декс.Директ / И. Цымбалист, А. Лысенко [Электронный ресурс]. – 2014. – 121 с. – (https://issuu.com/igorabdulaev/docs/).

8. Джейкобсон Х. Google AdWords и контекстная реклама для чайников / Х. Джейкобсон. – М. : Диалектика, ООО «ИД Вильямс», 2009. – 432 с.

References:

1. Cockrum J. *Free Marketing 101 Low and No-Cost Ways to Grow Your Business, Online and Off.* 4th ed. New York, Wiley Publ., 2011. 327 p. (Rus. ed.: Plostak L. *Internet-marketing: luchshie besplatnie instrumenti.* Moscow, Mann, Ivanov and Ferber Publ., 2013. 382 p.) (Rus.)
2. Babaev A., Evdokimov N., Ivanov A. *Contextnaya reklama* [Contextual advertising]. St. Peterburg, Piter Publ., 2011. 304 p. (Rus.)
3. Yakovlev A.A., Dovzhikov A. *Contextnaya reklama: Osnovy, secrety, tryuki* [Contextual advertising. Fundamentals, secrets, tricks]. St. Peterburg, Piter Publ., 2012. 246 p. (Rus.)
4. Alieva B., Basov A., Virin F., Grin'ko A. *Contextnaya reklama v Internete: Nastolnaya kniga reklamista* [Contextual advertising on the Internet. Handbook of the advertiser]. Moscow, Piter Publ., 2009. 223 p. (Rus.)
5. Tsarevsky F. *Jandeks.Direkt : kak poluchat' pribyl', a ne igrat' v lotereju* [Yandex.Direct: how to make a profit, not to play the lottery]. Moscow, Piter Publ., 2016. 223 p. (Rus.)
6. Smirnov V.V. *Pribilnaya contextnaya reklama. Bistriy sposob privlecheniya klientov s pomoshchiu Yandex.Direct* [Profitable contextual advertising. A quick way to attract customers through Yandex.Direct]. Moscow, Mann, Ivanov and Ferber Publ., 2013. 192 p. (Rus.)
7. Tsymbalist I., Lysenko A. *Poshagovyi plan zapuska pribilnoy contextnoy reklamy na Yandex.Direct* [A step-by-step plan for launching profitable contextual advertising on Yandex.Direct]. Available at: https://issuu.com/igorabdulaev/docs/ (accessed 13 September 2016). (Rus.)
8. Dzhejkobson H. Google AdWords i kontekstnaja reklama dlja chajnikov [Google AdWords and contextual advertising for dummies]. Moscow, Dialektika, Vil'jams, 2009. 432 p. (Rus.)

Рецензент: В.П. Гранкін
д-р ф.-м. наук, проф., ДВНЗ «ПДТУ»

Стаття надійшла 14.03.2017

УДК 004.056.55, 004.421.5

© Levitskaya T.O.[1], Ganzina D.I.[2]

DATA PROTECTION BY USING THE «CHUA'S CIRCUIT» CHAOS GENERATOR

This article focuses on the justification of the use of cryptosystems based on a mathematical model of the chaos generator (an electric circuit, showing modes of chaotic oscillations), proposed by Leon Chua in 1983. This article also describes the principles of implementation of cryptographic algorithm and its application prospects. Reviewed the next questions: the problems of widespread cryptosystems, the theory of cryptographically strong algorithms, absolutely and computationally secure ciphers, particular theoretical method for solving the problem of increasing the reliability of hybrid computational proof systems by inclusion of a mathematical model of chaos as a generator to encrypt transmitted data key. Here described the recommendations on the implementation of cryptographic system and requirements on the Chua's circuit generator chaos.

Keywords: *chaos generator, mathematical model, Chua circuit, encryption, cryptography, information security, deterministic chaos.*

[1] *PhD, SHEE «Priazovskyi State Technical University», Mariupol, tlevitiisys@gmail.com*
[2] *master, SHEE «Priazovskyi State Technical University», Mariupol, camaro406@rambler.ru*

Левицька Т.О., Ганзіна Д.І. Захист інформації з застосуванням генератору хаосу «схема Чуа». *Стаття присвячена обґрунтуванню застосування криптосистеми, заснованої на математичній моделі генератору хаосу (електричного кола, яке демонструє режими хаотичних коливань), запропонованого Леоном Чуа у 1983 році, опису принципів реалізації криптоалгоритму та перспективам його застосування. Розглянуто проблеми традиційних криптосистем, теорії криптостійкості, абсолютно і обчислювально стійкі шифри, окремий теоретичний метод вирішення питання збільшення криптостійкості гібридних обчислювально стійких систем за допомогою включення в них математичної моделі генератора хаосу в якості генератора ключа для шифрування даних, що передаються. Описано рекомендації та вимоги щодо реалізації криптосистеми на генераторі хаосу «схема Чуа».*

Ключові слова: *генератор хаосу, математична модель, схема Чуа, шифрування, криптографія, захист інформації, детермінований хаос.*

Левицкая Т.А., Ганзина Д.И. Защита информации с использованием генератора хаоса «схема Чуа». *Статья посвящена обоснованию применения криптосистемы, основанной на математической модели генератора хаоса (электрической цепи, демонстрирующей режимы хаотических колебаний), предложенного Леоном Чуа в 1983 году, описанию принципов реализации криптоалгоритма и перспективам его применения. Рассмотрены проблемы традиционных криптосистем, теории криптостойкости, абсолютно и вычислительно стойкие шифры, частный теоретический метод решения вопроса увеличения криптостойкости гибридных вычислительно стойких систем с помощью включения в них математической модели генератора хаоса в качестве генератора ключа для зашифровки передаваемых данных. Описаны рекомендации и требования по реализации криптосистемы на генераторе хаоса «схема Чуа».*

Ключевые слова: *генератор хаоса, математическая модель, схема Чуа, шифрование, криптография, защита информации, детерминированный хаос.*

Formulation of the problem. Protection of information from violation of its confidentiality, integrity, and accessibility is one of the most important problems of the current time when technical means used for data transferring are subjected to intruder’s attack or the environment influence. Encryption is one of the methods of protecting transmitted data from attacks and unpredictability of the environment. Data encryption allows you to confirm their integrity, ensure confidentiality and availability of information for the ultimate recipient [1].

Modern cryptography is characterized by open encryption algorithms that involve the use of computing tools. In this case, there is a key of a certain length and a set of relatively simple transformations, the so-called cryptographic primitives, such as bit shift, XOR cipher, etc. [2]. However, due to the nature of these cryptosystems, there are a large number of methods for deciphering the information encoded by them.

Analysis of recent researches and publications. One of the main problems of traditional cryptosystems is that, in the end, the operations sequence of information stream encryption repeats itself (the length of the key is limited), and this leads to the fact that the sequence may be disclosed by a third party, and the stream can be decrypted. This defect is completely absent in ciphers, satisfying a number of the following requirements [3]:

– the key is generated for each block of encrypted data (each key is used only once);

– the key is statistically reliable (the probability of occurrence of each of the possible symbols are equal, the symbols in the key sequence are independent and random);

– the length of the key is equal to or greater than the length of the encrypted data;

– the original (open) text has some redundancy (which is the criterion for evaluating the correctness of the decryption).

The persistence of these systems does not depend on the computing capabilities of the cryptanalyst. However, the practical application of absolutely stable systems is limited due to the complexity and cost of their implementation, therefore in cryptographic systems, computationally stable systems are the most common. A computationally stable system is a system with the potential to open a cipher, but only with the chosen parameters and encryption keys. The persistence of such systems depends on the computing capabilities of the cryptanalyst [4].

The use of chaos generators that have complex, unpredictable and highly dependent on the initial parameters behavior, as part of a computationally robust hybrid cryptosystem, can significantly improve the cryptographic strength of the cipher.

The idea of using chaos generators in signal transmission is not new. Experiments on encrypting and deciphering signals by such methods, conducted in the 90s of the 20th century, showed the prospects, attractiveness and efficiency of using chaotic generators in confidential communication systems [5].

The objective of the article is to justify the creation of a cryptosystem based on the mathematical model of the chaos oscillator (an electrical circuit demonstrating chaotic oscillation modes), proposed by Leon Chua in 1983 [6], and a description of the prospects for its application.

Statement of the main material. Cryptosystems on chaos generators have a number of advantages over symmetric systems and systems with a public key (when encrypting information are used in the form of hybrid cryptosystems), the main problem of which, as already mentioned, is the key length, and as a result its repeatability. The length of the key obtained with the help of the chaos generator is practically unlimited, and since the same chaotic generator can create completely different processes with a slight change in the initial conditions, it is much more difficult to determine the structure of the generator and to predict the process for a long time [7], which makes it possible to create a burglary-resistant system with a high level of reliability.

The future use of chaos generators, in particular the Chua's circuit, which will be discussed below, in order to protect the transmitted information, consists of three features of chaotic processes [7]:

– a chaotic signal has a non-periodic, continuous spectrum occupying a sufficiently wide band, and its appearance can be specified;

– the irregularity and unpredictability of the behavior of the chaotic signal, as well as the ability of the chaos generator to create completely different processes with a very slight change in the initial conditions, significantly complicates the prediction of the process for a long time;

– because of the irregularity of chaotic signals, their autocorrelation function rapidly damps, which also complicates the prediction of the generation process and the determination of the structure of the generator.

Due to the fact that the Chua scheme is one of the simplest chaos generators (described by only three differential equations and at the same time possesses quite complex behavior peculiar to chaos oscillators), it was chosen for the information encryption system.

As shown in Figure 1, the Chua's circuit consists of two capacitors, one inductor, a linear resistor, and a nonlinear resistor with a negative resistance (commonly called the Chua diode), which in reality can be represented by the complication of a circuit based on operational amplifiers, inverters or using a tunnel diode [6].

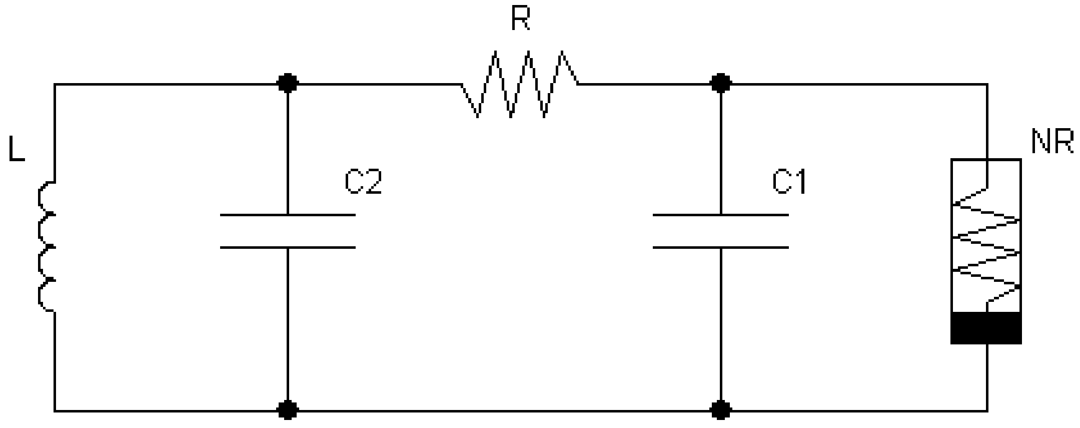

Fig. 1 – Chua Chain. L, R, C1, C2 - passive elements, NR - nonlinear resistance (Chua diode)

The Chua's circuit is described by the following system of equations [6]:

$$\begin{cases} C_1 \dfrac{dv_{C_1}}{dt} = G\left(v_{C_2} - v_{C_1}\right) - g\left(v_{C_1}\right) \\ C_2 \dfrac{dv_{C_2}}{dt} = G\left(v_{C_1} - v_{C_2}\right) - i_L \\ L\dfrac{di_L}{dt} = -v_{C_2} \end{cases}, \quad (1)$$

where $g\left(v_{C_1}\right)$ – piecewise linear function, defined as:

$$g\left(v_{C_1}\right) = G_b v_{C_1} + \frac{1}{2}\left(G_a - G_b\right)\left(\left|v_{C_1} + E\right| - \left|v_{C_1} - E\right|\right). \quad (2)$$

After replacing the coefficients in the system of equations by dimensionless, the system takes the following form [6]:

$$\begin{cases} \dfrac{dx}{dt} = a\left(y - x - h(x)\right) \\ \dfrac{dy}{dt} = x - y + z \\ \dfrac{dz}{dt} = -\beta y \end{cases}, \quad (3)$$

where $h(x)$ defined as:

$$h(x) = m_1 x + \frac{1}{2}\left(m_0 - m_1\right)\left(|x+1| - |x-1|\right). \quad (4)$$

The numerical solution of these equations shows that for certain relations between the components of the chain, the change in the values of the variables in time acquires a chaotic character, a strange attractor in the form of «double scroll» appears, shown in Figure 2 (the case of a model with dimensionless coefficients) [8].

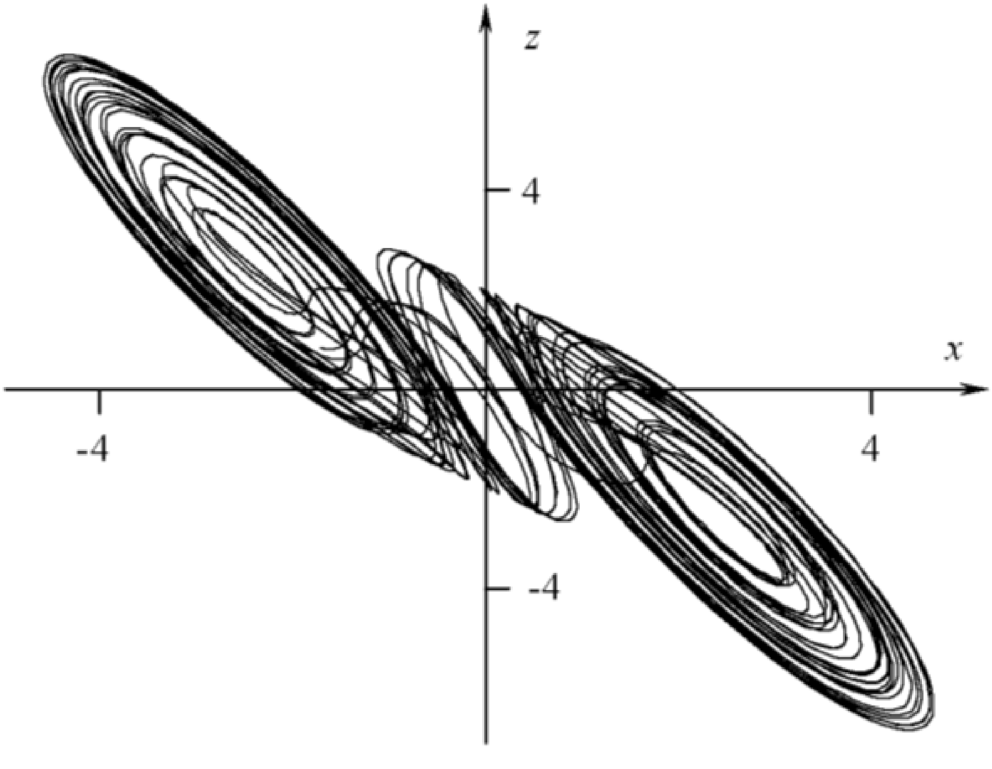

Fig. 2 – Attractor in the form of «double scroll»

The trajectory of such an attractor is non-periodic and the mode of operation is unstable, as a result even small deviations of the parameters cause significant changes. The result of this behavior is the non-periodicity in time of any of the coordinates of the system, the continuous spectrum and the autocorrelation function that decreases in time [9]. This causes chaotic dynamics of strange attractors, namely, it indicates that the prediction of the trajectory trapped in the attractor is difficult, because a small inaccuracy in the initial data after some time can lead to a strong discrepancy of the forecast with a real trajectory.

Figure 3 shows one of the possible time dependences of the change in the value of x for a model with dimensionless coefficients [8].

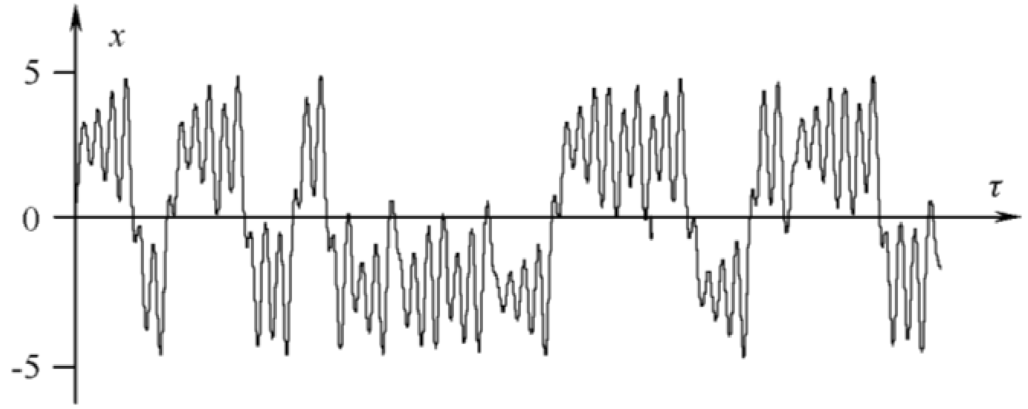

Fig. 3 – Time dependence of the change in *x*

The time dependence of the change in *x* is one of the parameters that can be used in a cryptosystem for encrypting transmitted information, for example, by imposing a chaotic signal on the information, XOR cipher. In general, encryption can be performed using several algorithms [5]:

– chaotic masking - the information signal is added together with a chaotic signal;

– switching modes - logical zero is encoded by one type of chaotic signal (for example, the received value of *x*), logical unit - by another (for example, the value of *y*);

– non-linear mixing - the information signal participates in the formation of the chaotic signal itself.

In the case of the first two algorithms, it is assumed that the parameters for starting the key generation by the cryptosystem are chosen randomly to ensure the uniqueness of the key for each block of encrypted data. This implies the need for the safe transfer of these data to the receiving side for synchronization of the generators.

The solution of the problem of transferring the start parameters of key generation (time parameter *t*, parameters of virtual capacitors *x*, *y* and inductance *z* or one of the mentioned parameters) assumes the use of asynchronous encryption algorithms effective and reliable for these purposes due to the small length of the transmitted parameters.

In the case of nonlinear intermixing, it is possible to partially refuse to transmit the synchronization parameters of the generators, for example, transmit only the parameter that was not used to encrypt the data block. Nonlinear mixing and chaotic masking can be optimally used to encrypt data presented in a bit-like form, in order to compress them, because The bit-zero missing during the decryption process will be easily detected due to the continuity of the generator function. However, the features of data compression are not within the scope of this article.

You can use a mixture of the above encryption algorithms.

It is necessary to take into account the probability of reversal of the parameter superimposed on the information signal, to zero or getting a zero as a result of nonlinear mixing. Depending on the implementation of the mathematical model of the Chua's circuit and the encryption algorithm, there is a possibility of reversing the encrypted data fragment to zero, which can lead to data loss.

Application of algorithms of asynchronous encryption defines this system as a hybrid cryptosystem and allows using the best features of both methods of information protection, asynchronous encryption and encryption on the chaos generator.

The system can be used to encrypt any kind of information.

Based on the analysis described above, a software module that was used in the transmission system of encrypted text messages was developed and implemented. The sequence diagram of the «Read message» variant of this system is shown in Figure 4.

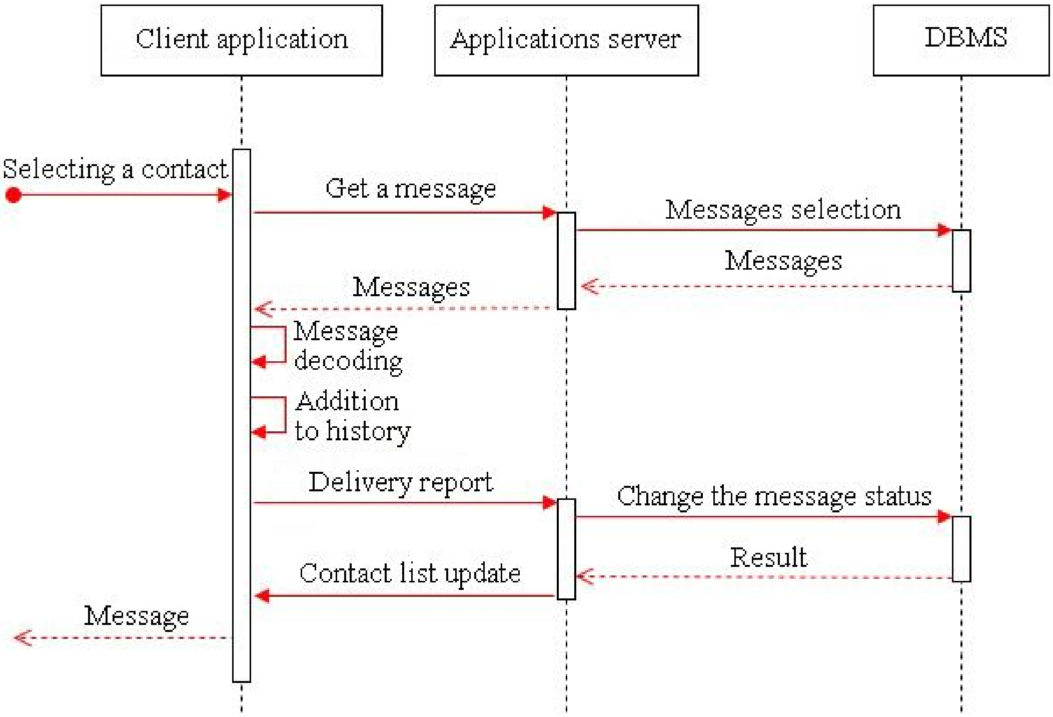

Figure 4 – Sequence diagram for use case «Read message»

As can be seen from the sequence diagram, the cryptosystem module was included in the client application. The application server and DBMS are not involved in the process of encrypting and decrypting messages and are used only to provide communication and data transfer between clients.

Due to the use of chaotic masking algorithm based on the exclusive XOR [10] operation, the same function was used for encryption and decryption. XOR allows you both to mix the key to the data, and to remove it without changes in the code (in contrast to, for example, the addition operation AND, which requires further subtraction to restore the original message).

Synchronization of client application cryptosystems is performed using a session key (in this case, the time parameter *t* of the chaos generator) transmitted using the asymmetric encryption method.

Conclusions

The review of literature data, analysis of publications and studies shows the prospects of creating and using cryptosystems on chaos generators, in particular, based on the Chua's circuit. This scheme has typical for chaos generators behavior and properties in combination with relative ease of implementation. Based on the theory of cryptographic strength of ciphers, systems on chaos generators are the closest to absolutely stable, because the length of the key can significantly exceed the length of the message and the uniqueness of its sequence is also high.

Based on the analysis carried out, recommendations on the creation of cryptosystems using chaos generators were proposed and justified, and a cryptosystem module used in the transmission system of encrypted messages was developed.

The tasks of further research are the improvement of the existing cryptosystem, including the modification and improvement of the mathematical model of the generator used.

Список использованных источников:

1. Мао В. Современная криптография: Теория и практика. – М. : Вильямс, 2005. – 768 с.
2. Баричев С.Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. – М. : Горячая линия-Телеком, 2002. – 175 с.

3. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон; под ред. Р.Л. Добрушина и О.Б. Лупанова. – М. : Изд-во иностранной литературы, 1963. – 829 с.
4. Фергюсон Н. Практическая криптография / Н. Фергюсон, Б. Шнайер; пер. с англ. Н.Н. Селиной, под ред. А.В. Журавлёва. – М.; СПб.; К. : Диалектика, 2005. – 421 с.
5. Агуреев К.И. Применение детерминированного хаоса для передачи информации / К.И. Агуреев // Известия Тульского государственного университета. Технические науки. – 2014. – № 11. – С. 197-212.
6. Кузнецов А.П. Наглядные образы хаоса / А.П. Кузнецов // Соросовский образовательный журнал. – 2000. – № 11. – С. 104-110.
7. Когай Г.Д. Методы и модели хаотических процессов в системах связи / Г.Д. Когай, Т.Л. Тен // Современные наукоемкие технологии. – 2014. – № 10 – С. 61-64.
8. Бугаевский М.Ю. Исследование поведения цепи Чуа : Учебно-методическое пособие / М.Ю. Бугаевский, В.И. Пономаренко. – Саратов : Издательство ГосУНЦ «Колледж», 1998. – 29 с.
9. Городецкий А.С. Минимальные аттракторы и частично гиперболические множества динамических систем : автореф. дис. …канд. физ.-мат. наук : 01.01.02 / А.С. Городецкий; Моск. гос. ун-т им. М.В. Ломоносова. – М., 2001. – 11 с.
10. Белоусов А. Алгебра логики и цифровые компьютеры / А. Белоусов [Электронный ресурс] // ALGLIB. – (http://alglib.sources.ru/articles/logic.php/).

References:

1. Mao B. *Sovremennaia kriptografiia: Teoriia i praktika* [Modern Cryptography: Theory and Practice]. Moscow, Vil'iams Publ., 2005. 768 p. (Rus.)
2. Barichev S.G., Goncharov V.V., Serov R.E. *Osnovy sovremennoi kriptografii* [Fundamentals of modern cryptography]. Moscow, Hotline-Telecom Publ., 2002. 175 p. (Rus.)
3. Shennon K. *Raboty po teorii informatsii i kibernetike* [Work on the theory of information and cybernetics]. Moscow, Publishing House of Foreign Literature, 1963. 829 p. (Rus.)
4. Ferguson N., Schneier B. *Practical Cryptography*. Indianapolis, Wiley Publ., 2003. 432 p. (Rus. Ed.: Selina N.N., Zhuravlev A.V., Fergiuson N., Shnaier B. *Prakticheskaia kriptografiia*. Moscow, Dialectika Publ., 2004. 432 p.). (Rus.)
5. Agureev K.I. Primenenie determinirovannogo khaosa dlia peredachi informatsii [Application of deterministic chaos to transmit information]. *Izvestiia Tul'skogo gosudarstvennogo universiteta. Tekhnicheskie nauki – The Tula State University news. Technical science*, 2014, no. 11, pp. 197-212. (Rus.)
6. Kuznetsov A.P. Nagliadnye obrazy khaosa [Visual chaos]. *Sorosovskii obrazovatel'nyi zhurnal – Sorosov Educational Journal*, 2000, no. 11, pp. 104-110. (Rus.)
7. Kogay G.D., Ten T.L. Metody i modeli khaoticheskikh protsessov v sistemakh sviazi [Methods and models of random processes in communication]. *Sovremennye naukoemkie tekhnologii – Modern high technologies*, 2014, no. 10, pp. 61-64. (Rus.)
8. Bugaevskiy M.Y., Ponomarenko V.I. *Issledovanie povedeniia tsepi Chua. Uchebno-metodicheskoe posobie* [Study of the behavior of Chua’s circuit. Training handbook]. Saratov, College GosUNTs Publ., 1998. 29 p. (Rus.)
9. Gorodetski A.S. *Minimal'nye attraktory i chastichno giperbolicheskie mnozhestva dinamicheskikh sistem.* Avtoref. diss. kand. f.-m. nauk [Minimum attractors and partially hyperbolic sets of dynamical systems. Thesis of cand. phys.-math. sci. diss.]. Moscow State University, 2001. 77 p. (Rus.)
10. Belousov A. *Algebra logiki i tsifrovye komp'iutery* (Logic algebra and digital computers) Available at: http://alglib.sources.ru/articles/logic.php/ (accessed 13 April 2017). (Rus.)

Reviewer: V.P. Grankin
Doctor of Physical and Mathematical Sciences, Professor, SHEE «PSTU»

Received 10.04.2017