UDC 004.9: 621.391.7

PRINCIPLES OF FORMATION, PROCESSING AND PROPERTIES OF OFDM SIGNALS

Alexandr Zamula[1], Vladislav Morozov[1], Vadim Serbin[2]

[1] V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine
zamylaaa@gmail.com, ilissar@hotmail.com

[2] Yuzhnoye State Design Office, 3 Krivorozhskaya St., Dnipro, 49008, Ukraine
buba75@i.ua

Reviewer: Alexandr Potii, Doctor of Sciences (Engineering), Full Professor, Department of Information Systems and Technologies Security, V. N. Karazin Kharkiv National University, 6 Svobody Sq., Kharkiv, 61022, Ukraine
potav@ua.fm

Received on May 2018

Abstract*. The article discusses the technology of forming signals used in mobile, information and telecommunication systems, and also provides an analysis of promising technologies that can be used in wireless communication systems of broadband access. It is shown that the widely used modulation scheme with orthogonal frequency division (OFDM) has a number of drawbacks, which can lead to a decrease in system performance. Alternative technologies for generating signals are presented, in particular, a technology based on windowed signal processing (W-OFDM), a technology based on time division (w-OFDM); UFMC technology and others to eliminate the disadvantages of OFDM technology. New points of view are proposed on the use of multi-carrier transmission technology in the form of multiplexing with orthogonal frequency division (in order to increase the security of modern wireless broadband access communication systems from external and internal threats), a class of non-linear discrete cryptographic sequences to form a physical data carrier - signal. It is shown that the use of such signals will improve the security of these systems from inserting (imposing) false messages into the system, falsifying messages, as well as ensuring the integrity and confidentiality of data, receiving noise immunity and secrecy of the system.*

Keywords*: noise immunity; information security; broadband access; signal; integrity; noise immunity; cellular communication; frequency division; interference; peak factor.*

1 Introduction

Modern wireless systems (for example, satellite systems, mobile telephony systems) belong to multi-user systems. When designing such systems, the main problem is to choose method of multiple access, i.e. the possibility of simultaneous use by many subscribers of a communication channel with minimal mutual influence [1,2]. Broadband signals are widely used in modern high-speed cellular communication systems of the WiMax, Mobile WiMax, MBWA standards, wireless discrete communication systems, such as LTE and Wi-Fi, in the transmission of information from digital television (DVB-T) and radio (DRM, DAB), in radiolocation, etc. The use of signals with orthogonal frequency division multiplexing (OFDM), including in the specified information transmission systems, allows to increase not only the information capacity of the system in case of multipath propagation with limited bandwidth, but also the data transmission speed, bringing it closer to the channel capacity, increase the secrecy of transmission and noise immunity of the system. Currently, there is a rapid development, research and standardization of technologies for the fifth generation of cellular networks (5G). The most priority tasks in this direction are: to achieve the maximum data transfer rate (up to 20 Gbit / s); ensuring the density of user devices (up to 10^6 devices / km2); providing users with highly reliable low latency communication services (URLLC) (data transmission delay not more than 1 ms) [3-4].

In order to achieve the above objectives for 5G networks, the following are considered: use of the spectrum in the millimeter range [5]; new types of signal modulation and coding methods; multiple access methods; improved technologies for building antennas and networks architecture [5-6]. In addition, it is worth noting studies devoted to: orthogonal frequency division multiplexing with filtering (F-OFDM) [7-9]; spatial diversity technologies (MIMO) [10]; radiocommunication cloud networks (C-RAN) [11], orthogonal frequency division technology with coding (C-OFDM) [12] and many others.

2 Implementation principles for OFDM technology

The main idea of OFDM is to achieve a high transmission rate, in the frequency domain, by dividing full signal frequency range into a number of non-overlapping frequency subchannels with lower speeds. In addition, each subchannel (subcarrier) is modulated by a separate symbol, then these channels are multiplexed in frequency domain and data are transmitted in parallel in orthogonal subchannels. Compared to single carrier transmission, this approach provides enhanced resistance to narrowband interference and channel distortion. Specified, in particular, allows for a high level of system flexibility, since modulation parameters, such as constellation size, coding rate, can be independently selected for each subchannel.

The structure of the OFDM modem contains a transmitter and receiver. In the transmitter, the original serial stream of information bits (Fig. 1) is encoded with an error-correcting code (according to the recommendation of LTE 3GPP TS 36.211, a convolutional turbo code with a base rate of 1/3 is used), interleaved (I) and demultiplexed into N parallel substreams.

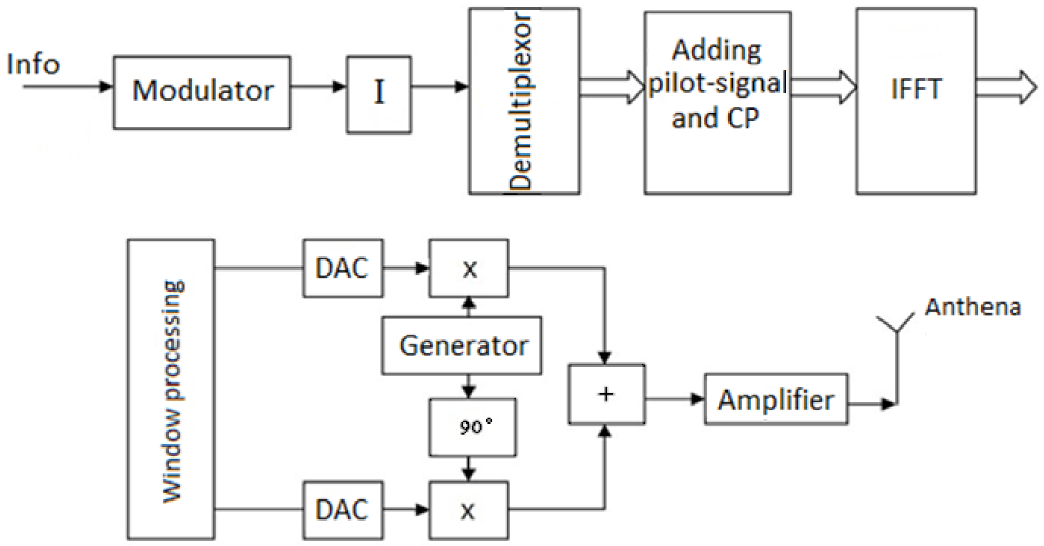

Fig. 1 – The structural circuits

Next, each of the streams is mapped to a stream of symbols using a phase modulation (BPSK, QPSK, 8-PSK) or amplitude-phase quadrature modulation (QAM). In case of BPSK modulation, a stream of binary numbers (1 and -1) is obtained, and for QPSK, 8-PSK, QAM – a stream of complex numbers. In addition to the information subcarriers, there are service subcarriers. These include guard intervals, pilot signals and additional overhead information for synchronization of the receiver and transmitter, and their modes of operation. Pilot signals may have a fixed position on the subcarriers, or variable, varying from symbol to symbol in OFDM frames. In this case, due to the insertion between the adjacent subchannels of a sufficiently long guard interval, the spectral overlap is excluded. In this case, the inter-channel interference (ICI) is reduced, the probability of bit error decreases, which means that the capacity of the wireless access system increases.

The operation of complex exponential multiplying with the corresponding subchannel frequency and then summing all the subchannels to form an OFDM signal is very similar to the operation of the inverse fast Fourier transform (IFFT). By using IFFT to form the required OFDM symbol, it greatly simplifies the implementation of modulators.

Maintaining orthogonality is necessary so that the receiver can correctly recognize the information on the subcarriers. To do this, you must fulfill the following conditions:

- the receiver and transmitter must be accurately synchronized;
- the analog components of the transmitter and receiver must be of very high quality;
- the channel should not be multipath.

Unfortunately, multipath distortion is almost inevitable in radio communication systems, which leads to a distortion of the received signal. To eliminate this type of interference, it is necessary to choose a guard interval, the duration of which is longer than the maximum propagation delay in the channel. Thus, it is possible to eliminate most types of inter channel interference (ICI) and between adjacent transmission units (i.e., inter-symbol interference (ISI)). To reduce the out-of-band emission of signals, window processing of the time signal is used, using a “raised cosine” window. Further, digital-to-analog converters (DAC) convert the real and imaginary components separately into analog form. After passing through the low-pass filter, the signal enters the quadrature mixer, which transfers the useful spectrum of the OFDM signal to the carrier frequency. These signals are then summed, amplified and the OFDM signal itself is formed.

The widespread use of the OFDM digital modulation scheme is due to a number of remarkable features of this technology:

- resistance to multipath effects;
- high noise immunity to narrowband interference;
- resistance to intersymbol interference due to the fact that the duration of the symbol in the auxiliary subcarrier is significantly longer compared to the propagation delay than in traditional modulation schemes;
- high spectral efficiency in comparison with traditional systems with frequency division of channels due to the large number of subcarriers;
- the ability to use different modulation schemes for different subcarriers, which allows you to adapt to the conditions of signal propagation and to different requirements for the quality of received signals;
- simple implementation using digital processing methods, etc.

3 Promising technologies for generating signals in modern mobile telecommunications systems

The effectiveness of the modern generation of mobile communications is largely based on the use of OFDM modulation. However, for further progress and transition to more advanced fifth-generation communication technologies, it is necessary to revise the OFDM technologies used, as well as explore other technologies. The following main differences between the 5G technology and previous generation mobile communication technologies [4-5] can be distinguished.

1. Mixed numerology. One of the goals of 5G is to ensure the use of various services, in particular eMBB, mMTC and URLLC. It is assumed that 5G technology should support more flexible use of the available frequency band to increase throughput. For this, it is necessary to develop and implement various options for using the available frequency and time resources for various services.
2. Increased bandwidth - a threefold increase in the efficiency of using the signal spectrum in 5G in comparison with eMBB services [3]. To increase the capacity in 5G networks, it is planned to reduce guard intervals [4].
3. With asynchronous data transmission in 4G networks, the base station is constantly synchronized with user equipment to reduce mutual interference between carriers [4]. Losses caused by such interference adversely affect the services, in particular, mMTC, which are associated with the mass connection of network subscribers. Thus, 5G support for asynchronous transmission is necessary in order to solve ICI-related problems and ensure operation over multiple connections [4].

As noted above, orthogonal frequency multiplexing is an access scheme that is used in modern 4G networks. Two separate signals are used to gain access to the network – an orthogonal frequency division multiplexing access (OFDMA) signal in the downlink and a single carrier frequency multiplex access (SC-FDMA) signal in the uplink. The advantages of this scheme are associated with the possibility of transmitting signals on multiple carriers. However, this OFDM scheme has a number of disadvantages, in particular: high sensitivity to frequency and clock frequency shifts; high ratio of peak signal power level to average – peak factor (PAPR); the use of guard intervals reduces spectral efficiency; sensitivity to the Doppler effect, which imposes some restrictions on its use in mobile networks; overlapping subcarrier bands leads to inter-bit interference; the OFDM signal is vulnerable to spectral conversion products caused by non-linear amplifiers, a constant component offset when using FFT. In addition, sensitivity to frequency and clock shifts necessitates the periodic addition of synchronization signals to the total amount of signals used and requires device and network synchronization before commencing communication (data exchange). The lack of continuity (phase transition) between two symbols during the generation of OFDM symbols triggers spectral spikes in the frequency domain, which leads to intense out-of-band emissions and else.

The limited capabilities of the signals based on the OFDM modulation scheme have become a prerequisite for research to select candidate signals for future generations of mobile communications, in particular 5G. In this regard, one of the tasks to be solved is to fulfill the requirement of a significant reduction in the delay in the introduction of new services and applications. Along with this, it becomes necessary to form a cyclic prefix and reduce the length of characters. These considerations led to the creation of a variety of signal conditioning technologies: with generalized frequency multiplexing (GFDM); filter bank multi-carrier (FBMC); time division OFDM (w-OFDM); universal multi-carrier filtered signal (UFMC); orthogonal frequency division multiplexing with F-OFDM filtering and others. Research is also being conducted on new multiple access schemes, including: sparse code multiple access (SCMA), non-orthogonal multiple access (NOMA) and resource-spread multiple access (RSMA).

FBMC is one of the most well-known spread spectrum modulation formats in wireless communications [14]. This modulation provides a significant advantage in the formation of each subcarrier and facilitates the flexible use of the spectral resource, allows you to meet various system requirements such as low latency, multiple access and others, which leads to improved system noise immunity under the signal scattering conditions in the time and frequency domains [15]. For example, rectangular filters are preferable for channels distributed in time, while a filter with a raised cosine characteristic is more resistant to frequency dispersion. Despite all the benefits of using FBMC, a considerable length of filters leads to a long symbol duration, which is a problem not only for applications with low latency requirements or a large number of users in communications, but also leads to an increase in computational complexity for MIMO detection technology, which, ultimately, will lead to problems in the operation of all major 5G applications.

The UFMC technology [13] is largely recommended for overcoming the ICI problem with multiple user access in asynchronous transmission mode and is based on frequency division and multiplexing by applying a subcarrier group filtering operation. UFMC is a generic version of the filtering technique for multiple sidebands. The sidebands are processed by the filter at the same time, instead of processing each power supply unit separately. Thus, mutual interference with power supply units is reduced in comparison with traditional OFDM. Also, the use of sidebands filtering operations is aimed at increasing the efficiency of a number of communications applications, such as systems with ultra-low packet latency. This type of modulation is more preferable for such applications in relation to the FBMC modulation scheme.

GFDM technology is a block modulation circuit with frequency channel multiplexing, designed to work with a variety of 5G applications, providing a variable waveform [16]. To improve reliability and communication latency without error correction, GFDM signals can be used along with the Walsh-Hadamard transform. When combining GFDM with quadrature amplitude modulation, in systems with multiple access, the problem of intra-system interference is solved subject to the use of non-orthogonal filters. From another point of view, GFDM can be considered as a scheme with flexible tuning of individual blocks, and not just one carrier as a whole. When manipulating the relevant GFDM signal parameters, it is possible to obtain various waveforms, such as OFDM, single-carrier frequency alignment (SC-FDE), etc. Despite the very promising possibilities that are opened by using signals with GFDM, this type of modulation is computationally complex [16].

F-OFDM technology is used in 4G downlink channels. For F-OFDM, the configured filter is applied to the OFDM symbol in the time domain to reduce the out-of-band emission level of the subband signal, while maintaining the orthogonality of the complex domains of the OFDM symbols. Since the filter bandwidth corresponds to the signal bandwidth, only a few subcarriers close to the edge are affected. The main consideration is that the filter length may exceed the cyclic prefix length for F-OFDM [6]. This reduces the level of inter symbol interference due to the selected filter design using window processing (*with soft truncation*). The generation of the F-OFDM signal is based on the formation of a block of M nearby sidebands in a number of consecutive OFDM symbols [17]. In particular, during the processing of each symbol, the following parameters are formed in the transmitter: an inverse fast Fourier transform (IFFT) dimension value equal to N, a duration of M information symbols together with a cyclic prefix, where N > M. Information symbols can be constellation points as in OFDM. Analytically indicated can be represented as follows:

$$s(n)=\sum_{(l=0)}^{(L-1)} s_l(n-l(N+Ng)) \tag{1}$$

and

$$S_l(n)=\sum_{(m=m`)}^{(m'+M-1)} d_{l,m}e^{(j2\pi mn/N)}, -N_g \le n < N, \tag{2}$$

where Ng is the cyclic prefix length (CP), d – information symbol of the subcarrier m of the OFDM system, L denotes the number of OFDM symbols, and $\{m_0, m_{0+1}, \cdots, m_{0+M-1}\}$ is the selected set of subcarriers. The F-OFDM signal is generated by processing the $s(n)$ signal using the appropriate filter, i.e.

$$\tilde{s}(n)=s(n)\cdot f(n). \tag{3}$$

The bandwidth of the filter is equal to the sum of the bandwidth capabilities of the selected sidebands and the time spent is the duration of the OFDM symbol. At the receiver, the received signal first passes through the filter $f(-n)$, which is identical to the filter of the transmitter. The received signal is processed using standard OFDM transforms, and then the filtered signal is divided into a sequence of individual OFDM symbols with the removal of the cyclic prefix. In this case, an FFT of dimension N is applied to each symbol and then informational symbols from the corresponding subcarriers are extracted.

The filter for F-OFDM must satisfy the following criteria: have a flat bandwidth over the subcarriers in the subband; have a sharp transitional strip to minimize guard bands. These criteria correspond to the filter with a rectangular frequency response. To meet these requirements, a low-pass filter is implemented using a “window”, which effectively cuts off the impulse response and provides smooth transitions to zero at both ends [17]. Thus, the F-OFDM implementation adds to the existing CP-OFDM processing procedure, the filtering step on both the transmit side and the receive side.

To reduce the out-of-band emission of signals, window processing of the time signal is used, using a raised cosine window. It is known that the spectrum of the OFDM signal has many side lobes that slowly fade out in the frequency domain, which leads to an increase in out-of-band emission. To reduce out-of-band emission, OFDM symbols use guard subcarriers that are added along the edges of the OFDM signal. Window signal processing is used for the same purpose. Such signal processing allows a smooth transition between the end of the previous and the beginning of the next character. Such a transition is carried out by overlapping in time the prefix of the current character and the suffix of the previous character by summing them up.

In this case, the use of window processing for the formation of OFDM symbols can significantly reduce out-of-band emission. The out-of-band emission level is also influenced by the choice of guard interval between subcarriers. Studies have shown that the longer the guard interval, the lower the out-of-band emission level [18].

4 Security indicators evaluation of modern wireless broadband access communication systems based on OFDM technology features

State level of informatization is determined primarily by the development of information communications, as a set of network resources intended for the production and provision of telecommunications, information and other services. With the advent of new information and communication technologies (ICT), the use of various transmission media (*optical fiber, radio frequency resources*), mobile communication systems, it has become possible to significantly increase the productivity, efficiency and quality of service of telecommunications networks, as well as expand the range of services that they provide. A variety of modern ICTs operate under conditions of external and internal influences caused, on the one hand, by natural interference, interference from other radio systems operating at close frequencies or in a common part of the frequency range, on the other hand, deliberate interference caused by counter stations for the purpose of electronic suppression of existing systems. Possible strategies of the counter station are: determining the content of messages when legal subscribers use cryptographic data protection algorithms; falsification of messages; violation of data integrity; statement of various types of interference, etc. Therefore, ICT, especially for critical purposes, have increasingly stringent requirements to ensure the effectiveness of their operation (*information transfer speed, reliability of information transfer, survivability, noise immunity, information security*). Increased requirements for quick decision-making and communicating information to executors (users) in the context of internal and external influences are largely not taken into account by existing information technologies. There is a contradiction between strict requirements to ensure secrecy, confidentiality, integrity, reliability of data stored and transmitted over wired and wireless communication lines, on one hand, and existing models, methods and technologies for managing telecommunications networks, information security, services and quality of service, on the other hand. The main ways to solve this contradiction is to increase the noise immunity (*in particular, noise immunity, energy, structural and information secrecy*) and information security of the ICS by improving the methodological foundations of ICT building by developing information exchange methods, synthesizing new classes of signals with the necessary ensemble, correlation and structural properties.

The development of wireless communications technologies has been constantly shaped based on studies of waveforms. As an example, we can use the technology of multiplexing signals with orthogonal frequency division multiplexing in modern wireless broadband access systems (WiMAX, Wi-Fi, LTE, etc.). The use of this technology allows to increase the information capacity of the system with a limited bandwidth, data reception and transmission speed, bringing it closer to the channel capacity, increasing the secrecy of transmission and noise immunity of signal reception, and as a result, to meet the ever-increasing needs of network users in high-speed connections services.

Analytically, the OFDM signal can be represented as [19]:

$$S(t)=\sum_{k=0}^{N-1} S_k(t)=\sum_{k=0}^{N-1} A_k e^{(j2\pi kf/T)}, 0\le t\le T, \tag{4}$$

where k is the subcarrier index, $S_k(t)$ is the signal on the k-subcarrier, A_k is the amplitude component of the sequence of information symbols, N is the number of subcarriers, T is the duration of the information symbol.

The block diagram of an OFDM modulator is presented in Fig. 2 [20,21]. In the transmitter, the serial stream of binary symbols $s[n]$ is encoded with an error-correcting code, interleaved further, using inverse multiplexing (*demultiplexing*), turns into N parallel streams, each of which is matched (*complexly*) with the output stream s[n] using a certain constellation modulations (*quadrature modulation QAM, quadrature phase modulation QPSK, etc.*). The number of outputs of the demultiplexer is determined by the number of subcarrier frequencies. Next, the modulated $X_0,\ldots,X_{N-1}$ symbol streams undergo a fast inverse Fourier transform, which translates them into digital responses $X_0,\ldots,X_{N-1}$ (in general, complex numbers) in the time domain. The real (Re$\{x_i\}$) and imaginary (Im$\{x_i\}$) components of the response x_i ($i = 0, ..., N-1$) are subjected to digital-to-analog conversion. The received analog signals are used for modulation in accordance with the sine wave and cosine wave (*obtained by shifting the sine wave by 90*) of the carrier frequency. After modulation, the signals are summed to form a signal s (t), which enters the communication channel.

Subcarriers orthogonality makes it possible to select each of them from the common signal at the reception even in the case of partial overlapping of their spectra. Since the subcarriers are located close to each other and even partially overlap, the spectral efficiency of the modulated OFDM signal is high. The parameters of the subcarrier signals are selected in such a way that they are orthogonal to each other, that is, the condition is met for them:

$$\int_0^T sin2\pi f_1(t) sin2\pi f_k(t)dt = 0, \tag{5}$$

where: t is the duration of the information symbol, f_1 and f_k are the frequencies of the l-th and k-th subcarriers, respectively.

The orthogonality of the carrier signals guarantees the frequency independence of the channels from each other and, therefore, the absence of inter-channel interference. For the fast implementation of this procedure, the inverse fast Fourier transform algorithm is used, that is, the signal values at the input of the IFFT block belong to the frequency domain. At the output of the block IFFT receive the signal value in the time domain. Combining all the values, a complex OFDM signal is obtained. Taking into account the fact that IFFT works effectively with arrays of dimension 2^k, the number of subcarriers is chosen with the same multiplicity. For example, in WiMAX wireless communication systems, the number of subcarriers is chosen from 128 to 2048 and can occupy frequency bands from 1.25 MHz to 20 MHz. For each of the subcarriers, a different modulation type is used depending on the requirements and the type of interference in the channel. At the receiving end, the inverse operations are performed, in this case, instead of a digital-to-analog converter, an analog-to-digital converter (ADC) is used, instead of a reverse FFT, direct FFT.

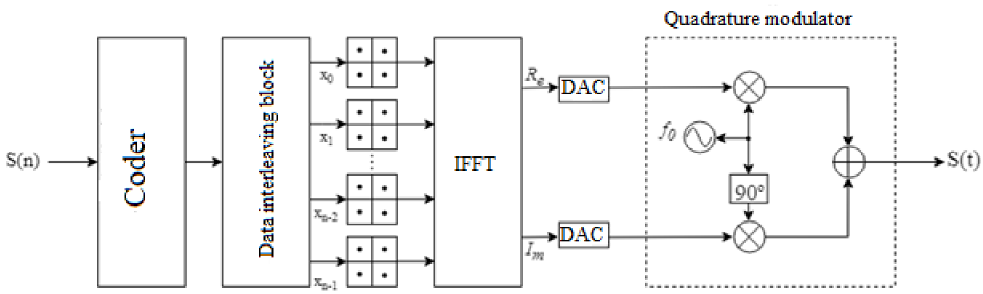

Fig. 2 – OFDM modulator circuit

The structure of the OFDM signal can be quite complex because it consists of many components:

- the structure of the time-frequency distribution, given by: initial frequency, frequency grid pitch, number of subcarriers;
- time slots specified by: the duration of the symbol, the duration of the guard interval;
- type of manipulation: phase (BPSK, QPSK, 8-PSK) or amplitude-phase quadrature modulation (QAM);
- discrete sequences that determine the law (rule) of manipulating the phase of the high-frequency carrier, and given the dimension of the signal space;
- type of symbol sync;
- the presence and type of noise-resistant coding (Reed-Solomon code, Bowes-Choudhury-Hokvingem code, turbo codes, etc.);
- the presence and type of data interleaving and so on.

The above features of the OFDM signal structure can be used in the construction of ICT, for which the ensuring requirements of the specified security indicators against the introduction (imposition) of spurious messages, falsification of messages; data integrity, confidentiality, noise immunity of reception, operation secrecy are decisive.

One of the components of information security (*along with information secrecy*) is imitation protection (*ensuring integrity*) of information. The mathematical apparatus of the imitation protection system includes a cryptographic algorithm for simulating the encryption of information (this may be an encryption algorithm, an authentication code, or another transformation) and an algorithm for deciding the truth of the information received, as well as a key system. In essence, imitational security is a complex service that is provided by the provision of such services as integrity, authenticity, (truth), as well as the use of various cryptographic protocols with certain properties [22,23]. As studies [24,25] have shown, it is possible to provide the imitability necessary in ICS at the source level of complex signals by increasing the dimension of the signal space, the degree of correlation between them, the complexity of the laws of their construction. In accordance with the above definitions, the theory of authentication by J. Simons [26] can be used to quantify the simulated security. It was Symons who showed that for the quantitative assessment of authenticity one can use the probability of deception:

$$P_{обм} \geq 2^{-\Delta I(C,K)}, \tag{6}$$

where $\Delta I(C, K)$ is the amount of information on the authentication key K entered into the C cryptogram.

Let us analyze the expression (3).

1. Systems in which equality (3) is achieved are referred to as systems that are absolutely resistant to deception.

2. To reduce the probability of fraud, it is necessary to increase $\Delta I(C, K)$.

Taking into account the peculiarities of the OFDM signal structure, imitability (I_c) depends on: the dimension of the signal space (I), the number of attempts (C) of imposing (simulating), the space (Z) of the component of the OFDM signal structure (*in particular: initial frequency, frequency grid spacing, ensemble of discrete sequences (signals), number of subcarriers, etc.*), imposition strategies (X):

$$I_c = F(I, Z, C, X). \tag{7}$$

At the complex signals source level (physical level), the probability of cheating or imposing a false signal is defined as

$$P_{обм} \geq 2^{-l_i}, \tag{8}$$

where l_i is the length authentication code, the dimension of the signal space.

Let us show the possibility of increasing the imitability of wireless communication systems based on the use of various classes of discrete manipulating sequences (*hereinafter referred to as DS*). In [1,2,27-29] presents the results of research, which are devoted to the issues of synthesis, formation and study of the properties of a new class of DS, nonlinear discrete cryptographic sequences (hereinafter – CS). The synthesis of DS and signals obtained, for example, by manipulating the phase of a high-frequency carrier according to the CS law, is based on the use of random (pseudo-random) processes, including key data of cryptographic algorithms, and at the same time, the signals must have: absolute structural secrecy regarding their laws formations; improved ensemble properties (*exist for almost any period value, have a significant amount of signal system*); improved correlation properties, which will provide the necessary (*for a particular application of the ICS*) values of the indicators of noise immunity, information security and secrecy of the system. A special property of cryptographic signal systems is the possibility of their recovery in space and time using keys and a number of other parameters that are used in the process of synthesizing such signals.

We will evaluate the imitation resistance of the ICS radio channel for solving the problem of distinguishing signals when applying a dynamic mode of compliance change: the message bit is a complex signal, and various signal systems. Table 1 shows the results of the evaluation of the ensemble properties of various complex signal systems (M-sequences, sequences with a three-level value of the cross-correlation function (PCCF), cryptographic signals (CS)), the maximum achievable values of the side lobes of the cross-correlation function (*the so-called "dense border" packaging*) for the corresponding periods of the DS, as well as the values of the probabilities of imposing, obtained in accordance with the expression (4), when used in the ICS as a physical transfer data of the indicated classes of signals. Analysis of the data in Table 1 shows that the proposed method for the synthesis of complex non-linear discrete cryptographic signals allows the formation of large ensembles of discrete sequences.

Table 1 – Signal properties

Signal class	Sequence period	Dense packing value	Signal ensemble volume	Imposing probability value
M-sequences	31	9	3	$3\ 10^{-1}$
PCCF	31	9	495	$2\ 10^{-3}$
CS	31	9	1465137	$7\ 10^{-7}$
M-sequences	63	17	20	$5\ 10^{-2}$
PCCF	63	17	975	$1\ 10^{-3}$
CS	63	17	12 214 869	$8\ 10^{-7}$
M-sequences	127	27	36	$2\ 10^{-2}$
PCCF	127	17	11610	$8\ 10^{-5}$
CS	127	27	9006648	$1\ 10^{-7}$
M-sequences	255	36	28	$3\ 10^{-2}$
CS	255	36	17599	$5\ 10^{-5}$
M-sequences	511	63	276	$3\ 10^{-3}$
PCCF	511	33	147500	$6\ 10^{-6}$
CS	511	63	2666671	$3{,}7\ 10^{-7}$
M-sequences	1023	100	435	$2\ 10^{-3}$
PCCF	1023	65	338000	$3\ 10^{-6}$
CS	1023	100	5293538	$2\ 10^{-7}$

So for the period of the sequence $N = 63$ the number of pairs of CS satisfying the maximum value of the maximum PCCF side lobes – 17 is 12214869. For a representative of the class of linear sequences – sequences with a three-level cross-correlation function (Gold set), which are optimal from the point of view of cross-correlation functions [30], the number of pairs of signals corresponding to a given boundary is 975. The excess of the volume of a CS over an ensemble composed of M-sequences is more than 10^7 times. For the period of a sequence of 1023 elements, the number of pairs of gearboxes satisfying the limiting value for the side lobes of the cross-correlation function (CCF) 100 is 5293538, whereas for a representative of the class of linear sequences of M-sequences, the number of pairs that meet this boundary is 435, then there is an excess of the volume of the signal system is more than 10^5 times. With a slight decrease in the requirements for the limiting value of the maximum lateral peak of PCCF, according to which the selection of signals is carried out (in fact, a reduction in the noise immunity of reception), the performance of the ICS system can be significantly improved. So, for the period of the sequence $N=127$, increasing the limit value by 1.2 dB will increase the ensemble volume from $M = 11610$ (at the border of 17) to 9006648 signals, with a limit value of 27, that is, 776 times. As follows from the data Table. 1, the probability values of imposing in the case of the application of the CS is much less. So, with a period of the sequence $L = 1023$, it is four orders of magnitude less than using M-sequences and an order of magnitude less than when using sequences with a 3-level PCCF. An improvement in the imitation resistance index of the ICS is achieved due to the fact that the CS have improved ensemble properties in comparison with linear classes of signals, in particular, M-sequences.

In Table 2 shows the results of calculating the statistical characteristics of various correlation functions for discrete signals widely used in communication systems, including the characteristics of cryptographic DS. Calculations were carried out for different values of the DS period. The statistical characteristics of the correlation functions were selected: the value of maximum lateral emissions R_{max}, the value of the expectation of the emission module $m_{|R|}$, the value of the standard deviation of the emission module $D_{|R|}^{\frac{1}{2}}$ and emission values $D_{|R|}^{\frac{1}{2}}$.

Analysis of the data given in Table 2, suggests that maximum lateral emissions values of the CS, as well as the statistical characteristics of this class of signals are not inferior to the corresponding characteristics of the signals constructed using M-sequences and characteristic discrete signals [31]. This, in turn, indicates that the use of a CS provides noise immunity for receiving signals no worse than when applying the decree of signals based on linear formation laws.

Table 2 –Statistical characteristics of correlation functions

Signal type	Characteristics	$\frac{R_{макс}}{\sqrt{N}}$	$\frac{m_{\|R\|}}{\sqrt{N}}$	$\frac{D^{1/2}_{\|R\|}}{\sqrt{N}}$	$\frac{D^{1/2}_{(R)}}{\sqrt{N}}$
Characteristic discrete sequences	AACF	1,0 – 1,8	0,5	0,4	0,5
	PACF	0,1 – 1,9	0,2	0,1	0,2
	MIACF	1,4 – 2,6	0,6	0,5	0,8
	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-sequence	AACF	0,7...1,25	0,32	0,26	0,41
	PACF	$1/\sqrt{N}$	$1/\sqrt{N}$	0	0
	MIACF	1,3...2,3	0,66	0,49	0,82
	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 sequences	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

From the data of Tables 1-2 it also follows that by varying the limiting values of the side-lobe level of the correlation function, depending on the requirements for the ICS, the tasks of achieving the required values of the noise immunity indicators for signal reception, imitation resistance and stealth of the ICS can be solved.

Let us make an ICS protection assessment from imposing false messages, for the case when the system uses a dynamic shift mode (according to the law of the control sequence) correspondence: the message bit is a complex signal. In this case, the value of the probability of imposing a false message ($P_{imp_{\overline{mes}}}$) (with equiprobable choice of characters of the control sequence) can be defined as:

$$P_{imp_{\overline{mes}}} = ((2)^{-k})^{n}, \tag{9}$$

where: the number of possible states of the source of the control sequence, which is determined by an ensemble of discrete signals of information carriers; n – message length provided in bits.

Table 3 shows the values of the probability of imposing $P_{imp_{\overline{mes}}}$. On the message for discrete signals obtained on the basis of carrier manipulation according to the law of M-sequences, PCCF and nonlinear cryptographic sequence. The message size is n = 32. In the calculations of $P_{imp_{\overline{mes}}}$, For the case of application in the system of nonlinear CS, sequences were selected whose correlation characteristics are close to the optimal limit values from the point of view of PCCF ($R_{max} \le 1{,}5\sqrt{N}$).

Data analysis from Table 3 shows that in ICS, which apply signal multiplexing technologies in orthogonal frequency division of channels, the value of $P_{imp_{\overline{mes}}}$ for nonlinear CS is much less than in the case of using linear classes of signals.

5 Models and methods for constructing a secure ICS based on the use of OFDM technology

The rapid development of communication systems and multimedia technologies has led to a significant increase in the amount of information transmitted and, consequently, the need to create reliable high-speed data transmission and information security technologies. Information security technologies in communication systems are widely used in the military sphere, copyright protection, personal data protection and in many other areas. Critical information should be inaccessible to attackers, which is one of the important requirements for modern communication systems.

Table 3 – Imposing message probability

Signal period	$P_{imp_{\overline{mes}}}$ Value for signal systems:		
	M-sequences	PCCF	nonlinear CS
31	2^{-96}	2^{-288}	2^{-672}
63	2^{-96}	2^{-320}	2^{-768}
127	2^{-160}	2^{-448}	2^{-640}
1023	2^{-192}	2^{-608}	2^{-736}

When transmitting important information, it is necessary to use a secretive data transmission system, which involves ensuring protection both from unauthorized access to information and hiding the fact of transmission itself [32].

Orthogonal Frequency Division Multiplexing is a multichannel modulation method used in a variety of modern mobile communication standards. The basic principle of this method is to divide a message into multiple messages transmitted in parallel with a lower speed, which allows for an increase in the transmission speed. Through the use of frequency guard intervals, OFDM successfully counters the inter-channel and intersymbol interference that occurs in other modulation schemes with multiple carriers. Due to the advantages of this method, OFDM is widely used as a modulation and multiplexing method, in many telecommunications applications, including digital television (DAB, DVB), wireless networks (Wi-Fi) and mobile communications (LTE) [33].

6 Secured communications

To meet the growing demand for fast, reliable, and secure wireless data transmission, further research is needed in scope to hide the fact of data transmission. As a rule, the disadvantages of the OFDM method are compensated by the implementation of cryptographic methods at the application level [34]. To transmit sensitive information over public networks, a secure communications system is required. However, in wireless systems, an information signal can be received by anyone, including an attacker. The mere fact of the possibility that data transfer process can be detected, can be of great importance for communication systems in which information that is critical for its owners circulates. Using the means of steganography, it is possible to hide confidential data in other data, in particular - multimedia. Modern communication systems use channel noise to hide data transmissions [35]. The review, the main limitations and possibilities of the developed methods of covert data transmission are discussed in [36] and the channel capacity with additive white Gaussian noise in [37]. The widespread use of computer systems and open source software increases the ability of attackers to gain access to critical data. A possible solution to this problem is to modify the properties of the physical layer. A new solution is proposed to protect critical information transmitted over communication networks. The essence of this solution is to encrypt data at the physical level using OFDM technology.

7 OFDM wavelet transform

The main advantage of the traditional OFDM method with fast Fourier transform for wireless systems is its speed. However, FFT-OFDM requires a cyclic prefix to eliminate intersymbol interference, which reduces throughput. As an alternative to the fast Fourier transform, one can use the wavelet transform (WT) [38]. Unlike the fast Fourier transform, the wavelet transform uses the frequency and time characteristics of the signals. Based on the OFDM wavelet transform (WPT-OFDM) using batch conversion, it is more efficient to resist interference due to the high spectral qualities of the wavelet filters compared to FFT-OFDM [39,40]. WPT-OFDM does not use a cycle prefix, which will increase system throughput compared to FFT-OFDM [41,42]. In addition, the WPT-OFDM technology can significantly increase the noise immunity of signal reception [43,44].

8 Hidden communication using FFT-OFDM

The implementation of the hidden communication model in the FFT-OFDM system was modeled using MATLAB, and the overall efficiency is estimated by comparing the error probability at the corresponding signal-to-noise values. The block diagram of the developed communication model is shown in Fig. 3.

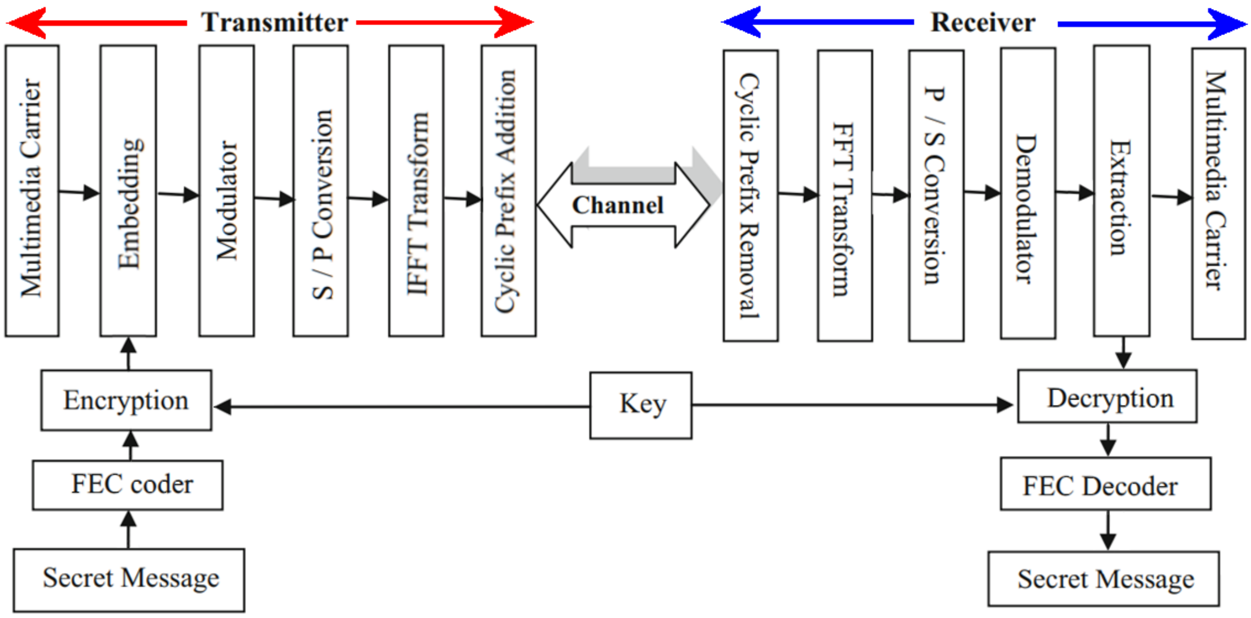

Fig. 3 – Hidden communication system model at the physical level FFT-OFDM

The message is encoded using Forward Error Correction (FEC). Using FEC, various encoding methods are supported, such as RS codes, convolutional codes (CC), etc. In this paper, we used convolutional codes to model the processing of information, which introduce redundancy in the transmitted message. In order to protect against unauthorized access to information, information bits are fed to the input of a data encryption device using a secret key. To decode the received message on the receiving side, the Viterbi algorithm is used. Encrypted data is embedded in a multimedia medium, in which image was used. The least-significant bit (LSB) replacement method was used to embed the message in the medium. The serial data stream is transmitted to the modulator and processed using M-ary PSK/QAM modulation. The pilot signal is used in the developed system to assess the quality of the channel and establish synchronism in the system. Modulated data is converted into multiple parallel streams with a low data rate, each of which is modulated by orthogonal carriers using an inverse fast Fourier transform (IFFT). The result of the IFFT transform is the summation of discrete signals in the time domain as follows [45]:

$$y_k = \frac{1}{N}\sum_{m=0}^{N-1} Y_m e^{\frac{j2\pi km}{N}} \qquad (10)$$

where $\{y_k|0 \le k \le N-1\}$ is a sequence in a discrete time domain, $\{Y_m|0 \le m \le N-1\}$ – complex numbers in the discrete frequency domain.

The cyclic prefix (CP) replicates the "L" number of samples from the end of the "N" sample of the FFT frame and uses them at the beginning of each "N+1" FFT frame. The received OFDM symbol is then transmitted over the channel. On the receiving side, the CP is deleted, and the data is transmitted to the block performing the fast Fourier transform. The result of the FFT is the summation of the received signal in the frequency domain as follows

$$Y_M = \sum_{m=0}^{N-1} y_k e^{\frac{-j2\pi km}{N}} . \qquad (11)$$

At the receiving side, in order to recover information, the process is reversed to that performed in the transmitter. Further, the received data is decrypted using the secret key.

9 Hidden connection using WPT-OFDM

The structure of the transmitter and receiver of the communication system using WPT-OFDM is shown in Fig. 4.

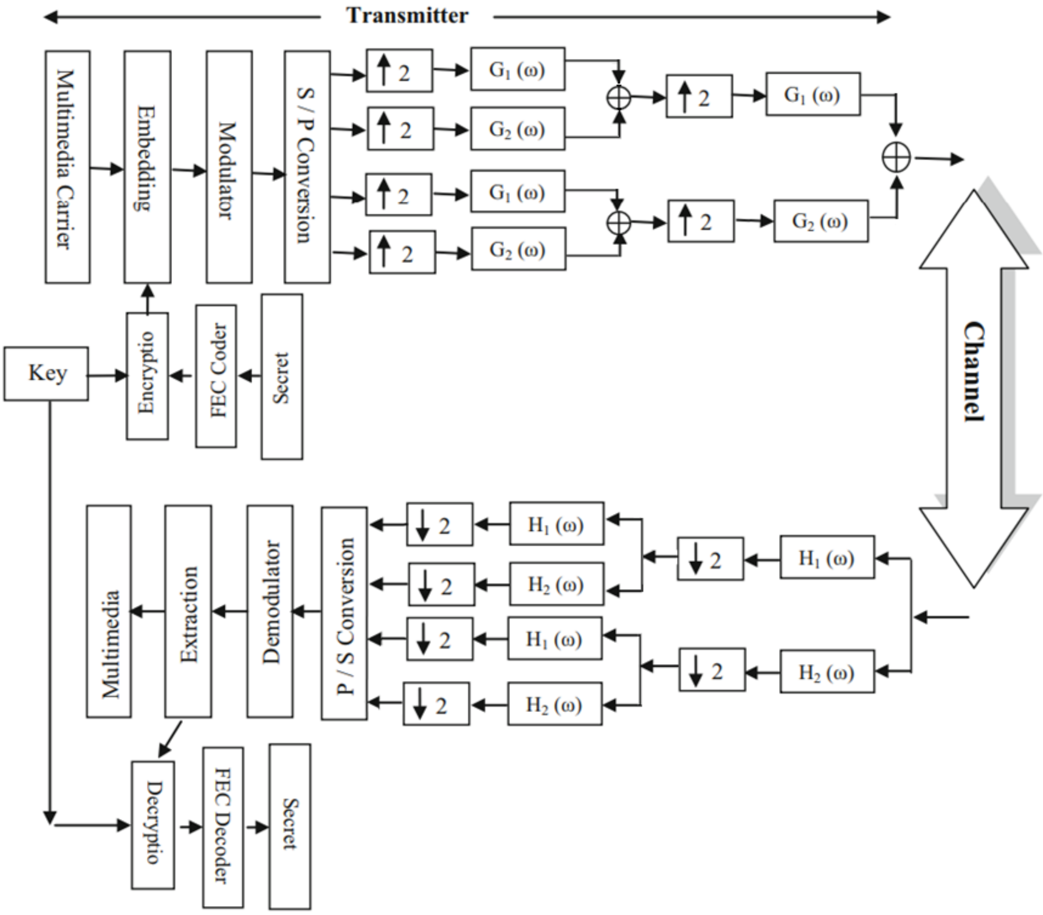

Fig. 4 – Block diagram of the WPT-OFDM communication model

The FFT technology is beneficial in terms of low computational complexity and cost, but at the same time, it has less bandwidth due to the addition of CP [46]. As shown in Fig. 4, the informational message is encoded, encrypted, and inserted into the image. In the model structure using the wavelet transform, the FFT and IFFT are replaced with WT and IWT, respectively. Wavelet-batch conversion decomposes the spectra of signals unevenly, limited to the low-frequency component of the signal. Wavelet transform (WT) is implemented using low-pass (LPF) and high-pass (HPF) filters, after which decimation is performed to increase the conversion efficiency. The WT signal 'z' is realized by passing it through a series of filters with a pulse response 'g' [45]:

$$y[n] = (z \otimes g)[n] = \sum_{k=-\infty}^{\infty} z[k]g[n-k] \quad . \tag{12}$$

The high-pass filter decomposes this signal and provides detailed coefficients. The output sampling rate of the output of the filter is reduced by 2 times. LPF and HPF results are as follows:

$$y_{LPF}[n] = (z \otimes g)[n] = \sum_{k=-\infty}^{\infty} z[k]g[2n-k] \tag{13}$$

$$y_{HPF}[n] = (z \otimes h)[n] = \sum_{k=-\infty}^{\infty} z[k]h[2n-k] \tag{14}$$

In the transmitter, encrypted and embedded data streams increase the sampling rate and are transmitted through the IWPT filter group. At the receiver, the data is transmitted through a filter, and then the encrypted data is extracted.

A communication system using FFT-OFDM has a lower throughput due to the use of the cyclic prefix. Moreover, the orthogonality of the carriers in FFT-OFDM systems is subject to channel attenuation. Resistance to such interference is higher in WPT-OFDM systems. In addition, the proposed WPT-OFDM model is more reliable for narrowband interference and multipath propagation.

10 Analysis of the effectiveness of the proposed covert communication systems

For comparison, BER estimates are presented with different SNR values for the carrier and messages in the developed OFDM system. Quality is estimated using the peak signal-to-noise ratio (PSNR), root mean square error (MSE) and average difference (AD) - the differences between the original image and the modified average difference between the transmitted and received data on the Rayleigh channel with fading:

$$MSE = \frac{\sum_{M,N}(T(r,c)-T'(r,c))^2}{M*N}, \quad (15)$$

$$PSNR = 10*\log_{10}[\frac{R^2}{MSE}], \quad (16)$$

$$AD = \frac{\sum_{M,N}(T(r,c)-T'(r,c))}{M*N}, \quad (17)$$

where: $T(r, c)$ is the original image; $T'(r, c)$ – modified image; r and c are the number of rows and columns in the input images, respectively; R – the maximum value of the image intensity.

An image of 512×512 in size was used as the transmitted container with critical information. The parameters of the communication system model are presented in Table 4.

Table 4 – Communication system model parameters

Parameter	Value
FFT size	256
CP size	1/4
Carrier quantity	12
Convolutional codes rate	1/2
Modulation	M-PSK
Modulation levels	2,4.8
Simulation channel	Rayleigh
Container	Image (512×512)
Cryptography method	XOR
Wavelet type	Haara

An increase in the signal-to-noise ratio results in a reduction in the amount of distortion when a message is extracted from the transmitted image. When used as a data channel WPT-OFDM, provides better communication quality and fewer errors. Fig. 5 shows a comparison of the BER parameter for hidden communication in FFT-OFDM and WPT-OFDM over the Rayleigh channel with fading for modulation of the form: BPSK, QPSK and 8-PSK. The assessment was carried out both for the transmitted container and for the critical message with different SNR values. Obviously, higher SNR values result in fewer errors in receiving the container, and therefore greater accuracy in retrieving the message. The results obtained demonstrate that hidden communication in WPT-OFDM provides better performance than hidden communication in a traditional OFDM system with different modulations, since the OFDM system is influenced by Doppler frequency changes. Fig. 5 (a) shows that to achieve a BER of 10^{-4} for data with modulated BPSK carrier, OFDM requires a SNR value of 9 dB, while for the proposed WPT-OFDM system, only 6 dB. To transmit a secret message with a code rate of CC 1/2, for normal OFDM, a SNR of 6 dB is required, against 3 dB in WPT-OFDM. When using QPSK modulation, the container requires 12 dB for FFT-OFDM and 7 dB for WPT-OFDM. For the transmission of the most critical message with a CC 1/2 rate, the ratio is 10 to 7 dB.

It should be noted that using M-PSK modulation under the same conditions, the BER value of the system begins to deteriorate, but it is possible to compensate for this degradation with a high SNR value. Thus, covert communication using WPT-OFDM provides an improvement in the signal-to-noise ratio of 3-6 dB compared to FFT-OFDM when transmitting data over the Rayleigh channel. A comparison of the performance of hidden communication systems is given in Table 5. Fig. 6 and fig. 7 show a comparison of the PSNR values and the average difference between empty and full containers.

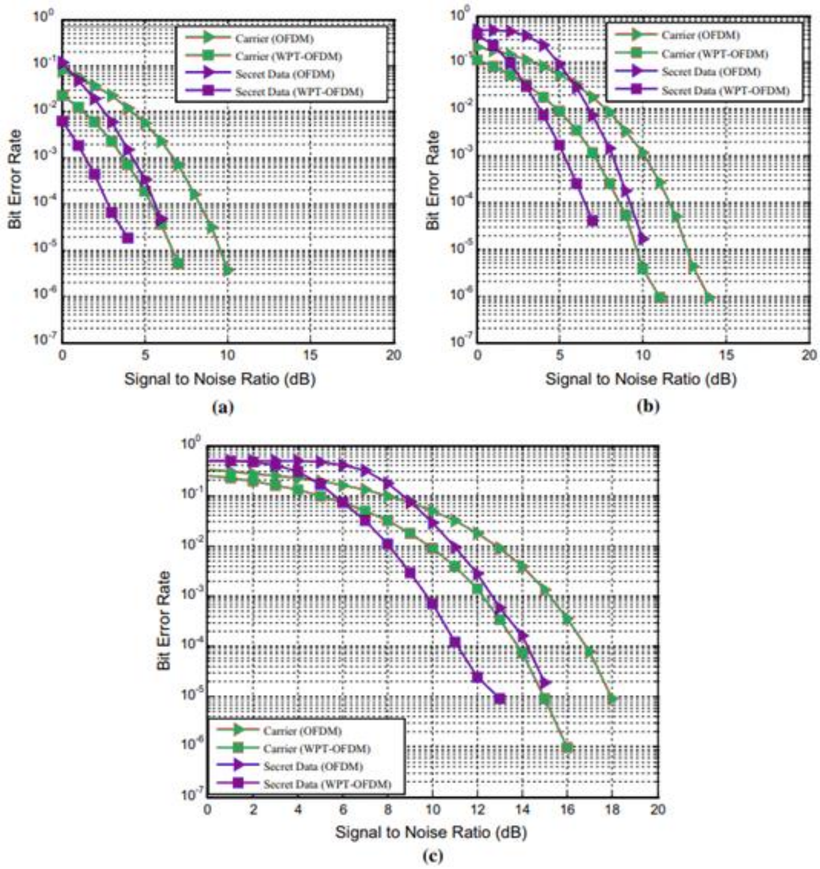

Fig. – 5 BER comparison for: BPSK *(a);* QPSK *(b);* 8-PSK *(c)*

Table 5 – Hidden communication systems performance

SNR	Modulation	Container BER	Message BER	PSNR	MSE	AD
1 dB	FFT	0.0775	0.1151	16.035	1.62×10^{3}	1.3103
	WPT	0.0228	0.0058	21.217	491.324	0.4497
2 dB	FFT	0.0551	0.0507	17.466	1.166×10^{3}	0.9215
	WPT	0.0124	0.0015	23.832	269.066	0.2489
4 dB	FFT	0.0221	0.0065	21.372	474.14	0.2763
	WPT	0.0023	4.691×10^{-5}	30.961	52.116	0.0490
6 dB	FFT	0.0057	4.7613×10^{-4}	27.189	124.24	0.0619
	WPT	1.864×10^{-4}	0	41.671	4.426	0.0027
8 dB	FFT	7.2861×10^{-4}	0	36.411	14.857	0.0073
	WPT	5.2452×10^{-6}	0	54.829	0.214	3.166×10^{-4}
10 dB	FFT	2.766×10^{-5}	0	51.291	0.4830	1.526×10^{-4}
	WPT	0	0	Inf	0	0

We used a message with a length of 243696 bits, which is transmitted in an image of 512×512 in size. Increasing the SNR value improves the values of the BER parameters for the received information sequence and the extracted message. When sending a message in a container, BERs are significantly better than direct transmissions in the same medium. Summarizing, we can say that hidden communication using WPT-OFDM provides better quality than conventional OFDM for all the cases considered.

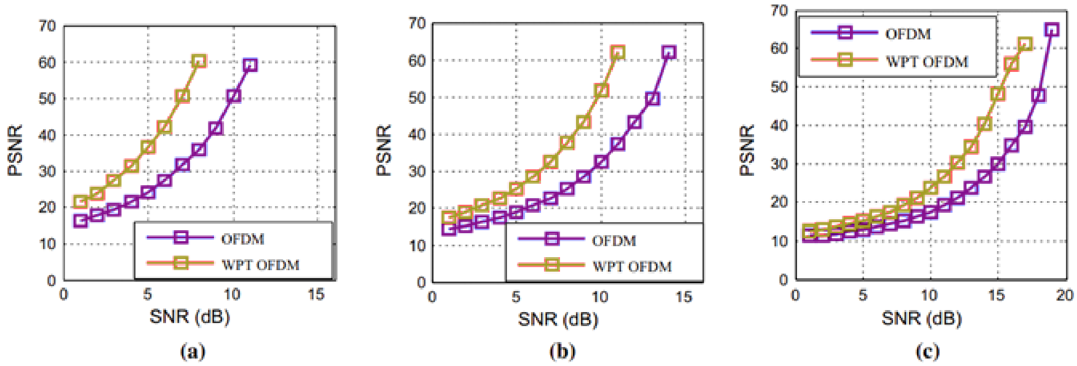

Fig. 6 – Comparison of PSNR for: BPSK *(a);* QPSK *(b);* 8-PSK *(c)*

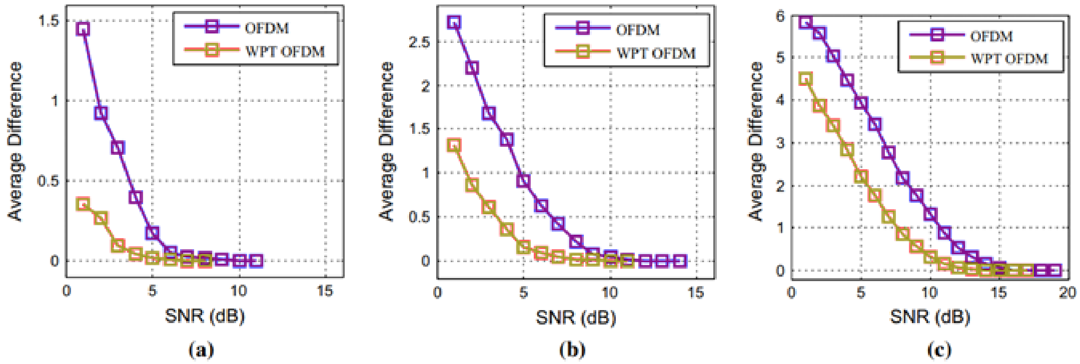

Fig. 7 – Comparison of AD for: BPSK *(a);* QPSK *(b);* 8-PSK *(c)*

11 Conclusions

This paper presents the technologies for generating signals that are already used in communication and telecommunication systems, and also provides an analysis of promising technologies that may be used in various new systems, including wireless broadband access communication systems. It is shown that the widely used OFDM modulation scheme has a number of shortcomings that can lead to a decrease in the performance indicators of the systems in which they are used, in particular: a reduction in the noise immunity of signal reception, due to distortions caused by multipathing when the electromagnetic field propagates between the base and mobile stations, as well as the effects of intersymbol and inter-channel interference; irrational, as compared with sequential waveforms, the use of transmitter power, which is associated with the use of a guard interval for protection against intersymbol interference and a high peak factor of a signal, etc. Alternative signal generation technologies are presented, in particular, signal generation technology based on window processing signals (W-OFDM) and providing a low level of out-of-band emission.

One of the main trends in the development of modern wireless broadband access communication systems is the rapid spread of technologies such as OFDM and MIMO. These technologies allow to achieve an increase in information efficiency in the conditions of multipath propagation and, as a result, to provide the ever-growing needs of wireless communication network users in high-speed connections and specific multimedia services. For some applications, ICS is a determining factor in their design and operation is the state of security of data processing and storage systems, which ensures the confidentiality, integrity and availability of information, as well as other properties of information and services: authenticity, observability, irrefutable and reliability. At the same time, the development of secure wireless communication systems that could reliably support multimedia applications faces a number of technological challenges that require serious research efforts. One of these calls is due to the choice of classes of discrete sequences, the properties of which largely determine the properties of physical data carriers in the ICS. In the work, on the basis of the analysis of the structure of the OFDM signal, the estimates of the security of the ICS from imposing false signals and messages by using non-linear discrete cryptographic signals as a physical data carrier are presented.

In this paper, a hidden communications system was proposed using WPT-OFDM. Hidden communications based on traditional OFDM are simpler in structure compared to WPT-OFDM, but the use of a protection bandwidth reduces bandwidth. The results showed that under equal conditions, the probability of an error in the transmitted data, the accuracy of extraction from the container and such quality parameters as PSNR, MSE and AD of the proposed system with wavelet transform are superior to traditional OFDM systems, and also allow increasing the system bandwidth.

References

[1] 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. – Vol. 75, 2016 Issue 2, pp. 169-178.

[2] I.D. Gorbenko, A.A. Zamula Cryptographic signals: requirements, methods of synthesis, properties, application in telecommunication systems Telecommunications and Radio Engineering. - Vol. 76, 2017 Issue 12, pp. 1079-1100.

[3] ITU-R, Recommendation M.2083-0, “IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond”, ITU recommendation, Sept. 2015.

[4] Pen Guan et al. “5G Field Trials: OFDM-Based Waveforms and Mixed Numerologies” IEEE Journal on Selected Areas in Communications, Vol. 35, No. 6, pp. 1234-1243, March 2017.

[5] T.S. Rappaport et al. “Millimeter Wave Mobile Communications for 5G Cellular: It Will Work!”, IEEE Access, Vol. 1, pp. 335-349, 2013.

[6] J.G. Andrews et al. “What will 5G be?”, IEEE Journal on Selected Areas in Communications, Vol. 32, no. 6, pp. 1065-1082, June 2014.

[7] J. Abdoli, et al. “Filtered OFDM: A new waveform for future wireless systems”, Proc. IEEE SPAWC, pp. 66-70, Jun. 2015.

[8] X. Zhang et al. “Filtered-OFDM – Enabler for Flexible Waveformin The 5th Generation Cellular Networks”, Proc. IEEE GLOBECOM, pp. 1-6, Dec. 2015.

[9] Li. Jialing et al. “A resource block based filtered OFDM scheme and performance comparison”, Proc. IEEE ICT, pp. 1-5, May 2013.

[10] T. L. Marzetta “Noncooperative Cellular Wireless with Unlimited Numbers of Base Station Antennas”, IEEE Transactions on Wireless Communications, Vol. 9, No. 11, pp. 3590-3600, Nov. 2010.

[11] China Mobile Research Institute, “C-RAN: The Road Towards Green RAN”, white paper, 2011. [On-line]. Available: http://labs.chinamobile.com/cran/

[12] H. Nikopour et al. “Sparse code multiple access”, Proc. IEEE PIMRC, pp. 332-336, Sept. 2013.

[13] 5G Forum. (2016, Mar.). 5G white paper: 5G vision, requirements, and enabling technologies [On-line]. Available: http://kani.or.kr/5g/whitepaper/5G%20Vision,%20Requirements,%20and%20Enabling%20Technologies.pdf.

[14] B. Farhang Boroujeny “Filter bank multicarrier modulation: a waveform candidate for 5G and beyond,”Advances in Electrical Engineering, vol. 2014, Dec. 2014. doi:10.1155/2014/482805.

[15] Zekeriyya Esat Ankaralı et al. “Enhanced OFDM for 5G RAN”, June 2017, doi: 10.3969/j. issn. 1673-5188. 2017. S1. 002.

[16] A. Şahin, I. Güvenç and H. Arslan “A survey on multicarrier communications: prototype filters, lattice structures, and implementation aspects, ”IEEE Communications Surveys & Tutorials, Vol. 16, No. 3, pp. 1312-1338, Aug. 2014. doi:10.1109/SURV.2013.121213.00263.

[17] Huawei and HiSilicon, “f-OFDM scheme and filter design,”3GPP Standard Contribution (R1-165425), Nanjing, China, May 2016.

[18] V.P. Fedosov, D.G. Kovtun, A.A. Legin, A.V. Lomakina Issledovanie modeli OFDM signala s malym urovnem vnepolosnogo izlucheniya / Izvestiya YuFU. Tekhnicheskie nauki. 2016, pp. 6-16.

[19] Harish Kumar Pal, Anand Kumar Singh PAPR Reduction technique using advanced peak windowing method of OFDM System. International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Vol.-3, Issue 2, May 2013.

[20] Bakulin, M. G., Kreindelin, V. B., Shloma, A. M., Shumov, A. P. Tekhnologiya OFDM. Uchebnoe posobie dlya vuzov. – M.: Goryachaya liniya – Telekom, 2015. - 360 p.

[21] Zamula O.A. Tekhnologii formirovaniya OFDM signalov v sovremennykh informatsionno-kommunikatsionnykh sistemakh Radiotekhnika: Vseukrainskii mezhvedomstvennyi nauchno – tekhnicheskii sbornik – 2018. – Vip. 193. pp. 152-159.

[22] Gorbenko, I.D., Gorbenko, Ju.I. Prykladna kryptologija. Teorija. Praktyka. Zastosuvannja: monografija / I.D. Gorbenko, Ju.I. Gorbenko. – Harkiv: Fort, 2012. – 880 p.

[23] Gorbenko, Ju.I. Metody pobuduvannja ta analizu, standartyzacija ta zastosuvannja kryptografichnyh system / Ju.I. Gorbenko. – Harkiv: Fort, 2016. – 959 p.

[24] 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 Vol. 76, 2017 Issue 19, pp 1705-1717.

[25] Zamula A.A., Morozov V.L. Informatsionnye tekhnologii peredachi dannykh v sovremennykh telekommunikatsionnykh sistemakh // Radiotekhnika: Vseukrainskii mezhvedomstvennyi nauchno – tekhnicheskii sbornik – 2016. – Vyp. 186. pp. 24-32.
[26] Simmons G. J. «Authentication theory coding theory» 1985.
[27] I. D. Gorbenko, A.A. Zamula, A. E. Semenko, V.L. Morozov Method for synthesis of performed signals systems based on cryptographic discrete sequences of symbols // Telecommunications and Radio Engineering Vol. 76, 2017 Issue 17, pp. 1523-1533.
[28] 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 Vol. 76, 2017 Issue 18, pp. 1581-1594.
[29] Gorbenko, I.D., Zamula, O.A. Modeli ta metody syntezu kryptografichnyh sygnaliv ta i'h optymizacija za kryterijem chasovoi' skladnosti // Matematychne ta komp'juterne modeljuvannja. Serija: Fizyko-matematychni nauky: zb. Nauk. prac' / Instytut kibernetyky imeni V.M. Glushkova Nacional'noi' akademii' nauk Ukrai'ny, 2017. Vyp. 15. 272 p.
[30] Sarvate D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun, 1980. – Vol. Com 68 – pp. 59–90.
[31] Sverdlik, M. B. Optimal'nye diskretnye signaly. / Sverdlik M. B. M: Radio i Svyaz', 1975. – 200 p.
[32] Tew, Y. & Wong, K. (2014). An overview of data hiding in H.264/AVC compressed video. IEEE Transactions on Circuits and Systems for Video Technology, 24(2), 305–319.
[33] Sharma, V. & Singh, G. (2014). On BER assessment of conventional- and wavelet-OFDM over AWGN channel. Jounal of Optik, 125, 6071–6073.
[34] Gupta, M. K. & Tiwari, S. (2013). Performance evaluation of conventional and wavelet based OFDM system. International Journal of Electronics and Communications, 67(4), 348–354.
[35] Dutta, A. et al. (2013). Secret agent radio: Covert communication through dirty constellations. In M. Kirchner & D. Ghosal (Eds.), Information Hiding. IH 2012. Lecture notes in computer science (Vol. 7692, pp. 160-175). Berlin, Heidelberg: Springer.
[36] Bash, B. A., Goeckel, D., Towsley, D. & Guha, S. (2015). Hiding information in noise: Fundamental limits of covert wireless communication. IEEE Communications Magazine, 53(12), 26–31.
[37] Bloch, M. (2016). Covert communication over noisy memoryless channels: A resolvability perspective. IEEE Transactions on Information Theory, 62(5), 2334–2354.
[38] Bouhlel A., Sakly A. & Mansouri N. (2015). Performance comparison of DWT based MIMO OFDM and FFT based MIMO OFDM. Procedia Computer Science, 73, 266–273.
[39] Khan, A. R. & Gulhane, S. M. (2017). A highly sustainable multi-band orthogonal wavelet code division multiplexing UWB communication system for underground mine channel. Digital Communications and Networks, 3, 1–13.
[40] Kaur, H., Kumar, M., Sharma, A. K. & Singh, H. P. (2016). Performance analysis of DWT based OFDM over fading environments for mobile WiMax. Jounal of Optik, 127, 544–547.
[41] Mushtaq, A. S., Ihsan, A. A. & Qasim, N. (2015). 2D-DWT vs. FFT OFDM systems in fading AWGN channels. Radioelectronics and Communication Systems, 58(5), 228–233.
[42] Mahapatra, C., Leung, V. C. M. & Stouraitis, T. (2017). An orthogonal wavelet division multiple-access processor architecture for LTE-advanced wireless/radio-over-fiber systems over heterogeneous networks. EURASIP Journal on Advances in Signal Processing, 1, 1–16.
[43] Villalobos, S., Aldana, F., Ladino, I., Diaz, I. (2017). A waveletbased OFDM system implementation on GNURadio platform vs. an FFT-based. In Springer workshop on engineering applications (WEA-2017), Vol. 742, 201–211.
[44] Kumar, S. & Sharma, S. (2013). Performance evaluation physical layer of IEEE 802.11 standards under Fourier transform and wavelet transform over Rician fading channel. In IEEE, 2nd international conference on information management in the knowledge economy, pp. 69–74.
[45] Kumar, S., Singh, A. & Kumar, M. Wireless Netw (2018). https://doi.org/10.1007/s11276-018-1775-3
[46] Kansal, L., Sharma, V. & Singh, J. (2017). BER assessment of FFT-OFDM against WHT-OFDM over different fading channel. Wireless Networks, 23(7), 2189–2196.

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

Надійшло: Травень 2018.

Автори:
Олександр Замула, д.т.н., доцент, Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна.
E-mail: zamulaaa@gmail.com

Владислав Морозов, аспірант, Харківський національний університет імені В.Н. Каразіна, м. Харків, Україна.
E-mail: ilissar@hotmail.com

Сербін Вадим, провідний фахівець, ДП «Конструкторське бюро «Південне», м. Дніпро, Україна.
E-mail: buba75@i.ua

Принципи формування, обробки та властивості OFDM сингалів.

Анотація. У статті розглянуті технології формування сигналів, використовуваних в системах мобільного зв'язку та інформаційно-телекомунікаційних системах, а також наводиться аналіз перспективних технологій, які можуть знайти застосування в бездротових системах зв'язку широкосмугового доступу. Показано, що широко використовувана схема модуляції з ортогональним частотним розділенням (OFDM) має низку недоліків, які можуть призвести до зниження показників ефективності систем. Представлені альтернативні технології формування сигналів, зокрема, технологія, заснована на віконної обробці сигналів (W-OFDM), технологія, заснована на тимчасовому поділі (w-OFDM); технологія UFMC і інші, що дозволяють усунути недоліки технології OFDM. Пропонуються нові погляди на використання в технології передачі з багатьма несучими в формі мультиплексування з ортогональним частотним розділенням (з метою підвищення захищеності сучасних бездротових систем зв'язку широкосмугового доступу від впливу зовнішніх і внутрішніх загроз), класу нелінійних дискретних криптографічних послідовностей для освіти фізичного переносника даних - сигналів. Показано, що застосування таких сигналів дозволить поліпшити показники захищеності зазначених систем від введення (нав'язування) в систему помилкових повідомлень, фальсифікації повідомлень, а також показники забезпечення цілісності та конфіденційності даних, завадостійкості прийому і скритності функціонування системи.

Ключові слова: перешкодозахищеність; інформаційна безпека; широкосмуговий доступ; сигнал, цілісність; стійкість; частотний поділ; стільниковий зв'язок; інтерференція; пік-фактор.

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

Поступила: Май 2018.

Авторы:
Александр Замула, д.т.н., доцент, Харьковский национальный университет имени В.Н. Каразина, г. Харьков, Украина.
E-mail: zamulaaa@gmail.com
Владислав Морозов, аспирант, Харьковский национальный университет имени В.Н. Каразина, г. Харьков, Украина.
E-mail: ilissar@hotmail.com
Вадим Сербин, ведущий специалист, ГП «КБ «Южное», г.Днипро, Украина.
E-mail: buba75@i.ua

Принципы формирования, обработки и свойства OFDM сигналов.

Аннотация. В статье рассмотрены технологии формирования сигналов, используемых в системах мобильной связи и информационно-телекоммуникационных системах, а также приводится анализ перспективных технологий, которые могут найти применение в беспроводных системах связи широкополосного доступа. Показано, что широко используемая схема модуляции с ортогональным частотным разделением (OFDM) обладает рядом недостатков, которые могут привести к снижению показателей эффективности систем. Представлены альтернативные технологии формирования сигналов, в частности, технология, основанная на оконной обработке сигналов (W-OFDM), технология, основанная на временном разделении (w-OFDM); технология UFMC и другие, позволяющие устранить недостатки технологии OFDM. Предлагаются новые взгляды на использование в технологии передачи со многими несущими в форме мультиплексирования с ортогональным частотным разделением (в целях повышения защищенности современных беспроводных систем связи широкополосного доступа от воздействия внешних и внутренних угроз), класса нелинейных дискретных криптографических последовательностей для образования физического переносчика данных – сигналов. Показано, что применение таких сигналов позволит улучшить показатели защищенности указанных систем от ввода (навязывания) в систему ложных сообщений, фальсификации сообщений, а также показатели обеспечения целостности и конфиденциальности данных, помехоустойчивости приема и скрытности функционирования системы.

Ключевые слова: помехозащищенность; информационная безопасность; широкополосный доступ; сигнал; целостность; помехоустойчивость; частотное разделение; сотовая связь; интерференция; пик-фактор.