

СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ INFORMATION PROTECTION SYSTEMS

UDC 621.391.1

DOI:10.30837/rt.2019.4.199.14

I.D. GORBENKO, Dr. Sc. (Technology), O.A. ZAMULA, Dr. Sc. (Technology), HO TRI LUC

SYNTHESIS OF DERIVATIVES OF COMPLEX SIGNALS BASED ON NONLINEAR DISCRETE SEQUENCES WITH IMPROVED CORRELATION PROPERTIES

Introduction

The most serious problems of radar, communication and information transmission are solved using complex broadband signals (BBS). Discrete-coded signals (DCS) are widely used, in which the manipulated parameters (amplitude, phase and frequency) change at strictly fixed time intervals (clock cycles). The law of variation of the manipulated parameters in the DCS is set by discrete sequences (DSs), which completely determine the properties of the DCS and are often identified with them. As a result, attention of the BBS researchers is focused on the analysis, synthesis, and processing of the DSs. The use of the DSs for the formation of complex broadband and super broadband signals as manipulating sequences in the systems of radar, sonar, navigation, communication and transmission of information made it possible to resolve the contradiction between the resolution and the range of the systems, increase their stability and electromagnetic compatibility, increase the efficiency of use of the radio band due to the code division of channels. The use of the DSs also made it possible to improve the ecology in the area of radio emitters action by reducing the peak radiation power, create satellite radar, radio navigation and communication systems, while providing observations, coordinates determination and information transfer to any point on the planet, including moving objects, make a secret location and communication. The article proposes a method for synthesis of a set of nonlinear, discrete, complex signals based on the use of derivatives of the DSs with given cross-correlation, structural and ensemble properties for use in information and communication systems (ICS), which are subject to increased requirements for noise immunity of receiving signals, secrecy and information security of the system.

1. Main results of the research

In multi-user systems with code division multiplexing, the DCS systems with specified cross-correlation properties are required. The synthesis of signal systems with the necessary cross-correlation properties consists in searching for families of sequences that have corresponding cross-correlation functions (CCFs). In addition, one of the main issues in the development of multi-user systems is the choice of signals, the number of which must be at least the product of the number of system subscribers by the number of signals in the alphabet (assuming that all subscribers use alphabets of the same volume). For modern multi-user ICS, it is necessary to use signal systems whose volume (M) grows according to a power law with respect to signal base B [1] that is

$$M = c \cdot B^k . \quad (1)$$

At the same time, the signals entering the system should provide the minimum possible level of mutual interference, which, in turn, is determined by the permissible level of the maximum lobes of the cross-correlation functions

$$R_{\max} = \beta / \sqrt{B} , \quad (2)$$

where β – is the peak factor of the cross-correlation function.

At present, there are no algorithms (rules for construction) of large systems of phase-manipulated (PM) signals, in which the peak factor would reach values of several units. For example, if the signal base $B=10^4$, then a signal system may be necessary, which includes signals of duration (the number of sequence elements) $N=10^8 \dots 10^{12}$, and the value of the peak factor $\alpha = 2, \dots, 5$ [1]. But such signals are not yet known, although the fact of their existence is not in dispute. Thus, today an insoluble problem is the development of methods for the synthesis of large PM BBS (phase-manipulated broadband signals) systems with good correlation properties. The algorithms, that must be created to build such signal systems, must be deterministic, since for the implementation of optimal reception schemes, it must be possible to reproduce the expected signals at the receiving point.

In multi-channel systems m -sequences or sequences with a three-level cross-correlation function (multiple Gold and Kasami sequences) are used, generated by m -cascaded shift registers with linear feedback. The volume of M system, made up of sequences of N duration, is $M = \varphi(N)/m$, $M = \varphi(N)/m$, ($\varphi(N)$ – the Euler function). Therefore, the scope of the above signal systems is limited. For example, the number of different signals that can be synthesized using a linear register for $m=10$ is $M = 60$. The maximum values of side peaks of mutually correlation functions in such systems are greater than in a number of other signal systems [1]. The use of Gold sequences in multichannel communication systems makes it possible to increase the volume of the system, however, such systems have a significant frequency peak factor and relatively large levels of side peaks of the autocorrelation functions. The above linear sequence classes exist only for $N = 2^m - 1$ duration values. Efforts to construct such signal systems for arbitrary values of the period leads to a significant deterioration of the properties of their auto- and cross-correlating characteristics. In addition, the rules for constructing such signal systems are based on the use of linear operations and therefore have low code stability [2] for determining the subject of counteraction to the rule for constructing such a signal. So, the law (rule) of signal construction, formed on the basis of Gold sequences with $N = 2^m - 1$ period, is determined by any segment of this sequence in $4 \cdot m$ size. When applied to generating a signal based on m sequence, such a segment forms $2 \cdot m$ characters. For these reasons, the use of linear signals in multichannel communication systems with code division of channels (subscribers) is limited.

It is known that the only way to achieve high reliability of data transmission is to increase the distance between competing signals in the system to the maximum possible value. Such an increase in distance can be achieved by increasing the energy of the signals (or the length of the corresponding vectors). Obviously, to maximize the distance between two vectors of fixed length, they should be chosen opposite. Providing exactly this probability of false reception is similar to the use of opposite signals, and is achieved on the basis of orthogonal pair with a twofold increase in the energy of the signals.

Many orthogonal signals can be constructed, for example, by signals time shifting. It is obvious that the scalar product of any two signals, that do not overlap in time, is zero. When using M signals that occupy together the entire T_c time interval, when the signal duration is not greater than $T = T_c / M$, and the time shift between adjacent signals, such encoding forms a family of orthogonal signals. Another way to ensure orthogonality is coding by frequency shift. Based on the Parseval theorem, the scalar product of signals $x(t)$, $y(t)$ and their spectra $x(f)$, $y(f)$ coincides [2]:

$$(x, y) = \int_{-\infty}^{\infty} x(t) \cdot y(t) dt = \int_{-\infty}^{\infty} x(f) \cdot y(f) df = (x', y'), \quad (3)$$

which makes it possible to transfer the time shift method to the frequency domain. With complete overlapping of signals in time, each of them occupies a band of not less than $W = 1/T_c$. Then the maximum number of orthogonal signals n_s formed by the shift of the spectrum will be $M = W_c / W = W_c \cdot T_c = n_s$. With this encoding method, the signal uses the entire time resource T_c and only the M -th portion of the total frequency resource W_c .

The considered methods of constructing orthogonal signals appear to be the best in terms of hardware implementation. However, as the number of signals M increases, the coding using a time

shift requires a significant peak factor, and the coding using a frequency shift provides optimal processing using a very significant number of frequency filters.

Under such conditions, the method of constructing orthogonal signals by sharing with all signals a common time-frequency resource without distributing the latter can be very attractive. In this method, all signals related to a given resource, are completely overlapped both in the time and frequency domain. The band occupied by each of the signals can be estimated as $W=1/\tau$ (τ - is the duration of the elementary pulse of the sequence N of some signal M). The duration of the signal is $T=M \cdot \tau$. Wherein $W \cdot T = M = W_c \cdot T_c$. The orthogonality of signals for this method is not achieved by dividing the time interval or band, but by choosing the law of modulation of the signal.

Let us evaluate the possibility of synthesis of large ensembles of orthogonal signal systems, and analyze the attainable correlation, ensemble and structural properties of such a class of signals.

Orthogonal discrete signals (ODS) can be specified in various ways [1, 2]. The most convenient, in our opinion, is the form of providing ODS using the Hadamard matrices, which are defined by symbolic equality

$$H_{2N} = \begin{vmatrix} H_N & H_N \\ H_N & -H_N \end{vmatrix}, \quad (4)$$

where H_N – is the Hadamard matrix of N order (the number of rows is equal to the number of N columns), and H_{2N} – is the Hadamard matrix of $2 \cdot N$ order. Using the last expression, it is possible to obtain the Hadamard matrices for any $N=2^m$ (m – is the integer). The Hadamard matrices are known not only for $N=2^m$ order but also for other values of N .

The Hadamard matrices satisfy the equation

$$H_N \cdot H_N^T = N \cdot I, \quad (5)$$

Where H_N^T – is the Hadamard transposed matrix; I – is the unit matrix.

Rows or columns of the Hadamard matrix can be used as code sequences. The number of code sequences of the Walsh system is equal to N order of the matrix.

The last equation determines the orthogonality of the Walsh code sequences, that is, the equality

$$\sum_{n=0}^{N-1} W_i(n) \cdot W_\nu(n) = \begin{cases} 0 & \text{at } i \neq \nu, \\ N & \text{at } i = \nu, \end{cases} \quad (6)$$

where W_i – i -th is the Walsh code sequence and $W_i(n)$ – is symbol of this sequence.

Studying the ensemble characteristics of the Hadamard matrices, taking into account the specific methods of their construction, requires considerable computational cost, moreover, these methods are very difficult to implement. Table 1 shows the values of the ensemble characteristics constructed using the Hadamard matrices for some N values.

Table 1
Ensemble characteristics of the signals
constructed using the Hadamard matrices

N	M
64	19
100	1
256	54
512	102
1024	162
1032	4
1088	4
1500	4
2000	9
4000	16
9000	12

Let us analyze the correlation properties of the ODS. It is shown in [1] that the signals have the minimum values of the maximal side lobes of the auto - and cross-correlation functions if the number of blocks μ in a row of identical sequence symbols satisfies the condition: $\mu \approx \frac{N+1}{2}$. It is known [1, 2] that none of the ODS systems satisfies these requirements. For example, for the Hadamard matrices (the structure of the Hadamard matrix is cyclic) a change in the number of blocks in rows (signals) from 1 to N is characteristic. Therefore, the signal system, which is built on the application of rows (columns) of the Hadamard matrix (Walsh sequences), should have poor correlation properties, since in most sequences the number of blocks is far from optimal. This is confirmed by the fact that most of autocorrelation functions (ACF) and cross-correlating functions (CCF) of the Walsh sequences have large side lobes. Thus, the level of the side lobes of the ACF and CCF of the ODS, built on the basis of the Hadamard matrices, reaches a value of $\pm N$, which leads to a significant decrease in the probability of correct detection of cycle phasing signals or signal tracking. The latter, in the general case, leads to a decrease in the reliability of information transmission. Analysis of the data in Table 1 shows that the ODSs have unsatisfactory ensemble characteristics.

Let us study the structural properties of the ODS of the Hadamard systems. Under the structural properties we will mean the ability to restore the laws of their formation at any number (1) of the known $1 < N$ symbols. The structural properties of the signals will be evaluated quantitatively by a coefficient

$$S = 1/N. \quad (7)$$

For example, if the Hadamard matrix is constructed according to the rule: for any prime number $p \equiv 3 \pmod{4}$ there is the Hadamard matrix of $m = P+1$ order, then it is necessary and sufficient to know $1 \geq N/2$ signal symbols to restore the law of the ODS formation.

An analysis of the methods for the ODS constructing [3] shows that the structural properties of the ODS of the Hadamard system do not exceed (by criterion (7)) the value of 0.5.

Thus, the ODS of the Hadamard system have poor correlation, ensemble and structural properties, and therefore, the use of the ODS in the ICS, which has increased requirements for the noise immunity of receiving signals, secrecy of functioning, information security, is limited.

For most applications of the ICS, especially for broadband systems with multi-station access, higher requirements are put forward to ensure appropriate information security indicators, noise immunity of receiving signals, secrecy of information exchange and more. Of course, large sets of signals – physical data carriers with reasonable, for the corresponding application, correlation, ensemble and structural properties must be applied for such systems at the physical level.

The ODS of the Hadamard system, as shown above, are orthogonal, which allows their differentiation in the presence of cycle synchronization without interference. In addition, the ODSs exist for a wide range of N values. The preservation of the stated advantages of the ODS of the Hadamard system, while improving the correlation, spectral, ensemble and structural properties, can be achieved through the use of derivative signal systems. The construction of the ODS derivatives is based on the studies of the invariance properties of rows and columns of the Hadamard matrix regarding operations of their inversion and mutual permutation [3]. Derivative signal systems $W(i)$, for the case of the phase-manipulated signals, are formed by multiplying symbol-by-symbol the so-called output signal $G(i)$ by the signal producing $H(k)$

$$W(i) = H(k) \cdot G(i). \quad (8)$$

At the same time, the signal system is used as output signals, which, on the one hand, does not fully satisfy the requirements for correlation properties, on the other hand, has some advantages, for example, the simplicity of technical implementation of the construction algorithms. The Hadamard systems' ODS can be used as such signal systems.

Let us determine what properties the producing signals must possess to ensure that derivative signal systems meet the increased requirements for information security, noise immunity, and

secrecy of the ICS functioning. Thus, to construct a set of ODS derivatives W , it is necessary to find a set of vectors H , the use of which in (8) will improve the correlation, spectral, ensemble, and structural properties of the ODS.

2. Selection of producing signals systems

Let us define the requirements for the correlation, structural and ensemble properties of producing discrete signals and propose algorithms for their construction.

First, let's find out what correlation properties $H(k)$ signal should possess.

To do this, let us define the limit of "dense packing", that is, what minimum levels of the periodic autocorrelation function (PACF) of H signal are attainable if $N \equiv 0(\text{mod } 4)$. It is shown in [4] that the minimum achievable PACF values for arbitrary values of N are the following

$$R_{H_{\max}}(l) = \begin{cases} 0, & \text{if } N = 0(\text{mod } 4) \\ 1, & \text{if } N = 1(\text{mod } 4) \\ 2, & \text{if } N = 2(\text{mod } 4) \\ 3, & \text{if } N = 3(\text{mod } 4) \end{cases} \quad (9)$$

It follows directly from (9) that, in principle, signals producing zero values of the side lobes of PACF can be constructed for $N \equiv 0(\text{mod } 4)$.

The complex envelope of the derived signal $U(t)$ is equal to the product of the complex envelopes of the output signal $G_k(t)$ and the signal that produces $V_l(t)$, i.e.

$$U(t) = S_i(t) \cdot G_k(t). \quad (10)$$

If the indices in (10) change at the intervals $k = \overline{1, K}$, $i = \overline{1, N}$, then the volume of the derivative signal system is

$$M = N \cdot L. \quad (11)$$

If $K = N = B$ – the signal base, then the volume of the system is $M = B^2$, that is, the received signal system will relate to large systems.

For the PM signals (including derivatives) of the same duration, integral ratios are known [1]

$$U_{kl}(\tau) = (T/2\pi) \cdot \int_{-\infty}^{\infty} R_{kl}(\tau - \Omega) \cdot R_{\mu\nu}(\tau, \Omega) d\Omega; \quad (12)$$

$$U(\tau) = (T/2\pi) \cdot \int_{-\infty}^{\infty} R_Z(\tau - \Omega) \cdot R_Y(\tau, \Omega) d\Omega, \quad (13)$$

where: $U_{kl}(\tau)$ – cross-correlation function;

$R_{kl}(\tau, \Omega)$ – reciprocal uncertainty function;

$R_{\mu\nu}(\tau)$ – reciprocal correlation function;

$U(\tau)$ – autocorrelation function of derivative signals;

$R_Z(\tau, \Omega)$ – uncertainty function of output signals;

$R_Y(\tau, \Omega)$ – uncertainty function of the producing signal.

Analysis of expressions (12) (13) shows that the correlation properties of the derivative signals depend on the properties of the output signals and the signals producing on the frequency-time plane. Expressions (12) (13) make it possible to find the following assessment:

$$U_{kl}(\tau) \leq (T/2\pi) \cdot \sqrt{\int_{\varphi} |R_{kl}(\tau, -\Omega)|^2 d\Omega \cdot \int_{\varphi} |R_{\mu\nu}(\tau, \Omega)|^2 d\Omega} \quad (14)$$

$$U(\tau) \leq (T/2\pi) \cdot \sqrt{\int_{\varphi} |R_Z(\tau, -\Omega)|^2 d\Omega} \cdot \sqrt{\int_{\varphi} |R_Y(\tau, \Omega)|^2 d\Omega} \quad (15)$$

Estimates (14), (15) depend to a large extent on the value of the width of the integration interval φ , that is, on the ratio of the width of the CCF output signals and the producing signals.

Let us assume that the output signals and the producing signals have the same duration T , and the width of the spectrum of the producing signal F_a is greater than the width of the spectrum of the output signal F_v . It is known that if the mutual uncertainty function (MUF) of the output signals and the producing signals are evenly distributed over the frequency-time plane, then the rms value

$$\sigma_{ukl} = 1/2 \cdot \sqrt{F_a \cdot T}, \quad \sigma_{u\mu\nu} = 1/2 \cdot \sqrt{F_v \cdot T}. \quad (16)$$

Since $F_a > F_v$, the width of the MUF of the output signals according to the axis Ω is less than the width of the MUF of the producing signals, therefore $\varphi = 1/2 \cdot \sqrt{F_a / F_v}$. After completing replacement of $R_{kl}(\tau, \Omega)$ and $R_{\mu\nu}(\tau, \Omega)$ by their rms value, we get

$$U_{kl}(\tau) \leq 0,5 \cdot \sqrt{F_a / F_v}. \quad (17)$$

From the last inequality, it follows that the values of the CCF of the derivative signals are less than or equal to $0,5 \cdot \sqrt{F_a / F_v}$, which in turn means that the maximum lobes of the CCF will be less than this value. Thus, to reduce the maximum side petals of the CCF, it is necessary to increase the width of the producing signal. It also follows from (17) that the method of derivative signals formation, that is, the signal multiplication process, leads to a decrease in the side lobes of the CCF derivative signals, if the base of the signals producing $F_a \cdot T$ is larger than the bases of the output signals so that $\sqrt{F_v} \cdot T > F_a \cdot T$.

It is quite clear that to obtain $U_{kl} < 1$ (in accordance with (17), there is an inequality

$$F_v > F_a, \quad (18)$$

and the frequency band with the width of $\varphi = 4 \cdot \pi \cdot F_a$ will be narrow compared to the width of the uncertainty function of the producing signal along the frequency axis. Since in the band φ the side lobes are close to the side lobes along the time axis τ at $\Omega = 0$, then as a producing signal should be chosen this one, whose side lobes of the autocorrelation function have small values.

As for the producing signals, they must have good autocorrelation properties, secondly, as many characters (elements) as the output signal, that is, the number of $N = 2^n$ characters, where n – is an integer. Table 2 lists the properties of existing signals with a period $N \equiv 0 \pmod{4}$ [4] that can be used as producing signals.

Analysis of Table 2 shows that most signals have an "uncomfortable" length. Multiplicity of four can be obtained only by supplementing or truncating the signal, which, of course, will change its correlation properties and lead to an increase in the level of the side lobes of the PACF of derivative signals. In this case, it should be expected that, according to (12), (15), the derivative signal systems, constructed using characteristic signals and cryptographic signals [5, 6], will have the best correlation properties.

Let us illustrate the possibility of constructing derivative discrete signals, for which the rows of the Hadamard matrix of the order of $N = 256$ are used as output signals, and the signals, based on the construction of random (pseudorandom) sequences of symbols (hereinafter cryptographic signals), are used as producing signals.

Table 3 provides examples of the characters sequences - the rows of the Hadamard matrix row of the order of $N = 256$. Table 4 shows examples of synthesized cryptographic signals that, in

Analysis of the data in Table 6 shows that the statistical characteristics of the derivative signals formed on the basis of cryptographic signals are close to the corresponding characteristics of others, listed in the table of signals. In this case, the values of the maximum lateral emissions of the function of cross-correlation of the derivative orthogonal signals formed on the basis of cryptographic signals are significantly smaller than the values of the maximum lateral emissions of linear M - sequences. It is shown in [5] that cryptographic sequences (signals) are close to random sequences in their statistical characteristics. Therefore, it is quite clear that derivative signals generated using cryptographic signals will have significant (according to criterion (7)), compared to signals formed on the basis of linear rules, improved indicators of structural secrecy in exposing the law of their formation.

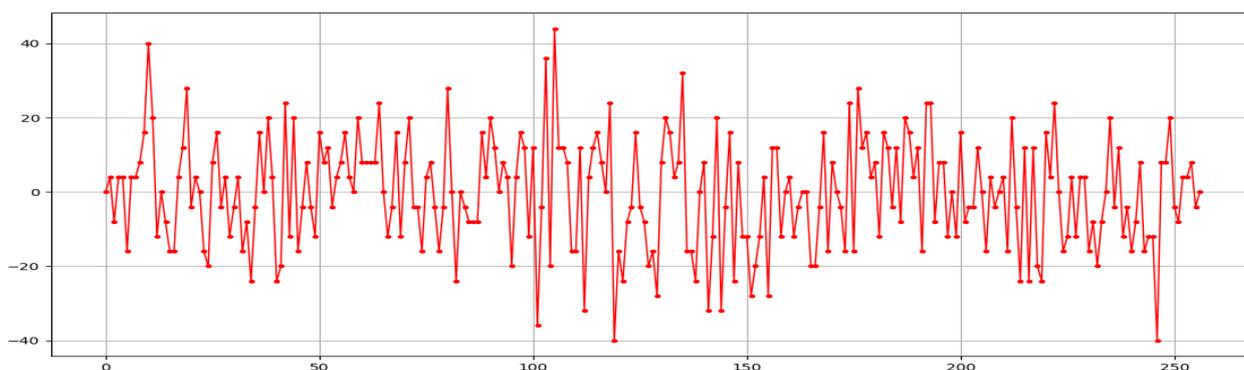


Fig. Kind of PFCC (periodic function of cross-correlation) derivative signal for $N = 256$ ($R_{\max} = 44 = 2.74\sqrt{N}$)

Table 6

Statistical characteristics of PFCC
(periodic function of cross-correlation) discrete signals

Signals type	$\frac{R_{\max}}{\sqrt{N}}$	$\frac{m_{ R }}{\sqrt{N}}$	$\frac{D_{ R }^{\frac{1}{2}}}{\sqrt{N}}$	$\frac{D_{(R)}^{\frac{1}{2}}}{\sqrt{N}}$
Signals formed on the basis of m-sequences	1,9 – 6,0	0,8	0,62	1,0
Cryptographic signals (CS)	1,64 – 3,4	0,8	0,6	1,0
Characteristic discrete signals	1,48 – 3,35	0,8	0,7 – 0,78	1,0
Derivative signals	1,63 – 3,35	0,79	0,6	0,994
Sequences with 3-level CCF	1,5	0,76	0,62	1,0

Conclusions

Modern wireless systems (e.g., satellite systems, discrete communications systems, high-speed cellular systems) are multi-user systems. When designing such systems, the main problem is the choice of multiple access, i.e. the possibility of simultaneous use of the communication channel by many subscribers with minimal mutual influence. The code separation of channels in the implementation of multiple access is based on differences in the signals provided to system subscribers, so the construction of such systems and their characteristics are determined by the choice of signals and their properties. Moreover, for most ICS applications, in particular, for

broadband systems with multi-station access, not pairs are of interest, but large sets of signals with good cross-correlation properties, improved ensemble and structural properties.

The article proposes a method for the synthesis of discrete derivatives of signals based on the use of nonlinear discrete complex cryptographic signals, as producing signals, and orthogonal signals, as the source signals. The proposed class of complex derivative signals obtained using the proposed method has improved, in comparison with orthogonal discrete signals, correlation, ensemble and structural properties. The use of this class of signals in modern information and communication systems will improve the indicators of secrecy, noise immunity, noise stability, information security of functioning of such systems.

References

1. Varakin L.E. Systems for communication with noise-like signals. 1985. 384 p. (In Russ.)
2. Ipatov Valery P. Spread Spectrum and CDMA. Principles and Applications / University of Turku, Finland and St. Petersburg Electrotechnical University 'LETI', Russia. John Wiley & Sons Ltd. The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. 2005. 385 p.
3. Gorbenko I.D., Zamula A.A., Semenko E.A., Morozov V.L. Method for complex improvement of characteristics of orthogonal ensembles based on multiplicative combining of signals of different classes // Telecommunications and Radio Engineering. 2017. Vol. 76, Is. 18. P. 1581 – 1594 . DOI: 10.1615/TelecomRadEng.v76.i18.10.
4. Sverdlik M. B. Optimal discrete signals. Moskva : Radio i svyaz', 1975. 200 p.
5. Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. 2016. Vol. 75, Is. 2. P. 169 – 178.
6. Gorbenko I.D., Zamula A.A., Semenko Ye.A., V. L. Morozov Method for synthesis of performed signals systems based on cryptographic discrete sequences of symbols // Telecommunications and Radio Engineering. 2017. Vol. 76. Is. 17. P. 1523-1533. DOI: 10.1615/TelecomRadEng.v76.i17.40.

*Kharkiv National V.N. Karazin University;
JSC "Institute of Information Technologies";*

Received 03.11.2019