частоти та двійковою частотною маніпуляцією) без використання кодування. В обох випадках ефективне придушення сигналу досягається за допомогою концентрації потужності генератора завад для "глушіння" певної частини переданих символів. Кодування із прямим виправленням помилок і використанням чергування може практично повністю відновити вихідну якість сигналу [1].

При визначенні рівня стійкості не враховувалася швидкість переналаштування частоти. Інтуїтивно можна припустити, що чим частіше відбуваються перегони частот, тим простіше "сховати" сигнал від навмисних завад.

## Ретрансляційні

При визначенні рівня стійкості не враховувалася швидкість переналаштування частоти. Інтуїтивно можна припустити, що чим частіше відбуваються перегони частот, тим простіше "сховати" сигнал від навмисних завад. Вважалося, що швидкість переналаштування частоти *досить велика*, так що генератор завад не встигає простежити за процесом передачі й, відповідно, змінити свою тактику. Проте, існують умови при яких це припущення може бути невірним.

Крім уже розглянутих, існують "інтелектуальні" постановники завад, так звані **постановники ретрансляційних завад** (repeat-back jammer), здатні простежити процес передачі сигналу, що, як правило, робиться за допомогою бічного променя передавальної антени. Такі генератори характеризуються високою швидкістю обробки сигналу, а також здатністю приймання сигналів у широкій області спектра. Це дозволяє сконцентрувати потужність завад у безпосередній близькості від сигналу системи FH/FSK. Перевага постановника завад такого типу перед широкосмуговим очевидна, оскільки завади можуть бути сконцентровані в тій смузі діапазону, яка використовується для зв'язку в кожний момент часу. Слід зазначити, що такий метод придушення сигналу ефективний тільки стосовно систем розширеного спектру зі стрибкоподібним переналаштуванням частоти, оскільки в системах, що використовують метод прямої послідовності, не існує миттєвого вузькосмугового сигналу, який можна було б запеленгувати [1].

Одним з можливих шляхів для зменшення негативного впливу постановника ретрансляційних завад може бути збільшення швидкості переналаштування частоти настільки, щоб протягом часу, потрібного генератору завад для обробки отриманого сигналу й створення завад, система переналаштовувалась на нову частоту. У такому випадку завади не зможуть вплинути на якість зв'язку.

## **Обґрунтування доцільності застосування технології розширеного спектру в системах захисту інформації**

На відміну від радіотехнологій з вузькосмуговою модуляцією, енергія сигналу не зосереджена на невеликому інтервалі навколо несучого коливання, а розподілена у всій виділеній смузі. У результаті введення такої частотної надмірності досягається цілий ряд переваг:

- підвищується завадостійкість;
- забезпечується протистояння впливу навмисних завад;
- не створюється завад для інших пристроїв (ЕМС);
- можливість повторного використання однієї ділянки спектра;
- підвищується енергетична прихованість завдяки низькому рівню спектральної густини;
- можливість збільшення енергоефективності;
- забезпечується можливість кодового поділу каналів для множинного доступу на його основі;
- забезпечується захищеність сеансу зв'язку.

### **Висновок**

З проведеного дослідження випливає, що канали зв'язку на основі технології розширення спектру є досить захищеними, оскільки вони вимагають від постановника завад дуже великих затрат на придушення сигналів, які передаються такими каналами зв'язку. Тому канали зв'язку з використанням технології розширення спектру можуть використовуватись у різного роду системах захисту інформації від яких вимагається висока захищеність каналу зв'язку, наприклад: бездротові системи охорони, системи зв'язку з підвищеною конфіденційністю передачі повідомлень і т.п.

### **Література**

1. Sklar B. *Digital Communications: fundamentals and applications (2nd Edition)*. Prentice Hall, New Jersey, 2001. 2. Simon M. K. and Polydoros A. *Coherent Detection of Frequency-Hopped Quadrature Modulations in the presence of Jamming. Part I. QPSK and QASK; Part II QPR class I Modulation*. IEEE Trans. Commun., vol. COM29, November, 1981, pp. 1644-1668. 3. Stark W. E. *Coding for Frequency-Hopped Spread-Spectrum Communication with Partial-Band Interference: Part I. Capacity and Cutoff Rate*. IEEE Trans. Commun., vol. COM33, n. 10, October, 1985, pp. 1036-1044. 4. Stark W. E. *Coding for Frequency-Hopped Spread-Spectrum Communication with Partial-Band Interference: Part II. Coded Performance*. IEEE Trans. Commun., vol. COM33, n. 10, October, 1985, pp. 1045-1057.