DOI 10.12851/EESJ201406C06ART09

Dmytro A. Vovchuk,
PhD student;

Leonid F. Politanskii,
DPh, Professor;

Serhii D. Haliuk,
PhD, assistant;
Yuriy Fedkovych Chernivtsi National University

Experimental Research of the Process of Masking of Digital Information Signals Using Chaotic Oscillations

Key words: *Chua's circuit, digital transmission, chaotic masking, hidden transmission*

Annotation: *The schematic implementation of digital data transfer method using chaotic masking that is based on summing of modulated carrying oscillation and chaotic oscillation was carried out in the work. It is possible to use harmonic, chaotic or noise oscillation with statistical and spectral characteristics close to the characteristics of masking signal as carrying oscillation. The phenomenon of full chaotic synchronization between chaotic oscillations of generators of transmitter and receiver is used for data recovery. The possibility of data recovery in the receiver under the conditions of noisy channel is investigated and the possibility of practical implementation of the given method is shown.*

Introduction

The development of digital systems of hidden data transfer using chaotic signals is a topical issue of scientific researches of the last decades (1),(7).

Communication systems using chaotic signals can be divided into the systems with application and without application phenomena of chaotic synchronization (3), (10). Numerous works offer analog communication systems using the synchronization of transmitter and receiver for data recovery (10), (11), (15), (18). The research has found that such systems possess low noise immunity caused by high sensitivity of chaotic synchronization to the noises in communication channel and detuning of parameters of drive and response generators. The use of digital systems provides for the rise of level of noise immunity of data transmission process compared to the analog ones as well as the possibility of the application of encoding (6) and cryptographic security methods (8), (12).

The most widely used circuit for hidden data transmission is the circuit with the use of chaotic masking (Figure №1*a*) (16, 17). Its working principle lies in the following. One of the output chaotic oscillations of the generator *x(t)* is added up with an analog data signal *m(t)* followed by transmission to channel. Security of data transmission process by channel is ensured by complete overlap of data signal spectrum by chaotic oscillation spectrum. The phenomenon of chaotic simultaneous response or chaotic synchronization can be used for data recovery. The receiver contains chaos generator (or generator decomposition) *u(t)* with parameters identical to the ones of transmitter generator. In arriving at synchronization (simultaneous response) between transmitter and receiver a data signal can be recovered by subtracting the output signal of response generator by the input signal of receiver. The control parameters variety of generators *v(t)* and *u(t)* and the presence of noise in communication channel results in the origin of synchronization error that equals the error of data signal recovery. Desynchronization of transmitter and receiver generators eliminates the possibility of data transmission by channel. Besides, it is necessary to ensure the ratio signal/noise no less than 35 dB for accurate data recover, which is its critical weakness (1, 2).

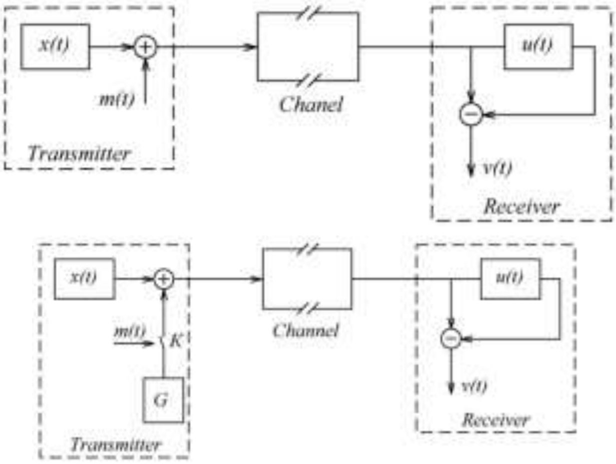
When using the circuit of chaotic masking in digital systems of data transmission, the hiding of transmission process by communication channel will be low as in the intervals that equal the duration of data bit transmission a strong constant component will take place. In order to close this gap we offer a modification of analog circuit of chaotic masking for digital data transmission. Its working efficiency is proved by computer based simulation (4),(5).

The aim of the work is schematic implementation and experimental research of the method of digital signals masking for the systems of hidden data transmission using chaotic oscillations and evaluation of its noise immunity.

The method of digital data transmission using chaotic masking

The modified circuit of chaotic masking of digital signals transmission is shown in Figure №1*b*. In contrast to the circuits of analog data transmission it contains a subsidiary generator *G*, the signal of which is modulated by digital data signal and added to the chaotic signal. The modulation is carried out with the aid of a key *K* which is turned on or off depending on the value of data bit.

The implementation of preliminary modulation and ensuring of identity of statistic and spectral characteristics of signals generated by the generator *G* and the masking oscillation *x(t)* enables to match the parameters of carrying and chaotic signals. The harmonic, chaotic or noise oscillation can be used as a signal *G(t)* (4),(5). The circuit of the receiver remained unchanged.



a) *b)*

Figure №1.The systems of analog and suggested circuit of digital data transmission using chaos generators *a)* and *b)* respectively, *x(t)* – drive generator; *m(t)* – digital data signal; *G* – subsidiary generator; *u(t)* – response generator; *v(t)* – recovered signal

The experimental research results

Figure №2 is a basic electric circuit of a transmitter using sine wave as a modulated signal. The generating of chaotic oscillations is carried out by Chua's circuit, where the inductor is implemented according to the equivalent circuit on resistors R1, R2, R3, R4, capacitor C1 and operational amplifier DA1, DA2 series TL084CN [9, 14] in order to eliminate non-zero parasitic inductor resistance. The non-linear element of the generator is implemented on the resistors R6, R9, R10, R12, R14, R15 and operational amplifiers DA5, DA7 [9, 13], and the key *K* - on the microcircuit ADG444B.

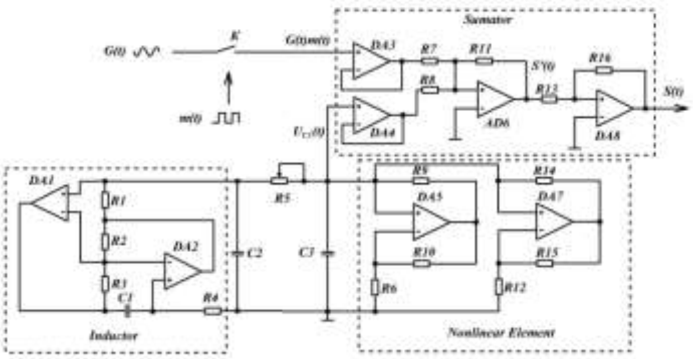


Figure №2. Basic electric circuit of a transmitter with the sine wave modulated by data signal

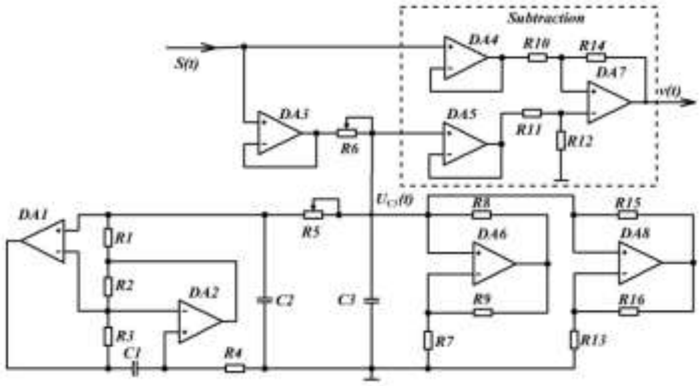
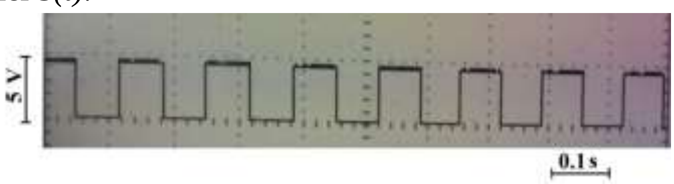


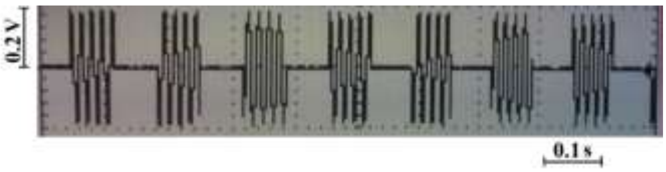
Figure №3. Basic electric circuit of a transmitter

The sequence of square waves was used as a digital binary message signal *m(t)* while conducting the experimental research. The data signal modulates the harmonic oscillation *G(t)* in such a way that in course of the «0» bit transmission (low level voltage on control key input) the harmonic signal is present and in course of the «1» bit transmission (high level voltage) on key output the signal is absent. The data sequence *m(t)* and the modulated harmonic signal *m(t)G(t)* are shown in Figure №4*a* and *b* respectively.

Masking of data signal consists in summing up of chaotic oscillation and modulated harmonic signal by means of inverting summator implemented on the elements R7, R8, R11, DA6. The sum signal *S'(t)* is inverted by the invertor on the elements R13, R16, DA8 and gives to the communication channel *S(t)*.



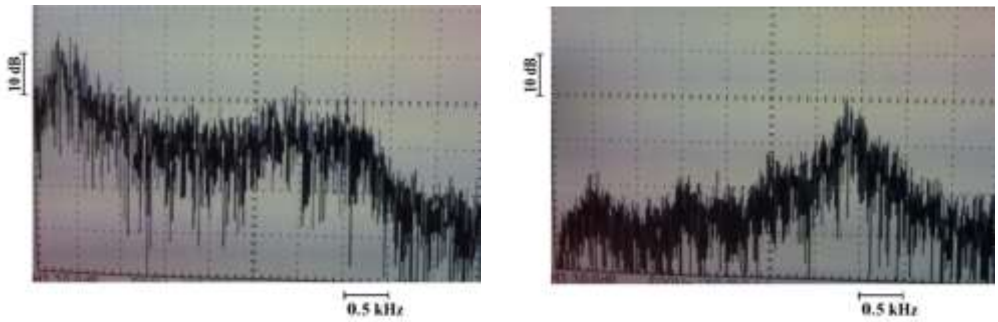
a)



b)

Figure №4.Time base diagrams of a digital message and modulated harmonic signal a) and b) respectively

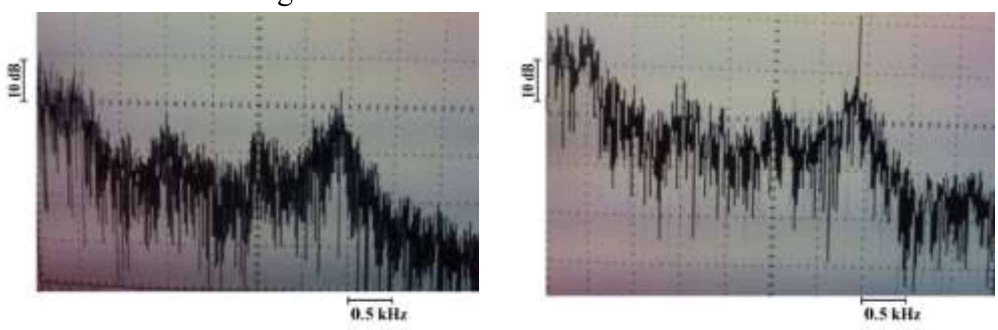
It is possible to use signals U_{C2} and U_{C3} formed on the capacitors C2 and C3 as masking oscillations, the spectral characteristics of which are shown in Figure №5*a* and *b* respectively. It was found that the signal U_{C3} has a more complex structure and wider frequency band. Besides, its usage ensures steadier synchronization of drive and response generators [15].



a) *b)*

Figure №5. Spectral characteristics of signals U_{C2} and U_{C3} a) and b) respectively

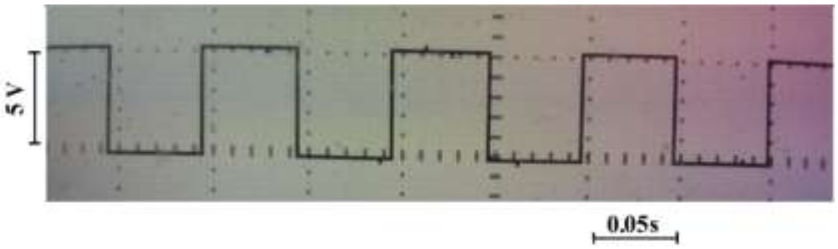
In order to ensure security of data transmission by communication channel the frequency value of a carrier harmonic signal has to range within the effective bandwidth of a masking signal [4]. While conducting the experimental research the harmonic signal with frequency of 3.5 kHz and amplitude of 0.3 V was used as a carrier oscillation. Besides the power ratio of harmonic and chaotic signals reached -25 dB. With the increase of the amplitude of sine wave the harmonic component will be in the spectrum of masking oscillation. The spectral characteristics of signals in communication channel with value of carrier oscillation amplitude of 0.3 and 1 V are shown in Figure №6.



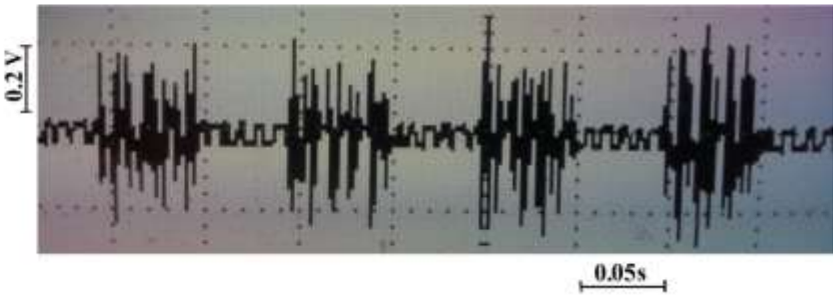
a) *b)*

Figure №6. The spectral characteristics of signals in communication channel with value of harmonic signal amplitude: *a)* 0.3 V; *b)* 1V.

Data recovery in the receiver was carried out with the aid of subtracting devicebased on the elements R10-R12, R14, DA7 (Figure №3). The oscillograms of the transferred data message and the received message by the receiver (output of subtracting device *v(t)*) are shown in Figure №7 *a* and *b* respectively.



a)



b)

Figure №7.Time base diagrams: *a)* digital data message *m(t)*; *b)* signal on the output of subtracting device *v(t)*

The error-free data reception in transferring of analog signals is possible when the value of parameters variety of generators of chaotic oscillations of transmitter and receiver are no more than 0.5% (1). The transition to the use of digital signals enables to desensitize the system to detuning of control parameters of chaos generators of transmitter and receiver. Experiments showed that the variety values are 0.8% and 1% for the parameters α and β respectively.

In order to increase the level of data security transmission process chaotic oscillations may be used as carrier signals. The analysis of the spectrum of chaotic oscillations generated by Chua's circuit shows that the U_{C3} *(t)* signal spectrum completely overlaps the U_{C2} *(t)* signal spectrum (Figure №5). It allows to make suggestions concerning the applicability of the use of U_{C3} *(t)* oscillation as a masking signal and U_{C2} *(t)* as a carrier one for hidden communication systems. Herewith a considerable simplifying of transmitter circuit compared to the circuit on Figure №2 takes place and it allows using the transmitter generator more effectively (Figure №8). The amplifier that consists of the elements R4, R6 and DA4 is used to control the value of modulated chaotic signal. The spectrum of the added signal in communication channel is similar to the spectrum of carrier oscillation (Figure №9).

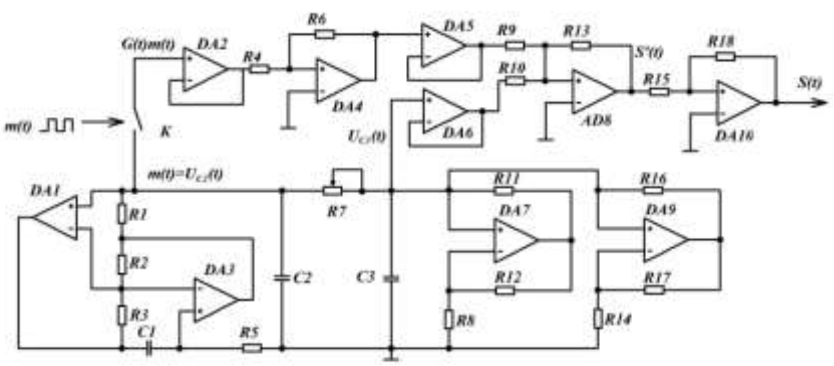


Figure №8. Basic electric circuit of a transmitter with chaotic signal used as a carrier signal

The transmitter circuit remains the same as in case of using of harmonic signal as a carrier signal. Time base diagrams of a digital data message and a signal on the output of the subtracting device are shown in Figure №10*a* and *b* respectively. It follows from their comparison that in the given case it is possible to recover the transmitted data in the receiver.

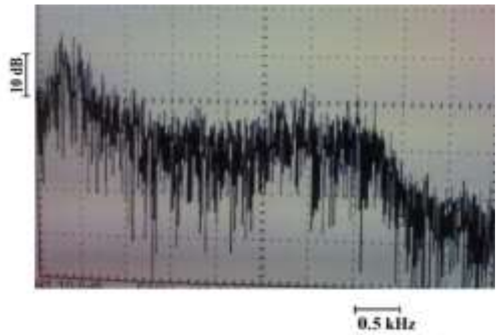
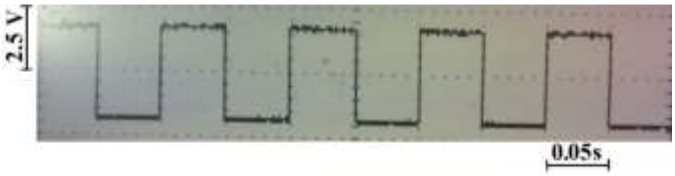
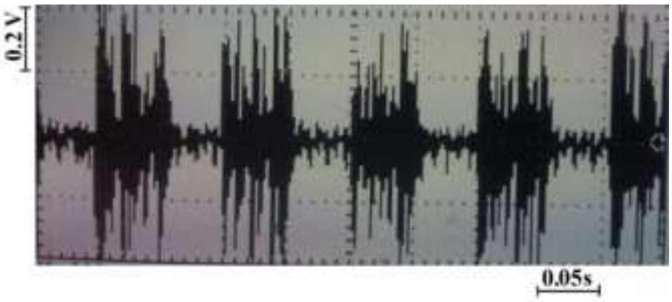


Figure №9. The spectrum of the sum signal in communication channel with chaotic signal used as a carrier signal



a)



b)

Figure №10. Time base diagrams: *a)* digital data message *m(t)*; *b)* signal on the output of the subtracting device *v(t)*

Noise immunity of data transmission

The state equations for the Chua's oscillator are given by

$$\begin{cases} \dot{x} = \alpha(y - x - f(x)) \\ \dot{y} = x - y + z \\ \dot{z} = -\beta y \end{cases}$$

where α and β – system control parameters; x, y, z – dynamic variables; $f(x) = m_2 x + 0{,}5((m_0 - m_1)(|x + a_1| - |x - a_1| + (m_1 - m_2)(|x + a_2| - |x - a_2|))$ – nonlinear characteristic, where a_1 = 1; a_2 = 6,88; m_0 = -1,238; m_1 = -0,6665; m_2 = 500. The VA characteristic of the nonlinear element is piecewise-linear.

In order to calculate the probability of an error of data recovery caused by the effect of additive white Gaussian noise in communication channel with different values of the signal/noise ratio we devised MatLab-Simulink models of the suggested system and a chaotic switching scheme.

The dependence of the probability of an error of the received data for different carrier signals from the value of signal/noise ratio in communication channel is shown in Figure №11. The results obtained show that the system of data transmission based on the usage of harmonic oscillation as a carrier signal yields to the chaotic switching scheme on the noise immunity (Figure №11 - curve 1 and curve 2 respectively). The increase of the amplitude of the carrier signal improves recovery process, however security is lost.

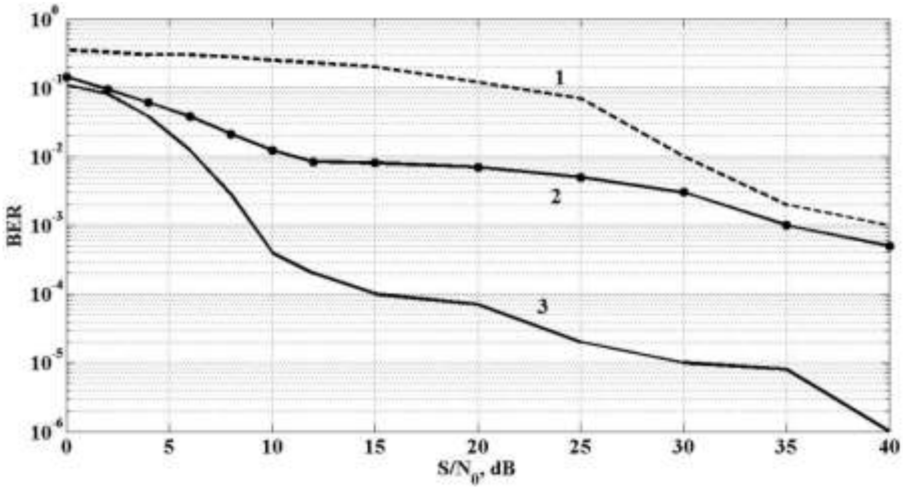


Figure №11. Dependence of the probability of incorrect bytes recovery from the value of signal/noise ratio in communication channel (1 – with harmonic oscillation used as a carrier signal; 2 –chaotic switching scheme; 3 – with chaotic oscillation used as a carrier signal)

The system based on the usage of carrier oscillation as a carrier signal is more resistant to noise impact in communication channel (curve 3).While modeling the modified system the parameters of master and slave generators were α = 10, β = 15. While modeling the chaotic switching scheme the modulation was carried out by changing the parameter β ranging between15 and 17. It follows from the results obtained that the modified circuit with data masking with chaotic signal used as a carrier signal is more resistible to noise impact in communication channel than the chaotic switching scheme. The probability of recovery error while using the modified circuit with the ratio S/N_0 of the order 10 dB is 10^{-3}, whereas its value constitutes 10^{-2} while using the chaotic switching scheme.

Conclusion

1. The paper offers the experimental studies of the modified system of chaotic masking for digital data transmission. Chua circuit was chosen as a generator of masking of chaotic signal. In order to increase the transmission data security it has been suggested that another chaotic oscillation generated by the same chaos generator shall be used as a carrier signal. It enabled to effectively use the capability of chaos generator.

2. Data security was researched with the aid of comparative analysis of spectrum characteristics of masking and sum signals. It has been shown that harmonic oscillation may be used as a carrier signal only with the value of its amplitude of 0.3 V. The most effective is the system based on the usage of chaotic oscillation generated by the generator of the transmitter as a carrying and hiding signal.

3. The probability of an error of data recovery was calculated. It was shown that the modified circuit with chaotic masking is more resistant to noise impact in communication channel compared to the chaotic switching scheme and with the signal/noise ratio of 10 dB is 10^{-3}.

The results obtained indicate the possibility of usage of the suggested method as a basic approach in the systems of hidden digital data transmission.

References:

1. *Dmitriev A, Panas A. Dynamic chaos: novel type of information carrier for communications system. M: Izdatel'stvo Fiziko–matematicheskoj literatury, 2002. vol. 251.*
2. *Koronovskii A, Moskalenko O, Hramov A. On the use of chaotic synchronization for secure communication: Uspekhi Fizicheskikh Nauk; 2009. № 12; 1282-1310.*
3. *Pikovsky AS, Rosemblum MG, Kurths J. Synchronization: a universal concept in nonlinear sciences. M.: Technosfera; 2007; Vol. 496.*
4. *Vovchuk D, Haliuk S, Politanskii L. Adaptation of the chaotic masking method for digital communication: Eastern-European Journal of Enterprise Technologies, 2013. № 2/4(62); 50-55.*
5. *Vovchuk D. Modelling of the Digital Data Transmission with the Use of Chaotic Masking: Technology Audit and Production Reserves, 2013; №5/5(13); 55-57.*
6. *Bollt E, LaiY-C. Dynanics of coding in communicating whits chaos: Phys. Rev. E.; 1998; № 2; 1724-1736.*
7. *Larson E, Liu J-M, Tsimring S. Digital Communications Using Chaos and Nonlinear Dynamics.*
8. *Jakimoski G. and Kocarev L. Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps, IEEE Trans. on circ. and syst. I: Fund. theory and appl; 2001; № 2; 163-169.*
9. *Fortuna L, Fraska M, Xibilia M. Chua's Circuit Implementations. Yesterday, Today and Tomorrow: World Scientific Series on Nonlinear Science, Series A; 2009. V. 65; 222.*
10. *Politansky L, Galiuk S, Kushnir M, Politansky R. Osoblivosti sinhronizacii̇ haotichnih sistem (ogljad): Izdatel'stvo Fiziko–matematicheskoj literatury: Skladni sistemi i procesi; 2011. №2; 3-29.*
11. *Pecora LM, Carroll TL. Synchronization in Chaotic Systems: Physical review letters, 1990. Vol. 64, N 8: 821-824.*
12. *Baptista MS. Cryptography with chaos: Phys, Lett. A.; 1998. № 1-2; 50-54.*
13. *Eliyashiv OM, Politanskii LF, Rusyn VB, Kushnir MYa, Politanskii RL. Doslidzhennya Vlastyvostey Neliniynoho Elementa Peredavacha Khaotychnoyi Systemy Zvyazku: Radiolektronika i Informatyka; 2011. №2; 12-16.*
14. *Eliyashiv OM, Politanskii LF. Non-inductive generator of chaotic oscillations of Chua circuit: Tekhnologiya i Konstruirovanie v Elektronnoi Apparature; 2012. №2; 12 – 15.*
15. *Eliyashiv OM, Galiuk S, Politanskii LF, Kushnir MYa, Tanasyuk VS. Continuous and pulse synchrozation of Chua oscillatiors: Tekhnologiya i Konstruirovanie v Elektronnoi Apparature; 2011. №3; 22-27.*
16. *Ivanyuk P, Politansky L, Politansky R, Eliyashiv O. Chaotic masking of information signals using generator based on the Liu System: Tekhnologiya i Konstruirovanie v Elektronnoi Apparature; 2012. №3; 11-17.*
17. *Downes Ph. Secure communication using chaotic synchronization: SPIE; 1993; 227.*
18. *Stasev YuV, Vasyuta KS, Zhenzhera SV. Informative Systems on the Basis of Dynamic Chaos: Systemy ozbroyennya i viys'kova tekhnika; 2009. № 1(17): 134-138.*