UDC 004.9: 621.391.7

# METHODS OF ENSURING ELECTROMAGNETIC COMPATIBILITY IN MODERN INFORMATION COMMUNICATION SYSTEMS

I. Gorbenko, V. Morozov, A. Zamula

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

**Reviewer**: Alexey Stakhov, Doctor of Sciences (Engineering), Full Prof., Academicians of the Academy of Engineering Sciences of Ukraine, International Club of the Golden Section, 6 McCreary Trail, Bolton, Ont., L7E 2C8, Canada
goldenmuseum@rogers.com

Received on September 2017

***Abstract.*** *Requirements are formulated for the choice of complex signals systems – data carriers for use in multi-user broadband telecommunication systems (BTS), which are increased requirements for noise immunity, electromagnetic compatibility, stealth operation and information security data. Conceptual bases are presented of synthesis for a new class of complex signals – cryptographic signals (CS). The justified advisability of application of CS protected BTS, including the construction of derivative signal systems to improve the performance of noise immunity, interference immunity, electromagnetic compatibility transmission security and information security data in protected BTS.*

***Keywords****: multi-user system; the Euclidean distance; the signal ensemble; cryptographic signal; orthogonal signal derivative signal system; the correlation function.*

## 1 Introduction

In the conditions of the development of modern technologies, the commissioning of new control and communication systems, as well as the development of computer and information technologies, a single information and telecommunication space is being created that covers many countries, a gradual transition of communication and automation systems to modern digital ways of transmitting and processing information, automation of management processes is carried out. Moreover, the requirements for electromagnetic compatibility of systems and facilities, integrity, reliability, confidentiality, data authenticity in the process of their storage, transmission and processing are constantly increasing, especially in critical systems of state and regional level. The fulfillment of these requirements is inextricably linked with the need to generalize the already accumulated world experience in the field of information communications and completely depends on the degree of deployment of advanced information technologies for the information transmission and processing.

The rapid growth of information communications and the continuous development of technical means for their provision contribute to the fact that setting the tasks of managing telecommunications networks, traffic, information security, services and quality of service are substantially changing. Meanwhile, such indicators of the effectiveness of information communications systems (ICS), such as electromagnetic compatibility, noise immunity, information security, depend to a significant extent on the properties of physical carriers of information – signals.

Electromagnetic compatibility (EMC) implies the conflict-free existence of various radio engineering systems. Obviously, it is impossible to completely exclude the mutual influence of different systems, the functioning of which is carried out in some relatively small area (*for example, frequency domain*). The task of the system's developer (user), e.g. telecommunications systems, is the elimination or reduction to an acceptable level of undesirable effects of the system, e.g. electromagnetic waves, on other systems. To the ICS, increasingly stringent requirements for ensuring the efficiency of operation in conditions of complex external influences: natural and deliberate interference, interference from other radio systems operating at close frequencies or in the general section of the frequency range.

Modern wireless ICS (*e.g. cellular and satellite systems*), refer to multi-user systems. In such systems, a plurality of channels is located within a common frequency-time resource, so that each

 

subscriber is able to transmit and receive information simultaneously with and independently of other subscribers. When designing such systems, the main problem is the choice of the multiple access method, i.e., the possibility of simultaneous use by many subscribers of the communication channel with minimal mutual influence. If it is necessary to service a large number of subscribers, the time-frequency resource should be significant. One of the problems of multi-user systems is the need to effectively use the frequency band, ensuring the maximum density of radio engineering means per unit bandwidth. This raises another problem of electromagnetic compatibility of radio equipment (subscribers) operating in the general frequency band allocated for the system. One of the methods for increasing the efficiency of using the frequency range in terms of electromagnetic compatibility is the use of code division of channels (subscribers) operating in the common frequency band, also known as code division multiple access (CDMA). With this method of information transfer, each subscriber is allocated in a wideband signal (signature) from a plurality of orthogonal signals, and each signal occupies the entire band and the entire time interval. In this case, when a user signal occupies both the entire available band and the entire time interval, that is, the need to apply an orthogonal multiple access scheme in which all user signals are broadband. Such a multi-user system will have all the advantages of broadband technology [1]. In an asynchronous multiple access method with CDMA, the delays of various signals at the input of the receiver can vary over a wide range. In this case, the procedure for synchronizing broadband signals (signatures) becomes problematic. This is due to the fact that the signatures of different subscribers, having overlapping spectrum, cannot remain orthogonal in a wide range of mutual delays. The consequence of this is the occurrence of an inter-user interference (*multiple-access interference*), the manifestation of which is the non-zero response of the receiver tuned to the i-th subscriber from the signals of other subscribers. For applications of telecommunication systems in which an asynchronous method with CDMA is used, the choice of signals must be made in such a way as to minimize mutual interference, i.e. ensure electromagnetic compatibility. In particular, such user signals (signatures) must have special properties of mutually correlating functions.

## 2 The problem of electromagnetic compatibility in information systems

When studying the EMC problem, we will assume that there are two parties involved in the information exchange process. The first of these is the system that carries out the data transfer (*let's call it the "radiating system"*). The second is the system adjacent to the first (the "interacting" system). For the radiating system, the signals of the interacting system can be interpreted as interference (*narrowband, broadband, structural, retransmitted, etc.*). We also assume that the most characteristic type of interference acts in the channel, described by a Gaussian random process whose spectrum coincides with the signal spectrum. With this approach, the error probability depends only on the ratio $q^2$ of the signal to the total interfering effect. The indicated parameter is found from the relation [1]:

$$q^2=2E/N_0+P_п/F, \quad (1)$$

where: E – signal energy; $N_0$ – spectral power density of thermal noise; $P_п$ – interference power; F – bandwidth.

The term $P_п/F$ – in fact, an additional white Gaussian noise with spectral density $P_п/F$.

As follows from the relation (1), the use of broadband technology (*broadband signals*) allows successfully solving the problems of EMC systems and withstanding interference effects. It is quite obvious that the wider the signal bandwidth F, the smaller the additional spectral density (*at a constant value of the interference power $P_n$*) and, thus, the ratio $q^2$ of the signal powers to the common interfering effect is greater. It is extremely important, from the EMC point of view, that the peak signal power may be limited by the relevant international and national regulatory documents, and the extension of the signal band is realized not by increasing the signal duration, resulting in a decrease in signal energy and value $q^2$.

Broadband (interference) interference affects the signal as an additional white Gaussian noise with a power spectral density $N_п=P_п/F$. In this case, the ratio $q^2_п$ the signal powers to the total inter-

fering effect at the output of the matched filter of the radiating system will be estimated from the relation

$$q^2_{п}=2E/N_0+N_{п}=2E/N_0+P_{п}/F. \quad (2)$$

The last relation coincides with the relation (1). The only difference is that the interacting system, the spectrum of which completely coincides with the signal spectrum of the radiating system, can realize a much greater suppression effect in comparison with white Gaussian noise. In the case where the ratio $P_{п}/F$ much bigger $N_{0,}$ expression (2) takes the form

$$q^2=2\cdot E\cdot F/P_{п}=2\cdot P\cdot F\cdot T/P_{п,} \quad (3)$$

where P, T – respectively, the power and duration of the signal of the radiating system.

It follows from (3) that when limiting the peak power of the radiating and interacting systems, the only method of ensuring EMC and noise immunity of data reception is the use of broadband signals, i.e. signals having a large value of the product F·T, the so-called processing gain. The task of the designer of ICS is to select such a processing gain that would provide a sufficiently low level of the power spectral density of the applied signals with respect to the noise spectral density at the input of the receiver of the neighboring system.

The above results are valid for the case when the noise is a normal random process and has a uniform spectral density. The neighboring system can use in the process of information exchange signals similar to those used by the radiating system, from the point of view of the law of manipulation, creating so-called structural interference with an uneven spectrum. Under such conditions of functioning of the ICS, noise immunity is largely determined by the similarity (difference) in signal structures and interference, i.e. the way in which individual elements of a signal are suppressed.

Let the signal power of the radiating system - $P_c$, and the power of the interfering component produced by the interacting system - $P_{п}$. The power of the signal component at the output of the matched filter at the time of making the decision (reference) is proportional $P_c$, and the power of the interfering component $P_{П}R^2_{jk}(\tau)$, where $R^2_{jk}(\tau)$ – the cross-correlation function (CCF) of the useful k-th signal and the j-th interfering signal. Value τ is determined by the shift of the CCF relative to the reference time. The signal-to-noise ratio at the output of the optimum reception device will be [2]:

$$q^2(\tau)=\frac{P_c}{P_{п}R^2_{jk}(\tau)}. \quad (4)$$

The smallest signal-to-interference ratio will be

$$q^2(\tau)=\frac{P_c}{P_{п}R^2_{max}(\tau)}, \quad (5)$$

where $R_{max}$ – is a maximum value $R_{jk}(\tau)$.

As follows from (5), in order to ensure a satisfactory EMC and in order to increase the noise immunity of receiving data in multi-user ICS, it is necessary to select signals for which the maximum CCF peaks are minimal.

If the maximum peaks of CCF are reduced to the root-mean-square level $\sigma_{j,k}=\sigma^2$, then the signal-to-interference ratio will be

$$q^2(\tau)=\frac{P_c}{P_{п}}\ \sigma^2\cdot \quad (6)$$

For example, if: $\sigma^2=\frac{1}{2FT}$, then

$$q^2 = \frac{P_c}{P_п} 2FT, \quad (7)$$

where FT=B – signal base.

For discrete phase-shifted signals $\sigma^2 = \frac{l}{2N}$ (N – number of signal elements). For such signals

$$q^2 = \frac{P_c}{P_п} 2N. \quad (8)$$

It follows from formulas (7), (8) that the increase in the signal base increases $q^2$ (*and hence the noise immunity of the system*). In addition, these expressions indicate the way of ensuring EMC of systems operating in a sufficiently close region. This decrease in the ratio $\frac{P_c}{P_П}$ (*in the case of an increase in the radiation power of the station* ($P_п$)) by increasing the signal base of the radiating system.

Typical for communication theory is the approach of developing an optimal receiver that will restore the information contained in the observed oscillation with the best quality. The determination of the optimal processing algorithm based on the account of the specific properties of the transmitted signal allows one to synthesize, in an optimal way, the signal itself, i.e. choose the best way of its coding and modulation [1-4].

In communication theory, the most common model is a channel with additive white Gaussian noise, in which the probability of a channel transforming a given input signal into an output observation $y(t)$ (transition probability - $P\left[y(t)|S(t)\right]$) exponentially decreases with increasing square of the Euclidean distance between the transmitted signal and the output observation [1]:

$$P\left[y(t)\,|\,S(t)\right] = k\exp\left(-\frac{1}{N_0}d(s,y)\right), \quad (9)$$

where k – constant independent of S(t) and y(t), $N_0$ – single-sided white noise spectral density.

The Euclidean distance between S(t) and y(t) is defined as

$$d(S,y) = \sqrt{\int_0^T [y(t) - S(t)]^2 dt}. \quad (10)$$

According to relations (9) and (10), the similarity of the signal (the probability that it is converted by the channel into observation y(t)) decreases with increasing Euclidean distance between S(t) and y(t). In the case of equal probability of all source messages, the maximum likelihood criterion (MLE) is the optimal strategy of the observer providing the minimum error in making a decision on the actually transmitted signal. According to this rule, after the y(t) oscillation is accepted, the decision is made in favor of the signal for which the probability of its channel transformation into the received observation y (t) is the largest *(in comparison with the probabilities for other signals*).

In view of the foregoing, the MP solution for the Gaussian channel can be transformed into a minimum distance rule

$$d(S_j, y) = \min d(S_i, y) \Rightarrow H_j, \quad (11)$$

i.e. the decision is made in favor of the signal $S_j(t)$, since it is closest (in the sense of the Euclidean distance) to the observation of y (t) among all possible signals.

Expanding the brackets in (10), we arrive at the relation

$$d^2(S_i, y) = \int_0^T y^2(t)dt - 2\int_0^T y(t)\cdot S(t) + \int_0^T S^2(t)dt = \|y\|^2 - 2Z_i + \|S_i\|^2, \quad (12)$$

where $Z_i$ - correlation between observation of $y(t)$ and $i$-th signal $S_j(t)$

$$Z_i = (y_i, S_i) = \int_0^T y_i(t)S_i(t)dt. \quad (13)$$

The first term on the right-hand side of relation (12) is fixed for this observation and does not affect the decision which of the signals was adopted. The last term is the energy of the i-th signal $E_i$. Then, the minimum distance rule (11) can be formulated as a rule of maximum correlation:

$$Z_j - \frac{E_i}{2} = \max(Z_i - \frac{E_i}{2}). \quad (14)$$

which means, in particular, that of M possible signals with the same energy, the one that has the maximum correlation with the observation $y(t)$.

One of the limitations in the synthesis of signals is the dimension of the signal space within which their packaging is carried out. The physical essence of this limitation is due to the practical resource, for example, the bandwidth of the frequency band. If the time-frequency resource in which the M signals can be located is limited by the parameters ΔF a T, accordingly, one of the limitations takes into account the bandwidth savings, while the second reflects the desire to transmit data at an acceptable rate $R=\log M|T$. Then, according to the counting theorem, there is about ΔFT independent samples that can be used in the synthesis of M signals, and each of the signals is treated as a vector in a space of dimensionality $n_S=\Delta FT$.

The problem of selecting a set of signals can be formulated as follows: find in a space of a given dimension $n_s$ a constellation of M vectors satisfying energy constraints and having the maximum possible minimum distance between vectors $dmin=max$. With allowance for expressions (13)–(14), signals with the smallest value of the maximum side lobe are preferred. Thus, the requirements for the best signal can be formulated in the form of the following optimization problem: on the set of all possible sequences of length N with symbols from a pre-selected alphabet, find a sequence or sequences with the minimum value of the maximum lateral lobe of the correlation function.

## 3 Discrete signals synthesis methods

At present, there are no regular methods for synthesizing discrete sequences (DS) optimal by the minimax criterion. Moreover, it is not possible to answer the question: how well-known signals with a large number of N positions are close to optimal. Therefore, it is urgent to find effective methods for synthesizing DS with good minimax properties.

One of these methods is based on the use of iterative algorithms [2]. With an appropriate choice of the initial approximation and the use of integer optimization with respect to the minimax or medium-level criteria, it is possible to obtain comparatively good signals in this sense. However, the lack of iterative methods is a dependence on the initial approximation, a sharp increase in the calculation time of the signal with increasing N, and the fact that they lead only to a local extremum.

The method of synthesizing DP by means of a homomorphic map of the multiplicative groups of the simple and extended Galois fields with the aid of the K-valued character [3] deserves attention. Studies have shown that with the increase in the field characteristics and the number of classes, the volume of calculations for directional search sharply increases.

Other methods assume the search for the necessary conditions for the existence of a DP with given parameters. An example of such an approach is the following. It is known [1-5] that sequences with a good aperiodic autocorrelation function (ACF) can be found only among sequences with good periodic ACF. At the first stage, a set of candidate sequences with a good periodic ACF is

formed. At the second stage, an exhaustive search is performed by the criterion of the lowest level of the side lobe maximum of aperiodic ACF among all cyclic shifts of one-period segments of candidate sequences. The result of the search is a sequence with a minimum value of the side lobes of aperiodic ACF.

The known methods of synthesis of DP with given correlation functions are almost always based on conducting operations to search through a variety of options for selecting the best result, and for a significant period of DP, the application of such methods becomes problematic.

In multi-user systems with code division, families of discrete signals with special mutual correlation properties are necessary. Synthesis of families of signals with the necessary cross-correlation properties consists in the search for a family of sequences with corresponding mutually correlating functions. In this paper, we present methods that allow the synthesis of systems of nonlinear discrete complex signals with given, for certain ICS applications, correlation, ensemble, and structural properties.

Since the code division is based on the difference in signals, the construction of multi-user systems and their characteristics are determined by the choice of signals and their properties. Usually the number of subscribers is large enough, so the choice of signals for ICS applications (*mobile communication systems, space communication systems, etc.*) is reduced to the synthesis of signal systems with given ensemble, correlation and other properties. The development of multi-user ICS based on code division of signals and led to research in the theory of signal systems.

The appearance in recent years of new areas of use of pseudorandom sequences required an additional and more thorough study of their ensemble, correlation, structural, and other properties. For example, the increased interest in broadband has stimulated the study of aperiodic correlation functions, and not just periodic ones. The application of code division multiplexing methods in systems with multiple access and, as a consequence, the problems of EMC of various systems, required a deeper analysis of the mutual-correlation properties. The necessity to counteract the mutual interfering influence of ICS led to the search (synthesis) of signals with specified correlation, structural, ensemble, technological and other properties.

For most applications, in particular for broadband systems with multiple access, interesting are not pairs, but large sets of sequences with good cross-correlation properties, improved ensemble and structural properties. In some systems, the number of concurrent sequences can exceed several hundred. There are large sets of periodic sequences (Kasami, Gold, etc.), which have comparatively small side lobes of mutual-correlation functions [6-10]. 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-physical carriers of information in the ICS.

The need to use protected radio channels forces researchers to look at the modes of functioning of the protected radio channels and the aspects of the formation and application of complex signals in a new way. Therefore, in our opinion, today new approaches and new views are needed on the application processes and functions of complex signals in order to create secure ISS. Fundamental here, in our opinion, is a new understanding of the methods of ensuring information stealth and imitation resistance, that is, functions that are implemented in traditional systems with the use of systems and means of cryptographic information protection [11]. 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, and at the same time, the signals must possess: absolute structural concealment with respect to the laws of their formation and signal change in a dynamic mode; improved ensemble properties (*exist for almost any period value, have a significant amount of signal system*); necessary to ensure the required value of noise immunity, correlation properties.

The authors formulated and solved the problem of synthesis of nonlinear cryptographic discrete signals (CS) providing the required values of noise immunity, information and structural stealth of the ICS operation [12-13]. In conditions of intensive information counteraction of the parties, interests and competition of which can manifest themselves in various spheres, including, as recent

events have shown, in the sphere of information and hybrid wars, the availability and use of secure ICS is of particular importance. To a significant extent, such systems are based on the use of protected radio channels. At the same time, under the security of systems, it is necessary to understand in a broad sense, first of all, their ability to provide the necessary EMC, noise immunity, imitating, information, energy and structural stealth. Increased requirements for the effectiveness of the operation of ICS in the context of internal and external influences are largely ignored by existing information technologies. There is a contradiction between the stringent requirements for the provision of EMC systems and facilities, reliability, secrecy, confidentiality, integrity of data transmitted via the ICS communication lines, on the one hand, and existing models, methods and technologies of control over ICS, information security (IS), services and quality of service, on the other hand. The main ways to solve this contradiction is to provide EMS systems and tools, increase noise immunity and ISS IR by improving the methodological foundations of ICS construction by creating new models, methods and technologies for managing telecommunications networks, information security, services and quality of service, developing information exchange methods, synthesis methods new classes of nonlinear complex discrete signals – data carriers with the necessary ensemble, correlation and structural properties.

By cryptographic discrete signals (CS) it is proposed to understand a set of sequences (vectors) of symbols of a certain alphabet, which necessarily have the necessary structural, ensemble and correlation properties, temporal and spatial complexity, and the possibility of forming on the basis of keys [12]. Rules for constructing the CS are based on the use of random or pseudo-random processes, which must meet the requirements of randomness, irreversibility, unpredictability, etc. [14].

## 4 Discrete cryptographic signals model

Let us formulate in general form the problem of synthesis of CS.

The task of constructing (synthesizing) the CS will be understood as the problem of constructing subsets of discrete sequences $(W_l^q), q=\overline{1,N}, l=\overline{1,L}$, the set of which forms a system of discrete signals of a given alphabet of dimension $M_k = N \times L$, such that in each of the subsets (the dictionary) the conditions imposed on the subsets of the CS in terms of structural, ensemble, correlation properties, the spatial and temporal complexity of their generation.

The construction of the CS is based on the analysis and use of periodic and aperiodic correlation functions and reduces to the following stages.

1. Ensuring the conditions for meeting the requirements for structural and ensemble properties, the ability to form a subset of the COP with allowable temporal and spatial complexity, including using keys.

2. Constructing a CS $W^q$, periodic autocorrelation function (PFAC) of each of which satisfies the system of nonlinear parametric inequalities (NPI):

$$R_{a_1}^q(l) \le \sum_{i=1}^{L} W_i^q (W_{i+l}^q)^* \le R_{a_2}^q(l), \quad l=\overline{1,L-1}, \quad q=\overline{1,N}, \tag{15}$$

where $R_{a_1}^q(l)$ and $R_{a_2}^q(l)$ – given PFAC implementations, and the indices are calculated modulo (*i*+*l*) *mod L*.

If $l=L$ for all $q=\overline{1,N}$ (15) gives convolution with value $L$:

$$\sum_{i=1}^{L} W_i^q W_{i+L}{}^q = \sum_{i=1}^{L} W_i^q W_i^q = L, q=\overline{1,N}, \tag{16}$$

3. Construction of pairs KC $W^q$ and $W^p$, the cross-correlation functions (CCF) which satisfy the requirements, which are determined by the set of NPI systems (16), and also meet the requirements for the cross-correlation joint function (CCJF) $W^q$ and $W^p$ concordant discrete words $W^{qp}$ and $W^{pq}$ (17-21):

$$R_{b_{1,1}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,1}}^{qp}(l); \quad (17)$$

$$R_{b_{1,2}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,2}}^{qp}(l); \quad (18)$$

$$R_{b_{1,3}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^q)^* \le R_{b_{2,3}}^{qp}(l); \quad (19)$$

$$R_{b_{1,4}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^q)^* \le R_{b_{2,4}}^{qp}(l); \quad (20)$$

$$R_{b_{1,5}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^p)^* \le R_{b_{2,5}}^{qp}(l); \quad (21)$$

Besides, $l=\overline{1,L-1}$ for all kinds of combinations $q$ and $p$, $q=\overline{1,N}$, $p=\overline{1,N}$, $q \ne p$, where $R_{b_{1,j}}^{qp}(l)$ and $R_{b_{2,j}}^{qp}(l)$, - specified (necessary) implementations PCCF and CCCF respectively ($j=\overline{1,5}$).

In systems NPI (15), (16) and (17–21) $W_i^q$ and $W_i^p$ are unknown values of random or pseudo-random CS symbols $W^q$ and $W^p$, $q=\overline{1,N}$, which are subject to determination in the process of their construction. In what follows, the systems (15–16) and (17–21) will be called the model of the subset (dictionary) of the CS.

We analyze systems of nonlinear parametric quadratic inequalities (hereinafter systems) (15), (16) and (17)–(21) using the introduced model.

The systems (18) and (20) with l=L for all $q=\overline{1,N}$ must give a complete convolution with the value of $L$, that is (18):

$$\sum_{i=1}^{L} W_i^q W_i^q = L, q=\overline{1,N} \quad (22)$$

and (20) gives

$$\sum_{i=1}^{L} W_i^p W_i^p = L, p=\overline{1,N}. \quad (23)$$

The systems (17), (19) and (21) with $l=L$ for all pairs $W^q$ and $W^p$ give the values of the cross-correlation function with zero shift:

$$\sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0); q, p=\overline{1,N}, \quad (24)$$

$$\sum_{i=1}^{L} W_i^q W_i^p = R^{qp}(0), q, p=\overline{1,N}, \quad (25)$$

$$\sum_{i=1}^{L} W_i^p W_i^q = R^{pq}(0), p, q=\overline{1,N}. \quad (26)$$

In what follows, the systems (15–16), (17–21) and the quadratic equation (24) will be called the model of the subset (dictionary) of the CS.

We will analyze systems (15–16) for the existence of solutions and independence. It follows directly from (15) that for each of q CS $W^q$ there are $L$ unknowns $W_1^q, W_2^q \cdots W_L^q$. To find them, ac-

cording to (15), we can construct a system of $L$–1 independent NPI. Further, using (16), we obtain one more expression, but an equation. The peculiarity of the system (15) is that it gives a convolution of each of the CS with the value L. On the basis of (15) and (16) in the construction of each N subset of the CS, one can compile N independent systems of quadratic NPIs, each of which will contain $L$–1 quadratic inequalities of the form (15) and formally one equation, so that there will be only $L$.

We also analyze the set of systems of parametric inequalities (17–21), taking into account (22), (26), for the existence of solutions and the independence of systems and individual equations. The systems (17–21) determine the permissible mutual properties relative to PCCF and CCCF of each pair of CS - $W^q$ and $W^p$. They define the requirements for PCCF and CCCF specifically for only two CS $W^q$ and $W^p$. When constructing three CS, we have 3!/2, and for N CS, respectively, N!/2 of such systems.

Thus, with increasing N, the number of systems of the form (17–21) increases exponentially (by factorial).

For N=2, among the (22)–(26) systems of NPI there are redundant nonlinear quadratic equations. Equation (16) coincides with (22) and (23) because the last two already enter the system (16), are dependent, and therefore cannot be used. Further, equation (24) and (25) coincide, and equation (26) is symmetric, in part of the correlation function, with respect to equations (23) and (25). Therefore, for each pair of p and q, (24) is independent.

On the basis of detailed analysis, we have that all (17–21) NPI systems determine the different implementations of PCCF and CCCF specifically for only two CS - $W^q$ and $W^p$. Therefore, the mathematical model for constructing two CS $W^q$ and $W^p$ is uniquely determined by the five NPI systems in the form (17–21) and, as already justified, by the equation (24).

The above analysis results allow to determine the complexity of the model and on its basis the complexity of constructing a subset of N CS.

1. When constructing one CS, it is necessary, depending on the allowable values $R^q_{a_1}(l)$ and $R^q_{a_2}(l)$, defined by the limits of dense packaging, consider v ≥ k systems of the form (15-16).

2. When constructing two CS, it is necessary to consider $v_2 \geq k_2$ systems of the form (17-21), where $k_2$ is determined from $R^{qp}_{b_{1,j}}(l)$ and $R^{qp}_{b_{2,j}}(l)$.

3. When constructing N CS, it is necessary to consider $v_N \geq k_N$ systems of the form (17-21), where $k_N$ is determined $R^q_{a_1}(l)$ and $R^q_{a_2}(l)$, and also $R^{qp}_{b_{1,j}}(l)$, and $R^{qp}_{b_{2,j}}(l)$ allowed values.

Thus, on the basis of accounting for the boundaries of the physical packing of the subset of CS [1], there are possibilities to construct subsets of the CS according to (15–16) and (17–21), using aperiodic autocorrelation functions (AACF). In this case, simplifications are possible. So the system (15–16) by analogy can be represented in the form of an NPI system on the basis of aperiodic correlation functions, that is,

$$r^q_{a_1}(l) \leq \sum_{i=1}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r^q_{a_2}(l),\ l=\overline{1,L},\ m=\overline{1,L}, \tag{27}$$

where $r^q_{a_1}(l)$ and $r^q_{a_2}(l)$ – prescribed, but feasible, implementations in terms of tight packaging. Further, the systems (15–16) and (17–21) can also be represented in terms of aperiodic mutual correlation functions (ACCF) in the form of a system of nonlinear parametric inequalities

$$r^{qp}_{b_{1,1}}(l) \leq \frac{1}{L-m} \sum_{i=0}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \leq r^{qp}_{b_{1,2}}(l); \tag{28}$$

$$l=\overline{1,L},\ m=\overline{1,L},$$

$$r_{b_{2,1}}^{qp}(l) \le \frac{1}{L-m} \sum_{i=0}^{L-m} W_i^p \left(W_{i+1}^q\right)^* \le r_{b_{2,2}}^{pq}(l); \quad (29)$$

$$l = \overline{1, L},\ m = \overline{1, L},$$

where $r_{b1,1}{}^{qp}, r_{b1,2}, {}^{qp}\, r_{b2,1}, {}^{qp}\, r_{b2,2}{}^{qp}$ - permissible from the point of view of close packing AACF and ACCF.

## 5 Problem solution for synthesis of a system of nonlinear discrete complex cryptographic signals

The use of CS will improve the performance of ICS, in particular: EMS, noise immunity (noise immunity of receiving signals under the influence of structural, obstructive, retransmitted and other types of interference, stealth operation) and information security. Such discrete signals have the necessary but limited ("tight packing" values), correlation and ensemble properties. With this approach, the structural concealment of the signal is provided by randomness or pseudo randomness, and noise immunity is provided by the correlation properties of the synthesized system of signals. Information security of ICS is provided on the basis of the fact that the statistical properties of CS are close to the properties of random sequences, as well as the use of cryptographic keys. It is necessary to note the special property of CS 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 authors proposed a method for synthesizing systems of complex nonlinear cryptographic signals, including the following stages [13].

1. Formation of random or pseudorandom discrete sequences using key data.
2. Estimation of statistical properties of potential CS.
3. Building the required number of potential CS $W^q$ in accordance with the system of inequalities (15) and key data.
4. Finding pairs or subsets of the CS $W^q$ and $W^p$, which satisfy the requirements (17–21).
5. The construction of the matrix of states of the mutually correlated functions of all possible pairs of potential CS, which were selected by the results of the previous step and have all the necessary properties.
6. The analysis of the matrix of states and the formation of the necessary number of subsets or pairs of CS according to (15–16) and (17–21) and selection in the subset of only those pairs that satisfy the requirements.

Examples of pairs and subsets of CS are given in [13].

Taking into account the need to ensure the cryptographic stability and structural concealment (complexity) of the cryptographic signal, the choice of the algorithm of symmetric block encryption with the counter is justified as a source of pseudorandom sequences of symbols (*the first stage of the method*): The national cryptographic standard of the block symmetric transformation of DSTU 7624:2014, "Kalyna" and its modes of operation to ensure confidentiality and integrity of information [15]. Alternatively, a source based on the AES algorithm (international standard ISO/IEC 18033) may be proposed. Preference in the selection is given to DSTU 7624:2014, taking into account the following factors.

Block symmetric ciphers (BSC) are one of the most common cryptographic primitives [16-18]. In addition to securing the confidentiality (*encryption*) of the main volumes of information transmitted over the network or stored locally, they are used as a constructive element of other primitives (hashing functions, message authentication codes, pseudorandom sequence generators, etc.). The importance of this cryptographic transformation is underscored by a number of international competitions, such as AES, NESSIE, CRYPTRACK, which were focused on the development of block cipher (*as the main goal or as part of a set of promising solutions*).

The national standard supports the block size and encryption key length of 128, 256 and 512 bits (*the key length is equal to the block size or twice as large*), providing a normal, high and ultra high

level of durability (*now it is the only block encryption standard in the world supporting 512- bit symmetric keys*). Different variants of the standard provide flexibility of choice of parameters for developers of cryptographic protection systems, which makes it possible to obtain both the highest level of performance and the largest margin of conversion stability. The high-level design uses a well-researched Square-like SPN structure used in the algorithms of AES/Rijndael, Whirlpool, Stribog and many others. The cycle transformation is constructed on the basis of tables of substitution (S-blocks) and multiplication by an MDS-matrix over a finite field, providing necessary cryptographic properties. The use of such a design makes it possible to provide provable stability with respect to differential, linear and other types of cryptanalysis, while simultaneously providing an effective implementation for a wide range of software and hardware/software platforms. When choosing the size of the MDR-matrix, the size of the L1 cache of modern and promising processors was taken into account, which made it possible to optimize the performance of the software implementation of the cipher [19-22]. The standard of Ukraine provides the greatest nonlinearity of Boolean functions, which gives an additional margin of stability in relation to linear cryptanalysis. In addition, in our opinion, the standard of block symmetric transformation of DSTU 7624: 2014 refers to post-quantum algorithms, i.e. it will ensure (*when selecting the appropriate parameters*) cryptographic resistance against attacks with the use of quantum computers [11].

## 6 Nonlinear discrete complex cryptographic signals properties

Tables 1 and 2 show the results of studies that illustrate the possibility of applying the above method of signal synthesis for a number of applications of ICS.

Table 1 – Correlation properties of cryptographic discrete sequences

| CS segment size | Limit values of the uncertainty function | PACF | | | AACF | PCCF | | |
|---|---|---|---|---|---|---|---|---|
| | | The number of CS satisfying the boundary | The smallest value $R_{6max}$ | The number of CS with the least $R_{6max}$ | The number of CS that satisfy the boundary | Total number of pairs | Number of pairs satisfying the boundary | The smallest value $R_{6max}$ |
| 64 | 17 | 9 545 | 8 | 14 | 4 931 | 45 553 512 | 5 451 589 | 10 |
| 1 024 | 90 | 2 209 | 72 | 3 | 1 149 | 2 439 840 | 26 638 | 82 |
| 30 | 9 | 2 479 | 2 | 2 | 973 | 3 072 720 | 95 722 | 6 |
| 31 | 9 | 7 743 | 5 | 155 | 3 622 | 29 977 024 | 1 465 137 | 5 |
| 63 | 17 | 10 868 | 9 | 14 | 7 166 | 59 056 712 | 12 214 869 | 11 |
| 127 | 25 | 6 798 | 17 | 51 | 3 636 | 23 106 402 | 1 266 098 | 19 |
| 127 | 27 | 10 006 | 17 | 51 | 6 491 | 50 060 018 | 9 006 648 | 19 |
| 511 | 63 | 7 662 | 45 | 6 | 4 783 | 29 353 122 | 2 666 671 | 51 |
| 1 023 | 100 | 8 513 | 70 | 4 | 6 194 | 36 235 584 | 5 293 538 | 81 |

So, in Table 1, in accordance with the method described above, the results of synthesis of discrete sequences for some values of the sequence period are presented, in particular, the following are given: boundary values for maximum emissions of correlation functions satisfying the "tight packing" boundaries [1-3]; the number of pairs of sequences constituting a complete ensemble of signals (*for estimating the cross-correlation properties of signals*); the number of signals satisfying the boundary values for different correlation functions. Table 2 gives estimates of the number of pairs of sequences of different classes (*M-sequences, sequences with a three-level cross-correlation function – PCCFT, cryptographic sequences (CP))* that satisfy the "close packing" boundary for the corresponding period [5,13].

Table 2 – The ensemble properties of various complex signal systems

| Type of signals | Sequence Period | "Dense packing" border value | Sequences pairs number satisfying the boundary |
|---|---|---|---|
| **M-sequences** | 31 | 9 | 3 |
| **PCCFT** | 31 | 9 | 495 |
| **CS** | 31 | 9 | 1465137 |
| **M-sequences** | 127 | 27 | 36 |
| **PCCFT** | 127 | 17 | 11610 |
| **CS** | 127 | 23 | 47 053 |
| **M-sequences** | 255 | 36 | 28 |
| **PCCFT** | – | – | – |
| **CS** | 255 | 36 | 17599 |
| **M-sequences** | 511 | 63 | 276 |
| **PCCFT** | 511 | 33 | 147500 |
| **CS** | 511 | 63 | 2666671 |
| **M-sequences** | 1023 | 100 | 435 |
| **PCCFT** | 1023 | 65 | 338000 |
| **CS** | 1023 | 100 | 5293538 |

The analysis of the data in Table 1-2 shows that the proposed method for synthesizing complex nonlinear discrete cryptographic signals using random or pseudorandom processes allows the formation of large ensembles of discrete sequences of almost any period with given, but physically realizable, side lobes of auto-mutual and butt correlation functions in periodic and aperiodic modes of operation, as well as statistical characteristics of correlation functions that are not inferior to anal tech characteristics of the best classes of linear signals. Thus, for the period of the sequence N=63, the number of pairs of cryptographic discrete sequences satisfying the established limit value of the maximum side lobes PCCF-17 is 12,214,869. For a representative of a class of linear sequences – sequences with a three-level cross-correlation function (*Gold sets that are optimal from the point of view functions of cross-correlation signals* [6]), the number of pairs of signals satisfying this boundary is -975. Exceeding the volume of cryptographic signals over the ensemble composed of M-sequences is more than $10^7$ times. For the period of the sequence 1023, the number of pairs of cryptographic discrete sequences satisfying the established boundary value for the side lobes of the cross-correlation functions (CCF) -100 is 5293538, whereas for a representative of the class of linear sequences of M-sequences, the number of pairs satisfying this boundary is -43 i.e. exceeding the volume of the signal system is more than 105 times. It should be emphasized that the law for the formation of each of the cryptographic signals is determined by the key, and the length of the key can be substantially smaller than the period (length) of the signal itself. With a slight decrease in the requirements for the maximum peak side peak CCF, according to which signals are selected (*in fact, decrease in noise immunity of reception*), the indicators of imitating resistance of IKS operation can be significantly improved. Thus, for the period of the sequence N=127, an increase in the boundary value by 1.2 dB, will increase the volume of the ensemble with M=11610 at the boundary $R_{bmax}$=17, to 9,006,648 signals, with a boundary value of 27, i.e. in 776 times.

The performed calculations and simulated simulation indicate that the maximum lateral emissions of the correlation functions of the CS, as well as the statistical characteristics of this class of signals, are not inferior to the corresponding characteristics of linear M-sequences [8].

Thus, varying the boundary values of the level of the side lobes of the corresponding correlation function, depending on the requirements imposed on the ICS from the point of view of noise immunity of receiving signals, the system can be solved to achieve the required noise immunity of signal reception, imitating and information stealth ICS.

In Table 3 shows examples of calculating the statistical characteristics of various correlation functions for discrete signals widely used in communication systems and, in particular, the characteristics of cryptographic DS These characteristics were obtained using the developed special software. Calculations were carried out for different values of the DS period. As statistical characteristics of the correlation functions:

- greatest lateral emissions values $R_{max}$;
- mathematical expectation value of the emission module $m_{|R|}$;
- standard deviation value of the emission module $D_{|R|}^{1/2}$ and emission values $D_{R}^{1/2}$.

Table 3 – Statistical characteristics of the correlation functions of discrete signals

| Type of signals | Characteristics | $\frac{R_{макс}}{\sqrt{N}}$ | $\frac{m_{\|R\|}}{\sqrt{N}}$ | $\frac{D_{\|R\|}^{1/2}}{\sqrt{N}}$ | $\frac{D_{(R)}^{1/2}}{\sqrt{N}}$ |
|---|---|---|---|---|---|
| Characteristic discrete signals | AACF | 1,0 – 1,8 | 0,5 | 0,4 | 0,5 |
| | PACF | 0,1 – 1,9 | 0,2 | 0,1 | 0,2 |
| | ACCF | 1,9 - 3,2 | 1,0 | 0,8 | 1,0 |
| | PCCF | 2,5 – 3,6 | 1,0 | 0,8 | 1,2 |
| | CCCF | 2.1 – 5,0 | 0,9 | 0,7 | 1,1 |
| 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 | 1,0 |
| | CCCF | 2,0...5,1 | 0,83 | 0,62 | 1 |
| Cryptographic signals | AACF | 1,2 – 1,9 | 0,5 | 1 | 1,1 |
| | PACF | 0,2 – 1,9 | 0,6 | 0,4 | 0,7 |
| | ACCF | 1,4 – 3,4 | 0,5 | 0,4 | 0,6 |
| | PCCF | 1,9 – 5,2 | 0,7 | 0,5 | 0,8 |

Analysis of the data given in Table 3, indicates that the values of the maximum lateral emissions of the CS, as well as the statistical characteristics of this class of signals, are not inferior to the corresponding characteristics of signals constructed using M-sequences and characteristic discrete signals [3]. As illustrations in Fig. 1 to 3, various correlation functions for the cryptographic DS synthesized according to the method described above.

For many applications of ICS, a situation is typical where individual stations intentionally have a negative effect on the functioning of the radiating system. In such cases, the electromagnetic compatibility, information security and noise immunity of ICS is largely determined by the structural or statistical properties of the data-sending signals in the system. In the face of EMC countermeasures, the radio channels interference immunity of ICS depends on the secretiveness of the selection and use of the system parameters. The interference will only be effective the case where the countermeasure station establishes the fact of the presence of the opposing system in the air and assesses its parameters frequency band occupied band, the law of modulation of the signal, and others.

Under the covertness of radio channels in general and the hiddenness of the parameters used in them, we will understand their ability to withstand the measures of the radio-electronic countermeasure aimed at detecting the fact of the system operation (*energy concealment*) and determining the signal parameters necessary for radio counteraction (*structural and information concealment*).

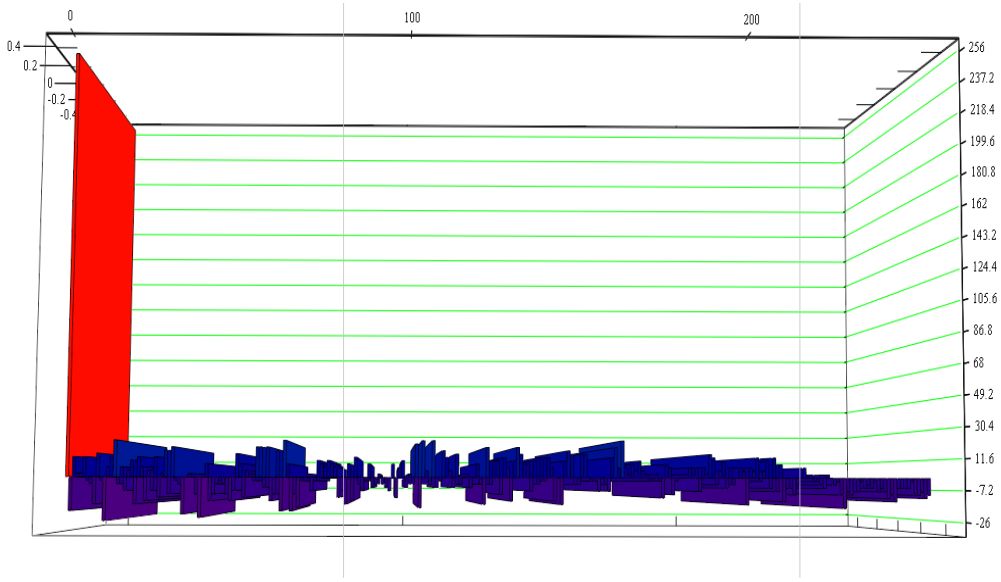


Fig. 1 – AACF for CS period L=256

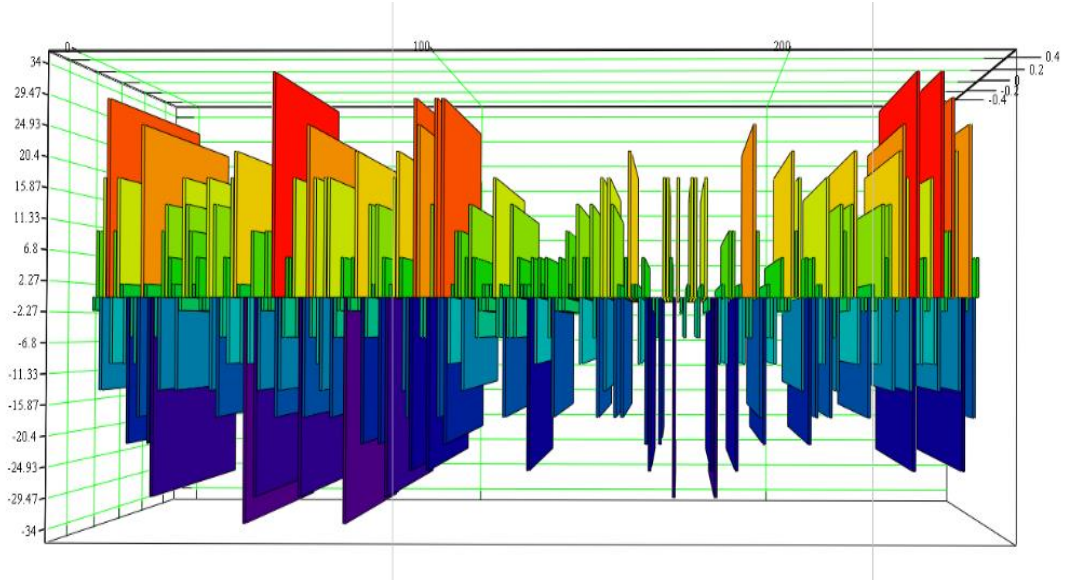


Fig. 2 – PCCF for CS period L=256

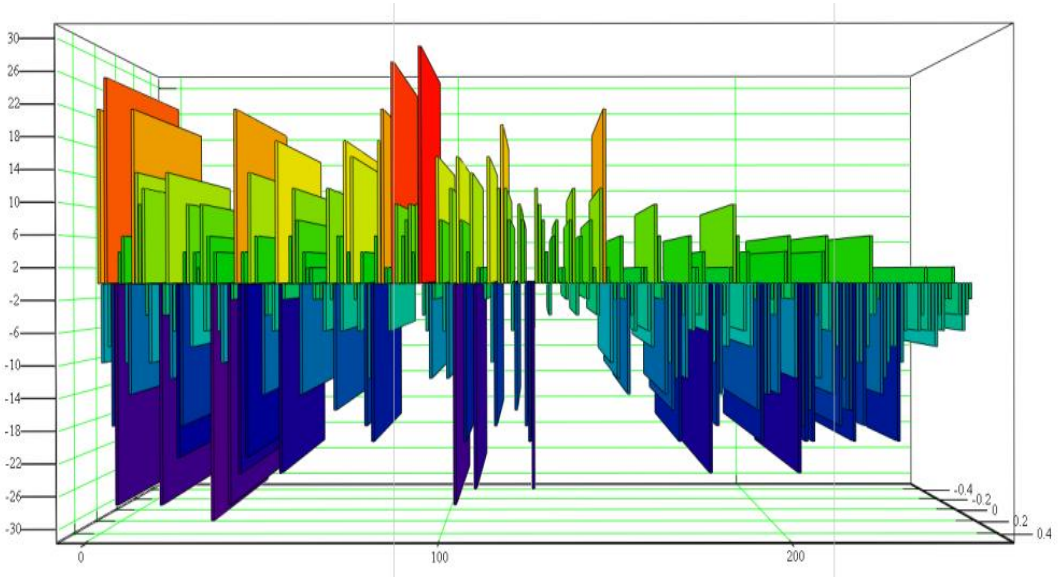


Fig. 3 – ACCF for CS period L=256

Energy concealment characterizes the ability of the system to withstand measures aimed at detecting by the station the counteraction to the fact of the functioning of the system. Structural concealment of used signals characterizes the complexity of reliable prediction of signals or their symbols (*according to known previous ones*). Information concealment (*difficulties in identifying received signals with a message that is transmitted*) predisposes the system's ability to conceal the semantic content of messages, the ways of generating messages (signals), the very fact of signal transmission.

If the radiating system uses a signal with a nontrivial modulation law whose parameters are unknown to the counter, the latter is unable to use a correlator or a matched filter to detect the signal. The only strategy of the opposing side in this case is the use of an energy detector [1], which is optimal from the point of view of detecting a band-limited noise signal against the background of Abelian white Gaussian noise. To prevent the station from detecting counteracting the signal, the radiating system should use signals with a distributed or wide spectrum, which have the highest possible value of the processing gain, and a practically undiscovered structure.

The ideal structural concealment of the signal means that the signal synthesis methods must implement signals that meet certain requirements. It is quite obvious that such requirements meet the requirements for generators, which form random (pseudo-random) sequences. In addition, there should be an opportunity to perform an assessment of the correspondence of the properties of the synthesized signals to certain requirements. Investigations of statistical properties are carried out within the framework of statistical tests based on statistical tests. The most acceptable (from the point of view of practical use) testing techniques are: NIST STS, FIPS PUB 140-1, AIS 20 and AIS 31, NIST 800-90b, NIST 800-22.

To investigate the structural properties of CS, we used the random number (pseudo-random) generator testing methodology defined by NIST 800-22 [23]. NIST 800-22 includes 16 statistical tests, and 188 probability values are computed. All tests are aimed at identifying various randomness defects (not meeting the requirements of randomness).

Testing procedure:

1. A null hypothesis is advanced $H_0$ – the assumption that the test binary sequence is random.

2. For the sequence generated by the generator, the test statistics are calculated.

3. Using the special function and test statistics, the probability value $P \in [0,1]$.

4. Probability value $P$ is compared with the level of significance $\alpha$, $\alpha \in [0,001; 0,01]$. If $P \geq \alpha$, then the hypothesis $H_0$ is accepted. Otherwise, an alternative hypothesis is adopted.

As a result of testing the memory bandwidth, a vector of probability values is generated $P = \{P_1, P_2, ..., P_{188}\}$. In the standard, the recommended length is the input data block – 106 binary symbols; one test uses 100 blocks of this length (*the input data length for one test cycle is 108 characters*). In NIST, two thresholds are used to decide the test results: 0.96 and 0.99, that is, for different significance levels it is established that out of 100 blocks cannot pass four and one test respectively.

With the use of NIST SP 800-22, the implementation of the cryptographic symbol sequence was tested. The test results are shown in the Table 4.

The results of testing showed that the statistical properties of nonlinear KS in terms of the values of the probabilities of this method are within the limits of acceptable values. And this, in turn, means that the CS satisfy the requirements for pseudo-random sequences [23-24]: - the unpredictability of the sequence of symbols, irreversibility, randomness, equal probability, independence, unpredictability, indistinguishability, etc. In essence, CS are indistinguishable from random sequences. Thus, the use of CS as a physical data carrier will increase the structural and information security (*cryptographic strength*) of the ICS.

Table 4 – Estimation of statistical properties of cryptographic discrete sequences using NIST SP 800-22

| № | c1 | c2 | c3 | c4 | c5 | c6 | c7 | c8 | c9 | c10 | Probability | Test result | Test title |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 14 | 5 | 11 | 10 | 10 | 12 | 7 | 14 | 8 | 9 | 0,574903 | 0,99 | Frequency |
| 2 | 10 | 8 | 10 | 11 | 12 | 5 | 6 | 13 | 14 | 11 | 0,574903 | 0,99 | BlockFrequency |
| 3 | 13 | 6 | 5 | 14 | 18 | 10 | 9 | 5 | 12 | 8 | 0,058984 | 0,99 | CumulativeSums |
| 4 | 14 | 9 | 4 | 10 | 8 | 8 | 15 | 15 | 12 | 5 | 0,122325 | 1 | CumulativeSums |
| 5 | 9 | 8 | 8 | 12 | 10 | 10 | 14 | 7 | 8 | 14 | 0,759756 | 1 | Runs |
| 6 | 8 | 14 | 15 | 8 | 8 | 7 | 9 | 12 | 10 | 9 | 0,657933 | 1 | LongestRun |
| 7 | 12 | 10 | 11 | 7 | 11 | 7 | 6 | 15 | 11 | 10 | 0,678686 | 1 | Rank |
| 8 | 10 | 7 | 9 | 12 | 9 | 11 | 14 | 10 | 8 | 10 | 0,935716 | 1 | FFT |
| 9 | 10 | 10 | 6 | 10 | 7 | 10 | 11 | 9 | 9 | 18 | 0,419021 | 1 | NonOverlappingTemplate |
| 10 | 11 | 7 | 9 | 12 | 9 | 14 | 9 | 8 | 11 | 10 | 0,924076 | 0,98 | NonOverlappingTemplate |
| 11 | 17 | 11 | 14 | 10 | 10 | 6 | 10 | 7 | 7 | 8 | 0,319084 | 1 | NonOverlappingTemplate |
| 12 | 16 | 9 | 7 | 8 | 6 | 7 | 10 | 13 | 9 | 15 | 0,275709 | 0,98 | NonOverlappingTemplate |
| 13 | 12 | 6 | 7 | 8 | 11 | 7 | 12 | 10 | 13 | 14 | 0,616305 | 0,99 | NonOverlappingTemplate |
| 14 | 15 | 15 | 10 | 9 | 7 | 11 | 6 | 9 | 7 | 11 | 0,455937 | 0,98 | NonOverlappingTemplate |
| 15 | 11 | 9 | 13 | 7 | 11 | 14 | 9 | 12 | 8 | 6 | 0,719747 | 1 | NonOverlappingTemplate |
| 16 | 13 | 12 | 12 | 9 | 12 | 12 | 7 | 8 | 8 | 7 | 0,816537 | 0,97 | NonOverlappingTemplate |
| 17 | 11 | 11 | 14 | 8 | 10 | 8 | 10 | 10 | 9 | 9 | 0,971699 | 1 | NonOverlappingTemplate |
| 18 | 8 | 12 | 11 | 11 | 12 | 7 | 12 | 12 | 6 | 9 | 0,851383 | 1 | NonOverlappingTemplate |
| 19 | 9 | 11 | 10 | 12 | 7 | 11 | 8 | 16 | 7 | 9 | 0,678686 | 1 | NonOverlappingTemplate |
| 20 | 14 | 10 | 13 | 10 | 12 | 12 | 6 | 7 | 11 | 5 | 0,494392 | 0,98 | NonOverlappingTemplate |
| 21 | 15 | 11 | 10 | 8 | 12 | 9 | 13 | 9 | 5 | 8 | 0,595549 | 0,95 | NonOverlappingTemplate |
| 22 | 9 | 5 | 14 | 10 | 7 | 6 | 14 | 9 | 13 | 13 | 0,334538 | 1 | NonOverlappingTemplate |
| 23 | 12 | 7 | 7 | 11 | 11 | 5 | 14 | 12 | 11 | 10 | 0,637119 | 0,99 | NonOverlappingTemplate |
| 24 | 10 | 12 | 12 | 11 | 15 | 10 | 7 | 10 | 6 | 7 | 0,657933 | 1 | NonOverlappingTemplate |
| 25 | 12 | 8 | 14 | 9 | 12 | 12 | 6 | 8 | 11 | 8 | 0,759756 | 0,98 | NonOverlappingTemplate |
| 26 | 6 | 7 | 7 | 10 | 14 | 7 | 8 | 15 | 15 | 11 | 0,249284 | 0,99 | NonOverlappingTemplate |
| 27 | 12 | 7 | 13 | 6 | 11 | 10 | 10 | 16 | 7 | 8 | 0,455937 | 0,98 | NonOverlappingTemplate |
| 28 | 12 | 9 | 9 | 12 | 9 | 10 | 6 | 7 | 17 | 9 | 0,474986 | 0,98 | NonOverlappingTemplate |
| ... 184 | 7 | 7 | 11 | 7 | 6 | 11 | 5 | 6 | 4 | 7 | 0,666838 | 0,9859 | RandomExcursionsVariant |
| 185 | 7 | 6 | 10 | 11 | 4 | 5 | 11 | 8 | 4 | 5 | 0,362174 | 1 | RandomExcursionsVariant |
| 186 | 6 | 11 | 11 | 1 | 9 | 11 | 4 | 4 | 6 | 8 | 0,076389 | 1 | RandomExcursionsVariant |
| 187 | 14 | 7 | 6 | 9 | 13 | 7 | 14 | 6 | 14 | 10 | 0,289667 | 1 | Serial |
| 188 | 11 | 8 | 13 | 5 | 6 | 11 | 14 | 8 | 14 | 10 | 0,419021 | 1 | Serial |
| 189 | 9 | 6 | 13 | 9 | 11 | 11 | 10 | 6 | 13 | 12 | 0,759756 | 0,99 | LinearComplexity |
| | | | | | | | | | | | 84,82113 | 186,0039 | |

## 7 Synthesis of derived signal systems based on cryptographic discrete sequences of symbols

Various signal systems (sets of linear recurrence sequences, Kasami, Gold, Kamaletdinov sets, etc.) that have relatively small values of the side lobes of auto and mutually correlated functions are found in the IKS as a physical carrier of information [1-3]. However, these signals have low structural latency, limited ensemble properties, and also exist only for a limited number of signal period values. In the case of truncation (increase) of the period of such signals, their correlation properties deteriorate. Therefore, the actual task is to develop the theory and practice of synthesis and analysis of discrete signal systems with the required correlation, structural, ensemble properties. Studies have shown [12] 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 [13], the problem of synthesizing nonlinear cryptographic discrete signals (CS) that provide the required values of noise immunity, information and structural stealth of the TKS operation, is formulated and solved. In general, the problem of synthesis of 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.

Among the systems of phase-shifted signals, many are formed on the basis of Walsh systems [1-4]. It is known that auto - and mutually correlated functions of Walsh sequences have large lateral peaks. To improve the correlation properties of the signals, the signal system derivatives (DSS) are generated by multiplying the Walsh sequences (source sequences) by a signal that has certain properties (the signal generator), in particular, has small side peaks of the autocorrelation function. The authors formulated a hypothesis about the possibility of using non-linear cryptographic sequences (CS) as generators, the theoretical bases of their synthesis are given in [12-13]. The method of synthesizing derived signal systems based on the use of CS includes the following steps.

1. A selection is made of M cryptographic sequences (CS) of a fixed period L having minimum values of maximum side lobes (Rmax.) 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 a cryptographic signal, forming N DSS.

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

As an illustration of this method of DSS synthesis, consider the Walsh code (Table 5).

Table 5 - The Walsh code *(of dimension N = 64)*

| | |
|---|---|
| N = 64 | 1111111111111111111111111111111111111111111111111111111111111111<br>1010101010101010101010101010101010101010101010101010101010101010<br>1100110011001100110011001100110011001100110011001100110011001100<br>1001100110011001100110011001100110011001100110011001100110011001<br>1111000011110000111100001111000011110000111100001111000011110000<br>1010010110100101101001011010010110100101101001011010010110100101<br>1100001111000011110000111100001111000011110000111100001111000011<br>1001011010010110100101101001011010010110100101101001011010010110<br>1111111100000000111111110000000011111111000000001111111100000000<br>1010101001010101100101010010101011010101001010101101010100101010<br>1100110000110011110011000011001111001100001100111100110000110011<br>1001100101100110100110010110011010011001011001101001100101100110<br>1111000000001111111100000000111111110000000011111111000000001111<br>1010010101011010010101101001011010101001011010010101011010010110<br>1100001100111100110000110011110011000011001111001100001100111100<br>1001011001101001100101100110100110010110011010011001011001101001<br>1111111111111111000000000000000011111111111111110000000000000000<br>1010101010101010010101010101010110101010101010100101010101010101<br>1100110011001100110011001100110000110011001100110011001100110011<br>1001100110011001100110011001100101100110011001100110011001100110<br>1111000011110000111100001111000000001111000011110000111100001111<br>1010010110100101101001011010010101011010010110100101101001011010<br>1100001111000011110000111100001100111100001111000011110000111100<br>1001011001101001011010011001011001101001100101101001011001101001 |

Table 6 shows the CS (M=14), selected from the set of sequences, according to the criterion of

the minimum value of the maximum side lobes PACF ($R_{max}$<10). The calculations of the statistical characteristics of the correlation functions (PACF) of the selected CS are also presented here.

Table 6 – Cryptographic sequences with minimum values of side peaks PACF

| | |
|---|---|
| **1** | 1110001111101000011111011100110011000101000110101101001001100101 |
| **2** | 1000010010000100101110011010000000110010010000010111001110011101 |
| **3** | 0000100100001001011100110100000001100100100000101110011100111011 |
| **4** | 0000100100001001011100110100000001100100100000101110011100111011 |
| **5** | 0001001000010010111001101000000011001001000001011100111001110110 |
| **6** | 0100100001001011100110100000001100100100000101110011100111011000 |
| **7** | 0000100101110011010000000110010010000010111001110011101100010110 |
| **8** | 0001001011100110100000001100100100000101110011100111011000101101 |
| **9** | 0010010111001101000000011001001000001011100111001110110001011010 |
| **10** | 0100101110011010000000110010010000010111001110011101100010110100 |
| **11** | 0000000010100010011000001111100001101101110001101000010111100101 |
| **12** | 0000000101000100110000011111000011011011100011010000101111001010 |
| **13** | 0000001010001001100000111110000110110111000110100001011110010100 |
| **14** | 0100011110001100000100110010000000011011111011100101011000010110 |

The results of the PCCF DSS based on CS show that the number of pairs of signals for a sequence of 64 symbols for which the $R_{max}$ values do not exceed 17 (*this, the so-called "close packing" boundary, achieved in the best CCF series from the CCF viewpoint three-level PCCF*) is 604 pairs (*about 30% of the total number of possible combinations of pairs of signals*). The number of pairs of signals for which the values of $R_{max}$ do not exceed 20 – 1577, which is 77% of the total number of pairs of signals. At the boundary $R_{max}$<25, the maximum number of selected pairs of signals is 1984 (96.8 %). The values of the maximum side peaks of PCCF $R_{max}$<25 occur for the sequences most widely used in modern M-sequences.

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: -8MO: 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

Table 7 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 different values of the sequence periods (from 30 to 2052).

Table7 – Statistical characteristics of correlation functions DSS

| **Type of signals** | **Characteristics** | $\frac{R_{макс}}{\sqrt{N}}$ | $\frac{m_{\lvert R\rvert}}{\sqrt{N}}$ | $\frac{D_{\lvert R\rvert}^{1/2}}{\sqrt{N}}$ | $\frac{D_{(R)}^{1/2}}{\sqrt{N}}$ |
|---|---|---|---|---|---|
| **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 |
| **Linear M-sequences** | AACF | 0,7 – 1,25 | 0,32 | 0,26 | 0,41 |
| | PACF | 1/√N | 1/√N | 0 | 0 |
| | ACCF | 1,4 – 5,0 | 0,54 | 0,48 | 0,73 |
| | PCCF | 1,9 – 6,0 | 0,8 | 0,62 | 1 |

Analysis of the data in Table 7 shows that the statistical characteristics of the DSS are close to the corresponding characteristics of linear signal classes. In this case, the values of the maximum lateral peaks of the DSS cross-correlation functions are less than for the linear M sequences used in modern ICS.

## 8 Conclusions

The methods of information exchange used in the ICS, based on a fixed correspondence: the message bit (m bit) - signal ($2^m$ signals) in the information channel, and the use (*for a long time*) of the same broadband signal in the synchronization channel (*the signals used are constructed using linear laws*), do not allow to provide the required electromagnetic compatibility (EMC) of systems and facilities operating in a relatively small to achieve the necessary values of noise immunity and information security of the operation of the ICS. Studies have shown [5,11,12-13,25] that the required (*in some or other conditions*) indicators of the efficiency of the operation of the ICS can be realized, including by using broadband radio systems for which the spreading of the spectrum is carried out using nonlinear discrete sequences.

A comprehensive solution to the problem of ensuring electromagnetic compatibility, noise immunity and information security of the operation of ICS can be achieved, including on the basis of the implementation of a dynamic information transfer mode, in which correspondence: the message bit - the signal changes over time according to a law whose prediction is possible with probability not exceeding the permissible value in the system, and applying signals with the necessary correlation, ensemble, statistical, structural properties. In this case, the signal systems must be based on nonlinear construction rules.

The proposed nonlinear discrete cryptographic signals, in contrast to the known signal classes used in various ICS applications, can be synthesized for any values of the period of discrete signals. The synthesis of this class of signals is based on the limitations associated with the boundary values of the auto and cross correlation functions of signals in the periodic and aperiodic modes of information transmission. The volume of the system of nonlinear cryptographic signals (*coding power*) is determined, first, by the requirements caused by the use of this class of signals (*detection and measurement of signal parameters, user data transfer mode, etc.*), and secondly, the requirements for the system with point of view of such indicators of the efficiency of the functioning of the telecommunications system, such as EMC noise immunity of signals reception, information concealment and imitation resistance of the system. The problem of synthesis of nonlinear discrete signals is formulated in general form. Under the cryptographic discrete signal, it is proposed to understand 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 possesses the necessary but limited values of "tight packing", correlation and ensemble properties. With this approach, the structural concealment of the signal is provided through randomness or pseudo randomness. 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. Taking into account the requirements of cryptographic stability and the complexity of generating a cryptographic signal as a signal generator, the choice of a symmetric block encryption algorithm with a counter is justified. As a block cipher it was proposed to use the national standard DSTU 7624: 2014. Alternatively, we can use the AES algorithm from the international standard ISO / IEC 18033. The preference is given to DSTU 7624: 2014, since in our opinion it refers to post-quantum algorithms, i.e. will provide (*when selecting the appropriate parameters*) cryptographic resistance against attacks with the use of quantum computers. CS are self-synchronized, and also have an ideal (absolute) structural concealment. The absolute structural concealment of such signals is that no subsequent bit, even the last, of such a signal can be uniquely determined with the prior symbols. It should be emphasized that the law for the formation of each of the cryptographic signals is determined by the key, and the length of the key can be substantially smaller than the period (length) of the signal itself.

The developed method for synthesizing a new class of nonlinear discrete signals allows changing the boundary values of the level of the side lobes of the corresponding correlation function, depending on the interference situation, as well as the requirements for the IRS, to achieve the necessary noise immunity of signal reception, imitating and information stealth of the system subscribers.

Synthesized systems complex signals possess, on the one hand, structural properties analogous to the properties of random (*pseudo-random*) sequences, and, on the other hand, the required ensemble and correlation properties, while improving the performance of ICS, in particular, EMC, noise immunity, information and structural stealth.

The characteristics of the auto- and mutual correlation functions of such signals are not inferior to those of the best ones from the point of view of the correlation properties of discrete sequences (*M-sequences, Gold and Kasami sets, Kamaletdinov ensembles, etc.).* In addition, cryptographic signal systems (CS) 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 improvement of the above mentioned indicators of the IKS operation is achieved, in particular, due to the possibility of forming, with the use of the obtained method, large discrete sequence ensembles of virtually any period with the necessary side-lobe values of the auto-mutual and butt-function correlation functions for various system applications periodic and aperiodic modes of operation, as well as statistical characteristics of correlation functions (CF), not inferior to similar characteristics of the best, in terms of CF, linear classes of signals. This makes it possible to improve the noise immunity of signal reception. The mathematical and software providing the proposed method and computational algorithms for the synthesis of systems of complex nonlinear discrete cryptographic signals, as well as derivatives of signal systems for which the coprocessors are used as the producing ones, are developed. During the research, an imitation (*software*) model was developed that implements the proposed method for synthesizing discrete cryptographic sequences. The obtained model allows: generating cryptographic signals of almost any period; to obtain minimum and maximum values of lateral emissions of periodic and aperiodic functions of auto- and cross-correlation of sequences; compare the values obtained with the known "close packing" boundaries; read selected, satisfying boundaries, sequences; assign unique identifiers to selected sequences for optimal signal processing in various applications of broadband systems. In addition, the proposed synthesis method makes it possible to synthesize pseudo-random sequences with zero values of the side peaks of the periodic auto and cross-correlation functions near the main peak, which is an important factor in maintaining stable synchronism in the system.

Software and mathematical support obtained in the course of research, realizing the methods of synthesis and research of the properties of nonlinear signal systems, including DSS, is practically

ready for possible use in the composition of prototypes and elements of modern digital communication means.

An improved method for synthesizing nonlinear discrete cryptographic signal systems is developed, based on the optimization of the synthesis of the signal system using the branch and boundary method, which makes it possible to reduce, in comparison with a full search, the volume of computational procedures for synthesizing signal systems and, consequently, necessary, for those or other applications of telecommunication systems, properties.

## References


[1] Ipatov Valery P. Spread Spectrum and CDMA.Principles and Applications / Valery P. Ipatov. 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.

[2] Varakin L. E. Sistemy svyazi s shumopodobnymi signalami / Varakin L. E. – 1985. – 384 s.

[3] Sverdlik M. B. Optimal'nye diskretnye signaly / Sverdlik M. B. - M: Radio i svyaz', 1975. – 200 s.

[4] Sarvate, D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun, 1980. – Vol. Com 68 – P. 59–90.

[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. - Volume 75, 2016 Issue 2. pages 169-178.

[6] Gold, R. Optimal binary sequences for spread spectrum multiplexing // IEEE Trans. Inform. Theory.– 1967. Vol. 13. – P. 619–621.

[7] Karpenko O., Kuznetsov A., Sai V., Stasev Yu. Discrete Signals with Multi-Level Correlation Function // Telecommunications and Radio Engineering. – Volume 71, 2012 Issue 1. pages 91-98.

[8] Naumenko N.I., Stasev Yu.V., Kuznetsov A.A. Methods of synthesis of signals with prescribed properties // Cybernetics and Systems Analysis, Volume 43, Issue 3, May 2007, Pages 321-326.

[9] Stasev Yu.V., Kuznetsov A.A., Nosik A.M. Formation of pseudorandom sequences with improved autocorrelation properties // Cybernetics and Systems Analysis, Volume 43, Issue 1, January 2007, Pages 1–11.

[10] Lavrovska, T., Rassomahin, S. Physical model of pseudorandom codes in multidimensional Euclidean space. // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 67-70.

[11] Gorbenko I.D., Gorbenko Ju.I. Prykladna kryptologija. Teorija. Praktyka. Zastosuvannja: monografija – Harkiv.: Vydavnyctvo «Fort», 2012. – 880 s. (in Ukrainian).

[12] Zamula A.A., Semenko E.A Perspektivy primeneniya nelineinykh diskretnykh signalov v sovremennykh telekommunikatsionnykh sistemakh i setyakh // Sistemi obrobki informatsiï:– Kh.: KhUPS, 2015. – Vip. 5 (130).– S. 129 - 134. (in Russian).

[13] Gorbenko I.D., Zamula A.A. Kriptograficheskie signaly: trebovaniya, metody sinteza, svoistva, primenenie v telekommunikatsionnykh sistemakh // Radiotekhnika: Vseukrainskii mezhvedomstvennyi nauchno – tekhnichneskii sbornik - 2016 g. - Vyp. 186. – S. 7–23. (in Russian).

[14] Application Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001.

[15] DSTU 7624:2014. Informacijni tehnologii'. Kryptografichnyj zahyst informacii'. Algorytm symetrychnogo blokovogo peretvorennja. – Vved. 01–07–2015. – K.: Minekonomrozvytku Ukrai'ny, 2015. (in Ukrainian).

[16] Kuznetsov O., Gorbenko Y., Kolovanova I. Combinatorial properties of block symmetric ciphers key schedule. // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 55-58.

[17] Kuznetsov O., Lutsenko M., Ivanenko D. Strumok stream cipher: Specification and basic properties // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 59-62.

[18] ISCI'2017: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2017. – 207 p.

[19] Kaidalov D., Oliynykov R., Kazymyrov O. A method for security estimation of the SPN-based block cipher against related-key attacks // Tatra Mountains Mathematical Publications. – Volume 60, Issue 1, Pages 25–45.

[20] Ruzhentsev V., Oliynykov R. Properties of Linear Transformations for Symmetric Block Ciphers on the basis of MDS-codes // Proceedings of the 6th International Conference on Network Architecture and Information System Security SAR-SSI 2011, pp. 193-196.

[21] Rodinko M., Oliynykov R.,Gorbenko Y. Improvement of the high nonlinear S-boxes generation method. // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 63-66.

[22] Krasnobayev V.A., Yanko A.S., Koshman S.A. A Method for arithmetic comparison of data represented in a residue number system // Cybernetics and Systems Analysis. – January 2016. – Volume 52, Issue 1, pp. 145-150.

[23] NIST 800-90 b Recommendation for the Entropy Sources Used for Random Bit Generation, 2012.

[24] Potii A.V., Pesterev A.K. A System Approach to Certification of Pseudorandom Numbers Generators Used in Information Protection Systems // Telecommunications and Radio Engineering. – Volume 52, 1998 Issue 4. pages 97-102.

[25] I. D. Gorbenko, A. A. Zamula, A. E. Semenko, V. L. Morozov Method for complex improvement of characteristics of orthogonal ensembles based on multiplicative combining of signals of different classes// Telecommunications and Radio Engineering Volume 76, 2017 Issue 18, pages 1581-1594 .

**Рецензент**: Олексій Стахов, д.т.н., проф., академік Академії інженерних наук України, Міжнародний Клуб Золотого Перетину, Онтаріо, Канада. E-mail: goldenmuseum@rogers.com

Надійшло: Вересень 2017.

**Автори:**
Іван Горбенко, доктор технічних наук, професор, лауреат Державної премії України, професор кафедри безпеки інформаційних систем і технологій, ХНУ імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: gorbenkoi@iit.kharkov.ua

Владислав Морозов, аспірант кафедри безпеки інформаційних систем і технологій, ХНУ імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: morozov@boiko.com.ua

Олександр Замула, доктор технічних наук, професор кафедри безпеки інформаційних систем і технологій, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, м. Харків, 61022, Україна.
E-mail: zamylaaa@gmail.com

**Методи забезпечення електромагнітної сумісності у сучасних інформаційно-комунікаційних системах.**

**Анотація.** Сформульовано вимоги до вибору систем складних сигналів – переносників даних для використання в багатокористувачевих широкосмугових телекомунікаційних системах (ШТС), в яких пред'являються підвищені вимоги до завадостійкості, електромагнітної сумісності, скритності і безпеки інформації. Наводяться концептуальні основи синтезу нового класу складних сигналів – криптографічні сигнали (КС). Обґрунтовується доцільність застосування в захищених широкосмугових телекомунікаційних системах похідних систем сигналів для підвищення ефективності, електромагнітної сумісності, завадостійкості прийому, скритності і інформаційної безпеки захищених ШТС.

**Ключові слова:** багатокористувачева система; евклідова відстань; ансамбль сигналів; криптографічний сигнал; система похідних ортогональних сигналів; кореляційна функція.

**Рецензент**: Алексей Стахов, д.т.н., проф., академик Академии инженерных наук Украины, Международный Клуб Золотого Сечения, Онтарио, Канада. E-mail: goldenmuseum@rogers.com

Поступила: Сентябрь 2017.

**Авторы:**
Иван Горбенко, доктор технических наук, профессор, лауреат Государственной премии Украины, профессор кафедры безопасности информационных систем и технологий, ХНУ имени В. Н. Каразина, площадь Свободы 4, г. Харьков, 61022, Украина.
E-mail: gorbenkoi@iit.kharkov.ua

Владислав Морозов, аспирант кафедры безопасности информационных систем и технологий, ХНУ имени В. Н. Каразина, площадь Свободы 4, г. Харьков, 61022, Украина.
E-mail: morozov@boiko.com.ua

Олександр Замула, доктор технических наук, профессор кафедры безопасности информационных систем и технологий, ХНУ имени В. Н. Каразина, площадь Свободы 4, г. Харьков, 61022, Украина.
E-mail: zamylaaa@gmail.com

**Методы обеспечения электромагнитной совместимости в современных информационно-коммуникационных системах.**

**Аннотация**. Сформулированы требования к выбору систем сложных сигналов – переносчиков данных для использования в многопользовательских широкополосных телекоммуникационных системах (ШТС), в которых предъявляются повышенные требования к помехоустойчивости, электромагнитной совместимости, скрытности и безопасности информации. Приводятся концептуальные основы синтеза нового класса сложных сигналов - криптографические сигналы (КС). Обосновывается целесообразность применения в защищенных широкополосных телекоммуникационных системах производных систем сигналов для повышения эффективности, электромагнитной совместимости, помехоустойчивости приема, скрытности и информационной безопасности защищенных ШТС.

**Ключевые слова:** многопользовательская система; евклидово расстояние; ансамбль сигналов; криптографический сигнал; система производных ортогональных сигналов; корреляционная функция.