УДК 004.056.55

Krulikovskyi O. V., Haliuk S. D., Politanskyi L. F. Yuriy Fedkovych Chernivtsi National University

TESTING TIMESERIES RING-COUPLED MAP GENERATED BY ON FPGA

In this paper we investigate four-dimensional chaotic ring-coupled map using FPGA. For implementation on FPGA was used Q4.28 fixed point arithmetic. Through analysis of balance bits defined which range of bits, that can use for creation pseudorandom sequences. Proposed and implemented method of generating pseudorandom sequences based on shift registers and XOR. The obtained sequences passed NIST statistical tests.

***Keywords*:** ring-coupled map, FPGA, PRNG, chaotic ciphers, NIST, pseudorandom sequence

1. Introduction. Currently ring-coupled maps [1, 2] are the greatest interest for construction of new encryption methods based on deterministic chaos. These discrete multidimensional maps use simple arithmetic operations as opposed to mathematical models that describe the classic continuous dynamic systems (Chua circuit, Lorenz system and other). From the point of view of cryptography these discrete maps are interesting with their statistical properties especially uniform distribution of generated values. In [3] it is noted that for cryptography priority were used discrete maps. This is because they are simple to implement and modify on different platforms. In addition, discrete map is easier to integrate into telecommunications protocols. Continuous systems require more resources as they are described by differential equations. In one-dimensional systems when arbitrarily high precision of calculations, will be observed collapse of chaos [4, 5]. Also limitations of numerical precision for one and two-dimensional systems make the behavior of these systems very periodic on time. Also, the length of the cycles depends on initial conditions and parameters.

The advantages of multidimensional systems over one or two-dimensional are better statistical properties (length of period, uniformity of distribution and other). One of these multidimensional discrete systems is the ring-coupled map proposed in [6]. This map is characterized by a uniform distribution of generated values in the range [-1; 1]. In perspective it can give good cryptographic means based on maps these type.

Balance, run and correlation can be identified as three basic properties of any periodic binary sequences that can be used as a test for randomness [7]. For all nonlinear systems is true, if the values generated by them have uneven distribution, then the significant bits in the binary representation of these numbers are unbalanced. So it is undesirable to use these bits to form pseudo-random sequences. This unbalanced bit goes into balance with decreasing significance of bits. In literature to solve this problem are usually use the following techniques:

– rejected unbalanced bits [8];

– XOR significant bits of different timeseries and mixed with fraction part [9].

For implementation chaotic systems on different platforms (CPU, FPGA, GPU) it is necessary to use arithmetic with floating or fixed point. Calculating with fixed-point is easier to implement on different devices. Therefore, we use fixed-point arithmetic Q4.28. Goal of our work is implementation on FPGA and testing timeseries generated ring-coupled map for Q4.28 arithmetic. In section 2 is describes ring-coupled map. FPGA realization of ring-coupled map is presented in section 3. In section 4 is described method of generation pseudorandom sequences. NIST statistical tests results are presented in section 5. In section 6 are conclusions and future work.

2. Describe of ring-coupled map. Ring-coupled map describe by [6]:

$$M_p: \begin{vmatrix} x_{n+1}^{(1)} = 1 - 2\left|x_n^{(1)}\right| + k^{(1)} \times x_n^{(2)} \\ x_{n+1}^{(2)} = 1 - 2\left|x_n^{(2)}\right| + k^{(2)} \times x_n^{(3)} \\ \vdots \\ x_{n+1}^{(p)} = 1 - 2\left|x_n^{(p)}\right| + k^{(p)} \times x_n^{(1)} \end{vmatrix}, \quad (1)$$

where the parameters $k^{(i)} = (-1)^{i+1}$.

In order to trajectory the system uniformly and densely visited all points on p-dimensional torus $T^p = [-1, 1]^p$ need to use next mechanism of improving randomness [6]:

$$\left\{ \begin{array}{lll} if & x_{n+1}^{(j)} = 1 - 2\left|x_n^{(j)}\right| + k^{(j)} \times x_n^{(j+1)} < -1 & add \quad 2, \\ if & x_{n+1}^{(j)})) = 1 - 2\left|x_n^{(j)}\right| + k^{(j)} \times x_n^{(j+1)} > 1 & substract \quad 2 \end{array} \right\}, \tag{2}$$

where $\left|x_n^{(j)}\right|$ denotes the absolute value of $x_n^{(j)}$, and $j \in [1, p]$.

This mechanism of improving randomness properties is very satisfactory for the PRNG applications. It is possible to obtain a uniform distribution of the generated timeseries. To obtain uniform timeseries we used system (2) with $p = 4$. Histohram of distribution values $x^{(1)}$, $x^{(2)}$, $x^{(3)}$ and $x^{(4)}$ is shown on Fig. 1.

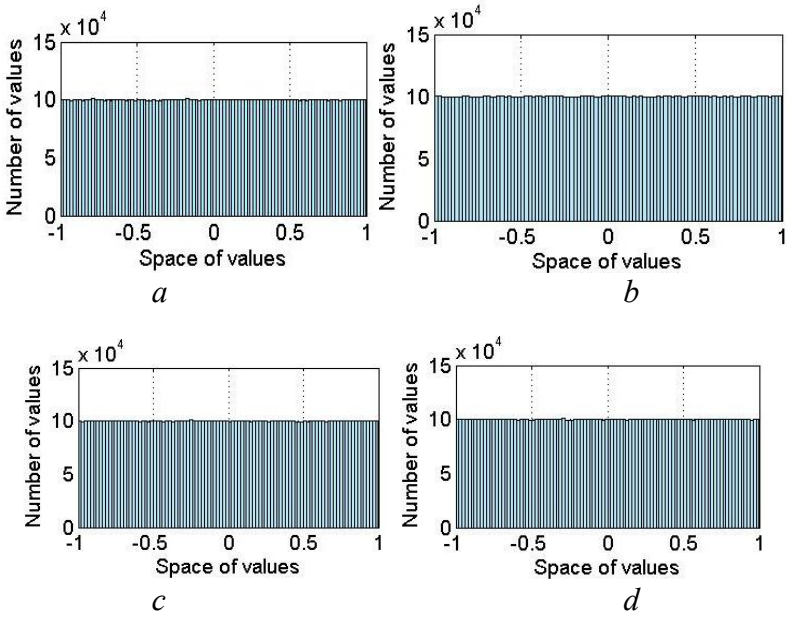

Fig. 1. Histohram of distribution values:
a – chanel $x^{(1)}$; b – chanel $x^{(2)}$; c – chanel $x^{(3)}$; d – chanel $x^{(4)}$

As can be seen from Fig. 1 the average value of the number of hits in each from 100 subranges of range [-1, 1] approximately equal to 10×10^4 for 10000000 iterations.

Phase portrait $x^{(1)}$, $x^{(2)}$ and $x^{(3)}$ for $p = 4$ realization in MATLAB with double precision is shown on Fig. 2.

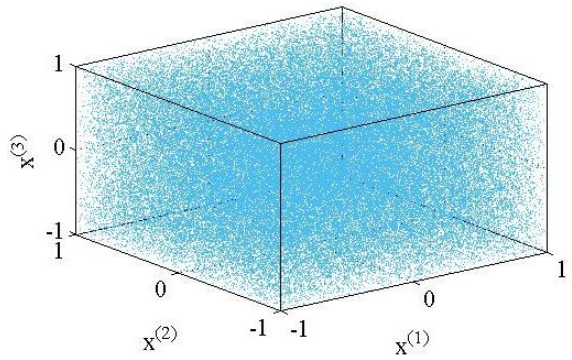

Fig. 2. Phase portrait $x^{(1)}$, $x^{(2)}$ and $x^{(3)}$ for $p = 4$

From Fig. 2 implies that the trajectory of the $x^{(1)}$, $x^{(2)}$ and $x^{(3)}$ due to the uniform distribution visits evenly all points of phase space. This is an advantage compared to other discrete and continuous systems that are uneven distribution and their attractor centered in one part of phase space.

3. FPGA realization ring-coupled map. For FPGA implementation we used *Altera Cyclone IV EP4CE115*. Simulink model, that calculates $x_{n+1}^{(1)}$ shown on Fig. 3. Block of conditional operators (2) we implemented based on 2 comparators. Comparator 1 responsible for $x_{n+1} > 1$. If $x_{n+1} > 1$ then the control signal is sent to the Subsystem 1 which subtracts 2 from the signal value. The Comparator 2 is responsible for $x_{n+1} < -1$. Then the control signal is fed to the subsystem and to value of signal x_{n+1} added 2. If the signal enters the range [0, 1] then control signals on comparators are 0. The two control signals are fed to the input of two inverters. Next logical operation is performed between the output signals of invertors and formed a control signal for the Subsystem 3. This subsystem transmits a signal intact.

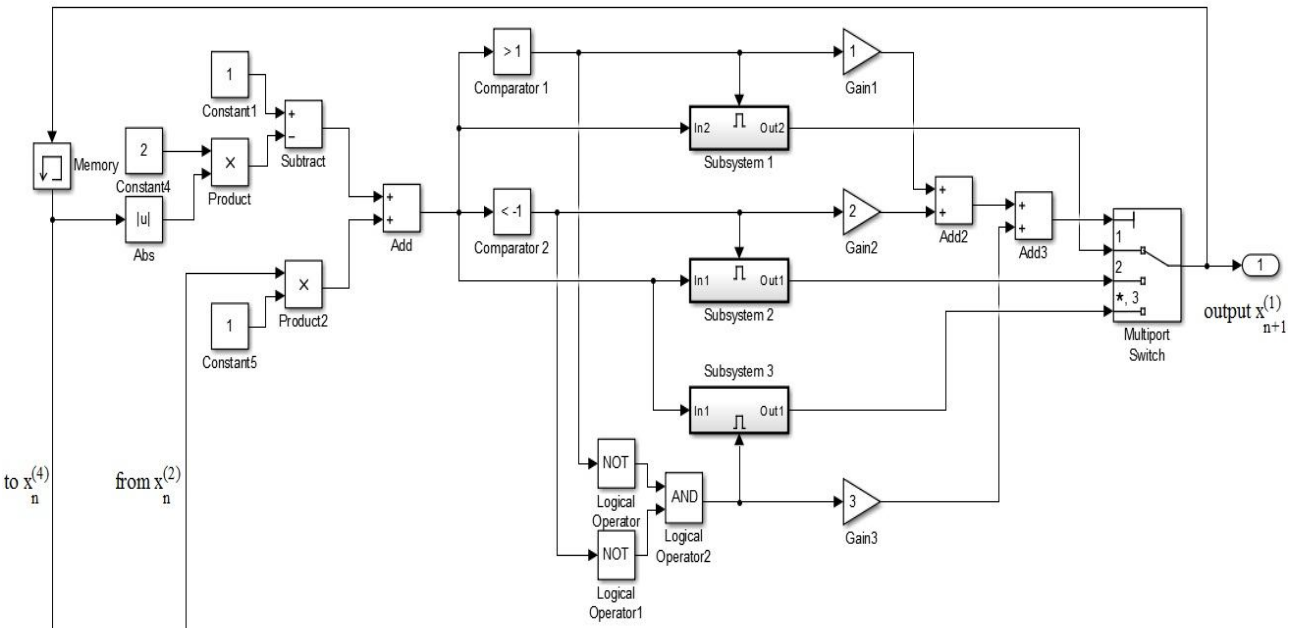

Fig. 3. Simulink block diagram realizing $x_{n+1}^{(1)}$

Switch is used to select the signal which satisfies one of the conditions (2). The switch is controlled by output signal of comparators multiplied by constant *D*. In our case $D = 1, 2, 3$. The level of output signal, which controls the switch corresponds to one of three conditions (2) for signal $x_{n+1}^{(1)}$.

PLL is set to a frequency of 1 MHz. For our realization 4-D ring-coupled map with Q4.28 arithmetic 1412 logic gates are required.

As we use Q4.28 fixed-point arithmetic in order to identify the bits which satisfy the criteria of balance we generate 4 matrixes. Size of these matrix is (32×*N*), which consists of the elements $l_{a,b}$.

$$\begin{Bmatrix} l_{11} \; . \; l_{12} \; \dots \; l_{1,32} \\ l_{21} \; . \; l_{22} \; \dots \; l_{2,32} \\ . \quad . \quad \dots \quad . \\ l_{K,1} \; . \; l_{K,2} \; \dots \; l_{K,32} \end{Bmatrix}, \tag{4}$$

where $a \in [1, K]$ – iteration number sequences of iterations $x^{(1)}$, $x^{(2)}$, $x^{(3)}$ and $x^{(4)}$, $b \in [1,32]$ – serial number of level in 32 – bit represented by $x^{(1)}$, $x^{(2)}$, $x^{(3)}$ and $x^{(4)}$. For each column we computed number of symbols "0" – N_0 and "1" – N_1, $N_0 + N_1 = N$, results are shown in Fig. 4.

From Fig. 4 can be seen that the bits at range 1 to 29 are balanced. Bits of the 30 to 32 range are unbalanced due to a factor of $2|x_{n+1}|$.

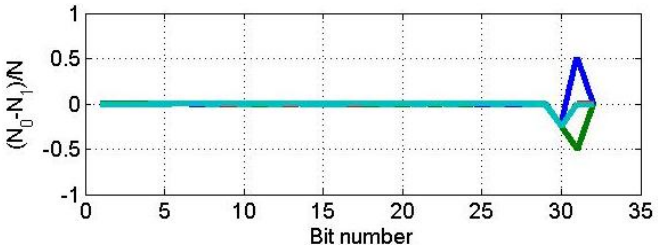

Fig. 4. The bits balance of timeseries generated (2).

Therefore, we will use the bit values of range 5 to 28 for forming the pseudorandom sequences. Phase portrait $x^{(1)}$, $x^{(2)}$ for $p=4$ of realization on FPGA with Q4.28 fixed-point arithmetic shown on Fig. 5.

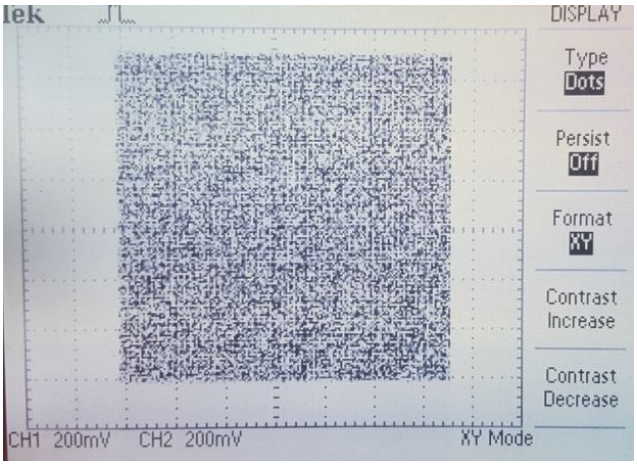

Fig. 5. Phase portrait of $x^{(1)}$ and $x^{(2)}$ for $p=4$ implemented on FPGA.

From Fig. 5 implies that the trajectory $x^{(1)}$ and $x^{(2)}$ uniformly and densely visited all points on p-dimensional torus.

4. Proposed PRNG. The basis of PRNG construction we used PRNG proposed in [2]. However, we introduce some differences. The block scheme of the proposed PRNG is shown on Fig. 6.

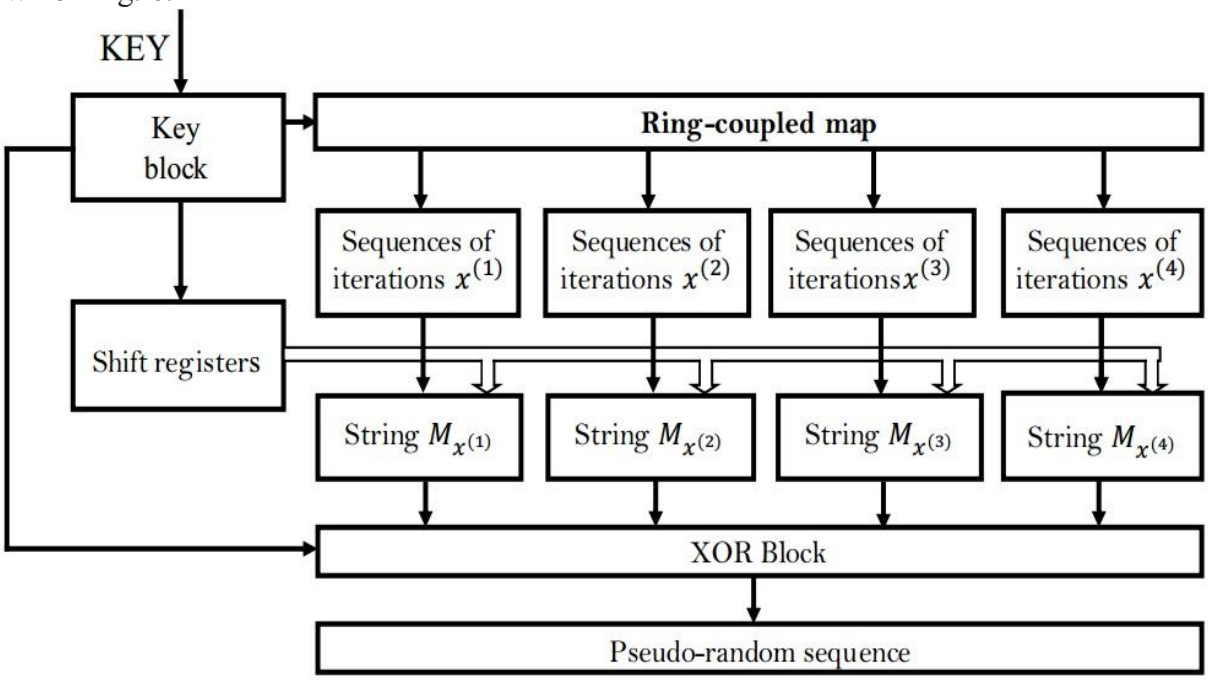

Fig. 6. Proposed construction of PRNG.

In our case $M_x = 24$ bits. It can be concluded that to build cryptographically safely PRNG should reject the first certain number of least significant bits. In block String M_x from Fig. 6., we took the 16 bits from each of the chaotic sequences of iterations within a range of 5 to 28 bits. As a result, we received 96 bits from all timeseries after one time iteration. In block XOR bitwise XOR operation carried out between 2 blocks of $x^{(1)}$, $x^{(2)}$, $x^{(3)}$ and $x^{(4)}$ and received two sequences of 24 bits. Selecting blocks performed random and is one of the subkeys. At the output of the PRNG after one cycle we have a block size of 48 bits. Shift register and XOR block introduced in order to cover the current state of the generator. *XOR* block performs the following operations:

$$\begin{Bmatrix} M_{x^{(1)}}\ XOR\, M_{x^{(2)}} \\ M_{x^{(3)}}\ XOR\, M_{x^{(4)}} \end{Bmatrix}.$$

From Key block are transmitted the initial conditions, parameters, setting of shift registers and XOR Block.

5. NIST testing. For statistical testing we used NIST tests suite. This suite consists from 15 tests. If sequences pass all tests, then they are marked as cryptographically safe [10]. Tabl. 1 presents the NIST statistical tests results for binary pseudo-random sequences generated by the chaotic system (2).

The NIST tests are performed on a binary sequence of length 10^9 bits which was divided on 1,000 subsequences (with 1 million strings). The parameters and initial condition for testing PRNG is next: $x_0^{(1)} = 0.292$, $x_0^{(2)} = -0.90258$, $x_0^{(3)} = 0.0258$, $x_n^{(4)} = 0.990258$, $k^{(1)}, k^{(3)} = 1$ and $k^{(2)}, k^{(4)} = -1$. In this case, the shift bits equal to 0 for all M_x. As we can see from Tab. 1. sequences generated 4-D ring-coupled map pass NIST tests.

NIST STATISTICAL TESTS RESULT Tabl. 1

Test	*P* - value	Proportion	Status
Frequency (Monobit) Test	0.958485	0.989	**Pass**
Frequency Test within a Block	0.377007	0.993	**Pass**
Runs Test	0.281232	0.986	**Pass**
Test for the Longest Run of Ones in a Block	0.049984	0.993	**Pass**
Binary Matrix Rank Test	0.231956	0.993	**Pass**
Discrete Fourier Transform (Spectral) Test	0.137282	0.983	**Pass**
Non-overlapping Template Matching Test	0.737915	0.990	**Pass**
Overlapping Template Matching Test	0.353733	0.993	**Pass**
Maurer's "Universal Statistical" Test	0.450297	0.992	**Pass**
Linear Complexity Test	0.353733	0.983	**Pass**
Serial Test	0.056069	0.992	**Pass**
Approximate Entropy Test	0.132640	0.988	**Pass**
Cumulative Sums (Cusum) Test	0.672470	0.989	**Pass**
Random Excursions Test	0.701024	0.990	**Pass**
Random Excursions Variant Test	0.947142	0.992	**Pass**

6. Conclusion and future work. In this paper, we investigated four-dimensional chaotic ring-coupled map implemented by FPGA *Cyclone IV EP4CE115*. Range of bits which need to use for build cryptographically secure PRNG are identified. Shown for Q4.28 fixed-point arithmetic that the trajectory $x^{(1)}$, $x^{(2)}$, $x^{(3)}$ and $x^{(4)}$ uniformly and densely visited all points on 4-dimensional torus. Proposed and implemented a FPGA method of generating pseudorandom sequences. For

improving the safety of the method of generating pseudorandom sequences proposed to use a shift register and block XOR. The obtained sequences passed statistical tests NIST.

Future work will consist of integration of the proposed PRNG in modern communication protocols.

References

1. Oleg Garasym, Ren´e Lozi, Ina Taralova. Exploring some topologies of coupled chaotic networks. NOMA'15, International Workshop on Nonlinear Maps and their Applications, Jun 2015, Dublin, Ireland. pp. 34-39, 2016, Proceedings of NOMA'15, University College Dublin.

2. Krulikovskyi O.V., Haliuk S.D., Politanskyi L.F. // PRNG based on discrete hyper chaotic system // Sychashyi zakhyst informatsii. – 2016. – № 2. – PP. 69-77.

3. Ljupco Kocarev and Shiguo Lian (Eds.). Chaos-Based Cryptography Theory, Algorithms and Applications // Springer-Verlag Berlin Heidelberg, 397 pp., 2011.

4. Yuan G. and Yorke J. A. 2000 Collapsing of chaos in one dimensional maps Physica D: Nonlinear Phenomena 136 18-30.

5. Oleg Garasym, Ren´e Lozi, Ina Taralova. Robust PRNG based on homogeneously distributed chaotic dynamics. Journal of Physics: Conference Series, IOP Publishing, 2016, NOMA'15 International Workshop on Nonlinear Maps and Applications, 692, pp.012001.

6. Andrea Espinel Rojas, Ina Taralova, Ren´e Lozi. New alternate ring-coupled map for multirandom number generation. Journal of Nonlinear Systems and Applications, 2013, 4 (1), pp.64- 69.

7. Bernard Sklar, "Digital Communications: Fundamentals and Applications (2nd Edition)", Prentice Hall PT R, pp. 1079, January 21, 2001.

8. Fernando Corinto, Oleh V. Krulikovskyi, Serhii D. Haliuk // Memristor-based chaotic circuit for pseudo-random sequence generators, 18th Mediterranean Electrotechnical Conference MELECON 2016, Limassol, Cyprus, 18-20 April 2016", 2016, IEEE

9. Mohamed L. Barakat, Abhinav S. Mansingka, Ahmed Gomaa Ahmed Radwan, Khaled Nabil Salama, Chaos-based pseudo-random number generation, US 2014/0101217 A1, Pub. Date: Apr. 10, 2014.

10. National Institute of Standards and Technology, U.S Department of Commerce. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication 800-22, Revision 1a, April 2010.

Автор статті

Круліковський Олег Валерійович – аспірант кафедри радіотехніки та інформаційної безпеки. Чернівецький національний університет імені Юрія Федьковича. E-mail: o.krulikovskyi@chnu.edu.ua.

Галюк Сергій Дмитрович – кандидат технічних наук, доцент кафедри радіотехніки та інформаційної безпеки. Чернівецький національний університет імені Юрія Федьковича. Тел.: +380 (66) 148 79 45. E-mail: galiuk.serge@gmail.com.

Політанський Леонід Францович – доктор технічних наук, професор, завідувач кафедри радіотехніки та інформаційної безпеки. Чернівецький національний університет імені Юрія Федьковича. E-mail: rt-dpt@chnu.cv.ua

Author of the article

Krulikovskyi Oleh Valeriiovych – PhD student of radio engineering and information security department. Yuriy Fedkovych Chernivtsi National University. E-mail: o.krulikovskyi@chnu.edu.ua

Haliuk Serhii Dmytrovych – candidate of science (technic), assistant professor of radio engineering and information security department. Yuriy Fedkovych Chernivtsi National University. Tel.: +380 (66) 148 79 45. E-mail: galiuk.serge@gmail.com

Politanskyi Leonid Frantsovych – doctor of sciences (technical), professor, head of radio engineering and information security department. Yuriy Fedkovych Chernivtsi National University. E-mail: rt-dpt@chnu.cv.ua

Дата надходження
в редакцію: 25.10.2016 р.

Рецензент:
доктор технічних наук, професор В. Л. Бурячок
Державний університет телекомунікацій