

# АНАЛІЗ КРИТЕРІЇВ ОЦІНЮВАННЯ ЗАВАДОЗАХИЩЕНОСТІ РАДІОКАНАЛІВ В УМОВАХ ШТУЧНИХ ПЕРЕШКОД

Вінницький національний технічний університет

## **Анотація**

*Наведено загальні фактори впливу на завадозахищеність, в основній частині проведено аналіз критеріїв оцінювання завадозахищеності, що є суттєвими в сучасних умовах роботи зовнішніх перешкод. Розглянуті особливості практичного застосування критеріїв завадозахищеності.*

**Ключові слова:** радіоканали зв'язку, завадозахищеність.

## **Abstract**

*General factors influencing interference immunity are presented, and the main part analyzes the criteria for assessing interference resilience, which are essential in modern conditions of external interference. Features of practical application are considered.*

**Keywords:** radio communication channels, interference resilience.

## **Вступ**

При створенні навмисних завад (перешкод) значно ускладнюється або унеможлиблюється нормальне функціонування радіоканалів. У таких умовах завадозахищеність радіоканалів стає визначальним фактором надійності зв'язку. В умовах складного електромагнітного оточення, зокрема при застосуванні перешкод, надзвичайно важливо мати об'єктивні критерії оцінювання стійкості радіоканалів до завад. Адже на основі цих критеріїв визначають оптимальні методи модуляції, кодування, адаптивної зміни параметрів системи зв'язку тощо. Мета даного дослідження – провести огляд і порівняльний аналіз основних критеріїв, що використовуються для оцінювання завадозахищеності радіоканалів, а також розглянути їх застосування в умовах радіоелектронної протидії.

## **Основна частина**

### **Базові фактори, які впливають на завадозахищеність.**

Радіоканал є вразливим до різних типів перешкод, починаючи від природних (термошуми, космічні шуми) і закінчуючи цілеспрямованими штучними завадами. Останні можуть генеруватися як широкопasmові, так і вузькопasmові перешкоди, імпульсні завади, характеризуватися частотною перебудовою завад тощо. При цьому сучасні системи радіоелектронного придушення (РЕП) здатні в реальному часі аналізувати спектр випромінювання та динамічно змінювати структуру та конфігурацію завад із метою найбільш ефективного “засліплення” або спотворення сигналу [1].

До основних факторів, що знижують ефективність радіоканалу у спеціальних застосуваннях, належать:

- Низьке відношення сигнал/шум (SNR) внаслідок потужних завад;
- Багатопроменеве поширення (фединг), що посилює або послаблює сигнал;
- Адаптивний характер завад, які можуть відслідковувати структуру сигналу й обирати ефективний метод впливу;
- Обмежені потужності передавача та приймача, що не дозволяють значно підвищувати енергетичний запас сигналу.

Існують методи, які можуть суттєво підвищувати завадозахищеність завдяки швидкому розвитку методів модуляції, кодування (LDPC, Turbo, Polar) та просторово-часових технологій (MIMO, методи формування діаграми спрямованості). Однак для якісного оцінювання всіх вжитих заходів існують формалізовані критерії.

### Критерії оцінювання завадозахищеності:

1. Відношення сигнал/шум (SNR) та  $E_b/N_0$ . Сигнал/шум один із найбільш базових критеріїв, який відображає рівень потужності корисного сигналу відносно шуму або завади. У системах зв'язку SNR часто вимірюється в децибелах (дБ). Для цифрових систем розглядають також  $E_b/N_0$  – відношення енергії біта до спектральної густини шуму.

В умовах РЕП корисно стежити не лише за середнім рівнем шуму, а й за рівнем активних завад:

$$SIR = \frac{P_{\text{signal}}}{P_{\text{interference}}},$$

де  $P_{\text{interference}}$  – потужність штучно створеної перешкоди [1, 5].

Значне падіння SIR свідчить про критичне погіршення умов зв'язку.

2. Бітова ймовірність помилки та ймовірність пакетної помилки. Бітова ймовірність помилки (BER) визначається як відношення кількості помилково прийнятих бітів до загальної кількості переданих. Для пакетно-орієнтованих систем (Wi-Fi, LTE, телекомунікаційні тактичні мережі) часто використовують ймовірність пакетної помилки (PER) [3, 6]. В умовах цілеспрямованих завад підвищення BER або PER є першим індикатором того, що рівень завад перевищує корекційні можливості системи. Завдяки кодуванню (наприклад, LDPC чи Turbo) та повторним передачам (ARQ) можна знижувати BER, але це часто призводить до зменшення реальної пропускної здатності й ускладнює протидію високопотужним перешкодам [1, 2].

3. Пропускна здатність (ПрЗ, Channel Capacity, Throughput). ПрЗ, або пропускна спроможність, радіоканалу визначається теоремою Шеннона:

$$C = B \cdot \log_2(1 + S/N),$$

де  $B$  – смуга пропускання каналу,  $S$  – потужність сигналу,  $N$  – потужність шуму (або завад). Якщо сигнал піддається активному придушенню, вираз  $(S/N)$  може значно зменшитися. У реальних системах часто використовують «throughput» – ефективну швидкість передачі даних, яка враховує всі накладні втрати (пакетний формат, повторні передачі тощо) [3, 4]. У середовищі РЕП пропускна здатність системи може суттєво падати внаслідок необхідності застосування надмірних механізмів захисту або навіть перейти в режим “мовчання”, якщо протоколи, що використовуються не здатні протидіяти потужним стороннім завадам.

4. Ефективність корекції помилок (FEC Efficiency). Сучасні FEC (Forward Error Correction) – коди (LDPC, Turbo, Polar) дозволяють виправляти значну кількість помилок на бітовому рівні, тим самим знижуючи BER/PER за певного рівня шумів та завад [2, 6]. Однак при цілеспрямованих перешкодах із використанням вузькосмугових або адаптивних методів у противника може бути можливість “атакувати” саме ті частоти або часові інтервали, де передається найбільш критична інформація. Оцінка ефективності FEC здійснюється за допомогою:

- Кривих BER залежно від  $E_b/N_0$  з увімкненим та вимкненим кодуванням;
- Порівняння кодового коефіцієнта (code rate) з фактичним зменшенням помилок;
- Врахування надмірності, оскільки надто високий рівень кодування зменшує корисну швидкість передачі [3, 8].

5. Запас завадостійкості (Fade Margin, Link Margin). У телекомунікаційних системах часто розглядають запас завадостійкості, або запас потужності, коли проектують радіоканал, щоби врахувати погіршення умов поширення чи наявність перешкод. Суттєвий запас (на 10–20 дБ) дозволяє витримувати значні коливання рівня сигналу чи появу штучних завад. Цей критерій тісно пов'язаний із чутливістю приймача та максимальною потужністю передавача [1, 4].

6. Чутливість приймача визначає мінімальний рівень сигналу, при якому повідомлення декодується зі встановленим BER (наприклад,  $10^{-3}$  або  $10^{-6}$ ). У разі впливу завад чутливість суттєво деградує, оскільки на вхід приймача надходить додаткова паразитна потужність [9]. Для сучасних спеціальних приймачів застосовують вузькосмугові фільтри, складні схеми автопідстроювання частоти й посилення, що дає змогу “відсікати” частину завад та покращувати ефективну чутливість.

7. Error Vector Magnitude (EVM) – критерій, широко вживаний у цифрових системах (QAM, PSK, OFDM), який відображає відхилення прийнятого символу від ідеальної точки на IQ-діаграмі [9]. У мирному середовищі EVM часто пов'язують із неточностями тракту передачі, частотними нестабільностями та побічними завадами. В умовах РЕП потужні завади, особливо якщо вони налаштовані на “спотворення” фази й амплітуди сигналу, можуть істотно збільшити EVM, що призведе до підвищення ймовірності помилки в декодуванні.

8. Ймовірність правильного виявлення сигналу. У середовищі зовнішніх перешкод важливим стає не лише коректне декодування повідомлення, а й сам факт виявлення наявності корисного сигналу в ефірі (наприклад, у радіолокації чи сенсорних мережах). Якщо завади є “маскуючими” або “шумоподібними”, приймач може взагалі не розпізнати корисний сигнал [8].

Серед поширених методів виявлення – некогерентні та когерентні детектори, а також CFAR (Constant False Alarm Rate) у радіолокації [9]. Усі вони можуть виявитися малоефективними, якщо перешкода адаптується до структурних особливостей сигналу.

### **Особливості застосування критеріїв у системах РЕП.**

В той же час, визначені критерії завадозахищеності необхідно застосовувати у системах РЕП з метою максимізації їх ефективності, дотримуючись наступних рекомендацій.

Застосування адаптивних методів протидії у системах РЕП. У станціях постановки перешкод може бути реалізований алгоритм оцінювання коефіцієнта шумоподібності сигналу, за результатами якого обирається метод перешкод (вузькосмуговий чи широкосмуговий). Для оцінювання завадозахищеності важливо застосовувати багатокритеріальний підхід, який одночасно враховує EVM, BER, пропускну здатність і запас завадостійкості.

Системи MIMO та просторової фільтрації намагаються використати багатопроменеве поширення для збільшення пропускну здатності та покращення стійкості. Умови РЕП можуть “погасити” окремі канали або вносити корельовані перешкоди. Тому для аналізу завадозахищеності варто враховувати показники, пов'язані з просторово-часовою обробкою сигналу [5, 6].

В той же час, сучасні системи РЕП можуть швидко перебудовуватись (Frequency Hopping, Adaptive Jamming) забезпечуючи динамічну зміну середовища. SNR чи BER бажано відстежувати в режимі реального часу, а пропускну здатність (Throughput) – вимірювати з певною часовою вибіркою.

У спеціальних системах часто важлива здатність системи зберігати неперервність зв'язку навіть із тимчасовим зниженням швидкості. Тому, крім класичних технічних критеріїв (SNR, BER), звертають увагу на оперативні вимоги, наприклад, гарантований час доставки критично важливого повідомлення [6].

Також, розробники спеціальних радіосистем спираються на стандарти та рекомендації ITU-R, 3GPP (для комерційних систем, які використовуються або модифікуються у спеціальних цілях) та внутрішні нормативи. Ряд параметрів (наприклад, мінімально припустимий BER за заданого рівня перешкод, запас посилення, чутливість) встановлюється відповідно до оперативних вимог і можливостей апаратури [7, 8].

### **Висновки**

Критерії завадозахищеності радіоканалів (SNR, BER, PER, пропускну здатність, EVM, запас завадостійкості тощо) дають багатогранне розуміння того, наскільки надійним є зв'язок в умовах РЕП. Зовнішній вплив у вигляді цілеспрямованих завад (адитивного шуму, імпульсних та вузькосмугових перешкод, підміни сигналів) істотно ускладнює роботу радіоканалів, що проявляється у зростанні BER і зменшенні пропускну здатності. Сучасні методи FEC, адаптивна модуляція, MIMO та динамічне управління спектром підвищують завадозахищеність, але потребують додаткової обчислювальної потужності та енергетичного ресурсу, що є важливим фактором у військових застосуваннях. Для комплексної оцінки у середовищі штучних завад доцільно використовувати набір показників одночасно (BER/PER, SNR, EVM, ймовірність виявлення) та проводити тестування в реальних сценаріях або наближених до них імітаційних середовищах. Подальший розвиток радіоелектронної протидії створює нові виклики для систем зв'язку: з'являються більш складні методи постановки перешкод, розширюються можливості застосування штучного інтелекту та машинного навчання. Отже, дослідження критеріїв завадозахищеності та розробка методів підвищення стійкості радіоканалів у наступних поколіннях бездротових систем має залишатись одним із пріоритетних напрямів.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Основи теорії електрозв'язку / За ред. В. М. Кузьміна – К.: КНУТД, 2014. – 347 с.
2. Proakis J. Digital Communications, 5th ed. / Proakis J. – McGraw-Hill, 2007. – 1150 p.
3. Bernard Sklar. Digital Communications: Fundamentals and Applications, 3rd edition / Bernard Sklar, Fredric J. Harris. – Publisher Pearson, 2021. – 1089 p.
4. Haykin S. Communication Systems. 4th ed / Haykin S. – Wiley, 2009. – 830 p.
5. Rappaport T. Wireless Communications: Principles and Practice, 2nd ed. / Rappaport T. – Prentice Hall, 2002. – 707 p.
6. Tse D. Fundamentals of Wireless Communication / Tse D., Viswanath P. – Cambridge University Press, 2005. – 660 p.
7. ITU-R. Official site [Електронний ресурс]. – Access the page: <https://www.itu.int/en/ITU-R/>
8. 3GPP. Official site [Електронний ресурс]. – Access the page: <https://www.3gpp.org/>
9. Skolnik M. I. (ed.) Radar Handbook, 3rd ed./ Skolnik M. I. – McGraw-Hill, 2008/ – 1312 p.

**Костишин Андрій Володимирович** – аспірант кафедри інфокомунікаційних систем і технологій, Вінницький національний технічний університет, м. Вінниця, e-mail:071kav@gmail.com

Науковий керівник: Крижановський Володимир Григорович – д.т.н., професор кафедри інфокомунікаційних систем і технологій, Вінницький національний технічний університет, м. Вінниця, e-mail: vkryzhanovskyi@vntu.edu.ua

**Andrii Kostishyn** – PhD-student of department of Information communication systems and technologies, Vinnytsia National Technical University, Vinnytsia, e-mail:071kav@gmail.com.

Scientific supervisor: Volodymyr Hryhorovych Kryzhanovskyi – Doctor of Technical Sc., Pr. of the Department of Infocommunication Systems and Technologies, Vinnytsia National Technical University, Vinnytsia, e-mail: vkryzhanovskyi@vntu.edu.ua