THEORY AND METHODS OF SIGNAL PROCESSING

UDC 681.51:519.7(045)
DOI:10.18372/1990-5548.53.12137

[1]V. V. Kyrychenko,
[2]Ye. V. Lesina

APPLICATION OF DYNAMIC SYSTEMS FOR ENCODING DATA IN TELECOMMUNICATION CHANNELS

[1]Aircraft Control Systems Department, National Aviation University, Kyiv, Ukraine
[2]Department of Automatic and Telecommunications, Donetsk National Technical University, Pokrovsk, Ukraine
E-mails: [1]vkir28@gmail.com, [2]lesina17@gmail.com

***Abstract*—*At present, dynamical systems with chaotic behavior are intensively investigated with different points of view, and the areas of their application are unusually wide. In particular, ideas of constructing cryptographic systems based on them appear. Dynamic chaotic systems in their implementation in microprocessor systems, because of the discreteness of the functioning of the latter, are replaced by discrete models. At this paper considered one of possible variants of such modeling, when a continuous system is replaced by a finite automaton with sufficiently large input, internal and output alphabets. Here we consider the features of implementation in microprocessor-based systems of coding algorithms based on the above systems.*

Index Terms—Finite automaton; invertible dynamic systems; finite-dimensional ring of integers; generators of pseudo-random sequences.

I. INTRODUCTION

Recently, a new direction in cryptology is being formed, which is associated with the use of dynamic systems with chaotic behavior. One of the main approaches to this area is based on the use of inverse control systems for constructing cryptographic algorithms [1], [2].

Dynamic systems with chaotic behavior are now intensively implemented and used in various fields, in particular, for cryptographic protection of information [3]. On the basis of such systems, pseudo-random sequence generators can be constructed, which are subsequently used to encode plaintext. On the other hand, any dynamic system having an input-output structure can be used directly for data conversion [4]. On the basis of such systems, an encoder is created. The input to the system is a digitized message, and the output is an encrypted signal sent to telecommunication network. A necessary condition for single-valued decoding is the existence of the inverse system.

Nowadays, a significant amount of dynamic systems generating chaotic signals are proposed and researched. "Minimal" chaotic generators are described by only three ordinary differential equations, and at least some of them are generators constructed by adding one or several elements into standard oscillators of regular oscillations. Other sources of chaos are not so easily associated with traditional electronic generators, but they can also be realized with the help of a modern element base either in circuitry, or in the form of an analog integrated circuit, or based on digital signal processors [5]. Examples of sources of chaos with one and a half degrees of freedom are the Ressler system, the Chua chain [6], the Lorentz system [7]. Chaos generators can be implemented on the basis of these models, just as it is done with generators closer in appearance to traditional ones. The choice of the model and its implementation is determined by the specific task that requires (or can require) the specific parameters to the source of chaos.

II. PROBLEM STATEMENT

Computation systems with limited accuracy can be performed by transforming differential equations to finite-difference equations. If, because of the finite digit capacity of any computer limit the finite number of values of all parameters and variables entering the initial system, then the resulting system of equations can be considered as a description of some finite automaton.

The finite state machine is understood as the five objects $A=(S,X,Y,\delta,\lambda)$, where S are (finite) states set; X is the (finite) input alphabet; Y is the (finite) output alphabet, $\delta: S\times X\to S$ is the converting function, $\lambda: S\times X\to Y$ is the output function.

The conversion from differential equations to their finite-difference equations analogs leads to equations in which there are 4 arithmetic operations.

The finiteness of the number of values involved in these quantities (due to the above considerations) and the need to save forms of equations, which reflects the relationships between these quantities make it natural to consider these equations as equations in finite fields (or, in simpler situations, in finite rings).

Let's suppose that the transmitter is a discrete dynamic system, right parts of which depend on the vector function u – digitized information message (system input):

$$x(k+1) = f\left(x(k), u(k)\right), \quad x(0) = x_0, \qquad (1)$$

$$y(k) = h\left(x(k)\right), \qquad (2)$$

where $x(k) \in R^n$, $u(k) \in R^m$, $y(k) \in R^p$ determine the state vectors of the system, its input and output, respectively. By communication channels transmitted the output signal – a function $y(k)$ dependent on the state of the system, which, in turn, depends on the parameters of the system (1) and the respond $u(k)$. To construct equations describing the dynamics of the receiving device, we consider the problem of determining the conditions under which the values of the input impact $u(k)$ can be reconstructed from the values of the output function $y(k)$.

Many theoretical and practical problems of control theory which are associated with the definition of the state and parameters of the system (1), the construction of stabilizing feedbacks, are leading to inversing this representation. One of the ways of such inversing can be realized with the help of the reverse system, i.e. system of input-output, in which the input serves information about $y(k)$ on a certain interval, and the output is the function $u(k)$.

Let us consider such a transformation with the example of a system n of non-linear differential equations of the first order:

$$\dot{x}_k = \sum_{i=1}^{n}\sum_{j=1}^{n} A_{i,j}^k x_i x_j + \sum_{i=1}^{n} B_i^k x_i, \quad k = (\overline{1,n}). \qquad (3)$$

Here the matrices A^k, $k = \overline{1,n}$ have dimension $n \times n$ and define nonlinear part of the system. The vectors $B^k(b_1^k, \ldots, b_n^k)$, $k = \overline{1,n}$ – are responsible for its linear terms. If all the coefficients of the matrices $A^k, k = \overline{1,n}$ are zero, then the system (3) becomes linear. Its solution can be written analytically, and the trajectories have a regular or periodic character. If at least one of the matrix coefficients, $A^k, k = \overline{1,n}$ is nonzero, then nonlinearity appears in the system. Such systems have both regular and stochastic trajectories, which considerably complicates, or even and makes their analytical investigation impossible. This fact, taking into account the simplicity of the structure of such systems, is widely used for the realization of various data protection systems.

Because of the lack of accurate methods for solving general nonlinear dynamical systems, numerical methods are often used to analyze the structure of an attractor, such as, for example, the combination of the explicit Euler scheme with the central difference Adams scheme, the use of higher derivatives, and also the fourth-order Runge–Kutta method. In the case of classical values of the parameters of the system, the instability of its solutions is observed, since the equilibrium positions of the system have a saddle type. This limits the application of these methods, since a general error increases with increasing integration interval. Thus, small changes in the initial conditions of the system (3) can lead to significant consequences over time. This property of the system allows it to be used for reliable information protection.

Let's consider the data transformation problem using the system (3). To do this, let's change the $\hat{k}$ th equation (here $\hat{k}$ – fixed number $1 \le k \le n$), adding the input signal $u(t)$, and the output signal is $y(t)$, as a result of which the $\hat{k}$ th equation acquires the form:

$$\dot{x}_{\hat{k}} = \sum_{i=1}^{n}\sum_{j=1}^{n} A_{i,j}^{\hat{k}} x_i x_j + \sum_{i=1}^{n} B_i^{\hat{k}} x_i + au.$$

Discretization with step h leads to equations which have such modified form:

$$\begin{aligned} & x_k(t+1) = x_k(t) \\ & +h\left(\sum_{i=1}^{n}\sum_{j=1}^{n} A_{i,j}^k x_i(t) x_j(t) + \sum_{i=1}^{n} B_i^k x_i(t) \right), \\ & \left(x_{\hat{k}}(t+1) - x_{\hat{k}}(t)\right)/h \\ & = \sum_{i=1}^{n}\sum_{j=1}^{n} A_{i,j}^{\hat{k}} x_i(t) x_j(t) + \sum_{i=1}^{n} B_i^{\hat{k}} x_i(t) + au(t), \\ & k = \left(\overline{1,\hat{k}-1}, \overline{\hat{k}+1,n}\right). \end{aligned} \qquad (4)$$

The output $y(t)$ is described by the equation

$$y(t) = x_{\hat{k}}(t+1).$$

In the reverse system, the input and output symbols are reversed, that is, the input of the inverse system is $y(t)$, and the output is – $u(t)$. It contains the same equations for $k = \left(\overline{1,\hat{k}-1}, \overline{\hat{k}+1,n}\right)$, and $\hat{k}$ th is replaced, respectively, by the following:

$$x_{\hat{k}}(t+1) = y(t),$$

$$u(t)=\frac{1}{a}\left(\frac{x_{\hat{k}}(t+1)-x_{\hat{k}}(t)}{h}-\sum_{i=1}^{n}\sum_{j=1}^{n}A_{i,j}^{\hat{k}}x_i(t)x_j(t)-\sum_{i=1}^{n}B_i^{\hat{k}}x_i(t)\right).$$

The automaton described by equations (4) is called a direct automaton $L(A,B,a,h),$, and the inverse automaton $L^{-1}(A,B,a,h$ which is corresponding to the inverse system.

Since it is usually a question of data processing by the microcontroller, they are represented by a sequence of bits, larger units – bytes or multiple bytes. In this case, the number of different elements described by all possible combinations of values of individual bits is $2^m=q,$ where $m=8k, k\in N.$ Therefore, corresponding calculations can be performed either in the ring $Z_q,$ or in the field $GF(2^m).$

III. The Particularity of the Implementation of the Encryption Algorithm

For study the properties of encryption algorithms using a system of the form (4), the authors of the work implemented a set of programs in the programming language C++. The system (3) was used with the following non-zero parameters: $A_{22}^1=p_1,$ $A_{13}^2=q_1,$ $A_{12}^3=r_1,$ $B_3^1=p_2,$ $B_1^2=q_2,$ $B_1^3=r_2,$ $B_2^3=r_3.$ In this case, the system (4) with sampling rate $h=1$ and with operations in the ring of integers Z_m can be presented in the form

$$\begin{cases} x_1(t+1)=x_1(t) \\ \qquad -x_2^2(t)+p\cdot x_3(t) \mod 2^m, \\ x_2(t+1)=x_2(t)+x_1(t)x_3(t) \\ \qquad -q\cdot x_1(t)+u(t) \mod 2^m, \\ x_3(t+1)=x_3(t)+r_1\cdot x_1(t) \\ \quad +r_2\cdot x_2(t)-x_1(t)x_2(t) \mod 2^m. \end{cases} \tag{5}$$

Here, $u(t)$ is the input signal, $x_2(t)$ is the encoded signal, which is transmitted on the data transfer channel. The parameters $key=(p,q,r_1,r_2)$ and the initial conditions $x^{in}=\left(x_1(0),x_2(0),x_3(0)\right)$ of the system, that uniquely determine the output signal form the key to the encryption system. Thus, the direct automaton $L(key,x^{in})$ determines the encryption system or the transmitter system.

The receiving system receives the encrypted signal and, with the help of the reverse automaton $L^{-1}(key,x^{in})$, decodes it to the original one. For both the operation of encoding and the operation of decoding the same key is required. Even a slight violation of its structure in at least one node will lead to impossibility of correct restoration of the transmitted signal.

To restore the signal, we must use the following system:

$$\begin{cases} x_1(t+1)=x_1(t)-x_2^2(t) \\ \qquad +p\cdot x_3(t) \mod 2^m, \\ u(t)=x_2(t+1)-x_2(t) \\ \quad -x_1(t)x_3(t)+q\cdot x_1(t) \mod 2^m, \\ x_3(t+1)=x_3(t)+r_1\cdot x_1(t) \\ \quad +r_2\cdot x_2(t)-x_1(t)x_2(t) \mod 2^m. \end{cases} \tag{6}$$

As a result of the tests performed using this complex, we meet the following problems and peculiarities of algorithms implementation are encryption.

For *demonstration*, usually the encryption algorithm is implemented by one of the following schemes.

Encrypting a text array occurs according to the following scheme:

Input Text → Symbol → Ascii Cod → $L(key,x^{in})$ →
→ ASCII Cod → Symbol → Output Text .

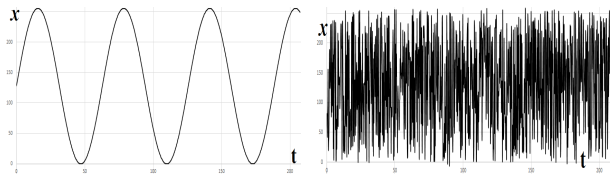
The input signal is a text message. One iteration considered as one symbol of the text. From the table of ASCII text codes (or another), the code corresponding to this symbol is taken, which is converted to another value by the direct automaton $L(key,x^{in})$. The automaton uses the specified key. The resulting value is converted to a text symbol using a symbol table. Thus, a new message is formed from the text symbols, which is an encrypted signal. Decoding is performed on the same principle, only the reverse automaton is used, and as the input text – the encrypted signal. The following is a source code, encrypted and decrypted. If the encrypted and decrypted are the same, then the algorithm works correctly. An essential disadvantage of this method is that according to the type of the encrypted signal nothing can be said about the effectiveness of such an algorithm.

Encryption of a numeric array. To demonstrate the operation of the algorithm a sequence of numbers of a special kind is generated (it also describes an analog signal). After this the sequence is transformed with the help of a direct automaton:

Input Decimal Array → Number → $L(key,x^{in})$ →
→ Number → Output Decimal Array .

In this case, the sequences are conveniently displayed graphically. Figure 1 shows a graph of an

analog signal that is periodic. And also the encrypted signal with the help of direct automaton described by the system (5).



(a) (b)

Fig. 1. Encryption of a periodic signal: (a) the original; (b) the encrypted

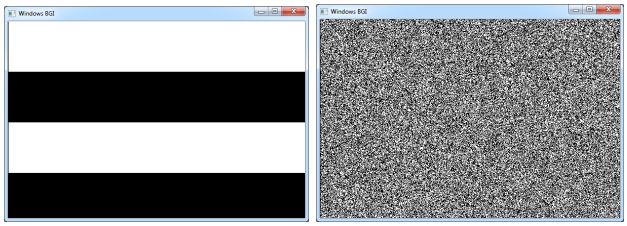
Here t is the time during which the signal is transmitted, x is its amplitude. The graph in Figure 1b shows the randomness of the encrypted signal. Thus, we can conclude that the proposed algorithm works quite effectively. However, for deeper analysis it is necessary to conduct statistical tests.

Binary stream encryption. Working with logical schemes that are used both in telecommunication and computer systems, often leads to the alphabet {0, 1}. Therefore, the urgent issue is the creation of a binary cryptosystem. In this case, the bitstream is encrypted. At each iteration, the sequence of k bits is read, which is then converted to a decimal number in the interval $[0, 2^k)$. With the help of a direct automaton the number is converted to another, and then, in turn, into a binary bit sequence. Thus, appears a new binary sequence of encrypted data:

$$\boxed{\text{Input Binary Array}} \rightarrow \boxed{k \text{ bits}} \rightarrow \text{Number } [0,2^k)$$
$$\rightarrow \boxed{L(key, x^{in})} \rightarrow \text{Number } [0,2^k) \rightarrow$$
$$\rightarrow \boxed{k \text{ bits}} \rightarrow \boxed{\text{Output Binary Array.}}$$

For visualization, the authors used binary sequences cards. Those, the construction of a graphic area of pixels in which each pixel corresponds to a specific bit of the stream. And if bit is set to 1, then the pixel is white, if the bit is set to 0, then the bit is black. Figure 2 shows the result of encryption of a periodic binary stream using system (5).

Figure 2b shows that the bits are distributed uniformly, which means that the resulting sequence is random and the investigator algorithm works quite efficiently.



(a) (b)

Fig. 2. Bit sequence map: (a) the original; (b) the encrypted

This method of visualization allows you to see the uniformity or non-uniformity of bits distribution, which makes it possible to draw conclusions about the randomness of the resulting sequence.

To prove the effectiveness of the encryption algorithm, a set of methods for determining the proximity measure is used on the given pseudo-random sequence to a random sequence. As such a measure is usually taken the presence of a uniform distribution, a large period, equal frequency of occurrence of identical substrings, etc.

One of the most obvious tests is a test for uniform distribution of the frequency of occurrence of each symbol. Let $\xi_0, \xi_1, \ldots, \xi_{255}$ be a sequence of different bytes of dimension $m = 256$. Further the frequency of occurrence of each byte in the binary array under the test is considered. Figure 3 shows the result of a frequency test. For that, a binary stream with the length 300000 was generated and converted using system (5). The graph shows the frequency of occurrence of each byte in the received sequence.

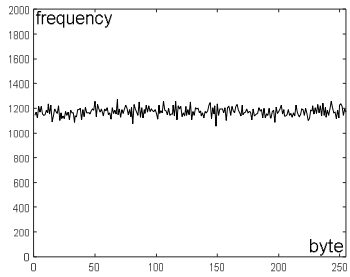


Fig. 3. Results of the frequency test

The frequency test shows that each byte occurs in sequence approximately equal number of times, which indicates a uniform distribution of symbols in the encrypted sequence. For the estimation of randomness of a number sequence exist tests that allow us to evaluate how much the random number generator is "similar" or "unlike" an ideal random sequence. Such tests can be divided into two groups.

Graphical tests, results of which are displayed in the form of graphs which characterize the properties of the sequence which is being examined. Results of such tests are interpreted by a person, so conclusions can be ambiguous on their basis.

The second group is statistical tests, which give us a numerical characteristics of the sequence and allow to say whether the test is passed. To assess the operation of the encryption algorithm on the basis of the system (5), the authors used the packet of statistical tests NIST. It consists of 15 statistical tests, the purpose of which is to determine the randomness of binary sequences generated by either hardware or software random number generators. These tests are based on various statistical properties inherent only

by random sequences. Most of the tests were passed, or showed an acceptable result, which indicates the high efficiency of the algorithm being investigated. Specific results and their analysis are planned to be published in a separate article.

The problem of the correct implementation of operations in the ring of integers. During the programming of calculations on the microcontroller a modular algebra is used. Those, all calculations are performed in a finite residue ring with respect to some natural modulus m, the value of which depends on the system capacity. However, when implementing such calculations by means of standard mathematical operations, the following problem arises. The principle of work of the function of the modular arithmetic functions is the following: to the operands applied corresponding ordinary (non-modular) function, and then the result is divided with the residue on the module. In this case, the size of the intermediate results can reach 2MAX bits from the input data, and in the case of subtraction, negative numbers may appear, which is not is permissible. This situation is called overflow and it causes the loss of significant digits. For example, to implement an automaton with an 8-bit input and an 8-bit output, a 16-bit controller is needed. So, even on modern 64-bit systems, no more than 32-bit data can be processed. The mechanism of processing such situations is impossible to be realized in the decimal system without the use of huge processor resources, which makes the work of such an algorithm very inefficient. At the program complex for implementing and testing the encryption algorithm, the authors implemented an automaton, the input and output of which are binary arrays, and all intermediate results have the same rank as all other data. The algorithm works on the following scheme.

$$\boxed{\text{Input Binary Array}} \rightarrow \boxed{k \text{ bits}} \rightarrow \boxed{L(key, x^{in})}$$
$$\rightarrow \boxed{k \text{ bits}} \rightarrow \boxed{\text{Output Binary Array.}}$$

This approach makes it possible for algorithm not to depend on the controller capacity, but it would still depend on the size of the buffer memory.

Another problem of the data protection algorithm is *the problem of interference and distortion in the encrypted signal*. When transmitting an encrypted signal through communication channels, especially over radio channels, there may be interference and data distortion, which makes it impossible to recover such data using the inverse automaton. In this case, two problems arise: to determine that in there are distortions and to describe the operation of the algorithm in the presence of distorted data. These tasks are planned to be investigated by the authors in future works.

When encrypting a binary stream, k bits are read sequentially, then they are converted by direct automaton. If the length of such a stream is not a multiple of k, then before the last step there will be several bits less than k. The following *problem with the last values arises*: how to process them? For example, the missing bits can be filled with zeros and the k bits received in this way can be transferred to the machine. However, how can this be used for unauthorized access to data during cryptanalysis of the system?

IV. Conclusions

Any managed dynamic system having an input-output structure, can be used directly to convert information. The idea of application of reverse control systems with complex behavior of trajectories lies at the heart of the task of synthesizing new effective algorithms for protecting information, primarily from unauthorized access.

In this article we propose a method of encryption using dynamical nonlinear systems. As such systems, was used the Lorentz system, as well as the system proposed by the authors. With the encryption-decryption program, a number of experiments were performed to transform the data, as a result of which a number of problems related to the implementation of the algorithm in microprocessor systems were identified. Considered the transition from continuous time to discrete for dynamical systems of general form. Their discrete analogues are recorded, and an example of encryption of binary data using these systems is given.

References

[1] V.V. Kirichenko, “Information security of communication channel with UAV,” *Electronics and control systems*, no. 3 (45), pp. 23–27, 2015.

[2] V.V.Kirichenko and Ye.V. Lesina, “Features of information UAV control system,” *Scientific works of Donetsk National Technical University, series: "Informatics, Cybernetics and Computer Science,"* no. 1 (22), pp. 111–116, 2016.

[3] A.M. Kovalev, V.A. Kozlovsky, and V.F. Scsherbak, “Reversible dynamical systems with variable dimensionality of phase space in problems of cryptographic information transformation,” *Applied Discrete Mathematics*, no. 2(2), pp. 39–44, 2008.

[4] Henk C.A. van Tilborg, *Fundamentals of cryptology*. Kluwer Academic publishers, 1988, 470 p.

[5] A.S. Dmitriev and A.I. Panas, *Dynamic chaos. New media for communication systems*. Moscow, Fizmatlit, 2002, 252 p.

[6] M.J. Sobhy and A. Shehata. “Secure computer communication using haotic algorithms,” *Int. J. of Bifurcation and Chaos*, vol. 10, no. 12, pp. 2831–2839, 2000.

[7] E. Lorenz, “Deterministic nonperiodic flow,” *J. of the Atmospheric Sciences*, 20 (2), pp. 130–141, 1963.

Received February 17, 2017

Kyrychenko Viktor. Candidate of Science (Phys. & Math.). Associate Professor.
Aircraft Control Systems Department, National Aviation University, Kyiv, Ukraine.
Education: Donetsk National University, Donetsk, Ukraine (1999).
Research interests: gyroscopes theory, control systems and data processing.
Publications: 49.
E-mail: vkir28@gmail.com

Lesina Yevheniia. Candidate of Science (Phys. & Math.). Associate Professor.
Automatic and Telecommunications Department, Donetsk National Technical University, Pokrovsk, Ukraine.
Education: Donetsk National University, Donetsk, Ukraine (2001).
Research interests: theory of differential equations, control systems and data processing.
Publications: 47.
E-mail: lesina17@gmail.com

В. В. Кириченко, Є. В. Лесіна. Застосування динамічних систем для захисту даних в телекомунікаційних мережах
У даній роботі досліджено модель криптографічної системи, створеної на основі нелінійної динамічної системи третього порядку. При цьому безперервна система замінюється кінцевим автоматом з досить великими вхідним, внутрішнім і вихідним алфавітами. Розглянуто особливості, що виникли при реалізації в мікропроцесорній системі алгоритму кодування, заснованого на вищевказаній системі.
Ключові слова: кінцевий автомат; оборотні динамічні системи; кінцевомірне кільце цілих чисел; генератори псевдовипадкових послідовностей.

Кириченко Віктор Вікторович. Кандидат фізико-математичних наук. Доцент.
Кафедра систем управління літальних апаратів, Національний авіаційний університет, Київ, Україна.
Освіта: Донецький Національний університет, Донецьк, Україна (1999).
Напрямок наукової діяльності: теорія гіроскопів, системи управління та обробка інформації.
Кількість публікацій: 49.
E-mail: vkir28@gmail.com

Лесіна Євгенія Вікторівна. Кандидат фізико-математичних наук. Доцент.
Кафедра автоматики та телекомунікацій, Донецький національний технічний університет, Покровськ, Україна.
Освіта: Донецький Національний університет, Донецьк, Україна (2001).
Напрямок наукової діяльності: теорія диференціальних рівнянь, системи управління та обробка інформації.
Кількість публікацій: 47.
E-mail: lesina17@gmail.com

Кириченко В.В., Лесина Е.В. Применение динамических систем для защиты данных в телекоммуникационных каналах
В данной работе изучена модель криптографической системы, созданной на основе нелинейной динамической системы третьего порядка. При этом непрерывная система заменяется конечным автоматом с достаточно большими входным, внутренним и выходным алфавитами. Рассмотрены особенности, возникшие при реализации в микропроцессорной системе алгоритма кодирования, основанного на вышеуказанной системе.
Ключевые слова: конечный автомат; обратимые динамические системы; конечномерное кольцо целых чисел; генераторы псевдослучайных последовательностей.

Кириченко Виктор Викторович. Кандидат физико-математических наук. Доцент.
Кафедра систем управления летательных аппаратов, Национальный авиационный университет, Киев, Украина.
Образование: Донецкий национальный университет, Донецк, Украина (1999).
Направление научной деятельности: теория гироскопов, системы управления и обработка информации.
Количество публикаций: 49.
E-mail: vkir28@gmail.com

Лесина Евгения Викторовна. Кандидат физико-математических наук. Доцент.
Кафедра автоматики и телекоммуникаций, Донецкий национальный технический университет, Покровск, Украина.
Образование: Донецкий национальный университет, Донецк, Украина (2001).
Направление научной деятельности: дифференциальные уравнения, системы управления и обработка данных.
Количество публикаций: 47.
E-mail: lesina17@gmail.com