UDC 621.391 **DOI:10.30837/rt.2021.3.206.02**

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

THEORETICAL APPROACHES TO THE SYNTHESIS OF DISCRETE SIGNALS WITH NECESSARY PROPERTIES

Introduction

Global trends of increasing threats to information and cybersecurity, increasing the level of vulnerability of information and communication systems (ICSs) necessitate the development and implementation of new models, methods and technologies for managing telecommunications networks, information security, services and service quality, development of information exchange methods, methods for synthesizing new classes of complex discrete signals-data carriers with the necessary ensemble, correlation and structural properties. Among the main areas of improvement of information security, noise protection and secrecy of ICSs one can identify the areas associated with the use of channels with high frequency redundancy, significant spatial, structural, energy and temporal secrecy. To ensure frequency redundancy at the physical level, discrete signals have been widely used, in which the manipulated parameters (amplitude, phase, frequency) are changed at strictly fixed time intervals. Efforts of researchers are aimed at finding ensembles of complex signals, the characteristics of which with increasing duration approach the limit of "dense packing" [1-3], i.e., the ensemble, all members of which have zero constant component, ideal periodic function of autocorrelation (PFAC) and periodic function of cross-correlation (PFCC), and have the largest possible volume.

Theoretical basis of synthesis of discrete derivative signals

A common criterion for such an approximation is the minimax criterion, focused on the synthesis of the ensemble by minimizing the maximum values of the side peaks on the set of all undesirable correlations. The limits for the root mean square and maximum (peak) values of auto- and cross-correlation functions are given in [2, 3].

In particular, the fundamentally achievable values of the maximum side peaks of the periodic autocorrelation function (the limits of "dense packing") for a given period of the sequence N are determined from the ratio [4]:

$$R_{\max}^{a} \geq \begin{cases} 0, \textit{якщо } N \equiv 0 \pmod 4; \\ 1, \textit{якщо } N \equiv 1 \pmod 4; \\ 2, \textit{якщо } N \equiv 2 \pmod 4; \\ -1, \textit{якщо } N \equiv 3 \pmod 4, \end{cases} \quad (1)$$

These limits specify the criteria for the synthesis of a set of DSs (signatures). The ensembles with values corresponding to the boundary (1) are optimal ones and called the minimax ensembles. For an ideal hypothetical ensemble $R_{\max}$ is zero, and for any real ensemble the minimum value of the correlation function can serve as an adequate measure of its proximity to the ideal.

The publication presents the results of research on methods of synthesis and analysis of the properties of different classes of signals, which can be attributed (in accordance with the above limits) to the minimax (optimal) signals. The possibilities are discussed to use the offered signals in modern ICSs as physical data carriers in order to improve, first of all, such performance indicators as information security, noise immunity and secrecy of these systems [4 – 6].

The section proposes a method for synthesis of discrete derivative signals based on the use of nonlinear discrete complex cryptographic signals as the signals generating orthogonal discrete signals (ODS) as initial ones. It is known [7, 8] that ODSs have unsatisfactory ensemble, structural and correlation properties, therefore, the use of the ODS in the ICS, which have increased requirements

for noise immunity, signal secrecy, information security is limited. Preservation of the advantages of the ODS, with simultaneous improvement of correlation, spectral, ensemble and structural properties, can be achieved based on formation of derivative signal systems. Derivative signal systems $^{W(i)}$, for the case of phase-manipulated (PM) signals, are formed by a symbol-wise multiplication of the so-called output signal by a signal that produces $^{H(k)}$:

$$W(i) = H(k) \cdot G(i) \tag{2}$$

In this case, the signal system is used as a source signal, which, on the one hand, does not fully meet the requirements for correlation properties, on the other hand, it has some advantages, for example, the simplicity of technical implementation of construction algorithms. Hadamard systems can be used as such signal systems. It is shown in [2, 3] that generating signals must have good autocorrelation properties (small values of lateral peaks of autocorrelation function) to ensure that derived signal systems meet the increased requirements for information security, noise immunity and secrecy of the ICS operation. Considering the above-said, it is advisable to use characteristic signals and cryptographic signals as generating signals [8, 9].

For the phase shift keyed (PM) signals (including derivatives) of the same duration, integral ratios are known [2]

$$U_{kl}(\tau) = (T/2\pi) \cdot \int_{-\infty}^{\infty} R_{kl}(\tau - \Omega) \cdot R_{\mu\nu}(\tau, \Omega) d\Omega; \tag{3}$$

$$U(\tau) = (T/2\pi) \cdot \int_{-\infty}^{\infty} R_Z(\tau - \Omega) \cdot R_Y(\tau, \Omega) d\Omega, \tag{4}$$

where: $U_{kl}(\tau)$ – cross-correlation function (FCC); $R_{kl}(\tau, \Omega)$ – reciprocal uncertainty function; $R_{\mu\nu}(\tau)$ – reciprocal correlation function; $U(\tau)$ – autocorrelation function of derivative signals; $R_Z(\tau, \Omega)$ – uncertainty function of output signals; $R_Y(\tau, \Omega)$ – uncertainty function of the producing signal.

Analysis of expressions (3) – (4) shows that the correlation properties of the derivative signals depend on the properties of the output signals and the signals producing on the frequency-time plane. Expressions (3) – (4) make it possible to find the following assessment:

$$U_{kl}(\tau) \le (T/2\pi) \cdot \sqrt{\int_{\varphi} \left| R_{kl}(\tau, -\Omega) \right|^2 d\Omega} \cdot \int_{\varphi} \left| R_{\mu\nu}(\tau, \Omega) \right|^2 d\Omega \tag{5}$$

$$U(\tau) \le (T/2\pi) \cdot \sqrt{\int_{\varphi} \left| R_Z(\tau, -\Omega) \right|^2 d\Omega} \cdot \int_{\varphi} \left| R_Y(\tau, \Omega) \right|^2 d\Omega \tag{6}$$

Estimates (5) – (6) depend to a large extent on the value of the width of the integration interval φ, that is, on the ratio of the width of the FCC output signals and the producing signals.

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

$$\sigma_{ukl} = 1/2 \cdot \sqrt{F_a \cdot T}, \quad \sigma_{u\mu\nu} = 1/2 \cdot \sqrt{F_v \cdot T}. \tag{7}$$

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

$$U_{kl}(\tau) \le 0{,}5 \cdot \sqrt{F_a / F_v}. \tag{8}$$

From the last inequality, it follows that the values of the FCC of the derivative signals are less than or equal to $0{,}5 \cdot \sqrt{F_a / F_v}$, which in turn means that the maximum lobes of the CCF will be less than this value. Thus, to reduce the maximum side petals of the CCF, it is necessary to increase the width of the producing signal. It also follows from (8) that the method of derivative signals formation, that is, the signal multiplication process, leads to a decrease in the side lobes of the FCC derivative signals, if the base of the signals producing $F_a \cdot T$ is larger than the bases of the output signals so that $\sqrt{F_v} \cdot T > F_a \cdot T$.

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

$$F_v > F_a, \tag{9}$$

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

As for the producing signals, they must have good autocorrelation properties, secondly, as many characters (elements) as the output signal, that is, the number of $N = 2^n$ characters, where n – is an integer.

Let us illustrate the possibility of constructing derivatives of discrete signals, for which the rows of the Hadamard matrix of $\mathrm{N} = 256$ order are used as output signals, and cryptographic signals (CS) are used as generating signals $\mathrm{H(k)}$. Tables 1 – 3 give examples of: sequences of symbols: rows of the Hadamard matrix of $\mathrm{N} = 256$ order synthesized by the CS, which in the properties of the periodic autocorrelation function (PFAC) are close to the limit of "dense packing" (1); derivative signals generated in accordance with (2), using the sequences shown in tables 1–2.

It was shown in [2] that the correlation and statistical characteristics of the functions of cross correlation (FCC) of signals used by the ICS subscribers have a significant impact on ensuring the required level of noise immunity of signals reception in multiuser ICSs. One of the statistical characteristics of the FCC is the excess coefficient, which affects the probability of error in signals reception. It was shown in [2, 10] that it is necessary to choose a signal system with the lowest value of the excess coefficient to ensure a lower probability of error.

Based on multiple calculations for signal lengths 64, 256, 1024, 2048, statistical and correlation character istics of the CS and characteristic discrete signals (CDS) [8], as well as derived signals, formed on the basis of these signals, were calculated, and the Hadamard matrix rows of appropriate order were used as source.

Table 1

Matrix row №	The row of the Hadamard matrix ($\mathrm{N} = 256$)
1	[1, -1, 1, -1]
2	[1, 1, -1, -1, 1, 1, -1, -1]

Table 2

Signal №	Cryptographic signal (N = 256)
1	[-1, 1, -1, 1, 1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, 1, -1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, 1, -1, -1, -1, 1, 1, 1, 1, 1, 1, -1, 1, -1, 1, 1, -1, -1, -1, -1, 1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, -1, -1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, 1, 1, 1, -1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, -1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, -1, -1, -1, 1, 1, -1, 1, 1, -1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1, -1, -1, 1, 1, -1, 1, -1, 1, -1, -1, -1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, -1, -1, 1, -1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, 1]
2	[1, 1, 1, -1, 1, -1, -1, 1, 1, 1, 1, -1, 1, 1, 1, 1, -1, 1, -1, 1, 1, 1, 1, -1, 1, 1, 1, 1, 1, -1, 1, -1, -1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, -1, 1, -1, 1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1, -1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, -1, -1, 1, -1, -1, 1, 1, 1, 1, -1, 1, -1, 1, 1, -1, 1, -1, -1, -1, -1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, -1, 1, 1, 1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, 1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, -1, 1, -1, -1, -1, -1, -1, -1, 1, 1, 1, 1, -1, 1, -1, -1, -1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, -1]

Table 3

Signal №	Derived cryptographic signal (N = 256)
1	[-1, -1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1, 1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, -1, -1, 1, 1, -1, -1, -1, -1, -1, -1, 1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, -1, 1, -1, -1, -1, -1, 1, 1, -1, 1, -1, -1, -1, 1, -1, 1, 1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, 1, 1, 1, 1, 1, 1, -1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, -1, -1, 1, 1, -1, -1, -1, 1, -1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, -1]
2	[-1, 1, 1, -1, 1, 1, -1, -1, 1, -1, -1, 1, 1, 1, -1, -1, 1, 1, 1, -1, -1, -1, 1, -1, -1, -1, -1, -1, -1, 1, 1, -1, -1, -1, 1, -1, 1, 1, -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, -1, -1, 1, 1, -1, 1, 1, -1, 1, 1, 1, 1, -1, -1, 1, -1, -1, -1, -1, -1, 1, 1, -1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, 1, 1, 1, -1, -1, 1, 1, 1, 1, 1, 1, -1, -1, -1, 1, -1, -1, -1, -1, -1, -1, 1, -1, -1, -1, -1, -1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1, -1, -1, 1, 1, -1, 1, -1, 1, -1, 1, -1, -1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, 1, 1, 1, 1, -1, -1, -1, -1, 1, 1, -1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, 1, -1, 1, -1, 1, 1, 1, -1, -1, -1, -1, 1, 1, 1, -1, 1, 1, -1, -1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1, -1, -1, 1, -1, -1, -1, -1, -1, 1, -1, 1, 1, 1, -1, -1, -1]

Based on multiple calculations for signal lengths 64, 256, 1024, 2048, statistical and correlation character(istics of the CS and characteristic discrete signals (CDS) [8], as well as derived signals, formed on the basis of these signals, were calculated, and the Hadamard matrix rows of appropriate order were used as source.

Table 4 shows the data on the results of calculations of the statistical characteristics of the FCC of the signal systems under study (all values are normalized relative to the number of elements of the discrete sequence of symbols). The following is used as the PFCC statistical characteristics: $\frac{R_{\delta\max}}{\sqrt{N}}$ is the maximum value of the PFCC side peaks; $\frac{m_{|R|}}{\sqrt{N}}$ is the mathematical expectation of the module of the FCC side peaks; $\frac{D_{|R|}}{\sqrt{N}}$ is variance of the modulus of the FCC side peaks; $\frac{\mathrm{D}_{|\mathrm{R}|}^{1/2}}{\sqrt{\mathrm{N}}}$ is standard deviation of the modulus of the PFCC side peaks; $\frac{D_R^{1/2}}{\sqrt{N}}$ is standard deviation of the PFCC side peaks; $\frac{\gamma}{\sqrt{N}}$ is the excess coefficient. Tables 5, 6 provide data on the statistical characteristics of the PFCC signal systems and values of the excess coefficient γ for different classes of signals, respectively.

Analysis of the data in Tables 4 – 6 shows that the statistical characteristics of the derived signals formed based on the CS are close to the corresponding characteristics of other signals indicated in the table. In this case, the values of the maximum side outliers of the cross-correlation function of

the derivatives of orthogonal signals formed on the basis of cryptographic signals are less than the values of the maximum lateral outliers of linear M – sequences.

Table 4

Signal	N	$\frac{R_{б\max}}{\sqrt{N}}$	$\frac{m_{\|R\|}}{\sqrt{N}}$	$\frac{D_{\|R\|}}{\sqrt{N}}$	$\frac{D_{\|R\|}^{1/2}}{\sqrt{N}}$	$\frac{D_{R}^{1/2}}{\sqrt{N}}$	$\frac{\gamma}{\sqrt{N}}$
Hadamard	64	2.877606	0.839302	7.505229	0.895450	0.578163	0.080803
CS		2.579922	0.800799	2.940059	0.602640	0.995338	0.045952
Derived		2.557872	0.789343	2.968220	0.605073	0.995257	0.063202
Hadamard	256	5.949502	0.971715	31.327805	1.296748	1.163056	0.226740
CS		3.143866	0.802731	6.078791	0.615274	1.013034	0.052455
CDS		2.919304	0.795529	6.012184	0.611412	1.004272	0.063475
Derived		3.060695	0.792919	5.963091	0.609151	0.992591	0.047281
Derived (CDS) and Hadamard		2.838905	0.786446	6.123228	0.61677	1.000319	0.032270
Hadamard	512	8.535875	1.077900	60.183554	1.514880	1.646411	0.279178
CS		3.302501	0.788752	8.310726	0.605370	1.007827	0.042325
Derived		3.292689	0.790902	8.206162	0.601609	1.004050	0.038807
Hadamard	1024	11.996921	1.182539	110.418690	1.724686	2.096328	0.308414
CS		3.573256	0.801196	11.976469	0.611492	0.991789	0.025411
Derived		3.467752	0.800130	11.831620	0.607747	1.000108	0.026396
Hadamard	2048	17.027296	1.304369	207.508662	1.988573	2.383674	0.314253
CS		3.614201	0.805799	16.805120	0.609234	0.994485	0.020321
Derived		3.575909	0.799557	16.474635	0.603198	0.998075	0.018530

Data analysis of Table 6 shows that derivative signaling systems have lower γ value compared to the generating signals. In addition, it was shown in [4] that for the ODS (rows of the Hadamard matrix of N = 64 order) the excess coefficient is equal to 20, while for derivative signals generated using the ODS and CS it is equal to 0.063202, which significantly (by an order of magnitude) reduces the probability of error when receiving signals.

Table 5

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

Table 6

Signal class	N	$\frac{\gamma}{\sqrt{N}}$
Cryptographic signals (CS)	64	0.045952
Derived signals (CS and ODS)	64	0.063202
Cryptographic signals (CS)	256	0.052455
Characteristic discrete signals (CDS)	256	0.063475
Derived signals (CS and ODS)	256	0.047281
Derived signals (CS and ODS)	256	0.032270
Cryptographic signals (CS)	512	0.042325
Derived signals (CS and ODS)	512	0.038807
Cryptographic signals (CS)	1024	0.025411
Derived signals (CS and ODS)	1024	0.026396
Cryptographic signals (CS)	2048	0.020321
Derived signals (CS and ODS)	2048	0.018530

Using NIST SP 800-22 [11] (frequency bitwise test (monobit test)), frequency block test (frequency within block test), test for a sequence of identical bits (runs test), test for the longest sequence of units in the block (the longest run test), spectral test (spectral test), series subsequence test (serial test), tests of implementations of derivative cryptographic sequences of symbols (DCSS) were performed. In addition, the DCSS was tested using the FIPS-140 standard (frequency bitwise test (monobit test)), poker test, runs test, the longest sequence of ones/zeros (the longest run test)). Tables 7, 8 show the results of tests carried out on these tests.

Table **7**

The name of the test	X	Condition for successful passing the test	X satisfies the condition
Monobit test	10104	$9654 < X < 10346$	Yes
Poker test	16.806400000000394	$1.03 < X < 57.4$	Yes
Test for the maximum length of the series	12	$X < 34$	Yes

Table 8

Symbol	Series length						Test passed
	1	2	3	4	5	6+	
«1»	2504	1245	605	298	159	187	Yes
«0»	2540	1248	605	303	141	162	Yes

Numerous studies of the statistical properties of derivatives of nonlinear cryptographic sequences of symbols using NIST SP 800-22, FIPS-140 have shown that these sequences, formed using the proposed method [8], meet the requirements for random sequences.

Principles of construction and general characteristics of software and hardware complex for synthesis, research of properties, generation and processing of signals

The presence of its own hardware and software complex for implementing the functions of synthesis, analysis, formation, processing, study of the signal systems properties is an important component in creating and applying the theoretical foundations of signal systems for data in modern ICSs.

The components of the software and hardware complex for the synthesis, study of properties, generation and processing of signals (hereinafter – the Complex) are as follows.

Component 1: software for generating/synthesizing signals with given parameters according to the available models (available models of signal construction are laid down at the programming stage, only the configuration parameters are variable). The result of the work of this tool is the generated files with discrete sequences, which can then be used for analysis or for implementation in the ICS (communication system), as a basis for signals – physical data carriers formation.

Component 2: complex software tool for research of statistical, correlation, ensemble and structural (cryptographic) properties of the sequences being synthesized. Particular attention has been given to the analysis of cryptographic properties of the DS, for which the appropriate tests are used. As a result, the complex generates source files that can be further used to display graphically the results in the form of 2D and 3D graphs.

Component 3: software tool for graphical display of research results, which may include third-party software, such as MathCad, MatLab (if necessary, input data processing), or Grafana. Both the source files of Component 1 and the source files of Component 2 can be used as source data. As a result, the user receives the constructed images of various types of correlation functions, the tables containing results of calculations (researches) of properties of signals.

It is possible to note such features of the created Complex.

1. A separate module for data access control (the database and system disk) has been introduced into the structure of the Complex. The functioning of the authentication and authorization system has been provided, which allows users to work simultaneously without interference and to get access their results. After performing the appropriate functions, the results can be sent to the user's e-mail.

2. Combination of these components of the Complex into a single web service. The main idea of creating the Complex consists in developing an accessible user interface that allows even a user who does not have certain qualifications in the field of construction and analysis of signals, to implement the functions of the complex. The decision to duplicate the results is due primarily to the desire to minimize the risk of data loss. The presence of a single web service opens the possibility of simultaneous use of the Complex's capabilities by many users. The presence of the user interface made it possible to expand the capabilities of the Complex without the need to make changes to the program code, as well as to increase the performance of the complex several times.

3. Modularity and openness of the Complex, in the sense of expanding the possibilities for the synthesis, formation, processing and analysis of various classes of signals. Considerable attention has been given to variability and expansion of possibilities for the synthesis of cryptographic signals (CS): generation of a cryptographic key; selection of the necessary library and algorithm of cryptographic algorithm, key data, etc., and all this without interfering with the program code.

4. An adaptive algorithm for configuring the number of simultaneous flows on the CPU has been used to increase the speed of the processes of signals formation, processing, analysis of their properties. This approach makes it possible to increase the overall performance of the software solution, depending on what hardware it is running.

5. All results are generated with the preservation of the original data and system parameters, which allows you to reproduce the obtained result at any time.

Hardware characteristics of the working machine currently used for signal synthesis and analysis (only parameters that have a direct impact on the performance of the complex and the preservation of the obtained results are indicated):

- CPU (central processor unit): Intel iCore i7, 7th Gen (2.9 – 3.4 GHz);
- RAM (random access memory): 16 Gb;
- media type: SSD Kingston (up to 550 Mb/s for recording and up to 520 Mb/s for reading)
- Software features of the constructed complex (programming languages, details of construction of the interface):
- programming language of the back-end part: Java 8 (using the latest features for parallel processing);
- additional libraries and dependencies (back-end): Spring Boot, Spring Security, BouncyCastle security lib;
- programming language of front-end (UI) parts: JavaScript, TypeScript, HTML, SCSS;
- additional libraries and dependencies (front-end): Angular 8;
- components for construction of graphic elements (graphs, diagrams): elements constructed with the use of Angular Framework, Grafana tools and modules;
- storage of results: file system (for source files) + duplication in MySQL database.

Conclusions

The method has been proposed for the synthesis of discrete derivative signals based on nonlinear discrete complex of CSs as producing signals and orthogonal signals formed on the basis of the Hadamard matrix rows as source ones. The choice of the CS is due to the fact that this class of signals has improved autocorrelation, ensemble, structural properties, as well as statistical properties of cross-correlation functions (primarily, the values of maximum side peaks, peak dispersion and excess coefficient). Based on computer simulation and calculations, it is shown that derived signals formed based on cryptographic sequences and rows of the Hadamard matrix have improved, com-

pared to orthogonal and linear signal classes, ensemble, correlation and structural properties. The complex of hardware and software has been developed making it possible to realize synthesis, formation, processing, study of nonlinear CS, nonlinear signals in the Galois finite fields, derivatives of the signal system, M sequences, etc. This complex is almost ready for possible use as part of prototypes and elements of digital communication tools of modern ICS. The architecture of the obtained software and hardware complex, with the use of additional mathematical apparatus, makes it possible to carry out synthesis and analysis of many classes of signals, including those given in this publication. The use of nonlinear complex signals with the necessary properties, the theoretical foundations of which are proposed in this publication, will increase the noise immunity of signals (probability of correct signal reception) and information security and secrecy of modern information and communication systems under conditions of cyber attacks, natural and organized, including structural, relayed and other interference.

References

1. Ipatov, Valery P. Spread Spectrum and CDMA. Principles and Applications / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electro technical University 'LETI', Russia / John Wiley & Sons Ltd, The Atrium, Southern Gate, Chi Chester, West Sussex PO19 8SQ, England. 2/
2. Varakin L. Ye. Sistemy svyazi s shumopodobnymi signalami [Communication systems with noise-like signals].1985.384 p.
3. Sarvate, D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Parsley // IEEE Trans. Commun. 1980. Vol. Com 68. P. 59–90.
4. Sverdlik M.B. Optimal discrete signals. M. : Sov radio, 1975. 200 p.
5. Sung-Moon, Michael Yang. (2019). Modern Digital Radio Communication Signals and Systems. Springer, 679. doi: https://10.1007/978-3-319-71568-1.
6. I.D. Gorbenko, A.A. Zamula, V.L. Morozov Information security and noise immunity of telecommunication systems under conditions of various internal and external impacts // Telecommunications and Radio Engineering. 2017. Vol. 76, Issue 19. P. 1705-1717.
7. Gorbenko I.D., Zamula A.A., Semenko E.A., Morozov V.L. Method for complex improvement of characteristics of orthogonal ensembles based on multiplicative combining of signals of different classes // Telecommunications and Radio Engineering. 2017. Vol. 76, Issue 18. P. 1581 1594. DOI: 10.1615/TelecomRadEng.v76.i18.10.
8. Ivan Gorbenko, Alexandr Zamula. Devising methods to synthesize discrete complex signals with required properties for application in modern information and communication systems. 2021 // Eastern-European Journal of Enterprise Technologies 2021-06-30. P. 16 – 26. DOI: 10.15587/1729-4061.2021.234674.
9. Ivan Gorbenko and Alexandr Zamula. Theoretical Basis of Synthesis of Complex Signal Quasiortogonal Systems. In.: ISCI'2020: Information Security in Critical Infrastructures : Collective monograph. Edited by Ivan D. Gorbenko, Victor A. Krasnobayev and Alexandr A. Kuznetsov. ASC Academic Publishing, USA, 2020, pp. 11-28 – ISBN: 978-1-7362833-0-1 (Hardback), ISBN: 978-1-7362833-1-8 (Ebook).
10. Gorbenko I., Zamula A., Morozov V. Information and communication systems based on signal systems with improved properties building concept. CEUR Workshop Proceedings, 2019, 2353. P. 974-991.
11. NIST 800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000.

Надійшла до редколегії 03.09.2021

Відомості про авторів:

Горбенко Іван Дмитрович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; АТ «Інститут інформаційних технологій», головний конструктор; Україна; e-mail: GorbenkoI@iit.kharkov.ua; ORCID: https://orcid.org/0000-0003-4616-3449

Замула Олександр Андрійович – д-р техн. наук, професор, Харківський національний університет імені В.Н. Каразіна, професор кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; email: zamylaaa@gmail.com; ORCID: http://orcid.org/0000-0002-8973-6190