Analysis of the information protection methods in telecommunication systems with channels split by code

Zhuk A.P.
NCFU
Stavropol
alekszhuk@mail.ru

Khachkizov R.A.
NCFU
Stavropol
rusik.khachkizov@mail.ru

Dzhamiev N.D.
NCFU
Stavropol
for-ncfu@mail.com

Ryabtsev S.S.
NCFU
Stavropol
Nalfartorn@yandex.ru

Ogur M.G.
NCFU
Stavropol
Ogur26@gmail.com

Sherbakov D.A.
NCFU
Stavropol
dmitry.sh23@gmail.com

North Caucasus Federal University

Abstract

In this article were considered methods and ways of information security implementation in wireless telecommunication networks, and was explored a method of increasing information security in telecommunications networks based on stochastic application of orthogonal signals.

1 Introduction

The widespread use of computer technologies in automated information processing and management systems has led to an exacerbation of the need to protect information circulating in computer systems from unauthorized access. To increase the security of information in wireless telecommunications networks, an algorithm is proposed that generates a large number of orthogonal signals with unpredictable structure, which will increase the security of the transmitted signal, and makes the work relevant.

In the article [Ge04], the author proposes using the low density parity check (LDPC) codes in combination with Walsh transform. The disadvantage of this method is the narrow specialization and low versatility of the method. The method in the article [Wan00] is more universal. The characteristics of the direct CDMA (code division multiple access) channel are analyzed and simulated to develop methods for optimizing combinations of Walsh codes. However, the disadvantage is that it is a pilot signal and hence it is not coherent.

To generate a family of almost orthogonal codes in CDMA, a simple but effective algorithm based on the Walsh-Hadamard sequence was proposed in the article [Cha16] (in this article, there is a simple but yet efficient algorithm for the generation of the Walsh- Hadamard sequence). Analytically established that the proposed WNO code acts as a perfect orthogonal sequence in synchronous mode of data transmission. However, the possibility of their stochastic application of signal assemblies is not considered, which can improve the level of security of the signal considered in the article. Topical issues considered in article [Cho10] shows how to construct

In: Marco Schaerf, Massimo Mecella, Drozdova Viktoria Igorevna, Kalmykov Igor Anatolievich (eds.): Proceedings of REMS 2018 – Russian Federation & Europe Multidisciplinary Symposium on Computer Science and ICT, Stavropol – Dombay, Russia, 15–20 October 2018, published at http://ceur-ws.org

effective signaling sequences for multi-user CDMA communication that show performance for binary sequences optimized for brute force. However, security problems of such sequences are not considered.

As part of the progress of IoT (Internet-of-Things), articles [Mat17, Sag17] propose a design of a PHY/MAC layer using Software Defined Radios (SDRs) that is backward compatible with existing OFDM based LTE protocols and supports CDMA based transmissions for low power IoT devices as well.. In the future, it is possible to use the method of increasing the low power IoT security in telecommunications networks based on the stochastic application of orthogonal signals. Nevertheless, in these works the problems of their safety are not fully covered. In the article [Ray18] The IoT make possible the physical things or home appliances or hand held devices or objects (e.g., smart phones, TVs, cars) can be interconnected by means of suitable communication protocols and information technology infrastructure to share the data to each other and access a range of applications and services like data storage, analytics. Hence, it is necessary to provide methods of ensuring wireless communication security, including increasing the structural concealment of information carrier signals to ensure the confidentiality of personal information.

1.1 Analysis of information security methods in wireless telecommunications networks

CDMA technology is widely used for ensuring confidentiality in the exchange of information between users.

The increase in energy secrecy is achieved due to the expansion of the spectrum of the NLS, which increases the time of signal analysis in the detector. Structural concealment is provided by choosing a signal close in appearance to the background.

The analysis showed that of all the above methods the most relevant is the second, due to the least elaboration of this direction. This is the reason for writing this work.

To ensure the structural concealment of signals, it is necessary that they be orthogonal, have good correlation properties.

To evaluate the characteristics of orthogonal signals, from the point of view of their possible application in real communication channels, correlation functions (autocorrelation, intercorrelation) are commonly used.

At the same time, the following requirements are imposed on orthogonal signals: the maximum CCF emission level should be as small as possible and the maximum level of the side lobes of the ACF should be as small as possible.

Determine the condition under which the requirement of minimum spectrum value for the broadband signal of the ensemble (condition y1) will be ensured and its maximum for the narrowband ensemble signal (condition y2). It follows from the analysis that the first side peak of the ACF R1($\Delta\tau$) of the ensemble signals can be for different signals at the same absolute value, both positive and negative. In this connection, the range in the spectral characteristic of a discrete signal is determined by the relation:

$$\frac{T^2}{\Delta t_k \Delta t \sum_{i=1}^{m} \Theta_{\text{ki}}^2} \left[1 - R_1\left(\Delta t\right)\right] \leq \frac{W_k^2}{W_o^2} \leq \frac{T^2}{\Delta t_k \Delta t \sum_{i=1}^{m} \Theta_{\text{ki}}^2} \left[1 + R_1\left(\Delta t\right)\right] \tag{1}$$

It is obvious that the left-hand side of the expression (1) determines the condition y2, , and the right-hand side of the expression (1) determines the condition y1. As noted above, when synthesizing ensembles of discrete orthogonal signals, the case in which the shift of the frequency spectra of the ensemble signals is minimal is of interest, that is, in other words, when the left and right sides of inequality (1) tend to one another in magnitude.

ACF and CCF of the Walsh sequences have large side peaks and, therefore, do not meet the requirements for orthogonal signals. Figure 1 shows the ACF of eight Walsh functions for a system of volume N=8.

From analysis of figure 1 it follows that Walsh functions as the largest side peaks: wal (7,0), wal (6,0), wal (4,0), wal (3,0). This disadvantage leads to high-level inter-channel interference, and it is therefore inappropriate to use Walsh functions as address sequences in communication systems with channels divided by code.

However, based on Walsh systems, it is possible to construct derivative (composite) signal systems that will have good correlation properties. Barker codes can be used as such systems.

Table 1 shows the levels of the side peaks of ACF of Walsh systems and derived systems, for systems with a volume N=8, 16, 32, 64.

Analysis of Table 1 showed that Walsh systems are significantly inferior to derived systems in terms of the quality of the correlation properties.

Thus, the main disadvantages of CDMA systems using Walsh sequences are: poor correlation properties, familiarity of the species of these sequencesm, limited number of them.

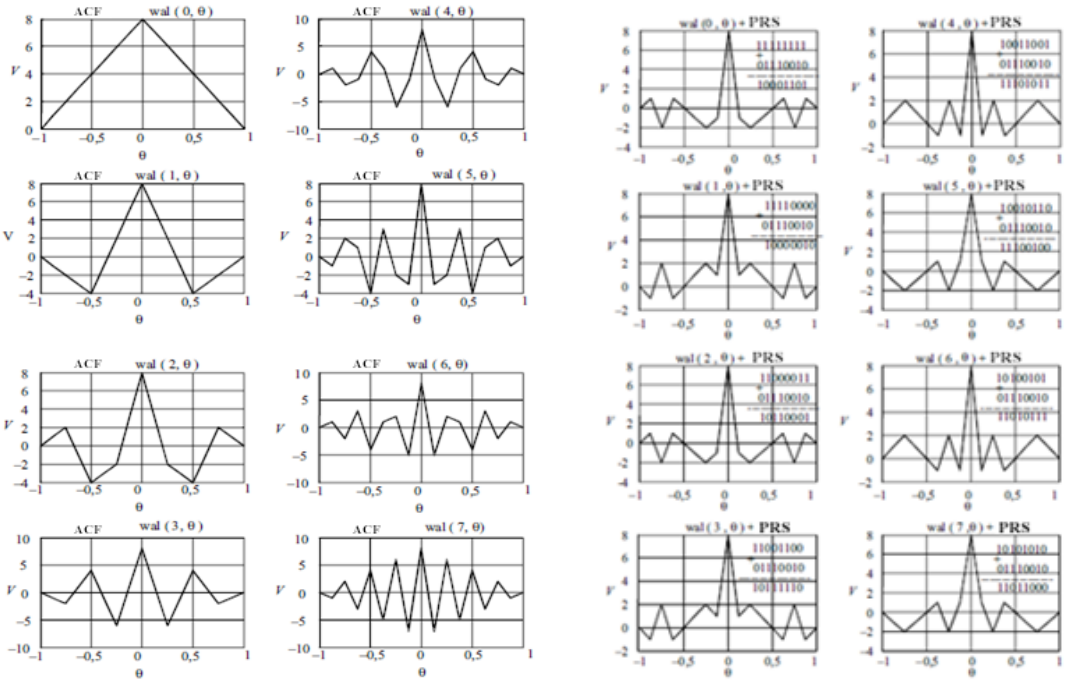

Figure 1: Diagram of the Anthropomorphic Manipulator with 7-Degrees of Mobility

Table 1: Levels of side peaks of ACF

Volume of the system, N	8	16	32	64
Walsh system	7	15	31	63
Derivative system	2	9	17	25

All this reduces the structural concealment of such communication systems. A disadvantage of systems with CDMA using derived signals is a limited number of volumes of derived signals (N = 8, 16, 32, 64) and their typicality, which also indicates a lack of structural stealth.

Consequently, systems with CDMA using Walsh sequences and derived signals will not allow the required structural stealthiness even with stochastic application of these signals.

1.2 Development of a method for enhancing the structural security of wireless telecommunications networks and its algorithmization

Since Walsh sequences and signal system derivatives do not allow to provide the required structural concealment even with their stochastic application, it is necessary to propose using orthogonal signals in systems with channels divided by code, the number of which will allow them to be used randomly, which will increase the security of information in the wireless telecommunication networks (WTN). Therefore, initially it is necessary to receive such signals, further investigate their characteristics and determine the number of unique signals. All of the above will make it possible to implement a mathematical model. A rational model for the synthesis of orthogonal signal systems (OSS) is the use of eigenvectors (EV) of Hermitian matrices (HM). In thimodel, the diagonal coefficients of the matrices are randomly assigned, which will determine the orthogonality properties of the signals.

Let's consider the given model on an example of HM of the fourth order with all zero arguments of factors in the second diagonals and zero coefficients in the main diagonal. Such a matrix has the form:

$$Q = \begin{vmatrix} 0 & A_{12} \cdot e^{i \cdot \varphi} & 0 & 0 \\ A_{21} \cdot e^{i \cdot \varphi} & 0 & B_{23} \cdot e^{i \cdot \varphi} & 0 \\ 0 & B_{32} \cdot e^{i \cdot \varphi} & 0 & C_{34} \cdot e^{i \cdot \varphi} \\ 0 & 0 & C_{43} \cdot e^{i \cdot \varphi} & 0 \end{vmatrix} \quad (2)$$

In the matrix (2), the coefficients of the second-second diagonals are symmetric, that is, $A_{12} = A_{21}, B_{23} = B_{32}, C_{34} = C_{43}$ and are complex numbers represented in exponential form. The symbol ϕ denotes the phases of the coefficients. Stochastic filling of the diagonal elements of HM allows to obtain a model of stochastic orthogonal signals, its EV have the following form:

$$X = \begin{vmatrix} a_{11}e^{i\cdot\varphi_{1,1}} & a_{12}e^{i\cdot\varphi_{1,2}} & \dots & a_{1m}e^{i\cdot\varphi_{1,m}} \\ a_{21}e^{i\cdot\varphi_{2,1}} & a_{22}e^{i\cdot\varphi_{2,2}} & \dots & a_{2m}e^{i\cdot\varphi_{2,m}} \\ . & . & . & . \\ a_{n1}e^{i\cdot\varphi_{n,1}} & a_{n2}e^{i\cdot\varphi_{n,2}} & \dots & a_{\mathrm{nm}}e^{i\cdot\varphi_{n,m}} \end{vmatrix} \tag{3}$$

The EV of the above matrix is one signal from this ensemble, which can be described as a set of unit cells as follows:

$$\dot{x}_y(t) = \left\{ \mathrm{a}_1 e^{j\psi_1}, a_2 e^{j\psi_2}, a_3 e^{j\psi_3}, \dots a_{m/2-1}\, e^{j\psi_{m/2-1}},\ a_{m/2} e^{j\psi_{m/2}}, a_{m/2+1} e^{j\psi_{m/2+1}}, \dots, a_m e^{j\psi_m} \right\} \tag{4}$$

2 Results

2.1 Investigation of the effect of the phases of the HM coefficients on their coordinates

The problem: to synthesize the ensemble of signals, described by the EV of a symmetric bidiagonal matrix of the fourth order. To synthesize the ensemble of signals, we choose an HM of the fourth order (N = 4) for which all the elements except the second diagonal are zero.

The phase coordinates of the synthesized signal ensemble take only two values: $\varphi = 180^0, 0^0$. The amplitudes of this ensemble of signals take four values: U=±0.6533, 0.2706.

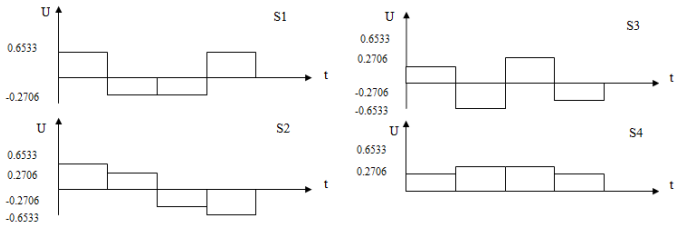

Figure 2: Time diagrams of the synthesized ensemble of signals

Analyzing Figure 2, it can be argued that for a fourth-order matrix with zero phase values of all coefficients, the program makes it possible to obtain an ensemble consisting of four non-repeating signals. Therefore, we can assume that using the entire range of degrees and Hermitian matrices of different orders, it is possible to obtain the required number of orthogonal signals for their stochastic application.

The purpose of this experiment is to determine the dependencies between the phase changes of each of the HM coefficients and their combinations and the resulting phases of the EV coordinates. The tasks of the experiment are:

1. calculation of EV and phases of their coordinates for the coefficients A, B, C, AB, AC, BC at φ=15,30,45;
2. compilation of tables indicating the number of changing phases of the EV coordinates for each of the coefficients and their combinations.

Below is only an analysis of calculations without listing the results of calculations of A, B and C. For this, let us analyze the calculated phases of the coordinates of the EV. Based on the results of the analysis, a table is drawn up, shown in Figure 3, cells with varying phase coordinates of the EV.

The orthogonal phase-shifted signals are denoted as S1-S4, and the digits 1-4 indicate their coordinates. Thus, analyzing Figure 3, we can conclude that

1. A change in the phase of the coefficient A leads to a change in the phases of the three signal coordinates.
2. A change in the phase of the coefficient B leads to a change in the phases of the two signal coordinates.

The phase matrix with phase A change

	1	2	3	4
S1	0			
S2	0			
S3			0	
S4			-0	

The phase matrix with phase B change

	1	2	3	4
S1	0			-0
S2	0			180
S3		180	0	
S4		0	-0	

The phase matrix with phase C change

	1	2	3	4
S1				0
S2				180
S3		180		
S4		0		

Figure 3: Influence of the phase of the coefficient A on the coordinates of the EV

3. Changing the phase of the coefficient C, as in the case of the coefficient A, leads to a phase change in the three coordinates of the signal.

Let us investigate the effect of changing the phases of combinations of the fourth-order HM coefficients on the coordinates of EV. The results of calculations are shown in Fig. 4.

The phase matrix with phase change AB

	1	2	3	4
S1				-0
S2				180
S3		180		
S4		0		

The phase matrix with phase change AC

	1	2	3	4
S1	0			-0
S2	0			180
S3		180	0	
S4		0	-0	

The phase matrix with phase change BC

	1	2	3	4
S1	-0			
S2	-0			
S3			0	
S4			-0	

Figure 4: Effect of the phases of the coefficients on the coordinates of the EV

Therefore, after analyzing the results of the experiments, it is necessary to draw conclusions:

- a change in the phases of the coefficients A and C leads to a change in the phases of the three coordinates EV, and in the case of the coefficient B, two;
- changing the phases of the combination of the coefficients AB and BC causes phase changes in the three coordinates EV, and AC - two;
- simultaneous change of phases of two coefficients leads to overlapping of their zones of influence on each other and the invariance of the phases of the coordinates of EV;
- the change in the phases of the HM coefficients entails a change in the amplitude of the EV.

The phases of the co-ordinate coordinates obtained when the amplitude of the coefficients A, B, and C are changed are shown in Fig. 6.

Figure 5 shows the initial phase matrix, for further changes in signs and amplitudes.

Initial matrix of phases

The phase matrix for a change in the amplitude A

	1	2	3	4
S1	0	-0	180	-180
S2	0	180	180	-0
S3	0	-180	-0	-180
S4	-0	-0	0	0

The phase matrix for a change in the amplitude B

	1	2	3	4
S1	0	180	-180	0
S2	0	180	0	180
S3	0	0	-180	-180
S4	0	0	0	0

The phase matrix for a change in the amplitude C

	1	2	3	4
S1	0	-180	0	-180
S2	0	-180	-180	0
S3	0	0	180	180
S4	0	-0	0	-0

Figure 5: Initial phase matrix

Based on the results of alternating changes in the amplitude of the coefficient, the following conclusions can be drawn:

- as the amplitude decreases, the first, second and third rows in the matrix of the phase coordinates of the change places;
- as the amplitude of the phase of the coordinates increases, EV have the same values as for the initial amplitude, respectively, of the coefficients A, B, and C;
- a decrease in the amplitude of the coefficient A leads to a decrease in the amplitude of one coordinate of the signals: for S1 and S2 (1.3); (2.3), for S3 and S4 (3.1); (4.1) and an increase in the amplitudes of the remaining coordinates of the signals;

	1	2	3	4
S1	0	180	180	0
S2	-0	-0	180	180
S3	-0	180	-0	180
S4	-0	-0	0	0

Figure 6: Phase matrices with a change in the amplitude of the coefficients A, B and C

- a decrease in the amplitude of the coefficient B leads to a decrease in the amplitudes of the two signal coordinates: for S1: (1,1), (1,4); S2: (2.2), (2.3); S3: (3.1), (3.4); S4: (4,2), (4,3) and an increase in the amplitudes of the remaining coordinates of the signals;

- an increase in the amplitude of the coefficient C leads to a decrease in the amplitudes of the two coordinate signals: for S1: (1.3), (1.4); S2: (2.2), (2.3); S3: (3.1), (3.4); S4: (4,1), (4,2) and an increase in the amplitudes of the remaining coordinates of the signals;

It is known from the source [Zhu13] that the absolute values of the coordinates of the eigenvectors of the bidiagonal symmetric matrix are determined by the absolute values of the coefficients of the diagonals of the matrix. Let's check this theoretical situation.

Thus, the purpose of this experiment is to determine the dependencies between the coefficients of HM, the values of EV and the phases of EV when the signs of the HM coefficients change. In Figure 7, three columns of the phase matrix are filled, therefore, a change in the sign of the coefficient A changes the phase of three coordinates for each EV.

The phase matrix when the sign of A changes

	1	2	3	4
S1	-0	-0	0	180
S2	-0	180	-0	0
S3	-0	-0	180	-0
S4	-0	180	180	180

The phase matrix when the sign of B changes

	1	2	3	4
S1	-0	180	-0	180
S2	-0	-0	-0	0
S3	-0	180	180	-0
S4	-0	-0	180	180

The phase matrix when the sign of C changes

	1	2	3	4
S1	-0	180	180	180
S2	-0	-0	180	0
S3	-0	180	0	-0
S4	-0	-0	0	180

Figure 7: Influence of the sign of the coefficient A on the coordinates of the EV

Experimental calculations are feasible for the matrix. In this case, we will successively change the sign of each of the coefficients, as well as their combinations by a negative one. An analysis of Figure 7 for B showed that the coefficient B is less influential than the coefficient A, since it changes the phases of the two coordinates EV. Thus, a change in the sign of the coefficient C leads to a change in the phase of one coordinate of the EV, so this coefficient can be considered to be insignificant. Next, we change the signs of the combinations of the coefficients of HM. The results of these changes are shown in Fig. 8.

Thus, changing the signs of the combination of the coefficients AB leads to a change in one coordinate of the EV (second). So, after analyzing the results of the experiment when changing the signs of the HM coefficients, it is necessary to draw the following conclusions:

- the results of the experiment fully correspond to the theory;

- the coefficient A changes the phases of three coordinates EV, B-two, C-one;

- changing the signs of a combination of coefficients leads to overlapping their zones of influence on each other.

The phase matrix when the signs AB change

	1	2	3	4
S1	-0	-0	180	0
S2	-0	180	180	180
S3	-0	-0	0	180
S4	-0	180	0	0

The phase matrix when the signs AC change

	1	2	3	4
S1	-0	-0	0	0
S2	-0	180	-0	180
S3	-0	-0	180	180
S4	-0	180	180	0

The phase matrix when the signs BC change

	1	2	3	4
S1	-0	180	-0	0
S2	-0	-0	-0	180
S3	-0	180	180	180
S4	-0	-0	180	0

Figure 8: Influence of the signs of the combination of coefficients on the coordinates of the EV

2.2 Calculation of the number of possible orthogonal signal structures

To calculate the number of possible orthogonal signal structures for matrices of the fourth, eighth, sixteenth, thirty-second and sixty-fourth order, it is necessary to derive a formula in which the following parameters will be taken into account:

So, the formula for calculating the number of possible orthogonal signal structures (C) taking into account the above parameters will take the form:

$$C = 2^{N-1} * \frac{\Delta\varphi}{\Delta} \tag{5}$$

The results of calculations of the number of possible orthogonal signal structures are shown in Fig. 9.

Thus, based on the results of calculations, it is possible to plot the dependence of the number of possible orthogonal signal structures on the order of the matrix, that is, C_n.

The initial data $N := 4, 8, 16, 32, 64 \varphi := 360 \Delta := 1$ and 10

The number of sequences obtained with the resolving power of the phase detector is 1 and 10 degrees, respectively

1	10
$C := 2^{N-1} \cdot \frac{\varphi}{\Delta} = 2.88 \times 10^{3}$	$C := 2^{N-1} \cdot \frac{\varphi}{\Delta} = 288$
$C := 2^{N-1} \cdot \frac{\varphi}{\Delta} = 4.608 \times 10^{4}$	$C := 2^{N-1} \cdot \frac{\varphi}{\Delta} = 4.608 \times 10^{3}$
$C := 2^{N-1} \cdot \frac{\varphi}{\Delta} = 1.18 \times 10^{7}$	$C := 2^{N-1} \cdot \frac{\varphi}{\Delta} = 1.18 \times 10^{6}$
$C := 2^{N-1} \cdot \frac{\varphi}{\Delta} = 7.731 \times 10^{11}$	$C := 2^{N-1} \cdot \frac{\varphi}{\Delta} = 7.731 \times 10^{10}$
$C := 2^{N-1} \cdot \frac{\varphi}{\Delta} = 3.32 \times 10^{21}$	$C := 2^{N-1} \cdot \frac{\varphi}{\Delta} = 3.32 \times 10^{20}$

Figure 9: Listings of settlements for $\delta = 1$ and $\delta = 10$

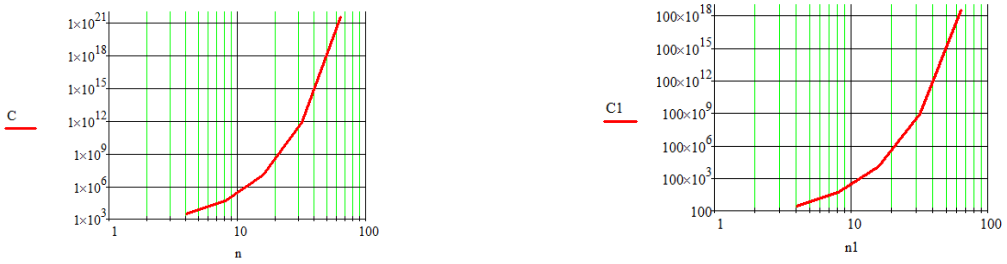

Figure 10: Graph of C(n) at $\delta = 1$ and $\delta = 10$

Thus, based on the results of the calculations in figure 10 the graph of the dependence of the number of possible orthogonal signal structures on the order of the matrix with the resolving power of the detector of the phase-modulated signals is equal to one and ten degrees respectively, i.e., C_n.

3 Discussion

For the mathematical modeling of orthogonal signals, a model and a program were developed which look for eigenvectors and their coordinates for given matrices, calculate the values of the ACF, CCF, and plot the graphs of these functions. The results of the work are analyzed and a conclusion is drawn that it will allow obtaining the necessary number of orthogonal signals for realization of their stochastic application. Therefore, it is advisable to apply the results obtained with the use of the program to improve the structural concealment of the WTN.

4 Conclusion

In this article, conclusions were drawn about the methods and possibilities for implementing information security in wireless telecommunications networks. The most relevant is to improve the structural concealment of signals-bearers of information to ensure the confidentiality of information. ZA method for increasing the security of information in telecommunications networks based on stochastic application of orthogonal signals was also investigated. A formula is proposed that allows obtaining the necessary number of orthogonal signals for their stochastic application, and a graph of the dependence of the number of possible orthogonal signal structures on the order of the matrix is presented.

References

[Ge04] Ge, Q., Yin, L., Lu, J., Mei, S. Channel estimation algorithm in OFDM systems combined with the Walsh transform and LDPC codes (2004) QinghuaDaxueXuebao/Journal of Tsinghua University, 44 (6), pp. 837-839.

[Wan00] Wang, B., Hong, X.N., Hui, T., Gao, B.X. Characteristics and optimal selection of Walsh codes in CDMA systems (2000) QinghuaDaxueXuebao/Journal of Tsinghua University, 40 (9), pp. 37-40.

[Cha16] Chakraborty, D., Tarafder, M.K., Chandra, A. A New Walsh-Like Near Orthogonal (WNO) Sequence for Asynchronous CDMA System (2016) Wireless Personal Communications, 88 (4), pp. 711-729.

[Cho10] Chonavel, T., Vincent, P. Spectral balancing techniques application to CDMA and UWB signaling (2010) 10th International Conference on Information Sciences, Signal Processing and their Applications, ISSPA 2010, article N 5605600, pp. 516-521.

[Mat17] Mathur, S., Sagari, S.S., Amin, S.O., Raychaudhuri, D., Wang, G. Demo abstract: CDMA-based IoT services with shared band operation of LTE in 5G (2017) 2017 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2017 8116509, p. 958-959

[Sag17] Sagari, S.S., Mathur, S., Saha, D., Raychaudhuri, D., Wang, G.Realization of CDMA-based IoT services with shared band operation of LTE in 5G (2017) MECOMM 2017 - Proceedings of the 2017 Workshop on Mobile Edge Communications, Part of SIGCOMM 2017 p. 37-42

[Ray18] Ray, A.K., Bagwari, A.Study of smart home communication protocols and security, privacy aspects (2018) Proceedings - 7th International Conference on Communication Systems and Network Technologies, CSNT 2017 8418545, p. 240-245

[Zhu13] Zhuk A.P., Petrenko V.I., Kuzminov Yu.V.., Zhuk E.P., Luganskaya L.A. Perfection of the method of information exchange in high-speed wireless information networks using new types of ensembles of discrete sequences // Journal of Contemporary Problems in Science and Education. - Moscow: Publishing House "Academy of Natural History", 2013. - 8 p.