UDC 004.9: 621.391.7

SYNTHESIS OF DERIVED SIGNAL SYSTEMS FOR APPLICATIONS IN MODERN INFORMATION AND COMMUNICATION SYSTEMS

I. Gorbenko, A. Zamula, V. Morozov

V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
gorbenkoi@iit.kharkov.ua, zamylaaa@gmail.com, morozov@boiko.com.ua

Reviewer: Alexandr Potii, Doctor of Sciences (Engineering), Full Professor, Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkov, 61022, Ukraine
potav@ua.fm

Received on April 2017

Abstract: *The specified requirements for complex signal systems selection – data carriers for utilization in information and communication systems (ICT), with higher demand for noise immunity, noise resistance, secrecy and information security. Conceptual framework for new class of complex signals presented – cryptographic signals. Proved appropriateness of utilization cryptographic signals in information and communication systems, as well as, for derived signal systems formation, in order to improve values of noise immunity, noise resistance, secrecy and information security in protected ICT.*

Keywords:: *information security, noise immunity, signal system, broadband systems.*

1 Introduction

In circumstances of intense counteraction, rivalry could exhibit in wide range of areas, as well as, as last events show, in area of information and hybrid wars, use of protected information and communication systems (ICT) become question of particular importance. Under protection we should understand, in wide sense, ability to provide wanted values of noise immunity, imitation resistance, information, energy and structural secrecy of systems functioning.

To the ICT, there are increasingly stringent requirements to ensure the effectiveness of their operation in the face of complex external influences: natural and deliberate interference, interference from other radio systems operating at close frequencies or in the general frequency range. High profile for providing needed values of noise immunity and information security have research dedicated to use new types of signals, which called complex, wideband, multidimensional and noise-type.

Goal of creating protected ITC – is to create system that resistant to influence from many different, actual for that system, effects (noises). An objective problem is that in process of informational exchange correspondence: bit message-signal if fixed and as data carries used signals built with linear rules. Premises allows intruder, based on parametric estimating used in signal systems, to accomplish radio jamming with minimal power expense. There are threats to information security, namely, the possibility of: unauthorized access to information assets, violation of integrity, confidentiality, accessibility of data by intruders.

The main ways of the solution are to increase the noise immunity and information security of the ICT on the basis of improving the methodological foundations of ICT construction by creating new models, methods and technologies for managing telecommunications networks, information security, services and quality of service, developing methods for information exchange, methods for the synthesis of new classes of nonlinear discrete complex signals with the necessary ensemble, correlation and structural properties.

The article proposes a method for discrete sequences synthesis with given mutually correlative, structural and ensemble properties for use in telecommunication systems in which high demands are placed on secrecy, noise immunity, noise immunity, and information security of system operation.

The distinction or code division of subscribers of a multiuser ICS is based on the fact that each subscriber is allocated an alphabet of signals (code sequences) with which he transmits the information. The most commonly used criterion for distinguishability is the minimum of the Euclidean distance [1]. The criterion is that two signals are easily distinguishable if and only if the rms distance between them is large. The need for joint consideration of signals $Y(t)$ and $X(t)$ arises when using manipulation, for example, in cases where the signal $X(t)$ is modulated by a binary sequence or when it is modulated by some carrier itself. Thus, as a measure of signal distinctiveness, the following quantity is used:

$$T^{-1}\int_0^T [Y(t) \pm X(t)]^2 =$$
$$= -T^{-1}\{\int_0^T [Y^2(t) + X^2(t)]dt \pm 2\int_0^T X(t)Y(t)dt\} , \qquad (1)$$

where T – signal period of $X(t)$ and $Y(t)$.

The first integral on the right-hand side of (1) is the sum of the energies of the signals $X(t)$ and $Y(t), 0 \le t \le T$. Consequently, for fixed energies, the signal $Y(t)$ is very different both from the signal $X(t)$, and from signal $-X(t)$ only if the parameter

$$R = \int_0^T X(t)Y(t)dt \qquad (2)$$

is small.

Parameter *R*, when solving problems of search, detection, estimation of parameters (in this case, a consistent filtering or correlation reception is used), is a response consistent with the signal $Y(t)$ filter on the input signal $X(t)$. For example, if in a multiuser ICS with code division signals $X(t)$ and $Y(t)$ are allocated to two different stations (subscribers), then the parameter *R* is a measure of the level of mutual interference created by each of the signals to the reception of the other.

In the ICT, various systems (sets of linear recurrence sequences, Kasami, Gold, Kamaletdinov, etc.) that have relatively small values of the side lobes of auto and cross correlated functions have found application as a physical carrier of information [2]. However, these signals have low structural secrecy, limited ensemble properties, and also exist only for a limited number of signal period values. In the case of truncation (increase) in the period of such signals, their correlation properties deteriorate. Therefore, the actual task is to develop theory and practice of synthesis and analysis of discrete signal systems with the required correlation, structural, ensemble properties.

Studies have shown [3] that the required (in various conditions) performance indicators of the system can be realized, including through the use of broadband radio systems, for which the expansion of the spectrum is carried out using nonlinear discrete sequences.

In some ICS, the number of simultaneously used signals can exceed several hundred. We know of large sets of periodic sequences that have correlation functions with relatively small side-lobe values of the mutually correlated functions. To generate such sequences, shift registers with linear feedback are used. The rules for constructing these classes of sequences indicate a low structural concealment of the generated sequences, and, consequently, signals providing information transmission in telecommunication systems. Here, by structural concealment, is understood the complexity of determining by an attacker the rule (law) of constructing a discrete sequence used to manipulate information bits.

The need to use secure radio channels forces researchers to look at both the modes of functioning of protected radio channels and the aspects of the formation and application of complex signals. Therefore, in our opinion, today new approaches and new views are needed on the application processes and functions of complex signals in order to build secure ISS. Fundamental here, in our opinion, is a new understanding of the methods of providing information secrecy and imitating resistance, that is, functions that are implemented in traditional systems with the use of systems and means of cryptographic information protection. A productive step, from the point of view of a new direction in the use of complex signal systems, is the synthesis of so-called cryptographic signal systems. Synthesis of such signals is based on the use of key data.

For protected radio channels, the signal systems under consideration are determined by the applications in which they are applied. In particular, it can be either separate signals or signal pairs, or large sets of discrete signals with the necessary but objectively limited values of "tight packing", mutual-correlation and ensemble properties.

A cryptographic discrete signal is proposed to be understood as a sequence of symbols of an arbitrary alphabet and an arbitrary period, the only rule of construction of which is randomness or pseudo-randomness. Such a discrete signal has the necessary but limited values of "dense packing", correlation and ensemble properties. With this approach, the structural concealment of the signal is provided through randomness or pseudo randomness.

In work [4] the problem of synthesis of nonlinear cryptographic discrete signals was formulated and solved, providing the required values of noise immunity, information and structural stealth of the functioning of the telecommunication system. In general, the problem of synthesizing optimal binary cryptographic signals of a given period is formulated as follows. It is necessary to find a lot of discrete binary sequences - cryptographic sequences (CS) with a given number of symbols possessing the permissible level of maximum side lobes of the periodic autocorrelation function (PACF). Further, the solution of the synthesis problem is reduced to the preliminary selection of a certain limited set of discrete sequences, which seems promising in terms of providing the necessary cross-correlation properties.

It should be noted that in the process of research, a hypothesis was voiced about the possibility of using a cryptographic algorithm for the synthesis of a signal system. For these purposes, the choice of the National cryptographic standard of the block symmetric transformation of DSTU 7624: 2014, which determines the code "Kalina" [5], was justified.

Table 1 shows the results of the synthesis of CS for certain values of the sequence period. Analysis of the data in Table 1 shows that for a sequence period, for example, 63 the number of pairs of CSs corresponding to the established limit value 17 is more than $12{\times}10^6$ (12214869). For sequences with a three-level cross-correlation function (CCF), the number of pairs corresponding to this "boundary" is only 975 pairs. Thus, the ensemble of nonlinear CSs is more than 10^5 times exceeds the ensemble of said linear signals. Exceeding the volume of cryptographic signals over an ensemble composed of m-sequences is more than 10^7 times.

Table 1 – Ensemble properties of cryptographic signals

CS period	Boundary values (*Dense packing*)	PACF	AACF	PCCF		ACCF
		The number of CS satisfying the border "Dense packing"	The number of CS satisfying the border "Dense packing"	Total number of pairs of signals	The number of CS satisfying the border "Dense packing"	The number of CS satisfying the border "Dense packing"
31	9	7 743	3 622	29 977 024	1 465 137	14 537 423
63	17	10 868	7 166	59 056 712	12 214 869	54 822 445
127	23	3482	1302	6 062 162	47 053	1 619 780
511	59	3819	1951	7 292 380	122 835	3 466 713
1 023	100	8 513	6 194	36 235 584	5 293 538	35 083 491

2 Derived signal systems synthesis based on cryptography discrete symbol sequences

Among the systems of phase-shifted signals, many are formed on the basis of Walsh systems [2]. It is known that auto and mutually correlated functions of Walsh sequences have large lateral peaks. To improve the correlation properties of the signals, derivative signal systems (DSS) are generated by multiplying Walsh sequences (source sequences) by a signal that has certain properties (producing a signal), in particular, have small side peaks of the autocorrelation function.

The authors formulated a hypothesis about the possibility of using nonlinear cryptographic sequences as production, the theoretical bases of their synthesis are given in [4]. The method of synthesizing derived signal systems based on the use of CS includes the following steps.

1. The selection of M cryptographic sequences of a fixed period N, which have the minimum values of the maximum side lobes (R_{max}.) PACF.

2. A set of Walsh codes (the matrix N · N) is formed in which each line corresponds to a separate code.

3. The sequences (each of the Walsh code lines of the original sequences) are multiplied by the cryptographic signal, forming N PSS.

4. Investigate the correlation properties of the generated PSS (in particular, PACF, AACF). To investigate the mutual correlation functions, they form a matrix of dimension N · N. The number of such matrices is L · N.

In Table 2, KP (M = 14), selected from the set of sequences, are given by the criterion of the minimum value of the maximum side lobes PACF ($R_{max} < 10$), on the basis of the Hadamar matrix (N = 64). The calculations of the statistical characteristics of the correlation functions (PACF) of the selected CS are also presented here.

Table 2 – CS having minimum values of the side lobes of PACF

1	1 1 1 0 0 0 1 1 1 1 1 0 1 0 0 0 0 1 1 1 1 1 0 1 1 1 0 0 1 1 0 0 1 1 0 0 0 1 0 1 0 0 0 1 1 0 1 0 1 1 0 1 0 0 1 0 0 1 1 0 0 1 0 1
2	1 0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1
3	0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1
4	0 0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1
5	0 0 0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0
6	0 1 0 0 1 0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0
7	0 0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0
8	0 0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0 1
9	0 0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0 1 0
10	0 1 0 0 1 0 1 1 1 0 0 1 1 0 1 0 0 0 0 0 0 0 1 1 0 0 1 0 0 1 0 0 0 0 0 1 0 1 1 1 0 0 1 1 1 0 0 1 1 1 0 1 1 0 0 0 1 0 1 1 0 1 0 0
11	0 0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 0 0 1 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1
12	0 0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 0 0 1 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1 0
13	0 0 0 0 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0 1 1 0 1 1 0 1 1 1 0 0 0 1 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 1 0 1 0 0
14	0 1 0 0 0 1 1 1 1 0 0 0 1 1 0 0 0 0 0 1 0 0 1 1 0 0 1 0 0 0 0 0 0 0 0 0 1 1 0 1 1 1 1 1 0 1 1 1 0 0 1 0 1 0 1 1 0 0 0 0 1 0 1 1 0

Table 3 shows the results of studies of the statistical characteristics of the correlation functions of various classes of signals, including DSS when used as generating cryptographic signals. Calculations were carried out for the values of the sequence periods (from 30 to 2052).

Analysis of the data in Table 3 shows that the statistical characteristics of the DSS are close to the corresponding characteristics indicated in the table of linear and nonlinear signal classes. In this case, the values of the maximum side peaks of the PSS cross-correlation functions are less than for linear M-sequences commonly used in modern telecommunication systems.

Table 3 – Statistical characteristics of correlation functions of different signal classes

Signal Type	Characteristics	$\frac{R_{макс}}{\sqrt{N}}$	$\frac{m_{\|R\|}}{\sqrt{N}}$	$\frac{D^{1/2}_{\|R\|}}{\sqrt{N}}$	$\frac{D^{1/2}_{(R)}}{\sqrt{N}}$
Nonlinear characteristic sequences	AACF	1,6 - 2,4	0,3 - 3,4	1,4 - 7,7	1,9 - 10,8
	PACF	0,02 - 0,5	0,02 - 0,3	0,03 - 0,3	0,06 - 05
	ACCF	1,3 - 3,3	0,5 - 0,7	2,4 - 18,2	3,6 - 27
	PCCF	0,8 - 3,3	0,7 - 0,8	5,8 - 45,3	5,9 - 45,3
DSS	AACF	0,8 - 2,4	0,4 - 0,5	0,9 - 1	1 - 1,1
	PACF	0,7 - 2,5	0,2 - 0,7	0,2 - 0,5	0,3 - 0,9
	ACCF	1 - 2,5	0,2 - 0,7	0,2 - 0,5	0,3 - 0,7
	PCCF	1,4 - 2,8	0,2 - 0,7	0,4 - 0,5	0,6 - 0,9
Nonlinear cryptographic sequences	AACF	0,7 - 2,5	0,4 - 0,5	0,9 - 1	0,9 - 1,2
	PACF	0,9 - 2,5	0,3 - 0,7	0,2 - 0,5	0,3 - 0,9
	ACCF	1,2 - 2,7	0,4 - 0,7	0,3 - 0,5	0,5 - 0,7
	PCCF	1,5 - 2,8	0,5 - 0,7	0,3 - 0,5	0,8 - 0,9
Linear m-sequences	AACF	0,7 - 1,25	0,32	0,26	0,41
	PACF	$1/\sqrt{N}$	$1\sqrt{N}$	0	0
	ACCF	1,4 – 5,0	0,54	0,48	0,73
	PCCF	1,9 – 6,0	0,8	0,62	1

Calculation of statistical characteristics of correlation functions (PACF) CS

1) 64 0 -8 -4 -4 0 -8 0 0 4 0 4 4 -8 -4 8 -4 -4 0 4 4 -4 4 -4 0 8 4 4 -4 -8 -4 0 -8 0 -4 -8 -4 4 4 8 0 -4 4 -4 4 4 0 -4 -4 8 -4 -8 4 4 0 4 0 0 -8 0 -4 -4 -8 0 PFAKmin: -4 PFAKmax: -8 MO: -0.09375 |MO|: 0.46875 DISP: 0.5763694553724894 |DISP|: 0.3384787011890674

2) 64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

3) 64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

4) 64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

5) 64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

6) 64 4 -8 8 4 8 0 -8 8 0 0 -4 -4 4 0 4 0 -8 4 -4 -8 8 4 4 -8 4 4 4 8 4 4 8 -8 8 4 4 8 4 4 4 -8 4 4 8 -8 -4 4 -8 0 4 0 4 -4 -4 0 0 8 -8 0 8 4 8 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.15625 |MO|: 0.59375 DISP: 0.6774495430488349 |DISP|: 0.3469815618916576

7) 64 4 -8 4 4 0 0 4 -4 4 0 -8 4 0 4 0 4 0 -8 0 0 8 0 0 -8 -4 -4 4 8 4 4 4 -4 4 4 4 8 4 -4 -4 -8 0 0 8 0 0 -8 0 4 0 4 0 4 -8 0 4 -4 4 0 0 4 4 -8 4 PFAKmin: 4 PFAKmax: -8 MO: 0.0703125 |MO|: 0.4296875 DISP: 0.5553298776598447 |DISP|: 0.350712702793093

8) 64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0 PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921

9) 64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0 PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921

10) 64 0 -8 4 4 0 -4 4 -8 8 4 -8 4 0 8 0 0 4 -8 0 -4 4 0 0 -8 -4 0 0 4 4 0 0 0 0 0 4 4 0 0 -4 -8 0 0 4 -4 0 -8 4 0 0 8 0 4 -8 4 8 -8 4 -4 0 4 4 -8 0 PFAKmin: 4 PFAKmax: -8 MO: 0.0 |MO|: 0.40625 DISP: 0.5634361794742422 |DISP|: 0.3836429502240921

```
11) 64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0
    0 4 8 8 4 -4 -8 -8 0 4 8           PFAKmin: 4      PFAKmax: 8 MO: 0.0703125       |MO|: 0.5234375
    DISP: 0.6476900319675074      |DISP|: 0.3767205345969094
12) 64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0
    0 4 8 8 4 -4 -8 -8 0 4 8           PFAKmin: 4      PFAKmax: 8 MO: 0.0703125       |MO|: 0.5234375
    DISP: 0.6476900319675074      |DISP|: 0.3767205345969094
13) 64 8 4 0 -8 -8 -4 4 8 8 4 0 0 -4 -8 4 8 8 0 8 4 0 0 -4 -4 -8 -4 0 0 4 -4 4 -4 4 -4 4 0 0 -4 -8 -4 -4 0 0 4 8 0 8 8 4 -8 -4 0
    0 4 8 8 4 -4 -8 -8 0 4 8           PFAKmin: 4      PFAKmax: 8 MO: 0.0703125       |MO|: 0.5234375
    DISP: 0.6476900319675074      |DISP|: 0.3767205345969094
14) 64 8 -4 4 4 0 0 4 -4 -4 4 -4 -8 0 -4 0 8 0 8 -4 -8 -4 -8 8 -8 0 0 4 0 -4 4 4 8 4 4 -4 0 4 0 0 -8 8 -8 -4 -8 -4 8 0 8 0 -4 0 -
    8 -4 4 -4 -4 4 0 0 4 4 -4 8  PFAKmin: -4  PFAKmax: 8 MO: 0.0      |MO|: 0.5
    DISP: 0.6236095697723273      |DISP|: 0.3618734420321171
```

The results of the PCCF DSS study based on CS show that the number of pairs of signals for a sequence of 64 symbols for which the values R_{max} do not exceed 17 (*this, the so-called "tight packing" boundary, achieved in the class of the best, from the VKF viewpoint, sequences with a three-level PCCF*), is 604 pairs (*about 30% of the total number of possible combinations of pairs of signals*). Number of pairs of signals for which the values R_{max} do not exceed 20 – 1577, which is 77% of the total number of pairs of signals. At the boundary $R_{max} < 25$ - maximum number of selected pairs of signals is 1984 (96,8 %). Such values R_{max} occur for sequences that have become most widespread in modern telecommunication systems of the M-sequence.

3 Conclusions

The considered class of complex derivative signals obtained using the proposed method on the basis of the use of nonlinear cryptographic signals has, on the one hand, structural properties analogous to the properties of random (*pseudo-random*) sequences, on the other, the required ensemble and correlation properties.

The characteristics of their auto- and mutual correlation functions of such signals are not inferior to those of the best ones in terms of the correlation properties of discrete sequences (*M-sequences, Gold and Kasami sets, Kamaletdinov ensembles, etc.*). In addition, cryptographic signal systems exist and possess the above properties for a wide range of sequence period values. It is also necessary to note the special property of such signal systems - the possibility of their recovery in space and time with the use of keys and a number of other parameters that are used in the synthesis of signals. The characteristics of the signal systems synthesized using the developed method allow us to talk about improving the quality of the performance of the telecommunications system: noise immunity and information security.

Improvement of these indicators is achieved, in particular due to the possibility of forming, with the resulting method, large ensembles of discrete sequences of almost any period necessary (*for certain system applications*) values side lobe functions cars - mutually and butt-correlation function in a periodic and aperiodic modes, as well as the statistical characteristics of the correlation functions (CF) are not inferior to those of the best in terms of CF, linear to asses signals. Said allows to increase the noise immunity of the reception signals.

The mathematical and software providing the proposed method and computational algorithms for the synthesis of complex nonlinear discrete cryptographic signals systems as well as derivatives of signal systems for which the coprocessors are used as the producing ones are developed. Software and mathematical support obtained in the course of research, realizing the methods of synthesis and research of the properties of systems of non-linear signals, including PSS, is ready for possible use in the composition of prototypes and elements of modern digital communication means.

References

[1] Sarvate D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun. – 1980. – Vol. Com. 68-5.

[2] Varakin L. E. Sistemy svyazi s shumopodobnymi signalami / L. E.Varakin. – Moskva: Radio i svyaz', 1985. – 384 s.

[3] Gorbenko I.D. Sintez sistem slozhnykh signalov s zadannymi svoistvami korrelyatsionnykh funktsii dlya prilozhenii mnogopol'zovatel'skikh sistem s kodovym razdeleniem abonentov / I.D. Gorbenko, A.A. Zamula, E.A. Semenko // Systemy obrobky informacii'. – 2014. – Vyp. 9 (125). – S. 25–30.
[4] Gorbenko I.D. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications / I.D. Gorbenko, A.A. Zamula, Ye.A. Semenko // Telecommunications and Radio Engineering. – 2016. – Vol. 75. – Issue 2. – P. 169–178.
[5] Informacijni tehnologii'. Kryptografichnyj zahyst informacii'. Algorytm symetrychnogo blokovogo peretvorennja: DSTU 7624:2014. – [Chynnyj vid 2015–01–07]. – Kyi'v: Minekonomrozvytku Ukrai'ny, 2015. – 48 s.

Рецензент: Олександр Потій, д.т.н., проф., Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: potav@ua.fm

Надійшло: Квітень 2017.

Автори:
Іван Горбенко, д.т.н., проф., лауреат Державної премії України, Харківський національний університет імені В.Н. Каразіна, Харків, Україна. E-mail: gorbenkoi@iit.kharkov.ua
Олександр Замула, д.т.н., доцент, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: zamylaaa@gmail.com
Владислав Морозов, аспірант, Харківський національний університет імені В.Н. Каразіна, Харків, Україна.
E-mail: morozov@boiko.com.ua

Синтез похідних систем сигналів для додатків сучасних інформаційно-комунікаційних систем.

Анотація. Розглянуто спеціальні вимоги щодо вибору складних сигнальних систем - переносника інформації в інформаційно-комунікаційних системах з підвищеними вимогами до завадозахищеності, завадостійкості, скритності і безпеки інформації. Концептуальна основа для представлення нового класу складних сигналів - криптографічні сигнали. Вказана доцільність використання криптографічних сигналів в інформаційно-комунікаційних системах, а також для формування похідних сигнальних систем з метою підвищення рівня їх завадозахищеності, завадостійкості, скритності і інформаційної безпеки.

Ключові слова: Інформаційна безпека, перешкодостійкість, система сигналів, широкосмугові системи.

Рецензент: Александр Потий, д.т.н., проф., Харьковский национальный университет имени В.Н. Каразина, Харьков, Украина.
E-mail: potav@ua.fm

Поступила: Апрель 2017.

Авторы:
Иван Горбенко, д.т.н., проф., лауреат Государственной премии Украины, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: gorbenkoi@iit.kharkov.ua
Александр Замула, д.т.н., доцент, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: zamylaaa@gmail.com
Владислав Морозов, аспирант, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: morozov@boiko.com.ua

Синтез производных систем сигналов для приложений современных информационно-коммуникационных систем.

Рассмотрены специальные требования по выбору сложных сигнальных систем - переносчика информации в информационно-коммуникационных системах с повышенными требованиями к помехозащищенности, помехоустойчивости, скрытности и безопасности информации. Концептуальная основа для представления нового класса сложных сигналов - криптографические сигналы. Указана целесообразность использования криптографических сигналов в информационно-коммуникационных системах, а также для формирования производных сигнальных систем с целью повышения уровня их помехозащищенности, помехоустойчивости, скрытности и информационной безопасности.

Ключевые слова: Информационная безопасность, помехоустойчивость, система сигналов, широкополосные системы.