The Hardware Implementation of Devices Forming Discrete Signals with Multi-Level Correlation Function

Alexey Smirnov
Professor in the Department of Software, Kirovohrad National Technical University, Kirovohrad, Ukraine

Abstract:
Algebraic approach to study the formation of large assemblies of discrete signals with multi-level correlation function, which is based on the section of circular orbits of group codes, is studied. The number and value of side-lobe levels of the correlation function of the generated sequences, and the power of the assembly signals are determined by remote and structural properties of polynomial rings over finite fields. Proposals for the hardware implementation of devices forming discrete signals with multi-function correlation are developed.

Keywords: ensembles of digital signals, multi-level correlation function

1. Introduction

A promising direction in the development of algebraic methods of the theory of discrete signals is the use of advanced mathematical apparatus of the theory of finite fields and, in particular, the theory of polynomial rings, which allows associating the correlation properties of the sequences, generated from the group and the structural properties of the code sequences [1 – 4]. The studies carried out in this work showed that thrived algebraic approach to the synthesis of discrete signals based on section of circular orbits of the group code allows creating large assemblies of sequences, the correlation properties of which have multi-level structure. The synthesized signals have the most practical interest in multiple access radio control systems [5 – 7]. The use of large assemblies of discrete signals with the improved properties will significantly increase subscriber capacity of radio control systems with code channels division.

Proposals for hardware implementation of devices forming discrete signals with multi-level correlation function are developed in this work. It is shown that the developed solutions allow to generate a sequence with improved correlation and assembly properties and to practically implement the developed in [1 – 4] method of forming of digital signals.

2. Algebraic approach to the formation of discrete sequences with multilevel correlation function

The proposed in [1 – 4] algebraic approach to the formation of large assemblies of discrete signals with multi-level correlation function is based on the section of circular orbits of group codes. The number and value of side-lobe levels of the correlation function of the generated sequences, and the power of signals assemblies are determined by remote and structural properties of polynomial rings over finite fields. Let's briefly examine these provisions constituting the theoretical basis for the formation of discrete signals.

Group code is uniquely determined by leaders (representatives) of its component cyclic orbits. An orbit hereafter refers to the set of code words equivalent to each other with respect to the operation of the cyclic shift. Under the section of the orbits of the group code let's understand the choice of one representative (leader) of each orbit. Distance (correlation) properties of the thus formed set of leaders are determined by remote properties of group codes; herewith the equivalence of cyclic shift operation is absent by definition of orbits section. Let's set this property in the basis of the assembly of discrete signals formation. Sectional diagram of nonzero cyclic orbits of group code is shown in Fig. 1.

Fig. 1 shows the decomposition of the vector space $GF^n(q)$ on the sets of non-intersecting orbit V_ξ, $\xi = 0,\ldots,L$, the group code V representation through the union of a finite number of orbits and the scheme of choosing of orbital leaders – one arbitrary representative from each cyclic subsets V_ξ, $\xi = 0,\ldots,M$ (for convenience the code words $C_{v,u} = \left(c_0^{v,u}, c_1^{v,u}, .. c_{n-1}^{v,u}\right)$ are marked by two indices: v – the number of orbit V_v of the code V, $v = 1,\ldots,M$; u – the number of a code word in the orbit $u = 1,\ldots,z_v$, where z_v – the number of code words in the orbit V_v, $z_v \le n-1$).

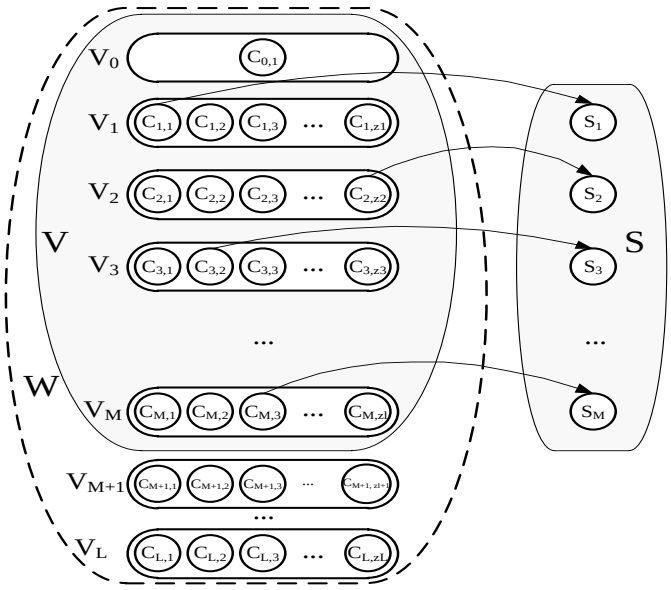

Fig.1. Scheme of nonzero cyclic orbits' section of a group code for the formation of an assembly of discrete signals

Representatives of the orbits of the selected form the set $S=(S_1,S_2,...,S_M)$, where $S_v=C_{v,u}$, $v=1,...,M$, and the selection of an index u with appropriate $C_{v,u}$ is determined by the rule of section of the v-th cyclic group code orbit.

Let's consider the binary case, i.e. restrict ourselves to the properties of the set $S=(S_1,S_2,...,S_M)$, formed by the section of the circular orbits of binary group code. The elements of the formed of discrete sequences (digital signals) $S_v=(s_0^v,s_1^v,..s_{n-1}^v)$ let's define the elements of the selected code words (the leaders of the orbits) as follows: $s_i^v=\begin{cases}1, c_i^{v,u}=1;\\ -1, c_i^{v,u}=0.\end{cases}$

Let's suppose that the considered (n, k, d) code V has a weight spectrum of:

$$\begin{cases} A(0)=1;\\ A(1)=0;\\ A(2)=0;\\ \quad ...\\ A(d-1)=0;\\ A(d);\\ A(d+1);\\ \quad ...\\ A(n). \end{cases} \qquad (1)$$

$w=0,...,n$, where $A(w)$ – the number of code words in the code V with the weight w.

Then the set of digital signals $S=(S_1,S_2,...,S_M)$ formed by the section of cyclic orbits of code V, has correlation and assembly properties, corresponding to the following statement [1 – 4].

Statement

1. Side lobes of the periodic function of auto – (PFAC) and mutual – (PFMC) correlation signals' assembly $S=(S_1,S_2,...,S_M)$ have the following values:

$$PFMC,PFAC=\frac{n-2w}{n}, \qquad (2)$$

for those $w=d,d+1,...,n,$ that $A(w)\neq 0$.

2. For all such $w=d,d+1,...,n$, that $A(w)=0$ the side lobes and PFAC and PFMC will never be $\frac{n-2w}{n}$.

3. The power M of the assembly $S=(S_1,S_2,...,S_M)$ is defined by the number of non-zero orbits of the code V and is bounded below by the expression:

$$M \geq \frac{2^k-1}{n}. \quad (3)$$

The equality holds in case of the maximum period of the sequence of all the orbits forming the code, i.e. if the code is V a set of orbits, formed by sequences of maximum length (m-sequences).

Let's consider the most general case where the binary group (n,k,d) code under $GF(2)$ is given by checking polynomial of:

$$h(x)=f_{i1}(x)f_{i_2}(x)..f_{i_u}(x)=\prod_{s=1}^{m-1}\left(x-\alpha^{i_1(2^s)}\right)\left(x-\alpha^{i_2(2^s)}\right)..\left(x-\alpha^{i_u(2^s)}\right), \quad (4)$$

where, $f_{i_1}(x)$, $f_{i_2}(x)$, ..., $f_{i_u}(x)$ – u arbitrary row of the following minimal polynomial elements $\alpha^{i_1}\in GF(2^m)$, $\alpha^{i_2}\in GF(2^m)$, ..., $\alpha^{i_u}\in GF(2^m)$ respectively, where the order of the elements α^{i_1}, α^{i_2}, ..., α^{i_u} is equal to the order of the multiplicative group of a finite field $GF(2^m)$, $n=2^m-1$, α – a primitive element of the finite field $GF(2^m)$, $n=2^m-1$.

Let's consider, without loss of generality that $i_1=1$. Let's define the check and generator polynomial as follows:

$$h(x)=\prod_{s=0}^{m-1}\left(x-\alpha^{(2^s)}\right)\left(x-\alpha^{i_2(2^s)}\right)..\left(x-\alpha^{i_u(2^s)}\right),$$

$$g(x)=\frac{x^n-1}{h(x)}=\prod_{j\neq 1,i_2,...,i_u}\ \prod_{s=0}^{m_j}\left(x-\alpha^{j(2^s)}\right).$$

Schematically, the process of forming of the check and generator polynomial is shown in Fig. 2. The symbol v stands for the number of the classes of conjugate elements that make up a multiplicative group of a finite field $GF(2^m)$. The first class (elements α^1, α^2, ..., $\alpha^{2^{m_1}}=\alpha^{2^{m-1}}$) contains m conjugacy (which determines the primitive element α). The following classes (elements α^j, α^{2j}, ..., $\alpha^{j2^{m_2}}$) contain m_j conjugacy (m_j divides evenly m) $j\in[1..v]$. For each $j\in[1..v]$ corresponding m_j is defined as the smallest positive integer for which the equality:

$$j=\left(j2^{m_j}\right)\bmod\left(2^m-1\right).$$

If the order of the multiplicative group of a prime number, that is, when:

$$2^m-1=\text{prime number},$$

then:

$$\forall j: m_j=m.$$

A single element of the field $\alpha^0=1$ forms an additional conjugate class of one element.

Fig. 3 shows the corresponding distribution of the elements of a finite field in the polynomials $h(x)$ and $g(x)$. Elements of a finite field of the first u conjugate classes are the roots of the check polynomial $h(x)$. A range of elements of a finite field, which holds the roots of the check polynomial $h(x)$, is determined by the largest value z, for which the condition $\alpha^z=\alpha^{(z)\bmod(2^m-1)}$, is done, that is:

$$z=\max_{s=0,...,m-1}\left\{\left(2^s\right)\bmod\left(2^m-1\right),\left(i_2 2^s\right)\bmod\left(2^m-1\right),...,\left(i_u 2^s\right)\bmod\left(2^m-1\right)\right\}.$$

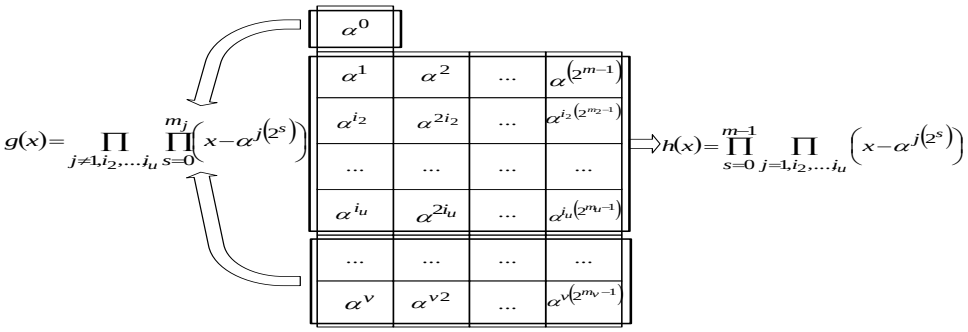

Fig. 2. Scheme of formation of check and generator polynomials of the group code

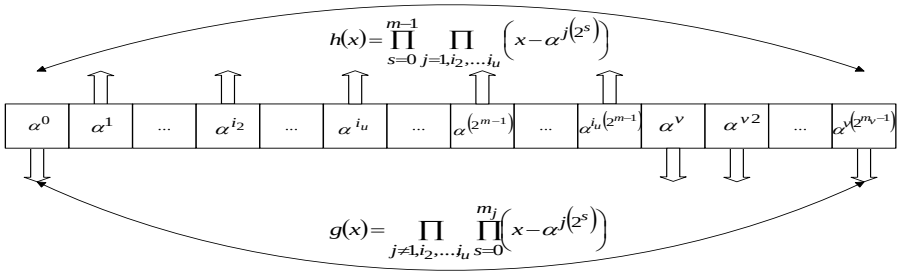

Fig. 3. Distribution of the elements of the finite field to check and generator polynomials of the group code

In general, the roots of polynomials $f_{i_1}(x)$, $f_{i_2}(x)$, ..., $f_{i_u}(x)$ are in the range:

$$\underbrace{\alpha^{i_1},\dots,\alpha^{i_1(2^{m-1})},\dots,\alpha^{i_2},\dots,\alpha^{i_2(2^{m-1})},\dots,\alpha^{i_u},\dots,\alpha^{i_u(2^{m-1})}}_{z\text{ values}},$$

whence:

$$2t=2^m-z-1,$$

and, accordingly:

$$d=2t+1=2^m-z.$$

The corresponding code parameters of a group code are as follows:

$$\left(n=2^m-1, k=zm, d=2^m-z\right). \quad (5)$$

Let's estimate the weight spectrum of the code. Verification polynomial of the code with the parameters (5) contains check polynomials of all the codes, as a cofactor with the check polynomials $h(x)=f_{i1}(x)f_{i_2}(x)..f_{i_y}(x), y\le u$.

It follows that all the code words from the group codes with $h(x)=f_{i1}(x)f_{i_2}(x)..f_{i_y}(x), y\le u$ are code words of considered code with parameters (5), i.e. nonzero components of the weight spectrum are formed by a successive addition (in order of addition of the cofactors in the polynomial $h(x)=f_{i1}(x)f_{i_2}(x)..f_{i_y}(x), y\le u$) of the corresponding pair of elements (for all $y=2,3,\dots,u$):

$$A(z_y)\neq 0,$$

$$A(2^m-z_y)\neq 0,$$

where:

$$z_y=\max_{s=0,\dots,m-1}\left\{\left(2^s\right)\bmod\left(2^m-1\right),\left(i_2 2^s\right)\bmod\left(2^m-1\right),\dots,\left(i_y 2^s\right)\bmod\left(2^m-1\right)\right\}.$$

When $y=1$ we have one non-zero component of the weight spectrum $A(2^{m-1})\neq 0$, which corresponds to $z_y=2^{m-1}$.

The considered in works [1 – 4] cases of building three – and five-level discrete signals correspond to:

$$y = 2:$$

$$z_y = 2^{m-1} + 2^{\frac{m+1}{2}-1},$$

$$A(2^{m-1} + 2^{\frac{m+1}{2}-1}) \neq 0,$$

$$A(2^{m-1} - 2^{\frac{m+1}{2}-1}) \neq 0$$

$$y = 3:$$

$$z_y = 2^{m-1} + 2^{\frac{m+1}{2}},$$

$$A(2^{m-1} + 2^{\frac{m+1}{2}}) \neq 0,$$

$$A(2^{m-1} - 2^{\frac{m+1}{2}}) \neq 0.$$

Thus, the three – and five-level digital signals are a special case of constructing of large assemblies of discrete signals with multi-level correlation functions.

The general expression for estimating the weight range of the group code specified by a check polynomial (4) let's put down as:

$$A(w) = \begin{cases} 1, w = 0; \\ 0, w = 1,\ldots,z_u - 1; \\ \neq 0, w = z_u; \\ \ldots \\ \neq 0, w = z_3 = 2^{m-1} - 2^{\frac{m+1}{2}}; \\ 0, w = z_3 + 1,\ldots,z_2 - 1; \\ \neq 0, w = z_2 = 2^{m-1} - 2^{\frac{m+1}{2}-1}; \\ 0, w = z_2 + 1,\ldots,z_1 - 1; \\ \neq 0, w = z_1 = 2^{m-1}; \\ 0, w = z_1 + 1,\ldots 2^m - z_2 - 1; \\ \neq 0, w = 2^m - z_2 = 2^{m-1} + 2^{\frac{m+1}{2}-1}; \\ 0, w = 2^m - z_2 + 1,\ldots 2^m - z_3 - 1; \\ \neq 0, w = 2^m - z_3 = 2^{m-1} + 2^{\frac{m+1}{2}}; \\ \ldots \\ \neq 0, w = 2^m - z_u; \\ 0, w = w = 2^m - z_u + 1,\ldots 2^m - 1. \end{cases}$$

The corresponding expression on valuing the side-lobe periodic correlation function generally takes the form:

$$\mathrm{PFMC,PFAC}=\begin{cases}\dfrac{2^m-2z_u-1}{2^m-1},\ w=z_u= \\ =\max\limits_{s=0,\dots,m-1}\left\{\left(2^s\right)\bmod\left(2^m-1\right),\left(i_2 2^s\right)\bmod\left(2^m-1\right)\dots,\left(i_u 2^s\right)\bmod\left(2^m-1\right)\right\}; \\ \dots \\ \dfrac{2^m-2z_3-1}{2^m-1}=\dfrac{-1-2^{\frac{m+1}{2}+1}}{2^m-1},\ w=z_3=2^{m-1}-2^{\frac{m+1}{2}}; \\ \dfrac{2^m-2z_2-1}{2^m-1}=\dfrac{-1-2^{\frac{m+1}{2}}}{2^m-1},\ w=z_2=2^{m-1}-2^{\frac{m+1}{2}-1}; \\ \dfrac{2^m-2z_1-1}{2^m-1}=\dfrac{-1}{2^m-1},\ w=z_1=2^{m-1}; \\ \dfrac{2^m-2(2^m-z_2)-1}{2^m-1}=\dfrac{-1+2^{\frac{m+1}{2}}}{2^m-1},\ w=2^m-z_2=2^{m-1}+2^{\frac{m+1}{2}-1}; \\ \dfrac{2^m-2(2^m-z_3)-1}{2^m-1}=\dfrac{-1+2^{\frac{m+1}{2}+1}}{2^m-1},\ w=2^m-z_3=2^{m-1}+2^{\frac{m+1}{2}}; \\ \dots \\ \dfrac{2^m-2(2^m-z_u)-1}{2^m-1},\ w=2^m-z_u= \\ =2^m-\max\limits_{s=0,\dots,m-1}\left\{\left(2^s\right)\bmod\left(2^m-1\right),\left(i_2 2^s\right)\bmod\left(2^m-1\right)\dots,\left(i_u 2^s\right)\bmod\left(2^m-1\right)\right\}.\end{cases} \quad (6)$$

Thus, the generated by the proposed method discrete signals have multilevel features of auto – and mutual-correlation. The values of the lateral emissions take a finite number of values given by the weight properties of a used group code.

Let's estimate the power of the assembly of the formed digital signals. The power of the used code is $2^k=2^{um}$, there are altogether:

$$2^k-1=2^{um}-1$$

of nonzero code words.

If we assume that each code word has the maximum period and each cyclic orbit contains exactly 2^m-1 code words, then the expression for the estimates of the power of the assembly of the formed signals becomes:

$$M=\frac{2^{um}-1}{2^m-1}=2^{(u-1)m}+2^{(u-2)m}+\dots+2^m+1.$$

The analysis of the last expression shows that the use of group codes allows creating large assemblies of discrete signals. Adding of a minimal polynomial as another cofactor in the check polynomial increases the power of the assembly $2^{(u-i)m}$, where $u-i$ – the number of the added minimum polynomials.

3. Development of proposals for the hardware implementation of devices forming discrete signals by a proposed method

The developed method of forming of digital signals allows building large assemblies of weakly correlated binary sequences. Let's consider the possibility of practical formation of large assemblies of weakly correlated discrete signals and constructing the corresponding hardware devices for binary sequences generating.

In case of multi-level sequences, we get the following scheme of formation of discrete signals. (Fig. 4). The device is built through connecting of shift registers to the adder output u. A wiring diagram to make appropriate provision in the register ring feedback shift is selected by the coefficients of primitive polynomials $h_1(x)$, $h_2(x)$, ..., $h_u(x)$ of m degree, respectively. In this case, the length of the binary sequences equals to $n=2^m-1$ and to form them one need to use u shift registers the shift registers with m binary digits. The initial state of the shift registers sets the mode of the formed sequence.

Functions of the feedback shift registers are set by coefficients of primitive polynomials of m degree:

$$h_1(x) = h_{1,0} + h_{1,1}x + h_{1,2}x^2 + \ldots + h_{1,m}x^m = f_{i_1}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_1(2^s)}\right)$$

$$h_2(x) = h_{2,0} + h_{2,1}x + h_{2,2}x^2 + \ldots + h_{2,m}x^m = f_{i_2}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_2(2^s)}\right),$$

$$\ldots$$

$$h_u(x) = h_{u,0} + h_{u,1}x + h_{u,2}x^2 + \ldots + h_{u,m}x^m = f_{i_u}(x) = \prod_{s=0}^{m-1}\left(x - \alpha^{i_u(2^s)}\right)$$

where $f_{i_1}(x),\ f_{i_2}(x), \ldots,\ f_{i_u}(x)$ – minimal polynomial of elements α^{i_1}, α^{i_2}, ..., α^{i_u}, respectively, from the end field $GF(2^m)$, which are defined by their roots $\alpha^{i_1(2^s)}$, $\alpha^{i_2(2^s)}$, ..., $\alpha^{i_u(2^s)}$, $s = 0, 1, \ldots, m-1$.

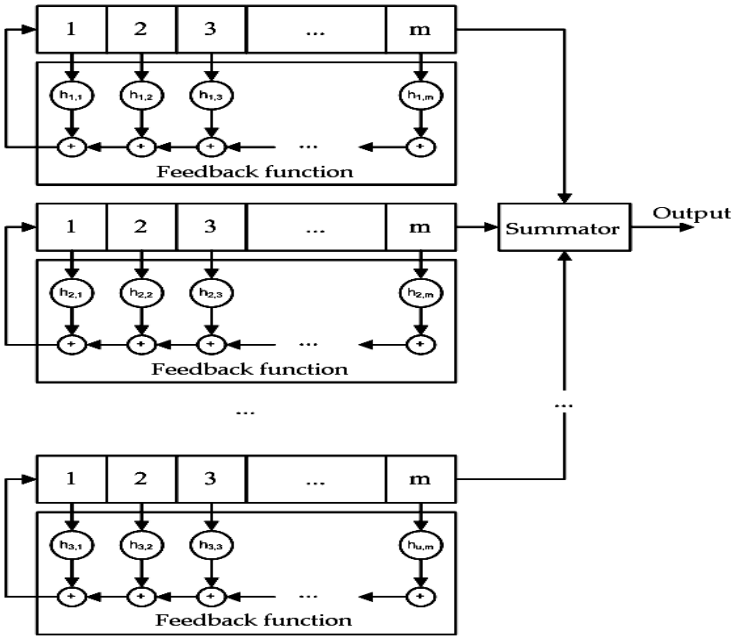

Fig. 4. Block diagram of the formation of discrete signals with multi-level correlation function

The order of elements α^{i_1}, $\alpha^{i_2}, \ldots, \alpha^{i_u}$ equals the order of the multiplicative group of a finite field $GF(2^m)$, α – a primitive element of the finite field $GF(2^m)$.

The device works in the discussed above manner and allows creating:

$$M = \frac{2^{um} - 1}{2^m - 1} = 2^{(u-1)m} + 2^{(u-2)m} + \ldots + 2^m + 1$$

sequences of length $n = 2^m - 1$.

4. Conclusions

Thus, in the course of a conducted research practical suggestions regarding the implementation of the hardware devices forming discrete sequences have been developed.

The designed schemes are implemented computationally by efficient converters, for example, based on circuits with a shift register and an adder (see Fig. 4 – 7). They allow creating large assemblies of discrete signals with improved correlation and assembly properties. Therefore, the developed proposals let to practically implement the developed method of forming discrete signals.

References

[1] Kuznetsov A.A., Smirnov A.A., Sai V. N., Digital Signals with Multi-Level Correlation Function // Radio: Ukr. Interag. Sc. and Eng. Sat – Kharkov: KhNUR. 2011. – Issue 166. ¬ P. 142-152.

[2] Kuznetsov A.A., Smirnov A.A., Sai V. N., Formation of Discrete Signals With Multi-Function Correlation // Information processing systems. – Kh.: KhAFU. – 2011 – Vol. 5(95). – P. 50-60.

[3] Kuznetsov A.A., Use of Complex Discrete Signals for Steganographic Information Security / A.A. Kuznetsov, A.A. Smirnov // International Journal of Engineering Practical Education. – Volume 1, Issue 1. – USA, Indiana: Science and Engineering Publishing Company. – 2012. – P. 21-25.

[4] A.A. Smirnov, Comparative Studies of Methods for the Synthesis of Digital Signals with Special Correlation Properties / A.A. Smirnov, E.V. Meleshko // Abstracts of V International Scientific and Technical Symposium "New Technologies in Telecommunications" (NIICT-Carpathian-2012), Kyiv. 17-21 January 2012 – Kyiv: NIICT. – 2012. – P. 80-81.

[5] Gryanik M.V., Frolov V.I., Technology CDMA – The Future of Mobile Systems in Ukraine. – The World of Communication, 1998, # 3. – P. 40-43.

[6] Naumenko N.I., Stasev J.V., Kuznetsov A.A, Evseev S.P., Theory Of Signal-Code Structures. Kh.: KhAFU, 2008 – 489.

[7] Sklar B., Digital Communication. Theoretical Basis and Practical Application. – M.: Williams, 2003. – 1104p.

Author Name

Alexey Smirnov was born in 1977. Graduated from Kharkiv Military University with a degree in "Automated Control Systems" in 1999.

Candidate of Technical Sciences (PhD). Professor of Department of Software of Kirovohrad National Technical University, Ukraine.

Field of interest: information security and routing issues.