***The development of data transmission systems based on wireless radio communication channels allowed the construction of fundamentally new networks – mesh networks, which are used not only in smart technologies, but are the basis for the construction of cyber-physical and socio-cyber-physical systems (objects of critical infrastructure). The object is the process of ensuring reliable and secure data transmission based on the use of wireless radio communication channels. A mathematical model of information resources protection system functioning is proposed to ensure the signs of immunity and security of the automated data transmission system. To identify threats, a unified classifier and flow state estimation technique are used, which take into account the hybridity and synergy of targeted (mixed) attacks on communication channels. The critical points of the infrastructure elements, as well as the information that circulates and/or is stored, are determined. The assessment of compliance with the regulators' requirements, both international and state regulatory acts, and the presence and ability of the security system elements to ensure the required level of infrastructure elements protection is taken into account. The proposed approach allows to determine: coefficients of information and internal availability of a wireless radio communication channel, the vector potential of the lagging magnetic field as a result of data transmission work. When evaluating the coefficient of a wireless radio communication channel internal availability, it is proposed to take into account coherent reception of the signal. At the same time, the immunity factor of the wireless radio communication channel is much higher than 1, which provides sufficient protection of information. A technical solution is proposed that will allow the level of confidentiality, integrity, authenticity and reliability of a wireless radio communication channel to approach 100 %***

***Keywords: data transmission system, radio signal emitter, magnetic field, radio monitoring, socio-cyberphysical system***

UDC 623.618.51
DOI: 10.15587/1729-4061.2024.310547

# DEVELOPMENT OF FUNCTIONALITY PRINCIPLES FOR THE AUTOMATED DATA TRANSMISSION SYSTEM THROUGH WIRELESS COMMUNICATION CHANNELS TO ENSURE INFORMATION PROTECTION

**Serhii Yevseiev**
*Corresponding author*
Doctor of Technical Sciences, Professor*
E-mail: Serhii.Yevseiev@gmail.com
**Stanislav Milevskyi**
PhD, Associate Professor*
**Vladyslav Sokol**
PhD*
**Vladyslav Yemanov**
Doctor of Sciences in Public Administration, Senior Researcher
National Academy of the National Guard of Ukraine
Zakhysnykiv Ukrainy sq., 3, Kharkiv, Ukraine, 61001
**Anatolii Volobuiev**
Doctor of Technical Sciences, Senior Researcher
Chef of Research Department
The Central Research Institute of the Armed Forces of Ukraine
Povitrianykh Syl ave., 28, Kyiv, Ukraine, 03049
**Larysa Dakova**
PhD, Associate Professor
Department of Mobile and Video Information Technologies***
**Mykola Brailovskyi**
PhD, Associate Professor
Department of Cyber Security and Information Protection
Taras Shevchenko National University of Kyiv
Volodymyrska str., 60, Kyiv, Ukraine, 01033
**Irada Rahimova**
PhD in Technology, Assistant Professor
Department of Computer Technologies
Azerbaijan Technical University
H. Javid ave., 25, Baku, Azerbaijan, AZ 1073
**Vladyslav Kravchenko**
PhD, Associate Professor
Deputy Director
Educational-Scientific Institute of Telecommunications***
**Oleg Cherniavskiy**
PhD Student
Department of Tactical and Special Disciplines**
*Department of Cybersecurity**
**National Technical University "Kharkiv Polytechnic Institute"
Kyrpychova str., 2, Kharkiv, Ukraine, 61002
***State University of Information and Communication Technologies
Solomyanska str., 7, Kyiv, Ukraine, 03110

*Received date 10.06.2024*
*Accepted date 19.08.2024*
*Published date 30.08.2024*
***How to Cite:*** *Yevseiev, S., Milevskyi, S., Sokol, V., Yemanov, V., Volobuiev, A., Dakova, L., Brailovskyi, M., Rahimova, I., Kravchenko, V., Cherniavskiy, O. (2024). Development of functionality principles for the automated data transmission system through wireless communication channels to ensure information protection. Eastern-European Journal of Enterprise Technologies, 4 (9 (130)), 18–33. https://doi.org/10.15587/1729-4061.2024.310547*

## 1. Introduction

Known methods of mathematical modeling of the functioning process of an automated data transmission system through wireless communication channels for assessing the level of information protection use the basic concepts of "reliability of systems with wireless communication channels" and "efficiency of radio monitoring" [1, 2]. The reliability

of wireless radio communication channels is a complex of technical and organizational measures aimed at improving the quality of data transmission and timely detection of information leakage channels for their closure [3]. By the effectiveness of radio monitoring, it is possible to understand the assessment of the degree of achievement of the goal of functioning of the automated data transmission system under the given conditions with the required reliability. Therefore, the purpose of the operation of radio monitoring means is to solve the main problem - uncovering the real state, composition, position, capabilities of radio communication channels by intercepting and analyzing electromagnetic radiation [3, 4]. The collection of information on the operation of wireless radio communication channels is carried out by accumulating and systematizing data on the interception of information transmitted by wireless communication channels. Modeling of such processes is used during the construction of mathematical models that allow evaluating the protection of radio communication channels of the data transmission system [5]. In addition, the impact of targeted (mixed) attacks on data transmission systems allows not only to predict adequate preventive security measures, but also to determine the critical points of the automated data transmission system itself.

Thus, an urgent scientific task is the development of the functioning principles for an automated data transmission system through wireless communication channels to ensure information protection in the conditions of targeted (mixed) attacks with signs of synergy and hybridity.

## 2. Analysis of literature data and problem statement

The analysis of the work [6] showed that secure broadband radio communication is becoming more and more important for high-speed connectivity in radio access networks, playing a crucial role in both mobile information systems and wireless information and computing technology (IOT) connections. The authors propose a two-channel chaos-based digital radio communication system that uses fiber-optic radio transmission technology. The system consists of two radio channels operating at speeds up to 1 Gbit/s using amplitude-shift keying (ASK) modulation followed by random-sequence modulation before conversion to the optical domain using an optical frequency thinning modulator (Mach-Zehnder Modulator MZM). To compensate for fiber losses, the system uses an erbium-doped fiber amplifier (EDFA) and uses optical channels over ITU-G.655 standard optical fibers. The presented results demonstrate the effective operation of the system on two channels with a fiber transmission range of up to 110 km, keeping the bit error rate below 10−9. This feature ensures reliable operation of high-speed radio links, especially in applications such as front-end networks in cloud radio access and connectivity to wireless sensor networks. But this does not take into account possible targeted attacks on the infrastructure elements of the automated data transmission system (ASPD). In [7], the authors propose the use of cognitive radio (CR) and the concept of wireless sensor networks (WSN), which is used as an intelligent wireless communication technology that has unique capabilities for monitoring spectrum bands. This allows detection of available channels for use of statically allocated spectrum. In addition, by dynamically adjusting its operating parameters, the channel can use the available channels and attack the future problem of spectrum reduction. But such a concept does not ensure the construction of multi-circuit protection systems taking into account the infrastructure of socio-cyber-physical systems. In the work [8], the authors analyze the current state of radio and podcasting, using specific case studies to analyze the interaction of sound media with art. This makes it possible to identify the main means of community formation, together with national, transnational and alternative identities, as a subject of academic and critical research. But at the same time, the authors do not take into account the possibility of combining targeted (APT) attacks with social engineering methods. In [9], the prerequisites for the revolution of modern autonomous driving are considered, based on the rapid development of 5G networks, which offer high-speed wireless broadband networks. To meet data traffic requirements, the forward link Intensity Modulation-Direct Detection (IM-DD) bandwidth connecting the Remote Radio Unit (RRU) and the Baseband Unit (BBU) has been scaled from 25 Gbps (NRZ) up to 50 Gbit/s (PAM4) for the advanced 5G network and 100 Gbit/s (PAM4) for the 6G network. In addition, radio access networks are undergoing a transition from distributed radio access networks (D-RAN) to centralized radio access networks (C-RAN). To ensure immunity, a multi-channel dispersion compensation scheme is proposed for IM-DD multi-channel long-distance transmission. On-chip losses are about 4 dB for both channels, which provides 20 ps/nm and −28 ps/nm dispersion compensation in each band. But at the same time, the authors do not consider cyber threats to the elements of the scheme, and the possibility of implementing exploits in the software and hardware part. In [10], the authors analyze possible losses of reliable radio communication in fire extinguishing systems due to the use of reinforced concrete in modern buildings, which reflect, refract and diffract radio waves. As such, they are the biggest obstacles to transmission and reception. To compensate for this aspect, it is proposed to install leaky coaxial cables and antennas to ensure stable radio communication between fire departments. But this approach takes into account active APT attacks on the elements of the data transmission system, their hybridity and synergism. In [11], the authors propose a wireless multiple access system with frequency division channels with one carrier frequency of the Single Carrier Frequency Division Multiple Access (SC-FDMA) type as an accepted communication standard. It presents a robust image transmission framework via SC-FDMA that includes digital image watermarking and encryption to enhance image security while maintaining high image reconstruction quality at the receiver side. The proposed framework allows image watermarking based on Discrete Cosine Transform (DCT) combined with Singular Value Decomposition (SVD) in the so-called DCT-SVD watermarking. However, cyber-threats to elements of the image transmission structure itself via SC-FDMA are not taken into account. In the work [12], the authors investigate that the decentralized network becomes not just a tool for emergency communication, but a symbol of resistance against censorship. Drawing parallels with events in the real world, the authors offer a comprehensive analysis of the technical, social and ethical aspects of radio amateurs. This highlights the importance of decentralized communication systems to support freedom of information, especially in scenarios where central systems are compromised. However, possible scenarios of compromising the decentralized system due to the combination of cyber attacks with social engineering

methods are not taken into account. In [13], the authors propose the use of chaotic encryption to ensure the security of data transmission through communication channels. Through comprehensive analysis, it evaluates the performance of chaotic encryption algorithms in terms of encryption strength, computational efficiency, and resistance to attacks. In addition, the research explores the integration of chaotic encryption with conventional cryptographic protocols to create hybrid encryption schemes capable of providing multi-layer protection. But the authors do not take into account the need to ensure efficiency and reliability in data transmission, as well as the possibility of building multi-contour security systems in the post-quantum period. In [14], a prototype of the transmitter and receiver was created, and the data was encoded using the technique of digital-to-analog modulation with two sidebands and carrier suppression (BPSK) and sent at different transmission rates: 4800, 9600, 19200, 76800 and 11500 bits in second (bit/s). The error rate was measured to evaluate the performance of the device, defined as the ratio between the number of bits transmitted and the number of bits received. As a result, a minimum error rate of 58 % at a speed of 4800 bps and a maximum of 61.25 % at 115200 bps was obtained; the system also allowed sending images up to 256 pixels in size. But the authors did not take into account the possible hacking of the data transmission system due to the use of ART attacks. In [15], a cognitive radio system based on energy spectrum detection (ED-SS) is implemented, which can analyze spectrum energy. Different fading channels such as additive white Gaussian noise (AWGN), Rayleigh and Nakagami noise are analyzed and compared using the ED-SS technique. Experimental results show that detecting the presence of the user's primary signal using the proposed ED-SS technique is easier with low computational complexity in cognitive radio (CR) networks. However, the issues of classification of cyber threats and their impact on immunity are not considered. In [16], the authors propose a geometry-based non-stationary stochastic channel model for communication channels of electric vertical take-off and landing (eVTOL) aircraft. The proposed eVTOL channel model framework takes into account the time-domain non-stationarity and arbitrary eVTOL trajectory and is general enough to support a variety of ranges. One of the critical challenges for eVTOL is the fast vertical take-off and landing patterns that affect the conventional propagation communication channel. In addition, a new method is presented to estimate the SNR on a non-stationary fast time-varying eVTOL dynamic channel using an adaptive sliding window filtering technique. Furthermore, let's present an information-theoretic approach to characterize the end-to-end transmission delay over an eVTOL channel and prove that the optimal transmission scheme strongly depends on the configuration of the eVTOL link. However, the authors do not take into account the possibility of ensuring security in the model. In [17], it was determined that among the available frequency ranges, the terahertz (0.1–10 THz) range was determined to be the most promising for overcoming the spectrum deficit and bandwidth limitations of current wireless systems. In addition, the unique properties of THz wave propagation provide new sensing and localization capabilities. Since wireless channels are the basis for wireless communication system development in new spectrum and new environments, it is necessary to study THz radio propagation channels for future 6G wireless communication. However, the authors do not take into account the absence of special security mechanisms other than authentication. But the Radius and Diameter authentication protocols are broken, which makes it impossible to provide the required level of service, and the provision of confidentiality and integrity services is practically non-existent. In [18], the authors proposed an algorithm for determining rational radio exchange routes with low intellectual availability in an automated military radio communication system, which is the basis for solving the problem of multipath routing and takes into account, in addition to known limitations, limitations on the permissible intelligence availability of information flow routes. A mathematical model of the functioning of the automated military radio communication system has been developed, which for the first time takes into account the process of protecting it from radio intelligence by means of radio exchange along rational routes with low intelligence availability. This approach is based on the tensor dependences of the intelligence readiness coefficients of individual direct radio communication lines on the quality indicators of information exchange with their further transformation into tensor dependences of the coefficients. However, the authors also do not take into account the need to implement multi-circuit protection systems for data transmission systems based on the use of post-quantum algorithms with minimal capacity. Work [19] presents a refined mathematical model for evaluating the quality of mobile radio channels in cyber-physical systems using topological transformation of stochastic networks. The operation of the radio channel is conceptualized as a stochastic network, which allows obtaining critical indicators, such as the equivalent function, mathematical expectation, variance, and the time distribution function of the implemented processes. The model uses the gamma distribution for initial distribution functions of random variables, increasing its analytical accuracy. A significant advance of this research is the development of a comprehensive model that describes the data transfer process through the phases of connection establishment, information transfer, and connection maintenance. But the model does not take into account the possibility of APT threats with signs of hybridity and synergism. In [20], the authors proposed consideration of spatial simultaneity (SSF) over time division multiple access (TDMA) in joint communication and sensing (JCAS) scenarios for improved resource utilization and interference reduction. SSF enables simultaneous operation of communication systems and sensors, increasing flexibility and efficiency, especially in dynamic environments. The authors proposed joint communication and sensing design scenarios for JCAS single-input single-output (SISO) and multiple-input multiple-output (MIMO) receivers. A MIMO-JCAS base station (BS) is proposed to process downlink communication signals and echo signals from targets simultaneously using interference cancellation techniques. In addition, a deep neural network (DNN)-based approach for channel estimation and signal detection in JCAS systems is presented. DNN outperforms traditional methods in bit error rate (BER) and signal-to-noise ratio (SNR) curves by leveraging its ability to autonomously learn complex patterns. The DNN learning process tunes performance based on specific problem characteristics, capturing the nuances of relationships in the data and adapting to different signal-to-noise ratio (SNR) conditions for consistently better performance compared to traditional approaches. However, the authors do not take into account cyber threats, which do not allow to ensure the necessary level of security.

Thus, it is justified to carry out a study on the development of a mathematical model of an automated data transmission system functioning through wireless communication channels to ensure information protection, taking into account targeted (mixed) cyber attacks with signs of

synergism and hybridity. In addition, in order to increase the level of protection and assess its current state, it is necessary to determine the general classification of threats, the possibility of hacking security services, and to assess the presence of the necessary special mechanisms for the protection of the data transmission system infrastructure elements.

## 3. The aim and objectives of the study

The aim of the study is to develop functioning principles for the automated data transmission system through wireless communication channels to ensure information protection. The developed principles make it possible to ensure the required level of security of information transmission via wireless communication channels.

To achieve the goal of the work, it is necessary to solve the following tasks:

– to obtain analytical relations for the coefficients of information and internal availability of a wireless radio communication channel;

– to obtain analytical relations for the vector potential of the delayed magnetic field as a result of work on data transmission by a radio communication channel and the conduction current density vector in the emitters of a digital antenna array of a wireless radio communication channel for different modes of operation;

– to assess the impact of obstacles on the reliability of data transmission;

– to develop a methodology for evaluating the current state of an automated data transmission system through wireless communication channels.

## 4. Research materials and methods

The object of the research is the functioning process of the automated data transmission system through wireless communication channels while ensuring the required level of information protection.

The research hypothesis is as follows. The mathematical model of the functioning of the automated data transmission system through wireless communication channels consists of two coefficients and the potential of the magnetic field, which is formed during the operation of the wireless radio communication channel. The coefficient of information availability of a wireless radio communication channel characterizes the energy spectrum of the data transmission signal. The coefficient of the radio communication channel internal availability is characterized by the reliability of data transmission – the absence (presence) of information leakage and data transmission without loss of information. The lagging vector potential of the magnetic field characterizes data transmission over a wireless radio communication channel. The current density in the emitter of the digital antenna array of the wireless radio communication channel was chosen as the indicator for evaluating the vector potential of the magnetic field.

The theory of radio engineering systems and the theory of propagation of electromagnetic waves (theory of the electromagnetic field) were used in the development of the principles of operation of the automated data transmission system through wireless communication channels.

The following software were used during the computer modeling of the obtained results of the development of the methodological foundations of the functioning of the automated data transmission system through wireless communication channels. The research hardware includes a computer (based on an Intel core i7 processor) with installed software.

According to the results of calculations in the environment of Excel spreadsheets, numerical values were obtained, on the basis of which the corresponding dependencies were built.

The initial data for the calculations are the operating parameters of the most common Wi-Fi network of the 802.11 b/g/n wireless standard. Such a network operates at a frequency of 2.4 GHz, has a fairly significant number of subscribers, a client base of devices, and provides a wide coverage area. At the same time, the 2.4 GHz radio band is sensitive to interference and is characterized by a decrease in the speed of information transmission due to congestion. Wi-Fi networks created by routers of other subscribers can interfere with a 2.4 GHz Wi-Fi network. In addition, the LTE cellular frequency band (900 MHz, 1800 MHz and 2600 MHz) can also interfere with the operation of a Wi-Fi network. This is due to the significant power of the radio communication signal of the cellular network (from 1 W to 2 W) compared to the power of the radio communication signal of the Wi-Fi network (0.1 W). The initial data for calculations are given in the Table 1. The scheme of the research is shown in Fig. 1.

Table 1

The initial data for calculations

| Signal type | Transmitter power, W | Number of transmitters | Antenna type | Type of interference, signal/interference ratio, dB | Distance to the subscriber, m |
|---|---|---|---|---|---|
| Interference | 1 | 3 | Panel directed | electromagnetic, – 50 | 500 |
| Useful signal | 0,1 | 1 (із 5) | mirrored | deterministic, –20 | 50 |

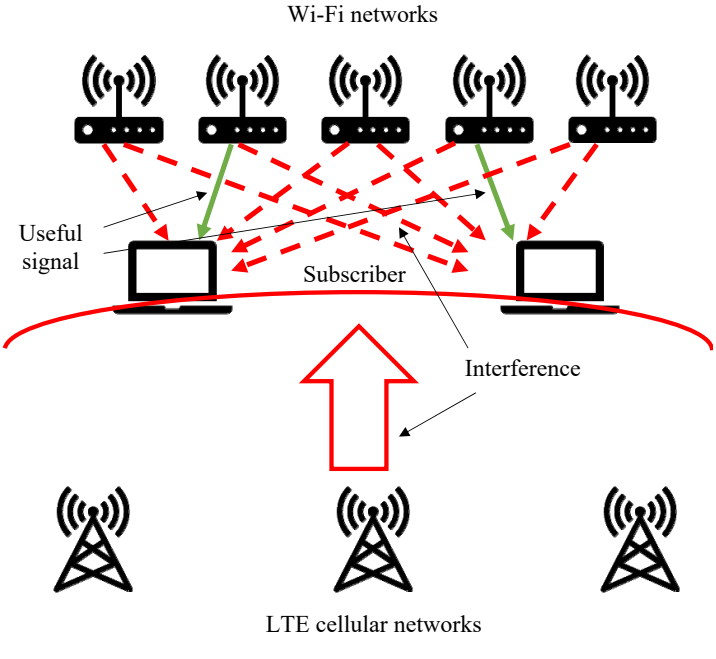


Fig. 1. Calculation scheme

Fig. 1 shows that the calculation solves the problem of providing two subscribers (personal computers) with a reliable connection (Wi-Fi router) to transmit information at the required speed (at least 150 MBit/s). The speed of information transmission decreases with a decrease in the set value of the signal/interference ratio in the receiving channel to the subscriber (Table 1). Five Wi-Fi routers are used (creating five Wi-Fi networks), while each subscriber is configured to receive information from only one Wi-Fi network (router). The quality of receiving information by each of the subscribers is affected by cellular networks (three) and Wi-Fi networks (four), which are not informative for the subscriber. Thus, the interferences are three cellular networks and four Wi-Fi networks with parameters according to Table 1. The wireless communication channel (according to the conditions of the task, the radio communication channel of the Wi-Fi network) provides information protection during data transmission at the set values signal/interference ratio in the receiving channel to the subscriber (Table 1). Based on the results of the study, it is necessary to assess the impact of obstacles on the reliability of data transmission to subscribers.

In this study, a limitation on the accepted condition of technical serviceability of a wireless radio communication channel is introduced. When evaluating the impact of interference on the reliability of data transmission, an assumption was made about the absence of internal interference during data transmission through the information channel of automated data transmission. In addition, an assumption is made about the absence of intentional interference (the work of suppliers of interference is not considered in this study).

When assessing cyber threats, a universal classifier is used, which is implemented on the basis of the framework.

The proposed principles are based on a mathematical model of the functioning of an automated data transmission system over wireless communication channels to ensure information protection and a methodology for assessing the current state of an automated data transmission system over wireless communication channels. The proposed model is based on the definition of theoretical provisions for modeling the processes of detecting the fact of information leakage, which allow evaluating the protection of radio communication channels of the data transmission system. The assessment methodology for assessing the current state of the automated data transmission system through wireless communication channels is based on an expert assessment of known cyberattacks with signs of hybridity and synergism with the possibility of integration with social engineering methods and the subsequent construction of multi-circuit information protection systems.

## 5. The results of the development of the operation principles of the automated data transmission system

### 5. 1. Development of a mathematical model of an automated data transmission system

The mathematical model of the functioning of the automated data transmission system through wireless communication channels was developed based on the evaluation of the useful signal at the receiver. For this purpose, the receiver of the radio monitoring tool was used as the receiver of the useful signal during data transmission via the radio communication channel.

Radio monitoring tools work in conditions of a priori uncertainty, when a number of parameters of useful signals of radio communication channels are unknown a priori. In the worst case for radio monitoring, all parameters of useful signals may be unknown. That is, for radio monitoring devices, the signal of a wireless radio communication channel is stochastic. Consider the additive mixture of the useful signal and the internal fluctuation noise (IFN) of the radio monitoring receiver. From the theory of statistical radio engineering, the optimal selection rule for the presence of a useful signal of a radio communication channel at the output of the receiver in such an additive mixture is determined [21, 22]:

$$\sum_{w=1}^{W}\frac{\lambda_w-1}{\lambda_w}x_w^2\geq 2\ln c+\sum_{w=1}^{W}\ln\lambda_w, \quad (1)$$

where $W$ – the sample size of the implementation of the stochastic additive mixture of the useful signal and the IFN at the output of the receiver of the radio monitoring tool during the observation period $T_{obs}$;

$x_w$ – uncorrelated coordinates of the stochastic additive mixture of the useful signal and the IFN, which are observed at the output of the receiver of the radio monitoring tool during the interval $(0; T_{obs})$;

$\lambda_w$ – unnormalized eigenvalues of a linear integral equation with a symmetric kernel in the form of a correlation function of a stochastic fluctuation received by a radio reconnaissance device:

$$\int_0^{T_{cn}} B_c(t-y)\varphi(y)\,dy=(\lambda-1)\int_0^{T_{cn}} B_{вфш}(t-y)\varphi(y)\,dy$$

at $t\leq T_{cn}$ ( $B_c(t-y)$,

signal correlation function, $B_{IFN}(t-y)$ – IFN correlation function);

$c$ – the constant of the quality criterion for choosing a decision regarding the presence of a useful signal of a radio communication device at the output of the receiver, which is selected from the Table 1 [6].

Table 2

The constant of the quality criterion for making a decision about the presence of a useful signal at the output of the receiver

| Quality criterion | Constant $c$ |
|---|---|
| Bayes- | $\frac{q_{s_0}}{p_{s_1}}\frac{\Pi_{01}-\Pi_{00}}{\Pi_{10}-\Pi_{11}}$, where $q_{s_0}$, $p_{s_1}$ – a priori probabilities of states $s_0$ and $s_1$; $\Pi_{00}$, $\Pi_{11}$ – gains from making the right decisions; $\Pi_{01}$, $\Pi_{10}$ – fee for error of the first and second kind |
| Maximum posterior probability | $\frac{q_{s_0}}{p_{s_1}}$ |
| Maximum plausibility | 1 |
| Neumann-Pearson | From the equation $F_{10}(c)=1-\alpha$, where $F_{10}(c)$ – integral function of the likelihood ratio under the hypothesis $H_0$; $\alpha$ – the probability of an error of the first kind |
| Minimax | $\frac{q_{mm}}{p_{mm}}\frac{\Pi_{01}-\Pi_{00}}{\Pi_{10}-\Pi_{11}}$ |

The right-hand side of the inequality (1) represents the threshold, the exceeding of which indicates the presence of a useful signal of the radio communication channel at the output of the receiver. Therefore, it is proposed to choose the following coefficient as an indicator of the information availability of a radio communication channel *RD*:

$$RD = \sum_{w=1}^{W} \frac{\lambda_w - 1}{\lambda_w} x_w^2. \quad (2)$$

When the radio communication channel is operating in the non-broadband signal (BBS) mode, eigennumbers $\lambda_w$ can be considered to be equal [7, 8]:

$$\lambda_w = \frac{\sigma_c^2 + \sigma_{IFN}^2}{\sigma_{IFN}^2},$$

where $\sigma_c^2$ – dispersion of the signal of a wireless radio communication channel, $\sigma_{IFN}^2$ – dispersion of the IFN of the receiver of the radio monitoring tool.

Then the coefficient of information availability of the radio communication channel in the non-BBS mode can be estimated using the following formula:

$$RD^{non\ BBS} = \frac{\sigma_c^2}{\sigma_c^2 + \sigma_{IFN}^2} \sum_{w=1}^{W} x_w^2. \quad (3)$$

Using the known ratio for an approximate estimate of the variance, it is possible to write that:

$$\sigma_c^2 = \frac{\sum_{w=1}^{W} \left( \left| \overline{\mathbf{E}} \right| - |\mathbf{E}|_w \right)^2}{W - 1}, \quad (4)$$

where $\left| \overline{\mathbf{E}} \right| = \frac{1}{W} \sum_{w=1}^{W} |\mathbf{E}|_w$ – average value of the modulus of the electric field intensity vector on the interval (0; $T_{obs}$) (V/m);

$|\mathbf{E}|_w$ – uncorrelated coordinates of the realization of the stochastic additive mixture of the modulus of the vector of the electric field strength of the useful signal and the IFN, which are observed at the output of the receiver of the radio monitoring device at the interval (0; $T_{obs}$) (V/m).

The classical approach of electromagnetic field theory is applied and an auxiliary function is introduced as the lagging vector potential of the magnetic field, **A** (Tl/m) [23–26], which is determined through the magnetic induction by the ratio **B**=*rot***A** (Tl). Then, taking into account one of the basic Maxwell equations $rot\mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$, the electric field strength vector can be given as $\mathbf{E} = -\frac{\partial \mathbf{A}}{\partial t}$ (if the gradient of the scalar potential is neglected), and relation (4) is written as follows:

$$\sigma_c^2 = \frac{\sum_{w=1}^{W} \left( \left| \overline{\frac{\partial \mathbf{A}}{\partial t}} \right| - \left| \frac{\partial \mathbf{A}}{\partial t} \right|_w \right)^2}{W - 1}, \quad (5)$$

where:

$$\left| \overline{\frac{\partial \mathbf{A}}{\partial t}} \right| = \frac{1}{W} \sum_{w=1}^{W} \left| \frac{\partial \mathbf{A}}{\partial t} \right|_w.$$

Taking into account the accepted assumption that the energy spectrum of the IFN receiver of the radio monitoring device is uniformly distributed in the *F* band (where *F* is the width of the spectrum of the signal emitted by the radio communication device (Hz)), and therefore its dispersion can be given as [22, 27]:

$$\sigma_{INF}^2 = \frac{k_b T_e (D_{rec} - 1) F}{\pi}, \quad (6)$$

where $k_b T_e (D_{rec} - 1) = N_{IFN}$ – spectral power density of the IFN receiver of the radio monitoring device;

$k_b$=1,38×10$^{-23}$– Boltzmann's constant, J/°K;

$T_e$=293° – effective temperature, °K;

$D_{rec}$ – noise coefficient of the radio monitoring device receiver (dB).

Then the coefficient of information availability of a radio communication channel operating in a non-BBS mode can be written in a general form as:

$$RD^{non\ BBS} = \frac{\frac{1}{W-1} \sum_{w=1}^{W} \left( \left| \overline{\frac{\partial \mathbf{A}}{\partial t}} \right| - \left| \frac{\partial \mathbf{A}}{\partial t} \right|_w \right)^2}{\frac{1}{W-1} \sum_{w=1}^{W} \left( \left| \overline{\frac{\partial \mathbf{A}}{\partial t}} \right| - \left| \frac{\partial \mathbf{A}}{\partial t} \right|_w \right)^2 + \frac{1}{\pi} k_b T_e (D_{rec} - 1) F} \sum_{w=1}^{W} x_w^2. \quad (7)$$

When operating a wireless radio communication channel in the BBS mode, eigennumbers $\lambda_w$ can be considered to be equal [1]:

$$1 + \frac{N_c}{N_{IFN}},$$

where $N_c$ – spectral density of the signal power of the radio communication device (W/Hz); $N_{IFN}$ – spectral power density of the IFN receiver of the radio monitoring device (W/Hz).

Therefore, the coefficient of information availability of a wireless radio communication channel in the BBS mode is estimated as follows:

$$RD^{BBS} = \frac{N_c}{N_c + N_{IFN}} \sum_{w=1}^{W} x_w^2. \quad (8)$$

The power spectral density of the signal generated by the radio communication channel at the location of the radio monitoring device can be obtained as follows. If the value of the rate of change of the energy of the electromagnetic field, i.e. its power, is known, then the power at this place in the general case is described by the expression [28]:

$$P = \frac{d}{dt} \int_V \left( \frac{\mu |\mathbf{H}|^2}{2} + \frac{\varepsilon |\mathbf{E}|^2}{2} \right) dV, \quad (9)$$

where *V* – the volume of the receiving antenna of the radio monitoring device;

**H** – magnetic field strength vector (A/m).

For wireless radio communication channels with antenna arrays, this integral can be replaced by the sum:

$$P = \frac{d}{dt} \sum_{n=1}^{N} \left( \frac{\mu |\mathbf{H}|^2}{2} + \frac{\varepsilon |\mathbf{E}|^2}{2} \right) \quad (10)$$

The following relation is obtained:

$$N_c = \frac{d}{2Fdt}\sum_{n=1}^{N}\left(\frac{\left|rot\mathbf{A}\right|^2}{\mu}+\varepsilon\left|\frac{\partial\mathbf{A}}{\partial t}\right|^2\right). \quad (11)$$

Thus, the coefficient of information availability of a radio monitoring tool operating in the BBS mode is generally written as follows:

$$RD^{BBS} = \frac{\frac{d}{2Fdt}\sum_{n=1}^{N}\left(\frac{\left|rot\mathbf{A}\right|^2}{\mu}+\varepsilon\left|\frac{\partial\mathbf{A}}{\partial t}\right|^2\right)}{\frac{d}{2Fdt}\sum_{n=1}^{N}\left(\frac{\left|rot\mathbf{A}\right|^2}{\mu}+\varepsilon\left|\frac{\partial\mathbf{A}}{\partial t}\right|^2\right)+k_bT\left(D_{rec}-1\right)}\sum_{w=1}^{W}x_w^2. \quad (12)$$

Calculation of the general expression for the coefficient of internal availability of a wireless radio communication channel. In this case, the signal of the radio communication channel is assumed to be deterministic, that is, it is about coherent reception, and the rule for detecting such a signal by the receiving channel of the radio monitoring tool has the form [29]:

$$\sum_{w=1}^{W}x_w\left|-\frac{\partial\mathbf{A}}{\partial t}\right|_w \geq \ln c+\frac{1}{2}\sum_{w=1}^{W}\left|\frac{\partial\mathbf{A}}{\partial t}\right|_w^2. \quad (13)$$

That is, if inequality (13) is fulfilled, then a decision is made that the observed process is stationary, normal with zero mean. If inequality (13) is not fulfilled, then this process is also normal, but with an average value that changes according to a precisely known law $\left(-\frac{\partial\mathbf{A}}{\partial t}\right)$.

Therefore, it is proposed to use the following coefficient as an indicator of the internal availability of a wireless radio communication channel:

$$VD = \sum_{w=1}^{W}x_w\left|-\frac{\partial\mathbf{A}}{\partial t}\right|_w. \quad (14)$$

Considering that the reception is coherent, it is possible to apply the coefficient of internal availability of the radio communication channel in the same form, both for BBS and non-BSS modes of operation.

### 5. 2. Obtaining analytical relations for the vector potential of the magnetic field

The vector potential of the lagging magnetic field as a result of work on data transmission of the radio communication channel is considered. Each of the wireless radio communication channels of the automated data transmission system will create an electromagnetic field in some space (network) during transmission. The dimensions of such an area are determined by the medium of propagation of electromagnetic waves. The properties of this field are characterized with sufficient completeness by the lagging vector 3-potential of the magnetic field, $\mathbf{A}=(A_x, A_y, A_z)$. That is why, when obtaining mathematical dependencies for the coefficients of information (7), (12) and internal availability (14) of wireless radio communication channels, their relationship with this vector 3-potential is shown as a model of the result of work on data transmission of a radio communication channel "link".

When modeling, first of all, the vector 3-potential in the locations of other radio communication channels of the data transmission system is of interest ($x_l$, $y_l$, $z_l$) and at known (or those that are predicted) locations of radio monitoring equipment ($x_q$, $y_q$, $z_q$). According to the theory of the electromagnetic field [30, 31], the vector 3-potential of a lagging magnetic field generally has the following vector notation:

$$\mathbf{A}(t) = \frac{\mu}{4\pi}\int_V\frac{1}{r}\delta\left(t-\frac{r}{v}\right)dV, \quad (15)$$

where $\mu$ – magnetic permeability of the operating area, as a medium for the propagation of electromagnetic waves (gn/m);

$\delta=(\delta_x, \delta_y, \delta_z)$ – conduction current density vector in the transmission antenna (A/m$^3$, relative to the bulk antenna);

$V$ – transmission antenna volume (m$^3$);

$r$ – distance from the radio communication channel to the observation point (m);

$v$ – propagation speed of electromagnetic waves (m/s).

In the case of antenna arrays, according to [25, 29], formula (15) will take the following form:

$$\mathbf{A}(t) = \frac{\mu}{4\pi}\sum_{n=1}^{N}\frac{1}{r}\delta\left(t-\frac{r}{v}\right), \quad (16)$$

where $N$ – the number of emitters in a digital antenna array of a wireless radio communication channel.

Previously, phased antenna arrays were used exclusively in large stationary radars. But modern advances in the methods of designing and manufacturing phased antenna arrays make it possible to reduce their overall dimensions and use them in various radio engineering systems and complexes. The principle of operation of a phased antenna array is presented on the example of a linear phased antenna array (Fig. 2).

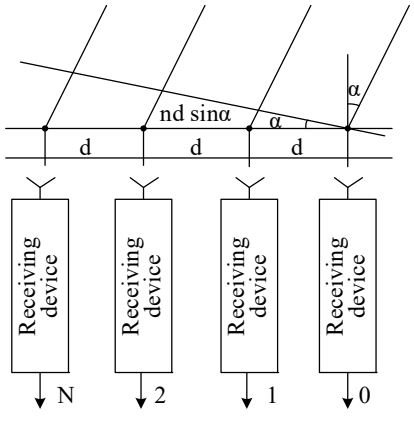


Fig. 2. The principle of operation of a linear phased antenna array

It should be taken into account that the emitters of the digital antenna array of the wireless radio communication channel can represent information leakage channels. Therefore, the conduction current density vector in the emitters of the digital antenna array of the wireless radio communication channel for different operating modes is considered. It can be seen from formulas (15), (16) that the vector 3-potential of the magnetic field is determined by the vector of the conduction current density in the transmitting antenna of the radio communication channel. Mathematical expressions for this vector during operation of the radio communication channel in modes [3, 25] were obtained:

– amplitude modulation (AM);
– frequency modulation (FM;
– phase modulation (PM);
– pseudo-random sequence (PRS) discrete-frequency modulation (DFM);
– continuous phase modulation (CFM) PRS,
– frequency-phase modulation (FPM) PRS;
– pseudo-random tuning of the operating frequency (PTOF).

When working in the AM mode, the conduction current density vector in the emitter of the digital antenna array of the radio communication device over time is determined as follows:

$$\delta^{AM}(t)=\sum_{i=1}^{\lambda T/\chi}\delta(i\Delta\tau)g(t)\sin(\varpi_0 t+\psi_0), \quad (17)$$

where λ – intensity of the information flow transmitted by the radio communication channel (bit/s);

χ – bit rate of the digital-to-analog converter of the digital antenna array;

δ ($i\Delta\tau$) – amplitude of the current density vector (A/m$^3$, for a volumetric antenna);

Δτ – period of discretization of information message (s);

$g(t)$ – the pulse envelope of the information message, which takes the value 0 or 1;

$\omega_0$ – carrier frequency of the wireless radio communication channel (Hz);

$\psi_0$ – the initial phase of the carrier oscillation of a wireless radio communication channel.

When operating in the FM mode, the current density vector in the emitter of the digital antenna array of the radio communication channel during time $T$ will look like this:

$$\delta^{FM}(t)=\sum_{i=1}^{\lambda T/\chi}g(t)\sin\left((\varpi_0+i\Delta\varpi)t+\psi_0\right), \quad (18)$$

where $\Delta\varpi_{m_n}$ – frequency deviation in the emitter of the digital antenna array of the radio communication channel of the data transmission system.

The current density vector in the emitter of the digital antenna array of the radio communication channel during time $T$ when operating in the PM mode will be as follows:

$$\delta^{PM}(t)=\sum_{i=1}^{\lambda T/\chi}g(t)\sin\left(\varpi_0 t+\frac{2\pi(i-1)}{\lambda T/\chi}\right) \quad (19)$$

When operating in the PRS DFM mode, the current density vector in the emitter of the digital antenna array of the radio communication device during time $T$ can be given as:

$$\delta^{PRS\ DFM}(t)=$$
$$=\sum_{i=1}^{\lambda T/\chi}\sum_{k=1}^{K}\delta(i\Delta\tau)u\left[t-(k-1)\tau_e\right]\sin\left((\varpi_0+\beta_k\Delta\varpi)t+\psi_0\right), \quad (20)$$

where $K$ – the number of PRS elements per bit of the information message;

$$u\left[t-(k-1)\tau_e\right]=\begin{cases}1, \text{at } (k-1)\tau_e\le t\le k\tau_e,\\ 0, \text{at } (k-1)\tau_e>t>k\tau_e\end{cases}$$

– single jump function;
$\tau_e$ – the duration of the PRS element;
$\beta_k\in\{0, 1\}$ – PRS.

The current density vector in the emitter of the digital antenna array of the radio communication channel over time when operating in the CFM PRS mode can be presented as:

$$\delta^{CFM\ PRS}(t)=$$
$$=\sum_{i=1}^{\lambda T/\chi}\sum_{k=1}^{K}\delta(i\Delta\tau)u\left[t-(k-1)\tau_e\right]\sin(\varpi_0 t+\psi_0+\alpha_k\pi), \quad (21)$$

where $\alpha_k\in\{0, 1\}$ – PRS.

When operating in the FPM PRS mode, the current density vector in the emitter of the digital antenna array of the radio communication channel for the period $T$ can be written as:

$$\delta^{FPM\ PRS}(t)=$$
$$=\sum_{i=1}^{\lambda T/\chi}\sum_{k=1}^{K}\delta(i\Delta\tau)u\left[t-(k-1)\tau_e\right]\sin\left((\varpi_0+\beta_k\Delta\varpi)t+\psi_{PTOF}\right), \quad (22)$$

The current density vector in the emitter of the digital antenna array of the radio communication channel during time T when operating in the *PTOF* mode can be given as:

$$\delta^{PTOF}(t)=$$
$$=\sum_{i=1}^{\lambda T/\chi}\sum_{k=1}^{K}\delta(i\Delta\tau)u\left[t-(k-1)\tau_e\right]\sin\left((\varpi_0+\beta_k\Delta\varpi)t+\psi_{PTOF}\right), \quad (23)$$

where $\psi_{PTOF\,m_n}$ – random phase uniformly distributed over the range $[0,2\pi]$.

**5. 3. Evaluation of the impact of interference on data transmission reliability**

The most negative for blocking radio communication channels is the case when the interference spectrum overlaps with the spectrum of the information signal emitted by the antenna [32–37]. That is, this is the case when part of the interference spectrum falls into the region of the main maximum of the spectrum of the information signal.

Three possible options for imposing interference to block a wireless radio communication channel are considered. Nominating through $\Delta\Omega$ the width of the interference spectrum $G$, and the frequency of the main maximum of the information signal of the wireless radio communication channel – $\omega_0$, the following options for the influence of interference on data transmission by an informational radio communication signal are considered:

– broadband interference ($\Delta\Omega>>\omega_0$);
– narrowband interference ($\Delta\Omega<<\omega_0$);
– the interference is narrowband and its center frequency is close to the frequency $\omega_0$.

Broadband interference ($\Delta\Omega>>\omega_0$).

Let the interference spectrum be in the area of the main maximum of the spectrum of the information signal of the wireless radio communication channel $\delta/\delta^{\max}$ (Fig. 3).

In Fig. 3 dependence G(Ω)` represents a useful Wi-Fi network information transmission signal, dependency $\delta/\delta^{\max}$ – broadband interference, for example, which is due to the influence of radio technical signals of radio transmitting and radio receiving systems. The frequency of the useful signal of the Wi-Fi network (2.4 GHz) in Fig. 3 matches the value Ω=0.

In the area of the main maximum, the interference spectrum can be considered approximately constant, then the interference immunity coefficient $k_p$ is calculated as follows [21]:

$$k_p \approx \frac{\Delta\Omega}{\omega_0}. \quad (24)$$

Narrowband interference ($\Delta\Omega << \omega_0$), and the center frequency of the interference spectrum $\Omega_0$ satisfies the condition $\Omega_0 \neq \omega$ (Fig. 4).

In Fig. 4 dependence G(Ω)` represents a useful Wi-Fi network information transmission signal, dependency $\delta/\delta^{max}$ – narrowband interference, for example, caused by the influence of the cellular network (frequency 2600 MHz). The frequency of the useful signal of the Wi-Fi network (2.4 GHz) in Fig. 4 matches the value Ω=0. Value Ω=0,5 corresponds to a frequency of 2600 MHz.

In this case, in the region of the main maximum, the interference spectrum partially affects the spectrum of the useful signal, and the interference immunity coefficient $k_p$ is calculated as follows [21]:

$$k_p \approx \frac{n^2}{8\left|\chi(\Omega_0)\right|^2}. \quad (25)$$

Narrowband interference ($\Delta\Omega << \omega$), and the center frequency $\Omega_0$ is near the frequencies $\omega_0$ or $\Omega_0=\omega_0$ (Fig. 5).

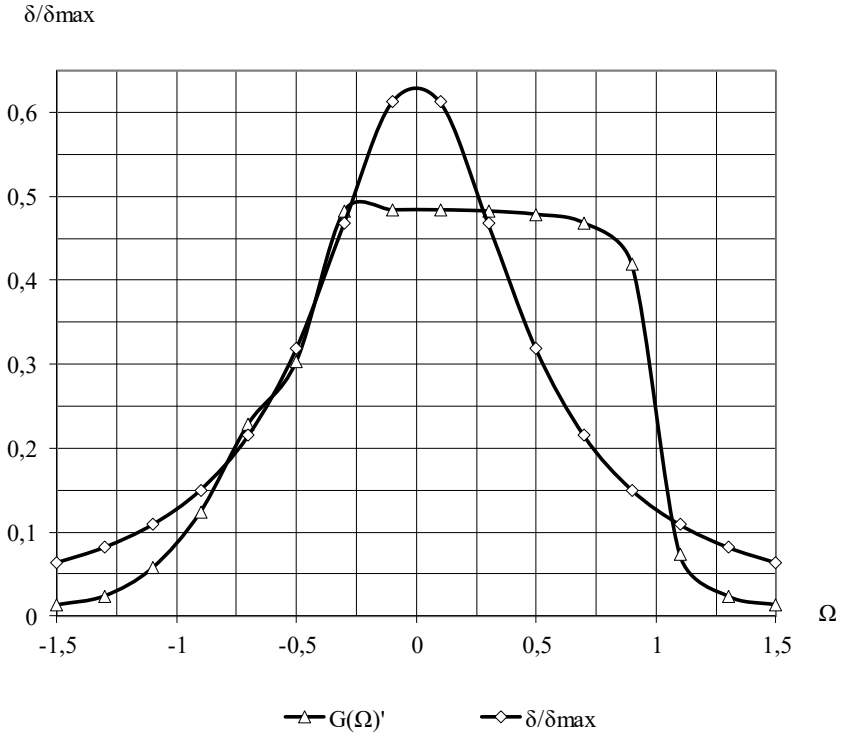


Fig. 3. Broadband interference

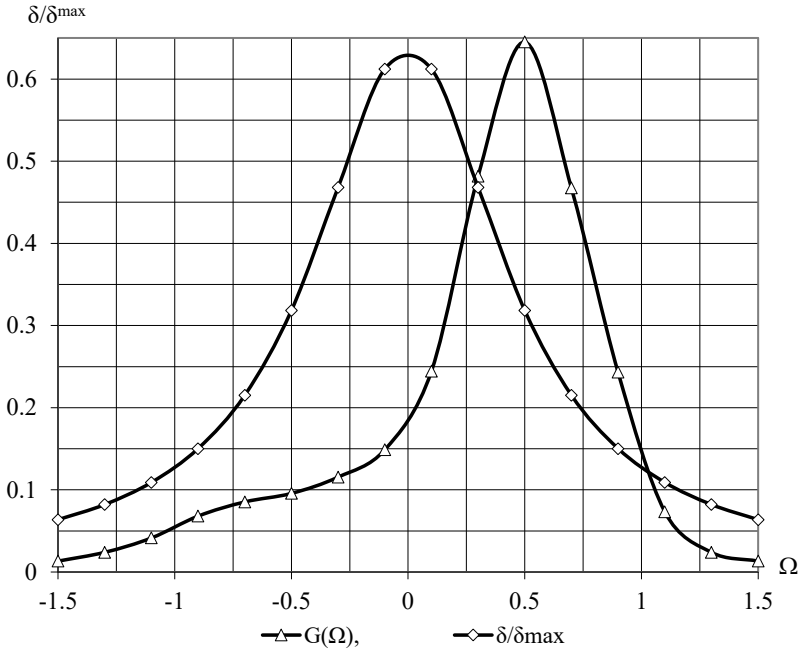


Fig. 4. Narrowband interference

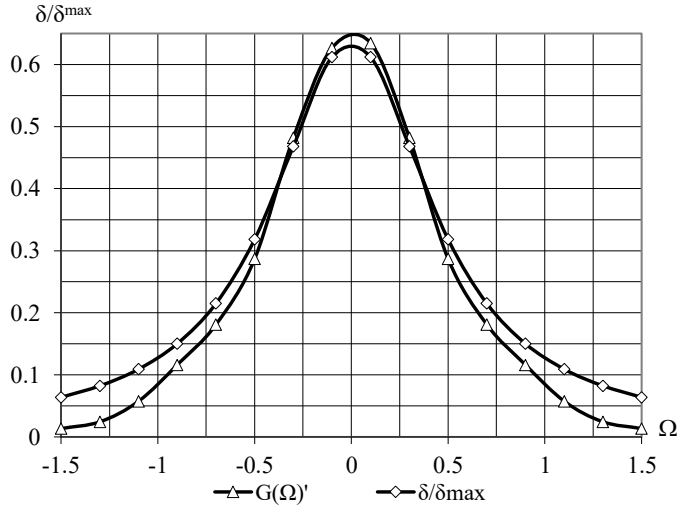


Fig. 5. Narrow-band central interference

In Fig. 5 dependence G(Ω)` represents a useful Wi-Fi network information transmission signal, dependency $\delta/\delta^{max}$ – narrowband interference, for example, which is due to the influence of another subscriber's Wi-Fi network (2.4 GHz frequency).

For such a case, the immunity factor $k_p$ is calculated by the formula [21]:

$$k_p \approx \frac{n^2}{4\left|\chi(\omega_1)\right|^2}, \quad (26)$$

where $\omega_1 \approx \omega_0$.

Thus, formulas (24)–(26) can be used to calculate the reliability of data transmission through wireless communication channels. Reliability of data transmission depends on the immunity factor.

**5. 4. Development of a methodology for assessing the current state of an automated data transmission system through wireless communication channels**

The assessment of target threats to automated data transmission systems with signs of hybridity and synergism, as well as the possibility of their integration with social engineering methods, is proposed to be carried out based on the classification of threats by a unified classifier based on the proposed framework [38, 39]. In Fig. 6 shows the mathematical formalization of the unified classifier, which allows forming tuples-classifiers of cyberthreats taking into account not only the signs of their hybridity and synergism, integration with social engineering methods, as well as their focus on other cloud platforms of socio-cyberphysical systems. At the same time, it is proposed to divide their infrastructure into three platforms: a physical systems platform, a management platform (as a rule, located in the cloud) and a social network platform.

At the same time, the sign of hybridity of targeted (mixed) attacks means the impact of an attack on one of the security services (C, I, Ac, Aut, Ut) on all security components (cyber security, information security, security of information). The sign of synergism of targeted (mixed) attacks means the impact of an attack on one component of security (cyber security, information security, security of information), but at the same time on all services at the same time (C, I, Ac, Aut, Ut).

In [39], it is possible to analytically assess the flow state of any transmission and/or circulation system (storage, etc.) of the level of security of both information resources and infrastructure elements.

At the same time for information resources is taken into account, the degree of their "confidentiality" – $\beta_i$ – metric of the ratio of time and the degree of confidentiality of information (critical – 1.0; high – 0.75; medium – 0.5; low – 0.25; very low – 0.01)), and also to assess the level of possibility of protection mechanisms based on the proposed methodology. The main stages of the technique are presented in Fig. 7.

$$C^i_{\substack{\text{threat}\\\text{vector}}} = \left\{ L^1_{\substack{\text{criticality}\\\text{of the threat}}}, L^2_{\substack{\text{security}\\\text{component}}}, L^3_{\substack{\text{security}\\\text{service}}}, L^4_{\substack{\text{the nature of}\\\text{the threat's direction}}}, L^5_{\substack{\text{threat impact}\\\text{level}}}, L^6_{\substack{\text{social impact}\\\text{engineering}}}, L^7_{\substack{\text{platform}\\\text{contour}}} \right\},$$

$$L^1_{\substack{\text{criticality}\\\text{of the threat}}} \in \left\{ \begin{matrix} \text{01 - critical, 02 - high, 03 - medium,} \\ \text{04 - low, 05 - too low} \end{matrix} \right\};$$

$$L^2_{\substack{\text{security}\\\text{component}}} \in \left\{ \begin{matrix} \text{01 - cybersecurity, 02 - information security,} \\ \text{03 - security of information} \end{matrix} \right\};$$

$$L^3_{\substack{\text{security}\\\text{service}}} \in \left\{ \begin{matrix} \text{01 - integrity, 02 - confidentiality, 03 - availability,} \\ \text{04 - authenticity, 05 - involvement} \end{matrix} \right\};$$

$$L^4_{\substack{\text{the nature of}\\\text{the threat's direction}}} \in \left\{ \begin{matrix} \text{01 - engineering-technical, 02 - organizational,} \\ \text{03 - legal and regulatory} \end{matrix} \right\};$$

$$L^5_{\substack{\text{threat impact}\\\text{level}}} \in \left\{ \begin{matrix} \text{01 - physical level, 02 - network level,} \\ \text{03 - OS level, 04 - DBMS level,} \\ \text{05 - applications and services level, 06 - IoT level,} \\ \text{07 - IPS level} \end{matrix} \right\};$$

$$L^6_{\substack{\text{social impact}\\\text{engineering}}} \in \left\{ \begin{matrix} \text{01 - system hack, 02 - system compromise,} \\ \text{03 - data compromise,} \\ \text{04 - finding critical points of the system,} \\ \text{05 - information gathering} \end{matrix} \right\};$$

$$L^7_{\substack{\text{platform}\\\text{contour}}} \in \left\{ \begin{matrix} \text{01 - internal, 02 - external,} \\ \text{03 - internal and external} \end{matrix} \right\}.$$

Fig. 6. Mathematical formalization of the unified classifier

Stage 7 is separately defined, which allows assessing the capabilities of special mechanisms for providing security services for automated data transmission systems and socio-cyber-physical systems. For this, the following components of the proposed algorithm are defined:

1 step. Determination of the assessment of possible APT attacks on infrastructure elements as:

$$S^*_{\text{malefactors/ISO}} = \left\| S_{ISO_{pl}} \right\|,$$

where $p$ – type of attecker.

At the same time, the type of intruder is determined as in [40] and shown in Fig. 8.

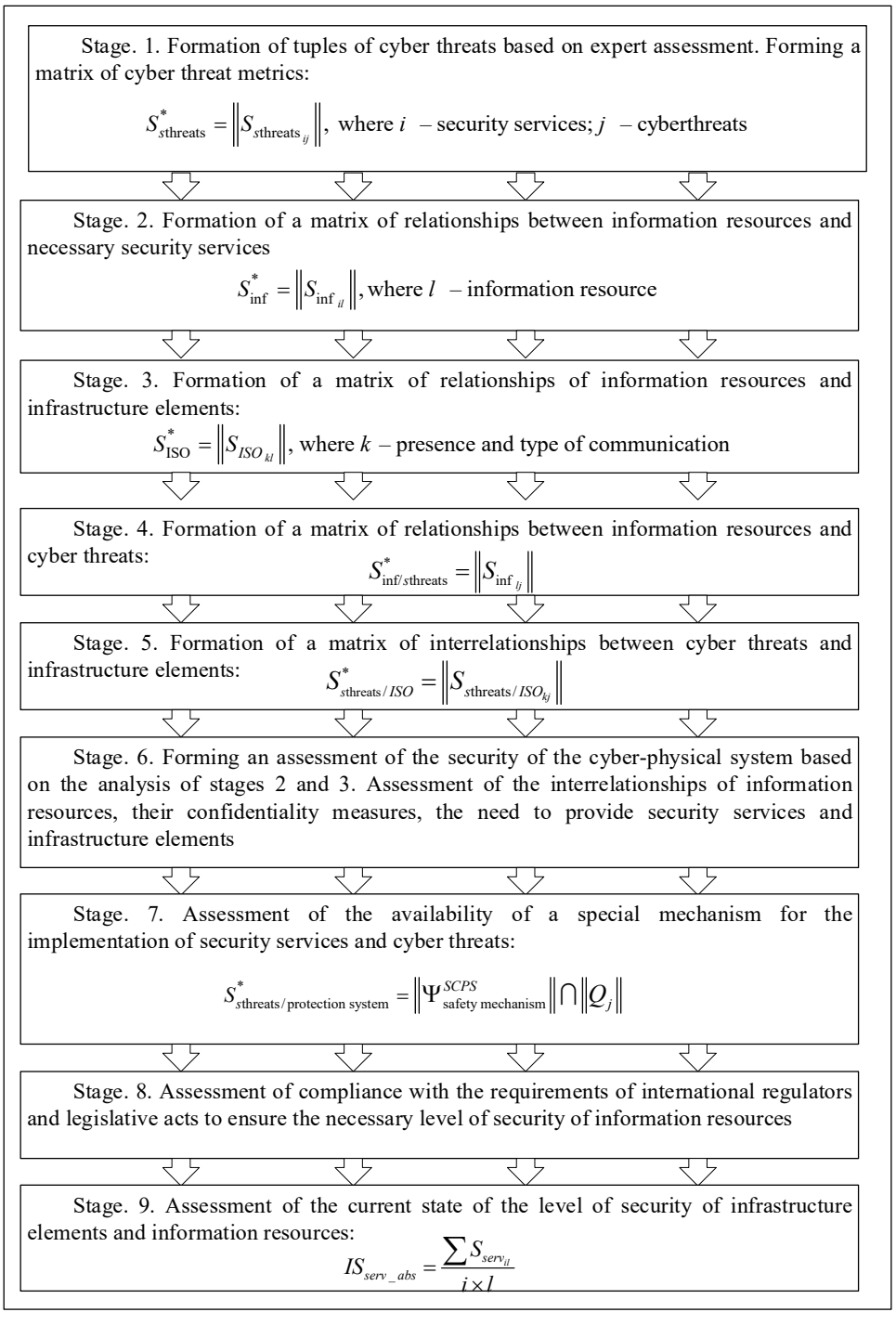


Fig. 7. Stages of assessment of the current state of the security level of cyber-physical systems

2 step. Assessment of attackers' capabilities (financial, computational, human). Let's determine the weight coefficient of the "danger" of the attacker using the formula:

$$p^{SCPS}_{\text{malefactors}} = \frac{1}{N}\sum_{i=1}^{N} \beta^{SCPS}_{p\ i}, \quad (26)$$

where $\beta^{SCPS}_i = Q^{SCPS}_{\substack{\text{computing}\\ \text{resources}}} \cap Q^{SCPS}_{\substack{\text{financial}\\ \text{resources}}} \cap Q^{SCPS}_{\substack{\text{human}\\ \text{resources}}}$ – the coefficient of the violator's opportunities, $Q^{SCPS}_{\substack{\text{computing}\\ \text{resources}}}$, $Q^{SCPS}_{\substack{\text{financial}\\ \text{resources}}}$, $Q^{SCPS}_{\substack{\text{human}\\ \text{resources}}} \in$ {1 – unlimited resources of cyber terrorists, 0.75 – resources of the state (special services), 0.5 – resources of cybercriminals, 0.25 – resources of criminals, competitors, hackers, 0.001 – resources of vandals}.

3 step. The estimation of the probability of implementation of APT-attacks taking into account the coefficient of "danger" of the attacker is defined as:

$$\left\| Q_j \right\| = p^{SCPS}_{\text{malefactors}_j} \times P^j_{\alpha},$$

where $j$ – threat, $\alpha$ – cyberthreat appearance probability, $P^j_{\alpha} \in$ {1 – the threat is realized every day, 0.75 – the threat is realized within a week, 0.5 – the threat is realized within a month, 0.25 – the threat is realized within a year, 0.001 – unlimited time }.

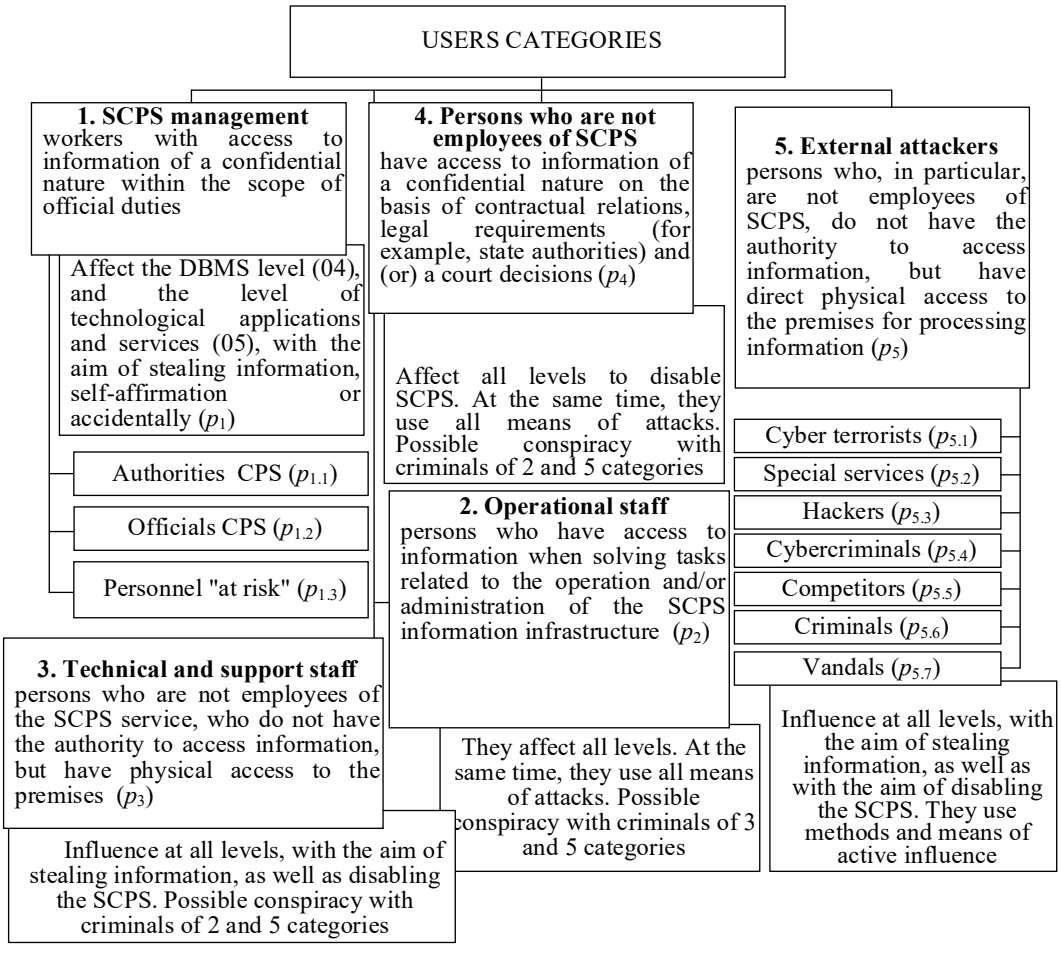


Fig. 8. Categories of users of socio-cyberphysical systems

4 step. The assessment of the availability of special mechanisms for providing security services is determined in accordance with the Table 3 [41–44]:

$$\Psi^{SCPS}_{\text{safety mechanism}} = \left\| F_{ij} \right\| \times \Psi_i,$$

where $i$ – special security (trust) mechanism, $j$ – threat.

5 step. The assessment of preventive measures against APT attacks is determined:

$$S^{*}_{\text{sthreats/protection system}} = \left\| \Psi^{SCPS}_{\text{safety mechanism}} \right\| \cap \left\| Q_j \right\|.$$

Thus, the presented mathematical apparatus makes it possible to increase the level of objectivity in assessing "possible" targeted (mixed) attacks on SCPS infrastructure elements of both the first (physical systems) platform and the second (control systems) platform. In addition, a timely assessment of the current level of "capability" of the information protection system to resist (assessment of the presence of special mechanisms) targeted attacks on elements of the SCPS infrastructure is provided.

Table 3

Weighting coefficients $\Psi_i$ of special mechanisms availability for providing security services and reliability of the data transmission system

| Mechanism type | Special mechanisms that provide: | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Detection | | | | | Signaling | | | | | Blocking | | | | |
| | Level of resistance | | | | | Level of resistance | | | | | Level of resistance | | | | |
| | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 |
| IDS | + | + | + | + | + | + | + | + | + | + | – | – | – | – | – |
| IPS | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| SIEM | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |

| Mechanism type (bit) | Mechanisms that provide the service: | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Confidentiality | | | | | Integrity | | | | | Authenticity | | | | | Accessibility | | | | |
| | Level of resistance | | | | | Level of resistance | | | | | Level of resistance | | | | | Level of resistance | | | | |
| | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |

Continuation of Table 3

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 89 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Symmetric block ciphers (BSC) | | | | | | | | | | | | | | | | | | | | |
| BSC with key 128 | + | – | – | – | – | + | – | – | – | – | + | – | – | – | – | – | – | – | – | – |
| MAC+BSC with key 256 | + | + | – | – | – | + | + | – | – | – | + | + | – | – | – | – | – | – | – | – |
| BSC with key 256 | + | + | + | – | – | + | + | + | – | – | + | + | + | – | – | – | – | – | – | – |
| MAC+BSC with key 256 | + | + | + | + | – | + | + | + | + | – | + | + | + | + | – | – | – | – | – | – |
| BSC with key 256 | + | + | + | + | + | + | + | + | + | + | + | + | + | + | – | – | – | – | – | – |
| Symmetric stream ciphers (SSC) | | | | | | | | | | | | | | | | | | | | |
| Uniform movement of registers | + | + | + | – | – | + | + | + | – | – | + | + | + | – | – | + | + | + | – | – |
| Uneven movement of registers | + | + | + | + | – | + | + | + | + | – | + | + | + | + | – | + | + | + | + | – |
| Asymmetric algorithms | | | | | | | | | | | | | | | | | | | | |
| Digital signature (DS) | + | + | + | – | – | + | + | + | – | – | + | + | + | – | – | – | – | – | – | – |
| on *EC* | + | + | + | + | – | + | + | + | + | – | + | + | + | + | – | – | – | – | – | – |
| Post-quantum algorithms | | | | | | | | | | | | | | | | | | | | |
| DS | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | – | – | – | – | – |
| HCCC on MEC | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + | + |
| CCC on MEC (EC) | + | + | + | + | – | + | + | + | + | – | + | + | + | + | + | + | + | + | + | + |
| CCC on LDPC | + | + | + | – | – | + | + | + | – | – | + | + | + | – | – | + | + | + | + | + |

*Note: $\Psi_i \in$ {1 level – 0.1, 2 level – 0.25, 3 level – 0.5, 4 level – 0.75, 5 level – 1}, BSC – block-symmetric cipher, SSC – stream symmetric cipher, DS – digital signature, EC – asymmetric algorithms on elliptic curves, HCCC – hybrid crypto-code constructions, CCC – crypto-code constructions (McEliece, Niederreiter), CCC on MEC (EC) – CCC on modified (shortened, lengthened) elliptical codes (EC).*

## 6. Discussion of the results of the development of a mathematical model of an automated data transmission system

The proposed mathematical model of the functioning of the automated data transmission system by wireless communication channels allows to evaluate the reliability of the transmission of information signals.

According to formula (24), for broadband interference, for which the condition is fulfilled $\Delta\Omega >> \omega$, the immunity factor is $k_p >> 1$. So, in this case, there is high immunity. This is ensured by a sharp narrowing of the effective (useful) band of the information signal and a filtering function $\delta/\delta^{max}$. The data conclusion does not contradict the graphic representation of the process (Fig. 3). Broadband interference cannot completely cover the spectrum of the useful signal if the narrowly directed beam of the useful signal dominates the power of the interference. To create high-power broadband interference, it is necessary to create a large antenna and have a powerful power system, which limits the creation of such blocking systems.

It can be seen from formula (25) that for this narrowband interference, the interference immunity coefficient is $k_p >> 1$. So, in this case, the automated data transmission system has a high level of immunity. This conclusion does not contradict the obtained graphic implementation (Fig. 4).

From the relation (26), it follows that the interference immunity factor can be approximately written as $k_p \sim 1$. Therefore, with narrowband interference of sufficient power, the central frequency of which is close to the frequency $\varpi_0$, there is practically no interference protection of the wireless radio communication channel. This conclusion corresponds to the graphical implementation of the case shown in Fig. 5.

The resulting formulas (24)–(26) and the data in Table 3 show that to increase the level of immunity when narrowband interference is detected, it is suggested to use hybrid crypto-code designs. This will protect information from possible leakage due to interference. At the same time, the possibility of automatic reconfiguration of the main frequency of the wireless radio communication channel should be provided. Such a technical solution, together with the use of hybrid crypto-code structures, will allow the level of confidentiality, integrity, authenticity and reliability of the wireless radio communication channel to approach 100 %.

Thus, the obtained analytical relations (24)–(26) generally do not contradict the graphical implementation of the given cases (according to Fig. 3–5) and the physical content of the propagation of electromagnetic waves in space. This confirms the adequacy of the developed mathematical model of the functioning of the automated system of data transmission through wireless communication channels.

The limitations of this study are the accepted condition of the serviceability of the data transmission channel. Therefore, during the technical implementation of the developed model, in order to improve the quality of modeling, it is necessary to provide for the condition of control of the technical condition of the system (or its component blocks, elements).

The disadvantage of this study is the assumption that there are no obstacles in the transmission of data through the information channel. The presence of interference, especially caused by the electromagnetic field, can affect the reliability of data transmission. And this can create prerequisites for the leakage of information or its loss during transmission.

The development of this research consists in the process of developing methods of protecting automated data transmission systems from information leakage and substantiating the most appropriate options for the functioning of this system.

## 7. Conclusions

1. The study presents the theoretical foundations of the functioning principles of the automated data transmission system through wireless communication channels in the process of its protection from radio monitoring devices. The obtained model allows to determine:

– coefficients of information and internal availability of a wireless radio communication channel;

– vector potential of the delayed magnetic field as a result of operation for data transmission by a wireless radio communication channel and vector of conduction current density in the emitters of a digital antenna array of a wireless radio communication channel for different modes of operation.

The spectral power density of the signal generated by a wireless radio communication channel is proposed to be estimated by the value of the rate of change of the energy of the electromagnetic field. When evaluating the coefficient of internal availability of a wireless radio communication channel, it is necessary to take into account the coherent reception of the signal. At the same time, the coefficient of internal availability of the radio communication channel does not differ for broadband and non-broadband signals.

2. It is shown that the emitters of the digital antenna array of the wireless radio communication channel can represent information leakage channels. Therefore, the conduction current density vector in the emitters of the digital antenna array of the radio communication channel for different operating modes is considered. For this purpose, mathematical expressions were obtained for this vector during the operation of a wireless radio communication channel in the modes of amplitude, frequency, phase, discrete-frequency, continuous phase, frequency-phase modulation and pseudo-random tuning of the operating frequency. Such expressions were obtained on the basis of vector calculations of the conductivity current density in the emitter of the digital antenna array of the radio communication channel.

3. The obtained analytical ratios for the immunity factor of the wireless radio communication channel generally do not contradict the graphical implementation of the given cases and the physical content of the propagation of electromagnetic waves in space. This confirms the adequacy of the developed mathematical model of the functioning of the automated system of data transmission through wireless communication channels.

4. The proposed technique for assessing the flow state of an automated system of data transmission via wireless communication channels provides an increase in the level of objectivity in assessing not only targeted attacks (taking into account the financial, computing and human capabilities of the attacker). In addition, an analysis of critical points (points of possible unauthorized penetration into the infrastructure) is provided, as well as the possibility of countering cyber attacks based on special mechanisms, taking into account the security levels that are defined.

The computer implementation of the proposed method made it possible to substantiate that for the assessment of the coefficient of internal availability of a wireless radio communication channel, it is proposed to take into account the coherent reception of the signal. At the same time, the value of the interference immunity coefficient of the wireless radio communication channel is much greater than 1, which indicates the provision of sufficient protection of information. A technical solution is proposed that will allow the level of confidentiality, integrity, authenticity and reliability of a wireless radio communication channel to approach 100 %.

## Conflict of interest

The authors declare that there is no conflict of interest regarding this research, including financial, personal, authorship or other nature, which could affect the research and its results presented in this article.

## Financing

The study was conducted without financial support.

## Data availability

The manuscript has no associated data.

## Use of artificial intelligence

The authors confirm that they did not use artificial intelligence technologies when creating the presented work.

References

1. Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M., Hrytsyk, V., Milov, O. et al.; Yevseiev, S., Hryshchuk, R., Molodetska, K., Nazarkevych, M. (Eds.) (2022). Modeling of security systems for critical infrastructure facilities. Kharkiv: PC TECHNOLOGY CENTER, 196. https://doi.org/10.15587/978-617-7319-57-2
2. Yevseiev, S., Kuznietsov, O., Herasimov, S., Horielyshev, S., Karlov, A., Kovalov, I. et al. (2021). Development of an optimization method for measuring the Doppler frequency of a packet taking into account the fluctuations of the initial phases of its radio pulses. Eastern-European Journal of Enterprise Technologies, 2 (9 (110)), 6–15. https://doi.org/10.15587/1729-4061.2021.229221

3. Sokolov, A. Y. (1999). Algebraic approach on fuzzy control. IFAC Proceedings Volumes, 32 (2), 5386–5391. https://doi.org/10.1016/s1474-6670(17)56917-7
4. Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O., Korol, O., Milevskyi, S. et al.; Yevseiev, S., Ponomarenko, V., Laptiev, O., Milov, O. (Eds.) (2021). Synergy of building cybersecurity systems. Kharkiv: PC TECHNOLOGY CENTER, 188. https://doi.org/10.15587/978-617-7319-31-2
5. Shao, R., Ding, C., Liu, L., He, Q., Qu, Y., Yang, J. (2024). High-fidelity multi-channel optical information transmission through scattering media. Optics Express, 32 (2), 2846. https://doi.org/10.1364/oe.514668
6. Dao, V. A., Thanh Thuy, T. T., Quoc Bao, V. N., Dung, T. C., Quyen, N. X. (2024). Design of A Chaos-based Digital Radio over Fiber Transmission Link using ASK Modulation for Wireless Communication Systems. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 11 (1). https://doi.org/10.4108/eetinis.v11i1.4530
7. M, S., Kandasamy, R., Kumar, S. S. (2022). A Novel Approach on Cognitive Radio Sensor Networks for Efficient Data Transmission. https://doi.org/10.21203/rs.3.rs-1735166/v1
8. Lacey, K. (2024). Communication in the Radio Century. The Oxford Handbook of Radio and Podcasting, 733–748. https://doi.org/10.1093/oxfordhb/9780197551127.013.34
9. Ren, Y., Wu, Y., Tu, Z. (2024). A Multi-Channel Chromatic Dispersion Compensation for 15-km Front-Haul Transmission. Optical Fiber Communication Conference (OFC) 2024. https://doi.org/10.1364/ofc.2024.w2b.11
10. Park, J., Choi, D. (2023). Improvement and Utilization of Auxiliary Radio Communication System. Journal of the Korean Society of Hazard Mitigation, 23 (3), 83–93. https://doi.org/10.9798/kosham.2023.23.3.83
11. Soliman, N. F., Fadl-Allah, F. E., El-Shafai, W., Aly, M. I., Alabdulhafith, M., El-Samie, F. E. A. (2024). A Hybrid Cybersecurity Algorithm for Digital Image Transmission over Advanced Communication Channel Models. Computers, Materials & Continua, 79 (1), 201–241. https://doi.org/10.32604/cmc.2024.046757
12. Youvan, D. (2024). Silent Waves: The Role of Ham Radio in a Fictional Communication Blackout Scenario. https://doi.org/10.13140/RG.2.2.23193.19044
13. Kolawole, W. (2024). Enhancing Data Security through Chaotic Encryption for Secure Transmission. Available at: https://www.researchgate.net/publication/380179574_Enhancing_Data_Security_through_Chaotic_Encryption_for_Secure_Transmission
14. Renteria, L., Jínez, J., Torres, K., Ramos, J. (2023). Data transmission system through FM radio applying Data over Sound techniques. Novasinergia, 6 (2), 129–139. https://doi.org/10.37135/ns.01.12.08
15. Soni, V. (2024). ED-SS based Cognitive Radio (CR) over Various Fading Channels for Modern Wireless Communications. Journal of Electrical Systems, 20 (7s), 1406–1423. https://doi.org/10.52783/jes.3713
16. Mak, B., Arya, S., Wang, Y., Ashdown, J. (2023). Characterization of Low-Latency Next-Generation eVTOL Communications: From Channel Modeling to Performance Evaluation. Electronics, 12 (13), 2838. https://doi.org/10.3390/electronics12132838
17. Guan, K., Kürner, T., Rupp, M., Nekovee, M. (2024). Guest Editorial: Channel Modeling and Signal Processing for Terahertz Communications. IEEE Communications Magazine, 62 (2), 14–15. https://doi.org/10.1109/mcom.2024.10439199
18. Yakovlev, M., Volobuev, A., Pribyliev, Yu. (2024). Mathematical modeling of the processes of functioning of automated military radio communication systems in terms of their protection against radio reconnaissance. The Collection of Scientific Works of the National Academy of the National Guard of Ukraine, 1 (43), 130–144. https://doi.org/10.33405/2409-7470/2024/1/43/307934
19. Makhmudov, F., Privalov, A., Privalov, A., Kazakevich, E., Bekbaev, G., Boldinov, A. et al. (2024). Mathematical Model of the Process of Data Transmission over the Radio Channel of Cyber-Physical Systems. Mathematics, 12 (10), 1452. https://doi.org/10.3390/math12101452
20. Luat, P. N., Taparugssanagorn, A., Kaemarungsi, K., Phoojaroenchanachai, C. (2024). Spatial Simultaneous Functioning-Based Joint Design of Communication and Sensing Systems in Wireless Channels. Applied Sciences, 14 (12), 5319. https://doi.org/10.3390/app14125319
21. Kumar, P., Saxena, V. (2024). Nested Levels of Hybrid Cryptographical Technique for Secure Information Exchange. Journal of Computer and Communications, 12 (02), 201–210. https://doi.org/10.4236/jcc.2024.122012
22. Mikoni, S. V. (2023). Approach to assessing the level of intelligence of an information system. Ontology of Designing, 13 (1), 29–43. https://doi.org/10.18287/2223-9537-2023-13-1-29-43
23. Ramsden, J. (2023). The Transmission of Information. Bioinformatics, 75–91. https://doi.org/10.1007/978-3-030-45607-8_7
24. Laue, F., Jamali, V., Schober, R. (2023). RIS-Assisted Device Activity Detection With Statistical Channel State Information. IEEE Transactions on Wireless Communications, 22 (12), 9473–9487. https://doi.org/10.1109/twc.2023.3271365
25. Vähä-Savo, L., Veggi, L., Vitucci, E. M., Icheln, C., Degli-Esposti, V., Haneda, K. (2023). Analytical Characterization of a Transmission Loss of an Antenna-Embedded Wall. https://doi.org/10.36227/techrxiv.170244520.01558910/v1
26. Elzinga, R., Janssen, M. J., Wesseling, J., Negro, S. O., Hekkert, M. P. (2023). Assessing mission-specific innovation systems: Towards an analytical framework. Environmental Innovation and Societal Transitions, 48, 100745. https://doi.org/10.1016/j.eist.2023.100745
27. Kramer, G. (2023). Information Rates for Channels with Fading, Side Information and Adaptive Codewords. Entropy, 25 (5), 728. https://doi.org/10.3390/e25050728

28. dos Santos, A., Barros, M. T. C. de, Correia, P. F. (2015). Transmission line protection systems with aided communication channels – Part II: Comparative performance analysis. Electric Power Systems Research, 127, 339–346. https://doi.org/10.1016/j.epsr.2015.05.010
29. Enquist, M., Ghirlanda, S., Lind, J. (2023). Acquisition and Transmission of Sequential Information. The Human Evolutionary Transition, 167–176. https://doi.org/10.23943/princeton/9780691240770.003.0012
30. Menezes, T. S., Barra, P. H. A., Dizioli, F. A. S., Lacerda, V. A., Fernandes, R. A. S., Coury, D. V. (2023). A Survey on the Application of Phasor Measurement Units to the Protection of Transmission and Smart Distribution Systems. Electric Power Components and Systems, 52 (8), 1379–1396. https://doi.org/10.1080/15325008.2023.2240320
31. Ribeiro, E. P. A., Lopes, F. V., Silva, K. M., Martins-Britto, A. G. (2023). Assessment of communication channel effects on time-domain protection functions tripping times. Electric Power Systems Research, 223, 109589. https://doi.org/10.1016/j.epsr.2023.109589
32. Shmatko, O., Herasymov, S., Lysetskyi, Y., Yevseiev, S., Sievierinov, O., Voitko, T. et al. (2023). Development of the automated decision-making system synthesis method in the management of information security channels. Eastern-European Journal of Enterprise Technologies, 6 (9 (126)), 39–49. https://doi.org/10.15587/1729-4061.2023.293511
33. Herasymov, S., Tkachov, A., Bazarnyi, S. (2024). Complex method of determining the location of social network agents in the interests of information operations. Advanced Information Systems, 8 (1), 31–36. https://doi.org/10.20998/2522-9052.2024.1.04
34. Kozhushko, Ya., Karlov, D., Klimishen, O., Bortsova, M., Herasymov, S., Hrichanuk, O., Bykov, V. N. (2018). Comparison of the Efficiency of Some Images Superposition Algorithms Used in Aircraft Map-Matching Navigation Systems. 2018 IEEE 17th International Conference on Mathematical Methods in Electromagnetic Theory (MMET). https://doi.org/10.1109/mmet.2018.8460319
35. Fedushko, S., Molodetska, K., Syerov, Y. (2023). Analytical method to improve the decision-making criteria approach in managing digital social channels. Heliyon, 9 (6), e16828. https://doi.org/10.1016/j.heliyon.2023.e16828
36. Mookerjee, R., Samuel, J. (2023). Managing the security of information systems with partially observable vulnerability. Production and Operations Management, 32 (9), 2902–2920. https://doi.org/10.1111/poms.14015
37. Marabissi, D., Abrardo, A., Mucchi, L. (2023). A new framework for Physical Layer Security in HetNets based on Radio Resource Allocation and Reinforcement Learning. Mobile Networks and Applications, 28 (4), 1473–1481. https://doi.org/10.1007/s11036-023-02149-z
38. Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O., Korol, O., Milevskyi, S. et al.; Yevseiev, S., Khokhlachova, Yu., Ostapov, S., Laptiev, O. (Eds.) (2023). Models of socio-cyber-physical systems security. Kharkiv: PC TECHNOLOGY CENTER, 184. https://doi.org/10.15587/978-617-7319-72-5
39. Framework for assessing the current state of protection. Available at: http://skl.khpi.edu.ua/
40. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et al. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (105)), 6–19. https://doi.org/10.15587/1729-4061.2020.205702
41. Aragon, N., Barreto, P. S. L. M., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C. et al. (2020). BIKE: Bit Flipping Key Encapsulation. Available at: https://bikesuite.org/files/v4.1/BIKE_Spec.2020.10.22.1.pdf
42. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M. et al. (2018). CRYSTALS - Kyber: A CCA-Secure Module-Lattice-Based KEM. 2018 IEEE European Symposium on Security and Privacy (EuroS&P). https://doi.org/10.1109/eurosp.2018.00032
43. Supersingular Isogeny Key Encapsulation (2022). Available at: https://sike.org/files/SIDH-spec.pdf
44. HQC: Hamming Quasi-Cyclic An IND-CCA2 Code-based Public Key Encryption Scheme. NIST 4 th PQC Standardization Conference. Available at: https://csrc.nist.gov/csrc/media/Presentations/2022/hqc-update/images-media/session-4-gaborit-hqc-pqc2022.pdf