УДК 621.3.052.63

СИНТЕЗ ШИРОКОСМУГОВОЇ ТЕЛЕКОМУНКАЦЙНОЇ СИСТЕМИ З ПІДВИЩЕНОЮ КОНФІДЕНЦІЙНІСТЮ ПЕРЕДАЧІ ІНФОРМАЦІЇ ШЛЯХОМ ВИКОРИСТАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ХАОСУ

DOI 10.36994/2707-4110-2020-1-28-06

Семенко А.І., *д.т.н., проф. Відкритий міжнародний університет розвитку людини «Україна»,Київ,Україна. setel@ukr.net*
Кушнір М. Я., *к.ф.-м.н., доц., Чернівецький національний університет ім. Ю. Федьковича, Чернівці, Україна. kushnirnick@gmail.com.*
Бокла Н.І., *к.т.н. Національний університет «Львівська політехніка», Львів, Україна . nataloshka_77@ukr.net*
Шестопал Є.О., *Одеська національна академія зв'язку ім. ОС. Попова, Одеса, Україна. ie.shestopal@gmail.com*

Анотація. *В даний час особлива увага приділяється створенню широкосмугових телекомунікаційних систем з шумоподібним сигналом.Такі системи мають безперечні переваги в завадозахищеності, в конфіденційності передачі інформації, електромагнітній сумісності з сусідніми електронними пристроями. Формування широкосмугового сигналу в більшості випадків здійснюється методом прямого розширення спектру шляхом маніпуляції сигналу несучої частоти імпульсною псевдовипадковою послідовністю (ПВП) –т-послідовністю,послідовністю Голда, Касамі, Уолша. Такі послідовності як загальновідомі зловмисник може підібрати в приймачі і вони не можуть вважатись надійним захистом інформації.*

Використання явища динамічного хаосу забезпечує можливість пошуку нового класу ПВП, структуру яких практично неможливо відтворити, тому їх використання забезпечує підвищену конфіденційність передачі інформації. Генератори ПВП побудовані на основі одновимірних хаотичних відображень-логістичного, квадратичного та кубічного, що являють собою хаотичні системи.

При створенні ПВП на основі хаосу викристовуються три секретних ключі шифруваня: наприклад, для логістичного відобрвження це початкове значення, параметр рівняння і початок відліку послідовності.

Для підвищення криптозахищеності телекомунікаційних систем запропоновано створення ПВП на основі 2-х хаотичних сигналів (за логістичним та квадратичним відображеннями), що забезпечує збільшення секретних ключів від трьох до шести. В роботі запропонована схема побудови телекомунікаційної системи з високою конфіденційністю передачі інформації завдяки використанню таких ПВП.

Ключові слова: *хаос, шумоподібний сигнал, псевдовипадкова послідовність, конфіденційність інформації, секретний ключ.*

SYNTHESIS OF STRIP-BAND TELECOMMUNICATION SYSTEM WITH INCREASED CONFIDENTIALITY OF INFORMATION TRANSMISSION THROUGH USE OF PSSEVDOVIDOVYPOVY

Anatoly Semenko, *Dr.habil.,Prof., Open University of Human Development "Ukraine",*Kyiv, Ukraine, *setel@ukr.net*
***Nikolaj Kushnir**, P.h.D., Ass. Prof, Yury Fedkovtch Chernivtsi National University Chernivtsi, Ukraine.kushnirnick@gmail.com*
***Natalia Bokla**, Ph. D., National Universitof Lviv Polytechnic, Lviv, Ukraine, nataloshka_77@ukr.net*
***Yevhen Shestopal**, O. Popov Odesa National Academy of Telecommunications Odessa, Ukraine ie.shestopal@gmail.com*

Abstract. *Currently, special attention is paid to the creation of broadband telecommunications systems with a noise-like signal. Such systems have indisputable advantages in noise immunity, in the confidentiality of information transmission, electromagnetic compatibility with neighboring electronic devices. The formation of a broadband signal in most cases is carried out by the method of direct spreading of the spectrum by manipulating the carrier frequency signal by a pulse pseudo-random sequence (PVP) –m-sequence, Gold, Kasami, Walsh sequence. Sequences such as a well-known attacker can pick up in the receiver and they can not be considered reliable protection of information.*

The use of the phenomenon of dynamic chaos provides an opportunity to find a new class of PVP, the structure of which is almost impossible to reproduce, so their use provides increased confidentiality of information transmission. PVP generators are built on the basis of one-dimensional chaotic mappings - logistic, quadratic and cubic, which are chaotic systems.

When creating a PVP based on chaos, three secret encryption keys are used: for example, for logistic separation, this is the initial value, the equation parameter, and the start of the sequence.

To increase the cryptosecurity of telecommunication systems, it is proposed to create PVP based on 2 chaotic signals (by logistic and quadratic mappings), which provides an increase in secret keys from three to six. The paper proposes a scheme for building a telecommunications system with high confidentiality of information transmission through the use of such PVP.

Keywords: *chaos, noise signal, pseudo-random sequence, confidentiality of information, secret key.*

Вступ

В телекомунікаціях особливе місце належить системам з широкосмуговим шумоподібним сигналом, безперечною перевагою яких є підвищена завадостійкість як при вузькосмугових, так і широкосмугових завадах, конфіденційність передачі інформації , а також електромагнітна сумісність з сусідніми радіоелектронними пристроями [1,2].

Встановлено, що незалежно від конкретної смуги спектру завади $W_з$ відношення сигнал/завада (власними шумами нехтуємо) на виході

узгодженого фільтра поводиться так, якби потужність завад була рівномірно розподілена в смузі частот сигналу W_c, додаючи до власного шуму додатковий шум зі спектральною щільністю $P_з/W_c$.($P_з$-потужність завади) Причому, сумарний шум має властивості нормального Гауссова шуму [27].

Тоді на виході корелятора (узгодженого фільтра) відношення сигнал/завада буде [2]

$$\gamma_{вих} = \gamma_0 (1-W_з / W_c) \quad (1)$$

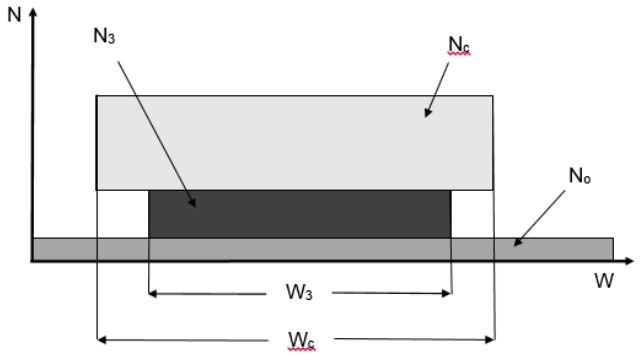

Рис.1. Спектри сигналу та загороджувальної завади: N_c , N_0 , $N_з$ – спектральна щільність потужностей сигналу, власного шуму та завади.

При цьому відношення сигнал / завада буде визначатися також формулою (2).

Виграш відношення сигал/шум при збільшенні ширини спектру сигналу за формулою (2) надасть можливість зменшення потужності сигналу до величини , необхідної для одержання заданої помилки приймання сигналу.

Характерною ознакою електромагнітної сумісності систем є їх безконфліктне співіснування в даному регіоні. Для цього передавачі систем повинні випромінювати мінімальний сигнал в смузі частот приймачів, щоб спектральна щільність сигналу була менше деякого порогового рівня.Використання широкосмугового сигналу є найбільш ефективним способом забезпечення електромагнітної сумісності радіоелектронних систем.

Широкосмуговий шумоподібний сигнал формується з використанням ряду відомих модулюючих псевдовипадкових послідовностей (ПВП) методом прямого розширення спектру [3].

Для маніпуляції сигналу використовуються різні відомі псевдовипадкові послідовності (ПВП): m-послідовність, послідовність Касамі, Голда і ін., а також код Уолша[3]. Головна вимога при виборі виду маніпулюючої послідовності - отримання мінімальних бічних пелюсток автокореляційної функції - для одноканальних систем і також мінімальних пелюсток взаємокорелфційних функцій -для багатоканальних систем.

Перехоплювач може розгадати структуру сигналу методом простого перебору з використанням банку паралельних узгоджувальних фільтрів або фільтрів, які перебудовуються послідовно, якщо сигнал приймається довгий

час. Тому системи з використанням класичних відомих ПВП не можна вважати захищеними від несанкціонованого доступу.

Використання явища динамічного хаосу [4,5] забезпечує можливість абсолютно нового підходу до формування ПВП. При цьому принциповою особливістю алгоритмів, що описують систему з динамічним хаосом, є їх нелінійність, а особливістю генерованого часового процесу - його неперіодичність. Це відкриває можливість пошуку нового класу ПВП, структуру яких практично неможливо відтворити, тому їх використання забезпечує підвищену конфіденційність передачі інформації.

Генератори ПВП побудовані на основі одновимірних хаотичних відображень- логістичного, квадратичного та кубічного, що являють собою хаотичні системи. Дослідженням встановлено, що найкращі результати надає використання хаосу за логістичним відображенням.

Алгоритмічна схема створення ПВП на основі хаосу наведена на рис.3.

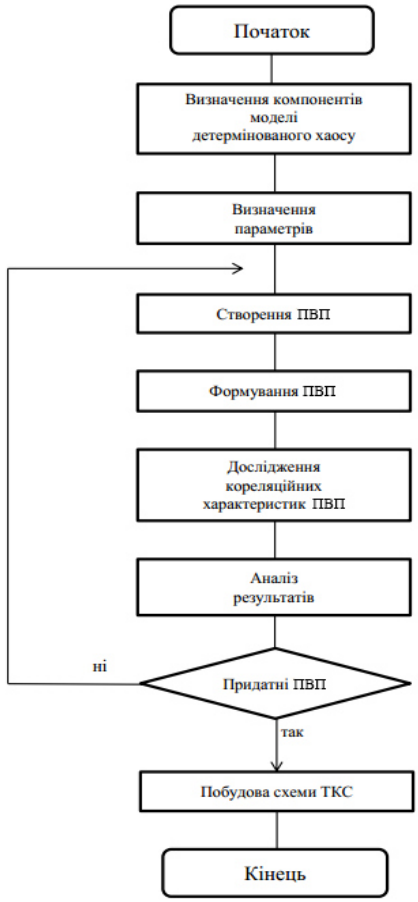

Рис.3. Алгоритмічна схема створення ПВП на основі хаосу

На основі хаосу з логістичним відображенням одержані 10 послідовностей довжиною 200 імпульсів за параметрами, показаними в табл.1.[5]

Перша послідовність з кількістю імпульсів 200 має вигляд -11-11-11-1-1-11-1-1-11-11-1-11-1-1111-1-11-1-1111-1-111-11-111-11-11-11-11-1 -11-111-1111111111-11-1-111-11-1-11-11-111-11-1-1-11-11-1-1-1111-1-11-1-1 -111-1-11-111-1-11-1-1-11-11-1-1-111-11-11-1-1111-1-11-11-11-1-111-11-11-1-11 11-111-11-111-111-11-1-1-11-11-1-1-111-1-11-111-11-1-1-11-1-1-11-11-11-11-1-1.

Таблиця 1.

АКФ ПВП хаосу на основі логістичного відображення

Кільк. імп →	10	20	30	40	50	100	150	200
№ ПВП ↓(x_0)								
1 (0,1)	0,6;-0,6	0,4;-0,4	0,4;-0,4	0,5	-0,4	-0,3	-0,3	-0,3
2 (0,2)	0,2;-0 ,2	0,5;-0,5	-0,5	0,4;-,4	0,3;-,3	0,2;-0,2	0,2;-0,2	0,2;-0,2
3 (0,3)	0,6	0,4	0,4	0,3	0,3	0,2;-0,2	0,2;-0,2	0,2;-0,2
4 (0,4)	0,6	0,4;-0,4	0,4;-0,4	0,4	-0,3	-0,3	0,2;-0,2	-0,3
5 (0,05)	-0,6	0,2;-0,2	\-0,4	0,4	0,3;-,3	0,2	0,2;-0,2	0,2,-0,2
6 (0,5)	0,6	0,4	-0,3	-0,3	0,3	0,2;-0,2	0,2;-0,2	0,2;-0,2
7 (0,6)	0,6	0,4;-0,4	0,4;-0,4	-0,3	-0,3	-0,4	0,2;-0,2	-0,3
8 (0,7)	0,6	0,4	0,4;-0,4	0,3	0,4	0,2;-0,2	0,2;-0,2	0,2;-0,2
9 (0,8)	0,2;-0,2	0,4;-0,4	-0,5	0,4;-,4	0,4	0,2;-0,2	0,3	0,2;-0,2
10 (0,9)	0,6;-0,6	0,4;-0,4	0,4;-0,4	0,4;-0,4	-0,4	-0,3	-0,3	-0,3

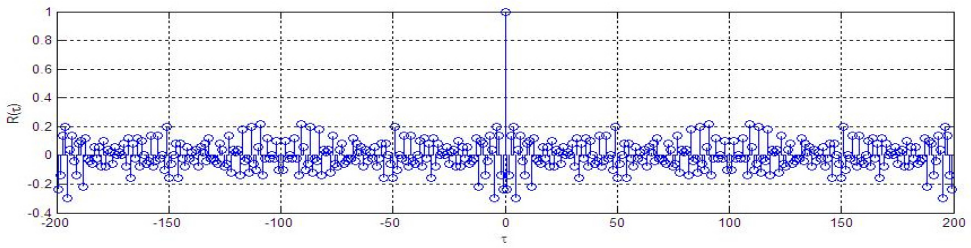

Рис. 4. АКФ ПВП , одержаної з хаосу за логістичним відображеннямпершої послідовності з кількістю імпульсів 200

При виконанні досліджень встановлено тенденцію, що прийнятні АКФ одержуються при кількості імпульсів ПВП більше 50.

При створенні ПВП на основі хаосу використовуються три секретних ключі шифруваня: наприклад, для логістичного відображення це початкове значення, параметр рівняння і початок відліку послідовності.

Для підвищення криптозахищеності телекомунікаційниз систем запропоновано створення ПВП на основі 2-х хаотичних сигналів (за логістичним та квадратичним відображеннями) з використанням їх секретних ключів, що забезпечує збільшення секретних ключів від трьох до шести .

При створенні запропонованої ПВП використовуються згенеровані ПВП із 2-х джерел хаотичних сигналів довжиною 15 , наприклад $f_1(x)$ (за логістичним відображенням) та $f_2(x)$ (за квадратичним відображенням) . Далі здійснюється складання за модулем «2» цих сигналів і одержуються остаточні ПВП $f_{\Sigma}(x)$, із яких за допомогою графічного інтерфейсу користувача відбираються ПВП із прийнятними рівнями бокових пелюсток[6].

$f_1(x)$ = 1 1 1-1 1-1-1 1 1-1 1-1-1 1-1

$f_2(x)$ = -1 1-1-1 1-1 1 1-1-1-1 1-1-1 1

$f_{\Sigma}(x)$ = 1-1 1-1-1-1 1-1 1 1-1 1-1 1 1

Одержана ПВП має вже 6 секретних ключів.

На рис.5. наведена алгоритмічна схема процесу створення ПВП із 2-х хаотичних сигналів.

На рис.6, 7, 8 наведені АКФ ПВП $f_1(x)$, $f_2(x)$. $f_{\Sigma}(x)$.

З використанням методу графічного інтерфейсу користувача [7] було досліджено АКФ створених ПВП .

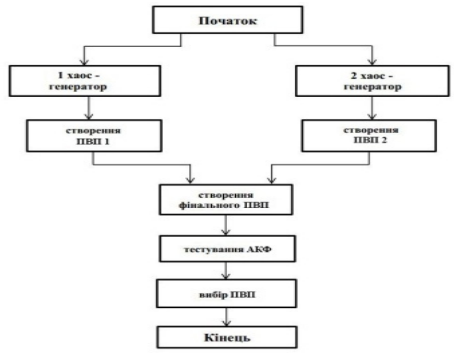

Рис. 5. Алгоритмічна схема процесу створення ПВП із 2-х хаотичних сигналів

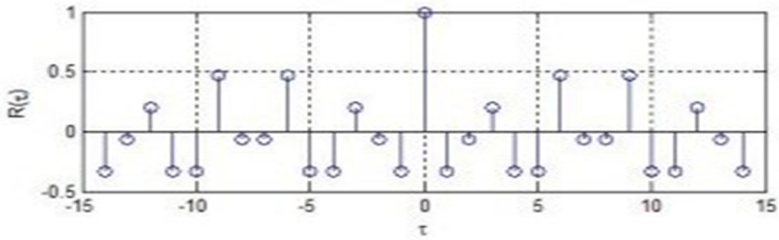

Рис. 6. АКФ ПВП $f_1(x)$

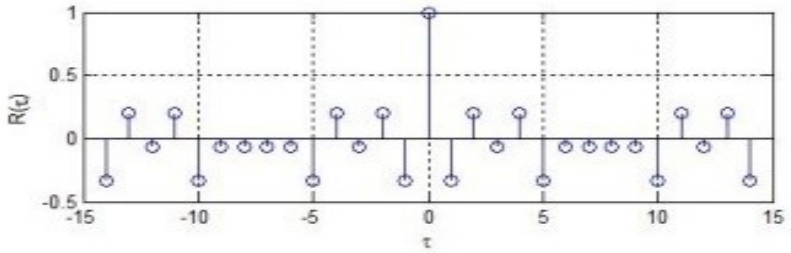

Рис.7. АКФ ПВП $f_2(x)$

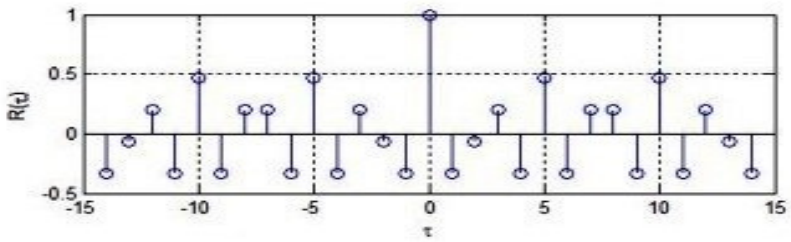

Рис.8. АКФ 2-х ПВП $f_\Sigma(x)$

В табл.4. 5 наведені значення бокових пелюсток досліджених ПВП.

Таблиця 2.

Значення бокових пелюстків досліджених ПВП

	+	-
$f_1(x)$	0.5	0.4
$f_2(x)$	0.5	0.4
$f_\Sigma(x)$	0.15	0.4

Очевидно, що запропонований метод створення ПВП із 2-х хаотичних сигналів дозволяє одержати АКФ з прийнятним рівнм бокових пелюсток не гірше 0.5. Причому ПВП із 2-х ПВП має не гірші АКФ , ніж кожна із 2-х використаних ПВП. Важливою перевагою ПВП на основі 2-х ПВП є суттєво підвищений криптозахист внаслідок використання шести секретних ключів, що практично виключає можливість прийняти інформацію сторонньому абоненту.

Створені ПВП з 2-х хаотичних сигналів, які мають найкращий криптозахист, доцільно використовувати при ствренні ТКС з підвищеною конфіденційністю передачі інформації .

У ряді випадків на часі створення одноканальної ТКС з широкосмуговим псевдошумовим сигналом з використанням ПВП на основі хаосу, що має підвищену конфіденційність передачі інформації [8] .При цьому доцільно використати ПВП , створену із 2-х ПВП, що має 6 секретних ключв.

На рис. 9 наведена схема побудови такої симплексної одноканальної ТКС

В передавачі 1 за допомогою ПК 3 за відомим методом здійснюється формування хаотичного сигналу та інформаційної послідовності великої довжини у вигляді бітів +1,-1, яка має ознаки ПВП завдяки створюючому її хаосу. З даної послідовності виділяються короткі ПВП потрібної довжини з

огляду одержання спектру сигналу, відповідного смузі пропускання радіоканалу.

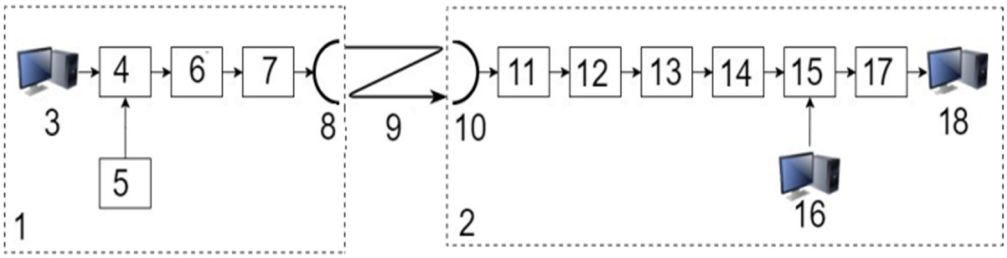

Рис. 9. Схема побудови одноканальної симплексної РРСЗ з широкосмуговим сигналом з використанням ПВП на основі хаосу:
1- передавач; 2- приймач; 3 – ПК для формування сигналу; 4 – модулятор; 5 – генератор сигналу проміжної частоти; 6- перетворювач частоти; 7 – підсилювач потужності; 8,10 – антени передавача і приймача; 9 – радіоканал; 11 – малошумний підсилювач; 12 – перетворювач частоти; 13 – RAKE- приймач; 14 – демодулятор; 15 – корелятор; 16 – ПК для формування опорного сигналу; 17 – вирішуючий пристрій; 18 – ПК для формування прийнятого сигналу.

З використанням розробленого методу графічного інтерфейсу автоматично здійснюється аналіз АКФ послідовностей та відбираються послідовності із прийнятним рівнем бокових пелюсток, не більше 0.5. Відібрана псевдовипадкова послідовність в модуляторі 4 використовується для фазової маніпуляції гармонічного сигналу проміжної частоти, одержаного від генератора 5. Потім в перетворювачі частоти 6 сигнал переноситься на високу робочу частоту , підсилюється за потужністю в підсилювачі 7 і через антену 8 надходить до радіоканалу 9. Прийнятий антеною 10 сигнал в приймачі 2 після підсилення малошумливим підсилювачем 11 переноситься на проміжну частоту за допомогою перетворювача частоти 12. Далі сигнал надходить до RAKE- приймача 13, де завдяки спеціальній обробці багатопроменевого сигналу одержується його максимальний рівень. Після демодуляції в демодуляторі 14 сигнал надходить до корелятора 15 , де здійснюється його оптимальна обробка з використанням унікального опорного сигналу, синтезованого в ПК 16. Далі вирішуючий пристрій 17 відтворює прийняті біти з мінімальною помилкою , з яких в ПК 18 формується передане конфіденційне повідомлення.

Таким чином в передавачі створюється ширикосмуговий шумоподібний сигнал з маніпуляцією гармонічного сигналу ПВП на основі хаосу. В приймачі здійснюється оптимальне кореляційне приймання сигналу з використанням обраної ПВП.

При використанні декількох ПВП можна створити багатоканальну систему з кодовим розділенням сигналів від каналів.

Висновки

1. Викоистання широкосмугового сигналу дозволяє підвищити завадостійкість телекомунікаційних систем,скритність їх роботи та їх електромагнітну сумісність.

2. Для створення широкосмугового сигналу доцільно використати псевдовипадкові послідовності на основі хаосу. Причому використання псевдовипадкової послідовності на основі 2-х хаотичних сигналів з шістю секретними ключами дозволить суттєво підвищити конфіденційність передачі інформації.

Література

1. Варакин Л.Е. Системы связи с шумоподобными сигналами. — М.: Радио и связи.- 1985. — 384 с.

2. Ипатов В.П. Широкополосные системы и кодовое разделение сигналов.М.: Техносфера.2007.-488 с.

3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Изд. 2-е, испр.: пер с англ. – М.: Издательский дом «Вильямс», 2004. -1104с.

4. Бобало, Ю.Я. Прикладне застосування теорії хаотичних систем у телекомунікаціях : монографія / Ю. Я. Бобало, С. Д. Галюк, М. М. Климаш, Р.Л. Політанський. – Дрогобич – Львів: Коло, 2015. – 184 с.

5. Semenko Anatoly. Characteristics Improvement of the Wideband Telecommunication System applying Chaos Based Pseudorandom Sequence/ Anatoly Semenko, Nikolay Kushnir, Natalia Bokla, Y. Shestopal // Information and Telecommunication Sciences.- 2018.- Volume 10.- Number 2.- pp 12-16.

6. Kushnir M., Increasing the Cryptosecurity of Telecommunication Systems with Spread Spectrum by Using Pseudorandom Sequences Based on Two Ergodic Chaotic Signals./M. Kushnir , A. Semenko, G. Kosovan, N. Bokla, Y. Shestopal// In *2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings* (pp. 455–458). Institute of Electrical and Electronics Engineers Inc.(Scopus).

7. Бокла Н.І. Дослідження кореляційних властивостей ПВП за кодом Голда з використанням системи MATLAB//Вісник ДУІКТ.-2011.-Том.9.- №4.-С.386-391.

8. Семенко А.І. Спосіб формування широкосмугового псевдошумового сигналу/А.І.Семенко,М.Я.Кушнір,Н.І.Бокла//Пат.125337,Україна: ПКН04В.3/60(2006.01), Н04В3/00. № u201711149;заявл. 14.11.2017;опубл.10.05.2018,бюл. № 9.

References

1. Varakin L.E. Sistemy svyazi s shumopodobnymi signalami. — M.: Radio i svyazi.- 1985. — 384 s.

2. Ipatov V.P. Shirokopolosnye sistemy i kodovoe razdelenie signalov.M.: Tehnosfera.2007.488 s.

3. Sklyar B. Cifrovaya svyaz. Teoreticheskie osnovy i prakticheskoe primenenie. Izd. 2-e, ispr.: per s angl. – M.: Izdatelskij dom «Vilyams», 2004. -1104s.

4. Bobalo, Yu.Ya. Prikladne zastosuvannya teoriyi haotichnih sistem u telekomunikaciyah : monografiya / Yu. Ya. Bobalo, S. D. Galyuk, M. M. Klimash, R.L. Politanskij. – Drogobich – Lviv: Kolo, 2015. – 184 s.

5. Semenko Anatoly. Characteristics Improvement of the Wideband Telecommunication System applying Chaos Based Pseudorandom Sequence/ Anatoly Semenko, Nikolay Kushnir, Natalia Bokla, Y. Shestopal // Information and Telecommunication Sciences.- 2018.- Volume 10.- Number 2.- pp 12-16.

6. Kushnir M., Increasing the Cryptosecurity of Telecommunication Systems with Spread Spectrum by Using Pseudorandom Sequences Based on Two Ergodic Chaotic Signals./M. Kushnir ,

A. Semenko, G. Kosovan, N. Bokla, Y. Shestopal// In *2019 3rd International Conference on Advanced Information and Communications Technologies, AICT 2019 - Proceedings* (pp. 455–458). Institute of Electrical and Electronics Engineers Inc.(Scopus).

7. Bokla N.I. Doslidzhennya korelyacijnih vlastivostej PVP za kodom Golda z vikoristannyam sistemi MATLAB//Visnik DUIKT.-2011.-Tom.9.- №4.-S.386-391.

8. Semenko A.I. Sposib formuvannya shirokosmugovogo psevdoshumovogo signalu/ A.I. Semenko, M.Ya. Kushnir, N.I. Bokla // Pat.125337, Ukrayina: PKN04B.3/60(2006.01), H04B3/00. № u201711149; zayavl. 14.11.2017; opubl.10.05.2018, byul. № 9.