УДК 621.391

І.С. ПЯТІН, В.І. ЛУЖАНСЬКИЙ, Л.В. КАРПОВА
Хмельницький національний університет

КОНФІДЕНЦІЙНА СИСТЕМА ЗВ'ЯЗКУ

В роботі вивчались принципи побудови систем конфіденційного зв'язку, засновані на використанні широкосмугових сигналів. Важливою перевагою таких систем є передача в ефір безперервних у часі шумоподібних сигналів з дуже низькою спектральною густиною. Хаотичні коливання використовують для передачі інформації завдяки наступним властивостям: широкосмуговість; складність; ортогональність. Розглядається алгоритм створення генератора хаоса на основі цифрового оброблення сигналів. Основним змістом чисельного розв'язку систем диференційних рівнянь є дискретизація інтервалів і функцій, для чого розроблений алгоритм у середовищі Matlab, наведені графіки спектральних і кореляційних властивостей хаотичних коливань. Розглянуті структури передавача і приймача системи широкосмугового конфіденційного зв'язку.

Ключові слова: конфіденційний зв'язок, детермінований хаос, сигнали з розширеним спектром.

I.S. PYATIN, V.I. LUGHANSKIY, L.V. KARPOVA
Khmelnytsky National University

CONFIDENTIAL COMMUNICATIONS SYSTEM

The paper studied the principles of confidential communication systems based on the use of broadband signals. An important advantage of such systems is broadcasting continuous time noise signals with very low spectral density. The rapid increase of information transmitted in communication networks, raises the issue of confidentiality of transmission. The development of information technology tools improves unauthorized access. Promising methods of information security are being implemented at the level of physical channels of transmission. This is especially important for wireless security standards Radio Ethernet, GPRS, CDMA, etc. Chaotic vibrations are used to transmit information through the following properties: wideband; complexity; orthogonality. We consider the algorithm for creating chaos generator based on digital signal processing. The main content of the numerical solution of differential equations is the sampling interval and functions for which the algorithm among Matlab, shows graphs of spectral and correlation properties of chaotic oscillations. The structure of the transmitter and receiver system broadband confidential communication.

Keywords: confidential communication, deterministic chaos spread spectrum signals.

Вступ

Сучасний розвиток телекомунікаційних засобів нового покоління заснований на використанні широкосмугових сигналів з великою інформаційною ємністю. За рахунок розширення спектра частот несучих сигналів досягається збільшення швидкості передачі інформації, підвищується стійкість і надійність систем зв'язку при наявності завад.

Широкосмугові сигнали використовуються для передачі інформації в багатоканальних і багатоадресних CDMA системах з кодовим поділом (Code Division Multiple Access Systems), а також в бездротових системах зв'язку з розширенням спектра (Wireless Spread Spectrum Systems). До сучасних бездротових засобів зв'язку з CDMA висуваються високі вимоги щодо захисту переданої інформації від несанкціонованого доступу.

Застосування широкосмугових сигналів забезпечує високу пропускну здатність каналів, дозволяє послабити вплив багатьох видів завад і приймати повідомлення при співвідношенні сигнал / шум багато менше одиниці, а також боротися з впливом багатопроменевого поширення радіохвиль. Важливою перевагою широкосмугових систем є висока скритність бездротового зв'язку і електромагнітна сумісність с іншими радіоелектронними засобами за рахунок передачі в ефір безперервних у часі шумоподібних сигналів з дуже низькою спектральною густиною [1].

Останнім часом у зв'язку з розвитком супутникових, мобільних, стільникових, волоконно-оптичних багато користувацьких багатоканальних систем і завантаженістю радіодіапазону, а також у поєднанні з необхідністю забезпечення завадостійкого зв'язку, велику увагу привертає клас широкосмугових хаотичних сигналів. При використанні технології розширення спектру смуга частот переданого сигналу може бути зроблена значно ширше смуги частот інформаційного повідомлення.

У техніці зв'язку такі сигнали можуть формуватися у вигляді псевдовипадкових імпульсних послідовностей, які мають задані спектральні та кореляційні характеристики.

В даний час в системах зв'язку з розширенням спектра використовуються псевдовипадкові послідовності максимального періоду. М-послідовності генеруються простими алгоритмами.

У широкосмугових системах зв'язку всі користувачі працюють в одному частотному діапазоні, більш широкому, ніж у випадку традиційних вузькосмугових систем зв'язку з частотно-часовим поділом. У кожному абонентському каналі використовується свій ідентифікаційний код для розділення користувачів. На вхід приймального пристрою індивідуального користувача одночасно з корисним сигналом в заданій смузі частот надходять не тільки звичайні атмосферні завади, а сигнали від інших абонентів та відбиття за рахунок багатопроменевого поширення. Складна електромагнітна обстановка в зоні дії телекомунікаційних засобів накладає додаткові вимоги на систему псевдовипадкових сигналів, яка використовується для кодування і передачі інформації по каналах зв'язку.

З теорії інформації відомо, що найбільшу інформаційну ємність мають стохастичні сигнали, породжувані випадковими процесами. Основна проблема при розробці інформаційних носіїв у цифрових телекомунікаційних каналах полягає в труднощах генерування випадкових двійкових послідовностей із

застосуванням короткого задаючого ключа. Математичні алгоритми, які з ключа отримують псевдовипадкові послідовності, повинні мати наступні властивості:

- як завгодно велика довжина періоду псевдовипадкової послідовності;
- статистична подібність отриманої послідовності чисел властивостям звичайної випадкової вибірки;
- можливість програмно-апаратної реалізації генератора випадкових чисел для використання у каналі зв'язку з відповідною швидкодією.

Особливості конфіденційних систем зв'язку

Стрімке збільшення обсягів інформації, що передається у мережах зв'язку, ставить питання забезпечення конфіденційності її передачі. Розвиток інформаційних технологій вдосконалює засоби несанкціонованого доступу (НСД). Перспективними стають методи захисту інформації, що впроваджуються на рівні фізичних каналів її передачі. Особливо це важливо для безпеки бездротових мереж стандартів Radio Ethernet, GPRS, CDMA, тощо. Одним з шляхів вирішення цієї проблеми є використання у конфіденційних системах зв'язку (КСЗ) радіоелектронного маскування (РЕМ), що являє собою комплекс технічних і організаційних заходів, спрямованих на зниження ефективності засобів радіотехнічної розвідки. РЕМ може бути здійснено за рахунок методів передачі, що забезпечують енергетичну, структурну, інформаційну та інші види скритності сигнальних конструкцій.

З врахуванням виконуваних завдань радіотехнічні системи можна поділити на три основні класи [1]:

1) радіотехнічні системи передачі та управління – відносяться до класу КСЗ, призначених для передачі даних і сигналів управління;

2) системи руйнування інформації – відносяться до систем радіоелектронної протидії (РЕП), метою яких є створення навмисних завад, імітація помилкових інформаційних сигналів і перехоплення управління;

3) системи вилучення інформації – відносяться до класу систем НСД і вирішують завдання по несанкціонованому перехопленню переданих повідомлень, визначенню структури і параметрів сигналів, тощо.

Для оцінки ступеня захищеності КСЗ від систем РЕП противника і НСД доцільно використовувати поняття завадозахищеності.

Завадозахищеність – це властивість системи не тільки найбільш точно відтворювати передану інформацію на приймальній стороні, але і здатність забезпечувати її безпеку і цілісність від засобів РЕП і НСД за допомогою реалізації ефективних методів скритності передачі.

Розрізняють енергетичну, структурну, інформаційну та інші показники скритності.

Для підвищення енергетичної скритності передачі сигналу потрібно знижувати потужність основного випромінювання КСЗ, що можливо при використанні широкосмугових сигналів з базою $B = \Delta f \cdot T >> 1$. Розширення бази сигналу дозволяє створювати сигнальні конструкції з дуже малою спектральною густиною потужності, що ускладнює їх виявлення при некогерентній обробці. Крім цього, використовуючи несучі сигнали з невідомою структурою можна збільшити апріорну невизначеність прийому при несанкціонованому доступі.

Застосування сигналів з великою базою дозволяє забезпечити високу енергетичну скритність сигнальних конструкцій. Таким чином, система зв'язку з складними широкосмуговими сигналами здатна працювати при співвідношенні $P_c << P_ш$ [1, 2].

Це забезпечує скритність роботи передавача конфіденційної системи і можливість кодового поділу каналів [1, 2].

Використання хаотичних коливань для передачі інформації перспективно завдяки наступним властивостям:

- широкосмуговість: хаотичні сигнали неперіодичні і мають безперервний спектр. Для багатьох хаотичних сигналів цей спектр займає широку смугу частот. Вони використовуються для боротьби з загасанням сигналу в деякій смузі частот;
- складність: хаотичні сигнали мають складну структуру. Один хаотичний генератор може створювати різні коливання при незначних змінах початкових умов. Це ускладнює визначення внутрішньої будови генератора і передбачення сигналу на будь-який тривалий час, що використовується в криптографії;
- ортогональність: автокореляційна функція хаотичного сигналу стрімко загасає. Тому сигнали від декількох генераторів можна вважати некорельованими, тобто ортогональними, що використовується у багато користувацьких системах зв'язку.

Передача інформації з малою імовірністю помилки може бути виконана в тому випадку, якщо швидкість генерування інформації хаотичною системою, тобто топологічна ентропія системи не менша швидкості надходження інформації від її джерела, не враховуючи обмеження в каналі зв'язку (наприклад, спотворення сигналу через наявність шуму в каналі).

Модель цифрового генератора хаосу на основі системи Лоренця

Розглянемо деякі схеми використання хаосу для передачі повідомлень. Створимо генератор хаосу на основі цифрового оброблення сигналів

При використанні цифрових сигнальних процесорів (ЦСП), або програмованих логічних інтегральних схем (ПЛІС) можна забезпечити високу ідентичність параметрів хаотичних модулів передавача і приймача.

Термін «цифрова обробка сигналів» (ЦОС) охоплює досить широку область. Цифрові сигнальні

процесори містять вузли, що виконують множення з накопиченням. Ця операція характерна для дискретного перетворення Фур'є. Операції множення з накопиченням можуть виконуватися одночасно кількома виконавчими пристроями (використовується паралельний розрахунок), що підвищує швидкодію алгоритмів ЦОС. Програмовані логічні інтегральні схеми (ПЛІС) мають більшу швидкодію в порівнянні з цифровими сигнальними процесорами (ЦСП). Для ЦСП продуктивність може падати через необхідність обробки переривань. Для ПЛІС тактова частота є постійною величиною. ПЛІС серії Virtex-6 фірми Xilinx мають тактову частоту 600 МГц, що дозволить обробляти сигнали частотою до 300 МГц.

Основу хаотичних модулів складають кільцеві генератори. Оскільки генератори описуються системою диференційних рівнянь, то за допомогою сигнального процесора необхідно реалізувати чисельне інтегрування цієї системи. В якості методу інтегрування можна використовувати метод Рунге-Кутта четвертого порядку.

Реалізацію хаотичного модуля приймача відрізняє поява в системі диференційних рівнянь зовнішнього сигналу. Тому для використання методу Рунне Кутта необхідно мати проміжні відліки вхідного сигналу для забезпечення відповідної точності методу. Частота дискретизації вхідного сигналу має у два рази перевищувати основну тактову частоту. Оскільки кодек має обмеження по частоті, то кожний другий відлік можна визначати інтерполяційними методами.

Розглянемо чисельні методи розв’язку системи диференційних рівнянь. Нехай задана система диференційних рівнянь:

$$\begin{cases} \dfrac{dx}{dt} = f(x, y, z) \\ \dfrac{dy}{dt} = g(x, y, z) \\ \dfrac{dz}{dt} = d(x, y, z) \end{cases}$$

Початкові умови: $x(0) = x_0$; $y(0) = y_0$; $z(0) = z_0$.

Основним змістом чисельного розв’язку таких систем є дискретизація інтервалів і функцій, що розглядаються. Для дискретизації відрізку часу $[t_0, t_0 + T]$ розіб’ємо його на N частин вузлами $t_0 < t_1 < \ldots < t_N = t_0 + T$ з кроком $h = T / N$, тобто $t_{m+1} = t_m + h$.

Для дискретизації функцій введемо позначення: x_m, y_m, z_m - наближене значення для невідомого точного значення $x(t_m)$, $y(t_m)$, $z(t_m)$ в момент t_m. Для визначення x_m, y_m, z_m будемо використовувати метод Рунге-Кутта.

Передавач може бути побудований як система Лоренця:

$$\begin{cases} \dfrac{dx}{dt} = -\sigma x + \sigma y \\ \dfrac{dy}{dt} = -xz + rx - y \\ \dfrac{dz}{dt} = xy - bz \end{cases} \quad (1)$$

Значення параметрів $\sigma = 10$; $r = 28$; $b = 8/3$, t - час.

Розрахунок наближених значень виконується за виразами:

$x_{m+1} = x_m + \left(K_1 + 2K_2 + 2K_3 + K_4\right)/6$

$y_{m+1} = y_m + \left(L_1 + 2L_2 + 2L_3 + L_4\right)/6$;

$z_{m+1} = z_m + \left(P_1 + 2P_2 + 2P_3 + P_4\right)/6$

$K_1 = hf(x_m, y_m, z_m)$; $L_1 = hg(x_m, y_m, z_m)$;

$P_1 = hd(x_m, y_m, z_m)$;

$K_2 = hf(x_m + 0,5K_1, y_m + 0,5L_1, z_m + 0,5P_1)$;

$L_2 = hg(x_m + 0,5K_1, y_m + 0,5L_1, z_m + 0,5P_1)$;

$P_2 = hd(x_m + 0,5K_1, y_m + 0,5L_1, z_m + 0,5P_1)$;

$K_3 = hf(x_m + 0,5K_2, y_m + 0,5L_2, z_m + 0,5P_2)$;

$L_3 = hg(x_m + 0,5K_2, y_m + 0,5L_2, z_m + 0,5P_2)$;

$P_3 = hd(x_m + 0,5K_2, y_m + 0,5L_2, z_m + 0,5P_2)$;

$K_4 = hf(x_m + K_3, y_m + L_3, z_m + P_3)$;

$L_4 = hg(x_m + K_3, y_m + L_3, z_m + P_3)$;

$P_4 = hd(x_m + K_3, y_m + L_3, z_m + P_3)$.

З наведених формул можна зробити висновок, що кожний наступний відлік сигналу розраховується з попереднього значення. Чим менший крок h, тим точніше ми можемо розрахувати хаотичний сигнал на

заданому відрізку, але буде використаний більший час. Тому для зменшення часу розрахунку необхідно вибирати крок h з врахуванням найменшої кількості точок, що відображають всі особливості поведінки системи Лоренця на осі часу. Наближення, що визначаються за методом Рунге-Кутта, мають похибки $\|x(t_m) - x(t)\| = O(h^4)$.

Моделювання розв'язку системи Лоренця у середовищі Matlab

В радіотехнічних системах з безперервним часом джерелом хаотичних коливань служать різні нелінійні коливальні системи з порядком не нижче третього: генератор на тунельному діоді з коливальним контуром і додатковою інерційністю, нелінійний неавтономний коливальний контур, кільцеві системи ФАП і ЧАП з відповідними фільтрами в колі зворотного зв'язку тощо.

Проаналізуємо у середовищі Matlab чисельний розв'язок системи Лоренця (1) методом Рунге-Кутта за формулами, наведеними вище. Розрахуємо також спектр такого сигналу, його автокореляційну (АКФ) і взаємокореляційну (ВКФ) функції за наступною програмою [3].

```
X0=0; y0=1; z0=1.05; h=0.07; sigma=10; r=28; b=8/3;
t0=0; t0T=100; t=t0:h:t0T;
S=length(t0:h:t0T); x=zeros(1, S);
y=zeros(1, S); z=zeros(1, S);
x(1)=x0; y(1)=y0; z(1)=z0;
for m=2:1:S
K1=h*sigma*(y(m-1)-x(m-1));
L1=h*(x(m-1)*(r-z(m-1))-y(m-1));
P1=h*(x(m-1)*y(m-1)-b*z(m-1));
K2=h*sigma*(y(m-1)+L1/2-(x(m-1)+K1/2));
  L2=h*((x(m-1)+K1/2)*(r-z(m-1)-P1/2)-(y(m-
1)+L1/2));
P2=h*((x(m-1)+K1/2)*(y(m-1)+L1/2)-b*(z(m-1)+P1/2));
K3=h*sigma*(y(m-1)+L2/2-(x(m-1)+K2/2));
  L3=h*((x(m-1)+K2/2)*(r-z(m-1)-P2/2)-(y(m-
1)+L2/2));
P3=h*((x(m-1)+K2/2)*(y(m-1)+L2/2)-b*(z(m-1)+P2/2));
K4=h*sigma*(y(m-1)+L3-(x(m-1)+K3));
L4=h*((x(m-1)+K3)*(r-z(m-1)-P3)-(y(m-1)+L3));
P4=h*((x(m-1)+K3)*(y(m-1)+L3)-b*(z(m-1)+P3));
x(m)=x(m-1)+(1/6)*(K1+2*K2+2*K3+K4);
y(m)=y(m-1)+(1/6)*(L1+2*L2+2*L3+L4);
z(m)=z(m-1)+(1/6)*(P1+2*P2+2*P3+P4); end
plot(t, x)
title('Часова діаграма сигналу детермінованого хаоса ')
SP=fft(x, 8192); SP1=fftshift(SP);
aSP=abs(SP1); figure; plot(aSP)
title('Спектр сигналу детермінованого хаоса ')
            ylim([0 1800])
            la=length(x);
            for i=1:la
             s1(i)=x(la-i+1);
               end;
           Ka=conv(s1,x); Na=length(Ka);
            figure; plot(-la+1:1:la-1, (1/Na)*Ka);
             title('АКФ сигналу детермінованого хаоса ')
```

Лістинг 1 – Код Matlab для дослідження розв'язку системи Лоренця в області часу

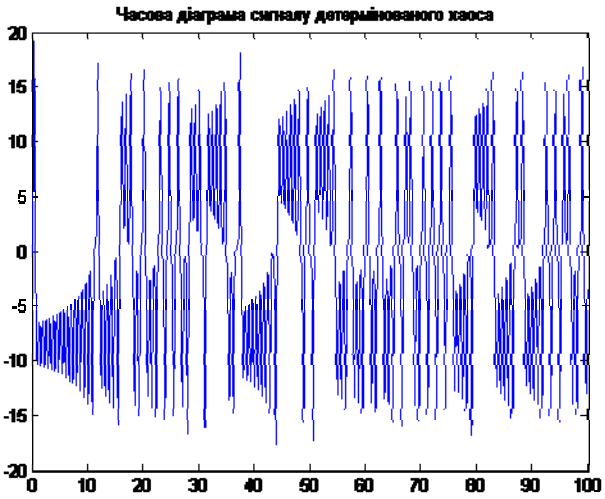

Рис. 1. Часова діаграма сигналу детермінованого хаосу

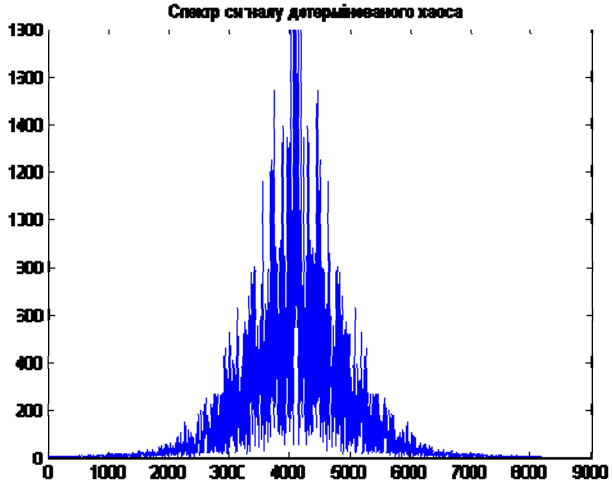

Рис. 2. Спектр сигналу детермінованого хаосу

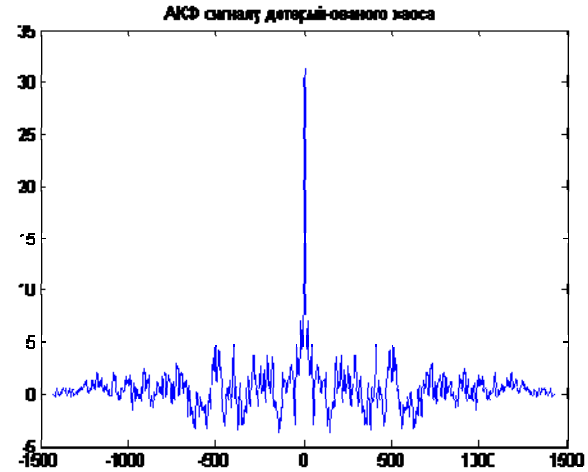

Рис. 3. АКФ сигналу детермінованого хаосу

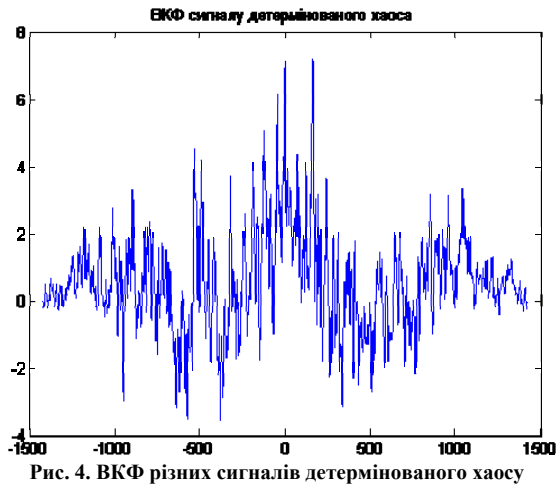

Рис. 4. ВКФ різних сигналів детермінованого хаосу

Результати виконання програми наведені на рис. 1 – рис. 3.

На рис. 4 приведена взаємна кореляційна функція (ВКФ) двох хаотичних сигналів, початкові умови яких по координаті x відрізняються на $1 \cdot 10^{-6}$. Відсутність чіткого максимуму кореляційної функції робить неможливим приймання таких сигналів.

Спектр, наведений на рис. 2 займає достатньо широку область частот, тобто хаотичний сигнал, що розглядається, широкосмуговий. АКФ, наведена на рис. 3, має яскраво виражений максимум, що дозволяє виявляти сигнали з однаковою хаотичною поведінкою. Результати, приведені на рис. 4 свідчать про велику залежність форми хаотичних коливань від початкових умов. І навіть, якщо противник знає алгоритм розв'язку диференційних рівнянь системи Лоренця, то початкові умови підібрати практично неможливо, що підвищує конфіденційність зв'язку.

Структурна схема системи цифрового конфіденційного зв'язку

За результатами дослідження, наведеними на рис. 1 – рис. 4 можна зробити висновок, що хаотичні коливання з певним набором початкових умов можуть використовуватись в якості ключа, за яким один абонент може з'єднуватись з іншим. Сигнали інших абонентів є шумовими коливаннями, оскільки ВКФ двох хаотичних коливань з різними початковими умовами, має вигляд шуму. Структурна схема передавача конфіденційної системи цифрового зв'язку приведена на рис. 5.

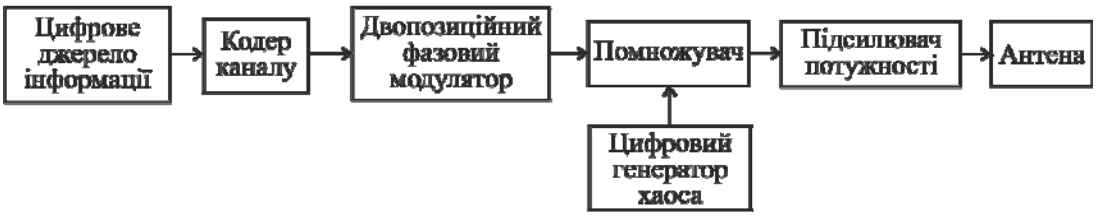

Рис. 5. Структурна схема передавача конфіденційної системи цифрового зв'язку

Цифрове джерело сигналу генерує цифровий сигнал – послідовність біт (символів) інформації. Цифровим джерелом може бути, наприклад, персональний комп'ютер, цифровий носій аудіо- або відеоінформації.

Кодер каналу використовується практично в усіх сучасних системах цифрового зв'язку. Його основне призначення – підвищення вірогідності переданої інформації. Збільшення достовірності передачі інформації відбувається шляхом додавання надмірності до переданої інформації. Це призводить до зниження швидкості передачі. Процес додавання надмірності до початкової інформації називається завадостійким кодуванням.

Вузькосмуговий модульований сигнал з довільним видом модуляції можна представити у вигляді:

$$s(t) = I(t)x(t) - Q(t)x(t), \quad (2)$$

де $x(t)$ – хаотична несуча радіосигналу, $I(t)$ і $Q(t)$ називаються відповідно синфазною і квадратурною складовими модулюючого сигналу.

Таким чином, для здійснення довільного виду модуляції сигналу необхідно виконати дві операції: а) сформувати синфазну і квадратурну складові модулюючого сигналу (вид даних складових буде визначати вид модуляції); б) виконати перетворення (2).

Операції (1) і (2) виконуються різними вузлами передавального тракту. Операція (а) здійснюється в низькочастотному модуляторі, а операція (б) в модуляторі. Обидва вузла представлені на рис. 5 блоком Двопозиційний фазовий модулятор.

У системах з двопозиційною фазовою модуляцією модульоване коливання є синусоїдним з сталою амплітудою, але початкова фаза його може набувати двох значень, які відрізняються на 180^0 залежно від поточного символу бінарної послідовності, що передається.

Двопозиційна фазова модуляція може виконуватись за допомогою цифрового сигнального процесора. В цьому випадку модуляція може бути довільною. Здійснення того чи іншого виду модуляції визначається програмою, що виконується в низькочастотному цифровому сигнальному процесорі, а саме алгоритмом формування квадратурних складових з закодованого інформаційного сигналу.

Помножувач, на один вхід якого подається сигнал цифрового генератора хаосу, а на другий – сигнал з двопозиційною фазовою модуляцією, потрібний для для перенесення вхідної бінарної послідовності в область хаотичної несучої частоти, а також для розширення спектра сигналу. Таким чином, структурно передавальний тракт можна розділити на цифрову і аналогову частини, розділені цифро-аналоговим перетворювачем (ЦАП), що підключається на виході двопозиційного фазового модулятора.

Цифрова частина системи зв'язку зазвичай містить керуючий контролер або процесор, що забезпечує керування блоками аналогового і цифрового тракту і інтерфейс з користувачем.

Приймальний тракт цифрової системи зв'язку містить набір блоків, більшість з яких виконують функції, зворотні до виконуваних в передавачі (рис.6). Вхідний сигнал через підсилювач потужності надходить на помножувач, що звужує спектр сигналу і переносить його в область низьких частот. Далі сигнал надходять на АЦП і потім в процесор цифрової обробки сигналу (DSP). Процесор виконує низькочастотну фільтрацію, містить декодер каналу і декодер джерела. Далі, при необхідності, інформація перетворюється на аналогову форму за допомогою ЦАП (наприклад, для звукового відтворення) або

видається відразу в цифровий приймач інформації.

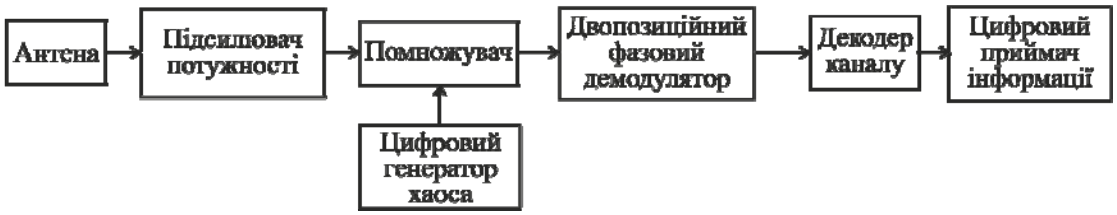

Рис. 6. Структурна схема приймача конфіденційної системи цифрового зв'язку

В приймальному тракті конфіденційної системи цифрового зв'язку обов'язкова наявність блоків синхронізації цифрових генераторів хаосу. При використанні цифрових генераторів хаосу достатньо точно задати початкові умови для розв'язку диференційних рівнянь системи Лоренця методом Рунге-Кутта. Однакові алгоритми на боці передавача і боці приймача будуть забезпечувати синхронні часові діаграми хаотичних коливань. Необхідна також синхронізація на етапі встановлення з'єднання і початку сеансу конфіденційного зв'язку. В цьому випадку кожний біт інформаційного повідомлення буде мати хаотичний код розширяючий спектр послідовності. Ці хаотичні коди розпізнати за допомогою засобів несанкціонованого доступу буде неможливо, що підвищить конфіденційність зв'язку.

Цифровий генератор хаосу можна реалізувати на ПЛІС типу FPGA (Field-programmable gate array), що містять блоки множення-підсумовування, які широко застосовуються при обробці сигналів (DSP), а також логічні елементи (як правило, на базі таблиць перекодування – таблиць істинності) та їх блоки комутації. Програма зберігається в розподіленої пам'яті, яка може бути виконана як на основі енергозалежних комірок статичного ОЗП (подібні мікросхеми виробляють, наприклад, фірми Xilinx і Altera), в цьому випадку програма не зберігається при зникненні електроживлення мікросхеми, так і на основі енергонезалежних комірок Flash-пам'яті або перемичок antifuse (такі мікросхеми виробляє фірма Actel і Lattice Semiconductor) – в цих випадках програма зберігається при зникненні електроживлення.

Висновки

Генератор хаосу формує шумоподібний сигнал. Для нього характерні неперіодичні траєкторій в часі, швидко спадаюча автокореляційна функція, суцільний безперервний спектр. Такі властивості роблять хаотичні сигнали перспективними з точки зору застосування в сучасних завадозахищених і конфіденційних системах зв'язку, де генератори хаосу грають роль формувачів несучих коливань. Специфіка хаотичного руху така, що найменші відхилення початкових умов генерації від номінальних значень призводять до істотної зміни форми коливання, що генерується. Отже, основною вимогою, що пред'являються до генераторів хаосу, є їх відтворюваність. Особливо важливою ця вимога стає при їх використанні в системах передачі інформації.

При побудові систем з розширенням спектру структура передаючої і приймальної апаратури залишається традиційною для даного класу систем зв'язку. Але генератор псевдовипадкової послідовності на передавальній стороні замінюється генератором хаотичного сигналу, аналогічний генератор поміщається також в приймач. Щоб ці генератори працювали синхронно, застосовується схема стеження за затримкою, а на початку сеансу зв'язку в канал передаються початкові умови для генерації. У разі втрати синхронізації відновити стеження можна тільки шляхом одночасного перезапуску генераторів хаосу у приймачі і передавачі. Перевагою такої CDMA-системи перед звичайною є практично необмежена ємність ансамблю послідовностей, що розширюють спектр. Недолік схеми – складність пошукової процедури при втраті синхронізації.

Література

1. Горохов С.М. Критерии эффективности скрытых методов передачи / С.М. Горохов, Н.В. Захарченко, В.В. Корчинский // Цифрові технології. – 2012. – № 12. – С. 147–150.

2. Дмитриев А.С. Динамический хаос: новые носители информации для систем связи / А.С. Дмитриев, А.И. Панас. – М. : Изд-во Физико-математической литературы, 2002. – 252 с.

3. Пятін І.С. Дослідження широкосмугових сигналів з двопозиційною фазовою маніпуляцією / І.С. Пятін, Р.В. Сорокатий, Ю.В. Лавренюк // Вісник Хмельницького національного університету. Технічні науки. –2014. – № 2. – С. 170–175.

References

1. Gorohov S.M. Kriterii effektivnosti skrytyh metodov peredechi. S.M. Gorohov, N.V. Zaharchenko, V.V. Korchinskiy. Tsifrovi tehnologii №12, 2012. s. 147-150.

2. Dmitriev A.S. Dinamicheskiy haos: novye nositeli informatsii dlia sistem sviazi. A.S. Dmitriev, A.I. Panas. M.: Izdatelstvo Fiziko-matematicheskoy literatury, 2002. 252s.

3. Pyatin I.S. Doslidgennia shirokosmugovih sygnaliv z dvopozitsiynoyu phazovoyu manipuliatsieyu/ I.S. Pyatin, R.V. Sorokatiy, Yu.V. Lavreniuk. Herald of Khmelnytsky National University. Technical sciences. № 2, 2014. s. 170-175.

Рецензія/Peer review : 11.1.2015 р. Надрукована/Printed :26.1.2015 р.
Рецензент: д.т.н., професор Ройзман В.П.