

Перспективи зменшення впливу направлених кібератак методами підвищення завадостійкості сигналів з багатопозиційною фазовою маніпуляцією

Розглянуто питання вирішення завдання по зменшенню впливу направлених кібератак методами підвищення завадостійкості сигналів з багатопозиційною фазовою маніпуляцією. Проаналізовано перспективні напрямки та запропоновано систему наукових завдання, вирішення яких забезпечить зниження ймовірності правильного прийому та обробки вхідного сигналу

Останнім часом у світі спостерігається тенденція бурхливого розвитку цифрових методів передачі даних. Переваги таких методів – це добрі показники якості зв'язку, висока пропускна спроможність каналів передачі та відносна простота побудови схем передавачів та приймачів на уніфікованій елементній базі. Серед безлічі використовуваних сигналів необхідно відзначити сигнали з багатопозиційною фазовою маніпуляцією (М-ФМ), які добре задовольняють сучасними енергетичним і спектральним вимогами і в порівнянні з іншими видами дискретних сигналів передачі інформації, наприклад з амплітудною і частотною маніпуляцією, забезпечують високу пропускну здатність каналів і перешкод приймально-передавальної апаратури в складній завадній обстановці.

Ці сигнали успішно використовуються у світі в багатьох цифрових системах передачі інформації, таких як супутникові лінії зв'язку, системи цифрового телебачення (DVB-S і DVB-S2/S2X), бездротові та стільникові мережі [1].

Відомо, що негативним фактором прийому сигналу в телекомунікаційній мережі є наявність гаусівського шуму. Природа та вплив якого цілком передбачувана та добре вивчена [2?3].

Необхідно відзначити, що у сучасних радіоканалах поруч із шумовими гаусівськими часто є і нефлюктуаційні перешкоди різної природи, викликані як природними причинами, і похибками апаратури, порушенням регламентів зв'язку іноді навмисними діями абонентів. Поява таких перешкод призводить до зниження якості зв'язку. До переліку таких впливів цілком слушно занести і створення навмисних завад та перешкод нефлюктуаційного характеру, що можуть бути кваліфіковані як цілеспрямовані кібератаки. Мета таких атак, це навмисне переривання або ускладнення процесу передачі корисних даних та зниження ефективності застосування телекомунікаційної мережі в цілому.

В таких умовах виникає цілком актуальне наукове завдання щодо оцінки можливостей сигналів з багатопозиційною фазовою маніпуляцією до підвищення завадостійкості в умовах впливу кібератак в вигляді навмисно створених нефлюктуаційних перешкод.

В сучасних телекомунікаційних мережах передачі корисних даних використовуються різні за конструкцією ансамблі дискретних сигналів, побудовані на основі багатопозиційної фазової маніпуляції:

Зазвичай це ансамбль, який містить M сигналів:

$$S_1(t), S_3(t), \dots, S_M(t).$$

Відповідно до теорії потенційної завадостійкості мінімум ймовірності помилки відображення сигналу на виході приймача (P_0) для рівно ймовірних сигналів багатопозиційних сигналів забезпечується оптимальним приймачем, алгоритм роботи якого має вигляд [1,2]:

$$\int_0^T [X(t) - S_i(t)]^2 dt \langle \int_0^T [X(t) - S_j(t)]^2 dt, i, j = 1, \dots, M; i \neq j$$

Вплив навмисної кібератаки в вигляді перешкоди буде приводити до росту ймовірності помилки, тобто до порушення вищеподаної залежності оптимального прийому сигналу.

В загальному випадку алгоритм обробки багатопозиційного сигналу по M каналам приймача має вигляд так:

$$Y_i \rangle Y_j, i = 1, \dots, M, j = 1, \dots, M; i \neq j.$$

Де наведені показники Y_i, Y_j – отримані при обробці сигналів та завд в каналах приймача. Рішення щодо сигналу, який надсилаємо до подальшої обробки виноситься по виходу каналу, в якому Y_i має найбільшу величину.

Якщо надісланий сигнал S_i , то ймовірністю правильного прийому (P_{np}) є ймовірність одночасного виконання $M-1$ нерівностей, або [2]:

$$P_{np}(S_i) = P\{Y_i \rangle Y_1, \dots, Y_i \rangle Y_{i-1}, Y_i \rangle Y_{i+1}, \dots, Y_i \rangle Y_M\}$$

При цілеспрямованому впливі направленою завадою в ході кібератаки зростає співвідношення сигнал/шум. При цьому розрахунок ймовірності помилки в багатопозиційній системі оцінимо сумарною ймовірністю помилки, що створюється сигналом S_i та кожному з $(M-1)$ інших сигналів [2,3]:

$$P_0(S_i) = \sum_{\substack{j=1 \\ j \neq i}}^N P_{0ij}$$

Для безпосереднього вирішення завдання щодо забезпечення мінімізації значення ймовірності помилки відображення сигналу на виході приймача (P_0) необхідно здійснити порівняльну оцінку впливу кібератаки в вигляді нефлуктуаційних перешкод різних видів, що проникли у канал радіозв'язку, та внутрішніх похибок синхронізації на загальну завадостійкість демодуляторів

тракту прийому дискретних сигналів з багатопозиційною фазовою маніпуляцією. Це забезпечить наступне визначення допустимих рівнів створених кібератакою перешкод та похибок при збереженні заданої якості зв'язку.

Поставлену мету можна вирішити при досягненні результатів вирішення наступних завдань:

1. Визначити основні видів перешкод, притаманних каналам радіозв'язку на основі багатопозиційних сигналів.

2. Провести аналіз завадостійкості когерентних демодуляторів дискретних сигналів з багатопозиційною фазовою маніпуляцією за наявності нефлюктуаційних перешкод різних видів.

3. Здійснити аналіз завадостійкості авто кореляційного демодулятора прийому дискретних сигналів з багатопозиційною фазовою маніпуляцією за наявності нефлюктуаційних перешкод різних видів.

4. Оцінити похибки системи синхронізації на завадостійкість прийому сигналів із багатопозиційною фазовою маніпуляцією та їх вплив на загальну завадостійкість системи.

Список літератури

1. Телекомунікаційні системи та мережі. Структура й основні функції. Том 1. / Поповський В.В., Лемешко О.В., Ковальчук В.К., Плотніков М.Д., Картушин Ю.П. та інші. [Електронний ресурс]. – Х.: ХНУРЕ. 2018. Режим доступу – <http://www.znanius.com/3534.html>.

2. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.

3. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков. – К. : Видавнича група ВНУ, 2009. – 608 с.