Methods of information systems protection

UDC 621.373.54 **doi:** https://doi.org/10.20998/2522-9052.2023.4.11

Nataliia Dzheniuk, Serhii Yevseiev, Bogdan Lazurenko, Oleksandr Serkov, Oleg Kasilov

National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine

A METHOD OF PROTECTING INFORMATION IN CYBER-PHYSICAL SPACE

Abstract. The subject of the study **is the** processes of ensuring the reliability and security of information in cyber-physical space. The **objective is to** develop recommendations for the implementation of a method of information security in cyber-physical space. The development is based on the technology of ultra-wideband signals circulating in wireless communication channels. The **task is to** ensure the stable and reliable operation of the airborne wireless mobile communication network, which is the main component of cyberspace and its most vulnerable link to destructive influences. **Methods** used: methods of analytical modelling and time-position pulse coding. The following **results were** obtained. It is shown that in order to ensure high quality of wireless network operation, it is necessary to expand its bandwidth, which is limited by the physical resource of the radio frequency spectrum. It is proposed to overcome this contradiction by applying the technology of ultra-wideband signals, the base of which is much larger than one. In this case, the information signal is emitted without a carrier frequency simultaneously in the entire frequency band, provided that the signal level is lower than the noise level. The method of positional-time coding is used, in which each information bit is encoded by hundreds of ultra-short chip pulses arriving in a certain sequence. In such wireless communication systems, the use of autocorrelation reception of modulated ultra-wideband signals is proposed. A comparative analysis has shown that the wireless network with the best reliability and noise immunity is the one where the time separation of the reference and information signals is applied. During the first half of the bit interval, the switch closes the transmitter output directly to the ultra-wideband signal generator, forming a reference signal. In the middle of the bit interval, the switcher switches the output to one of two possible positions depending on the signal "zero" or "one", forming the information part of the signal. **Conclusions.** Systems with autocorrelation reception and separate transmission of reference and information signals provide a high level of structural signal concealment, as well as reliable transmission of digital information, especially in conditions of interference.

Keywords: cyberphysical space; cybersecurity; ultra-wideband signal technology; mobile wireless network.

Introduction

The modern information and technological revolution are characterised by the factors of universal access to the global information space and widespread use of electronic information processing tools. At the same time, the scientific and methodological foundations of information influence on the individual and mass consciousness of humanity are constantly being developed with the introduction of mechanisms for reflecting these information influences on social, political and economic processes. The international standards on cybersecurity ISO/IEC 27032:2023 [1, 2] define the concepts of cyberspace and cybersecurity taking into account the trends in the development of the global Internet. ***Cyberspace is an*** environment that represents the consequences of the results of the interaction of people, software and services on the Internet through technologies, devices and networks connected to it, which do not exist in any physical form. The same standard defines cybersecurity through the concept of cyberspace. ***Cybersecurity*** is security in cyberspace [1, 2]. Recommendation X.1205 of ITU-T also defines cybersecurity through the concept of cyberspace and risk management. Moreover, the ISO/IEC 27032:2023 standard also defines the relationship of the term cybersecurity with network security, application security, Internet security and critical information infrastructure security. The standard provides a visualisation of the relationship between these different terms (Fig. 1). All these terms are united by the concept of ***information security. At the same time,*** cybersecurity is becoming an increasingly universal field, where a number of aspects, including beliefs, social influence, emotions in decision-making, determine the associated human vulnerability.

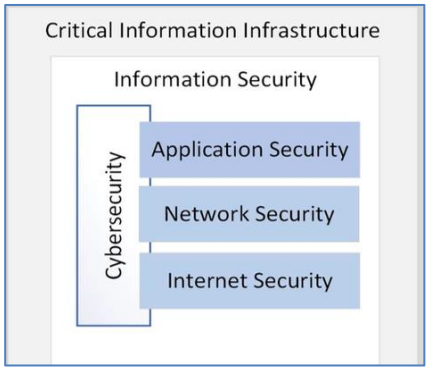

Fig. 1. The relationship between the term "cybersecurity" and the terminology of ISO/IEC 27032:2023 [1]

In the context of the formation of a high-tech society, social networks based on Internet services have become the most popular means of mass communication. At the same time, human and software vulnerabilities are used by attackers to breach the security of cyberspace, which makes cyber-physical systems a constant universal threat to cyberspace security.

The development of means of information influence in the technical sphere [3, 4] leads to significant complications in the use of widespread technical means of control and communication. At the same time, the use of existing hardware and software becomes virtually

impossible [5–9], which becomes a significant problem of ensuring the required level of security in cyberspace, in particular when using wireless mobile data transmission channels.

Thus, in order to successfully counteract targeted destructive information influences on the systems of state and military administration, it is necessary to develop and implement fundamentally new decision-making algorithms and secure technical means of control and communication.

The purpose of the study *is to* develop recommendations for implementing the method of information protection in cyber-physical space.

Analysis of information security methods in the face of interference

The presence of interference places additional demands on coding methods. A complex electromagnetic environment makes it difficult for a wireless network to operate efficiently, causing a failure in control systems and communication channels. This creates a real possibility of unauthorised access to information circulating in cyberspace.

Thus, from the security point of view, wireless communication channels are among the most vulnerable to interference and information distortion.

This is due to the fact that in addition to the destruction of information in the network, there is a possibility of its interception, distortion and addition of false information to wireless information channels in cyberspace [10–18].

A canonical digital system for transmitting or storing information in cyberspace includes a source, a receiver and an encoding device. The encoding device of a noise-resistant coding system receives information symbols, adds redundant symbols to them in such a way that most of the errors that occur during signal modulation and transmission over a channel with noise can be corrected.

To protect digital information from the effects of random and targeted interference, noise-resistant coding methods are widely used, the essence of which is the introduction of redundancy, which increases the amount of information and reduces the speed of its transmission.

In practice, Heminge, Golay, cyclic, block, and other codes are often used. In many wireless communication systems, the most common use is turbo codes and block codes, which combine noise-resistant coding with digital modulation. All error-correcting codes have a common idea, which is to add redundant symbols. They are added after the information ones, creating a code sequence or codeword that provides the redundancy needed to detect and correct errors.

Thus, coding allows to increase the noise immunity during data transmission and transmission efficiency, but at the expense of redundancy - an increase in the amount of service information.

Information security in wireless communication channels

It is usually assumed that in a communication channel, the additive noise count is added to the modulated noise. The noise counts are assumed to be independent of the noise source. This model is relatively easy to investigate and allows for the consideration of channels with Gaussian noise, channels with common Rayleigh fading, and a double symmetric channel. On the receiving side, the decoder uses redundant symbols to correct for errors introduced by the communication channel. In the error detection mode, the decoder behaves like an encoder received from the message channel and checks whether the calculated redundant symbols match the received ones. In the classical theory of error-correcting codes, a complex including a modulator, demodulator and a noisy signal propagation medium is called a discrete channel with no memory and an input and an output.

An example of such a channel is a system for transmitting binary signals over an additive white Gaussian noise (AWGN) channel, which is modulated as a binary symmetric channel with an error probability P equal to the error probability per bit for a binary signal in an AWGN channel.

$$P = Q\left(\sqrt{\frac{2E_b}{N_0}}\right),$$

where $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{z^2}{2}}\,\mathrm{dz}$, $x \geq 0$ is a Gaussian Q – error function; $\frac{E_b}{N_0}$ is the signal-to-noise ratio (SNR) per bit.

In 1974, Massey J.L [19] proposed to consider noise immune coding and modulation as a single unit. This ensures higher efficiency and greater energy gain from coding than the sequential application of noise immune coding and modulation.

The coding gain is defined as the difference between the signal-to-noise ratio of a coded system and a non-coded system, given the same transmission rate and error probability.

In digital wireless communication, the criterion of channel quality is the signal-to-noise ratio $\frac{E_s}{N_0'}$ (SNR signal - to - noise ratio), which relates the average signal power S to the average noise power N, where E_s is the energy of an information bit, which is the signal power S multiplied by the bit transmission time T_s, a N_0 is the spectral noise power, which is determined by the noise power N divided by the bandwidth W. It should also be noted that the bit transmission time T_s and its transmission rate R_s are mutually inverse $T_s = \frac{1}{R_s}$.

In digital communication systems, the dependence of the probability of a false bit P_s on the signal to noise ratio is a measure of the ***noise immunity of*** systems [3]:

$$\frac{E_s}{N_0} = \frac{S}{N}B,$$

where $B = WT_s$ is the signal base.

The analysis of this ratio shows that the main parameter that allows to ensure high noise immunity of the system is the signal base. With the expansion of the signal base $B >> 1$ it becomes possible to increase the information transmission rate by reducing the duration of the transmitted signal.

Thus, a certain redundancy is introduced into the transmitted signal, the value of which is determined by the spectrum expansion factor.

It is the presence of this redundancy that determines such properties of ultra-wideband systems as the ability to overcome the phenomena of multipath propagation of radio waves and efficient use of the spectrum when operating in a congested frequency range.

The difference between an ultra-wideband (UWB) communication system and a traditional narrowband system is the absence of a carrier frequency.

To transmit information in ultra-wideband systems, pulse signals with a very short pulse duration are used.

Such a signal, which has a small space-time volume, allows transmitting a large amount of information per unit of time and has a high level of noise immunity.

Thus, to transmit one bit of information, a narrowband system requires from 10 to 50 periods of carrier oscillation.

At the same time, the NSF communication system uses only one oscillation to transmit one bit of information.

Obviously, the use of NSF signals allows information to be transmitted at a speed that significantly exceeds the speed of traditional communications with high noise immunity.

Typically, the lower limit of the ratio of the spectral densities of the signal N_s and interference N_0 in – 7 dB at the receiver input guarantees its normal operation. This level corresponds to the following ratio:

$$\frac{N_s}{N_0} \le 0,2.$$

At the same time, the spectral density N_s is determined by the following relation:

$$N_s = \frac{P}{W} = \frac{E}{WT},$$

where P – signal power; W – signal spectrum width; E – signal energy; T – signal duration.

Thus, taking into account the above ratios, the criterion for meeting the protection requirements is the solution of the following inequality:

$$\frac{E}{WTN_0} \le 0,2.$$

According to the theory of potential noise immunity by V.A. Kotelnikov [20], the characteristics of an information signal depend on the ratio of the double signal energy E to the spectral density of the noise power N_0 and is equal to:

$$Q = \frac{2E}{N_0} = 2q_0 B,$$

where $q_0 = \frac{E/T}{N_0 W}$ is the ratio of the average signal power

$$p_{s0} = E/T$$

to the noise power

$$p_{N0} = N_0 W$$

at the receiver input, and $B = WT$ is the signal base.

In this case, the previously obtained ratio will take the following form:

$$, \frac{q^2}{WT} \le 0,4,$$

where the criterion itself is defined in terms of the signal-to-noise ratio at the receiver input q and the gain from processing WT.

Reducing the level of electromagnetic radiation is the main method of ensuring interference immunity and concealment of information in cyberspace. Therefore, the reduction of the information signal at the receiver input to the noise level ($q = 1$) is susceptible to ensuring steady-state interference-free operation. This determines the criterion for ensuring the interference immunity of wireless mobile communication systems in cyberspace ($WT \ge 2,5$). Thus, it is most appropriate to use the technology of ultra-wideband signals with a signal base $B \ge 2,5$. It should be noted that, according to the potential noise immunity theorem [20], the maximum possible reliability of signal reception can be ensured only by significantly exceeding the noise level. However, under the influence of natural and artificial interference, frequency redundancy leads to an increase in the probability of interference in the operating frequency band, distorting information signals in a wireless communication channel.

At the same time, due to the nonlinear processing of the additive mixture of signal and noise, according to the proven theorem of D. Slepian [21], when the width of the signal spectrum exceeds the width of the noise spectrum, reliable detection of an information signal is possible at any small signal-to-noise ratio.

The useful signal is extracted from the noise by correlating the received and reference signals. The correlator convolves the received signal with the reference signal to determine the time shifts of the received pulses relative to the reference. Thus, when receiving one, the correlation function is equal to +1, and when receiving 0, it takes the value -1. In all other cases, the correlation function is equal to 0.

The accumulation of a certain number of ultra-short pulses encoding each of the information bits in the receiver's correlator makes it possible to significantly increase the signal-to-noise ratio, providing the ability to transmit information in a wide frequency range well below the white noise level.

Thus, to ensure a high level of noise immunity of wireless information transmission channels in accordance with this criterion, it is possible only through the use of ultra-wideband signal technologies, combining the principles of noise-resistant coding and modulation as a whole.

At the same time, due to nonlinear digital processing, reliable detection of an information signal is carried out at any small signal-to-noise ratio. However, the physical limitation of the frequency spectrum has led to the need to use ultra-wideband communication technologies [22–25]. Thus, the wireless network with the best reliability and noise immunity is the one that uses time separation of the reference and information signals. Thus, during the first half of the bit interval, the switch closes the transmitter output directly to the ultra-wideband signal generator, forming a reference signal. In the middle of the bit interval, the switcher switches the output to one of two possible positions depending on the signal "zero" or "one", forming the information part of the signal [26–30].

In wireless cyberspace channels, the transmission medium is the physical path between the transmitter and the receiver. The most optimal range is between 1 and 10 GHz. This is because frequencies below 1 GHz are subject to significant interference from various industrial electronic devices. At the same time, at frequencies above 10 GHz, there is a large absorption of the useful signal by the transmission medium. Thus, the essence of ultra-wideband communication technology is the transmission of low-power coded pulses in a very wide frequency band without a carrier frequency. Usually, they do not emit a harmonic oscillation, but an ultra-short pulse. Typically, such signals are in the form of idealised Gaussian monocycles, with the bulk of the emission spectrum located in the frequency range from 1 to 10 GHz. Thus, when using a Gaussian monocycle with a duration of Δt from 2.0 nS to 0.1 nS, the bandwidth of the power spectrum will be from 500 MHz to 10 GHz, respectively. And the signal spectrum will occupy the entire frequency band from 0 to $\Delta F \approx 1/\Delta t$.

In this case, the information is encoded by means of time-position pulse modulation. Thus, the shift of a pulse relative to its reference position in the sequence forward sets a zero bit, and backward - a one bit. The shift time does not exceed a quarter of the pulse duration. One information bit is encoded by a sequence of many pulses (chips) per bit. To separate the information channels, the location of each pulse is additionally shifted by a time proportional to the current value of some pseudo-random sequence. The shift time is one to two orders of magnitude higher than the shift in time modulation. The use of short information chip pulses avoids inter-character distortion by dissipating the energy of the received pulse before the next one arrives. This also reduces the level of distortion of information signals caused by its multipath propagation. Such wireless communication systems use autocorrelation reception of modulated ultra-wideband signals [28].

A characteristic feature of the use of ultra-wideband signals is the low probability of detecting both the fact of establishing a communication channel and the impossibility of distorting information and intercepting it in cyberspace. The use of ultra-wideband signals in cyberspace requires the use of special antenna systems that allow for uniform coordination with the antenna system over a wide frequency band. For this purpose, an antenna with an open slot shape is usually used, which determines the frequency band for reception/ transmission. The energy pattern of such an antenna is characterised by a narrow main beam and the practical absence of side lobes. However, the preliminary formation of a Gaussian monocycle entering the antenna system causes difficulties in matching in a wide frequency band. This manifests itself in the form of re-reflection of individual signal components, which distorts the shape of the Gaussian monocycle. Therefore, the radiation pulse is formed directly in the antenna opening [16]. To do this, the information monopulse signal is split in half. A portion of the signal is inverted sequentially and delayed for a period of time equal to half the duration of the monopulse. Both mono-pulse signals are used to excite two TSA antennas located side by side on a single dielectric base. The electromagnetic fields of both monopulse signals interfere with the equivalent common aperture space of both antennas, creating a bipolar pulse electromagnetic field in it, while eliminating the time gap between the two parts of the radiated field, which is typical for a TSA antenna. Thus, such an antenna in an ultra-wideband communication system is capable of emitting and receiving both an ultra-short unipolar monopulse and a bipolar pulse information signal. This makes it possible to significantly increase (by 3-10 times) the range of propagation of pulsed electromagnetic signals. The design of the antenna unit for receiving/transmitting ultra-wideband signals is shown in Fig. 2.

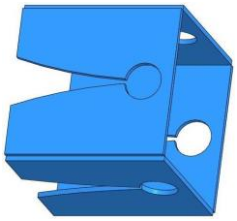

Fig. 2. Design of the antenna unit

Conclusions

The main method of ensuring interference protection and secrecy of information in cyberspace is to reduce the level of electromagnetic radiation. Over-the-air wireless networks are the most vulnerable link in cyberspace, where problems with information distortion, destruction and leakage are most likely to occur.

Information protection in cyber-physical space is realised through the use of ultra-wideband signals, the base of which is much larger than one. In this case, the information signal is emitted simultaneously without a carrier frequency in the entire frequency band, provided that the signal level is lower than the noise level. For emission and autocorrelation reception of modulated ultra-wideband signals, the design of an antenna unit capable of flickering polarisation was developed. Comparative analysis has shown that the best reliability and noise immunity is provided by a wireless network with time separation of reference and information signals. It ensures a high level of structural signal concealment and reliable transmission of digital information, especially in the face of interference.

REFERENCES

1. (2023), *Standard ISO/IEC 27032:2023. Cybersecurity. Guidelines for Internet security*, Released:28.06.2023, available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-2:v1:en
2. (2008), *ITU-T X.1205:2008. Cybersecurity overview*, Geneva: ITU-T, 2008. 162 p., available at: www.itu.int/ITU-T
3. Kravchenko V.I. and Serkov O.A. (2022), Radioelectronic means of struggle, suppression and force defeat, a monograph, "Madrid", Kharkiv, 422 p. (in Ukrainian), ISBN 978-617-8254-00-1.
4. Kovalenko, A. and Kuchuk, H. (2022), "Methods to Manage Data in Self-healing Systems", *Studies in Systems, Decision and Control*, Vol. 425, pp. 113–171, doi: https://doi.org/10.1007/978-3-030-96546-4_3
5. Yevseiev, S., Milevsky, S., Bortnik, L., Voropay, A., Bondarenko, K. and Pogasiy, S. (2022), Socio-Cyber-Physical Systems Security Concept. *4th International Congress on Human-Computer Interaction, Optimisation and Robotic Applications*, 9-11 June 2022, Ankara, Turkey, doi: https://doi.org/10.1109/HORA55278.2022.9799957
6. Kovalenko, A., Kuchuk, H., Kuchuk, N. and Kostolny, J. (2021), "Horizontal scaling method for a hyperconverged network", *2021 International Conference on Information and Digital Technologies* (IDT), Zilina, Slovakia, doi: https://doi.org/10.1109/IDT52577.2021.9497534
7. Yaloveha, V., Hlavcheva, D., Podorozhniak, A. and Kuchuk, H. (2019), "Fire hazard research of forest areas based on the use of convolutional and capsule neural networks*", 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering*, UKRCON 2019 – Proceedings, doi: http://dx.doi.org/10.1109/UKRCON.2019.8879867
8. Kuchuk, G., Nechausov, S. and Kharchenko, V. (2015), "Two-stage optimization of resource allocation for hybrid cloud data store", *International Conference on Information and Digital Technologies*, *Zilina*, pp. 266-271, DOI: http://dx.doi.org/10.1109/DT.2015.7222982
9. Kuchuk, G.A., Akimova, Yu.A. and Klimenko, L.A. (2000), "Method of optimal allocation of relational tables", *Engineering Simulation*, Vol. 17(5), pp. 681–689.
10. Mozhaev, O., Kuchuk, H., Kuchuk, N., Mykhailo, M. and Lohvynenko, M. (2017), "Multiservice network security metric", *2nd International Conference on Advanced Information and Communication Technologies*, AICT 2017 – Proceedings, pp. 133–136, doi: https://doi.org/10.1109/AIACT.2017.8020083
11. Lee E., A. (2015), "The past, present and future of cyber-physical systems: a focus on models", *Sensors*, Basel, Switzerland, Vol. 15(3), pp. 4837–4869, doi: https://doi.org/10.3390/s150304837
12. Kuchuk, N., Mozhaiev, O., Mozhaiev, M. and Kuchuk, H. (2017), "Method for calculating of R-learning traffic peakedness", *2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology*, PIC S and T 2017 – Proceedings, pp. 359–362, doi: https://doi.org/10.1109/INFOCOMMST.2017.8246416
13. Ayass, T., Coqueiro, T., Carvalho, T., Jailton, J., Araújo, J. and Francês R. (2022), "Unmanned aerial vehicle with handover management fuzzy system for 5G networks: challenges and perspectives", *Intell Robot*, Vol. 2(1), pp. 20–36, doi: https://dx.doi.org/10.20517/ir.2021.07
14. Datsenko, S. and Kuchuk, H. (2023), "Biometric authentication utilizing convolutional neural networks", *Advanced Information Systems*, Vol. 7, no. 2, pp. 87–91, doi: https://doi.org/10.20998/2522-9052.2023.2.12
15. Dun, B., Zakovorotnyi, O. and Kuchuk, N. (2023), "Generating currency exchange rate data based on Quant-Gan model", *Advanced Information Systems*, Vol. 7, no. 2, pp. 68–74, doi: https://doi.org/10.20998/2522-9052.2023.2.10
16. Mammadov, F. K. (2023), "New approach to book cipher: web pages as a cryptographic key", *Advanced Information Systems*, Vol. 7, no. 1, pp. 59–65, doi: https://doi.org/10.20998/2522-9052.2023.1.10
17. Petrovska, I. and Kuchuk, H. (2023), "Adaptive resource allocation method for data processing and security in cloud environment", *Advanced Information Systems*, Vol. *7*, No. 3, pp. 67–73, doi: https://doi.org/10.20998/2522-9052.2023.3.10
18. Zuo, Z., Liu, C., Han, Q.-L. and Song, J. (2022), "Unmanned Aerial Vehicles: Control Methods and Future Challenges", *IEEE/CAA Journal of Automatica Sinica*, Vol. 9, No. 4, pp. 601–614, doi: https://dx.doi.org/10.1109/JAS.2022.105410
19. Massey J.L. (1974), "Coding and Modulation in Digital Communications", *Proc. Int. Zurich Seminar on Dig Comm*., Zurich, Switzerland, pp. E2(1)–E2(4), available at: https://www.isiweb.ee.ethz.ch/archive/massey_pub/pdf/BI511.pdf
20. Klen, K. S. (2022), *Electronic systems. Lecture notes*, Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, 240 p., available at: https://ela.kpi.ua/bitstream/123456789/52115/1/Electronic_Systems_lecture_notes.pdf
21. Slepian, D. (1952), "Some comment on the Detection of Gaussian Signals in Gaussian Noise", JRE Transactions on Information Theory, No. 2, pp.65-68. doi: https://dx.doi.org/10.1109/TIT.1958.1057443
22. Serkov A., Kravets V., Yakovenko I., Churyumov G., Tokariev V. and Namnan W. (2019), "Ultra-Wideband Signals in Control Systems of Unmanned Aerial Vehicles", (DESSERT'2019), pp. 25–28, Leeds, United Kingdom, June 5-7, doi: https://dx.doi.org/10.1109/DESSERT.2019.8770039
23. Aleksandrov, Y., Aleksandrova, T., Kostianyk, I., and Morgun, Y. (2023), Selection of the set of allowable values of the variable parameters of the stabilizer of a complex dynamic object", *Advanced Information Systems*, Vol. *7*, No. 3, pp. 5–12, doi: https://doi.org/10.20998/2522-9052.2023.3.01
24. Serkov, A., Breslavets, V., Breslavets, J. and Yakovenko, I. (2023), "The influence of a potential barrier on the mechanisms of excitation of own fluctuations in radio products in conditions of exposure to electromagnetic radiation", *Advanced Information Systems*, Vol. 7, no. 1, pp. 36–40, doi: https://doi.org/10.20998/2522-9052.2023.1.06
25. Serkov, A.A., Lazurenko, B.A., Trubchaninova, K.A. and Horiushkina A.E. (2020), "Security Improvement Techniques for mobile applications of Industrial Internet of Things", *IJCSNS International Journal of Computer Science and Network Security*, Vol. 20, No. 5, pp. 145–149, available at: http://paper.ijcsns.org/07_book/202005/20200519.pdf
26. Jammine, A., Serkov A., Lazurenko, B. and Nait-Abdesselam, F. (2023), "The Order of Formation of Information Signals in IIoT", *IJCSNS International Journal of Computer Science and Network Security*, Vol. 23, No. 3, pp. 139–143, available at: http://paper.ijcsns.org/07_book/202303/20230314.pdf
27. Mukhin, V., Kuchuk, N., Kosenko, N., Kuchuk, H. and Kosenko, V. (2020),"Decomposition Method for Synthesizing the Computer System Architecture", *Advances in Intelligent Systems and Computing*, AISC, vol. 938, pp 289–300, doi: https://doi.org/10.1007/978-3-030-16621-2_27

28. Serkov, O.A., Lazurenko, B.O., Pevnev, V.Y., Tkachenko, V.A. and Kharchenko, V.S. (2021), *Method of information transmission by ultra-wideband pulse signals*, Ukrainian Patent for Invention No. 123519 U IPC H04B 1/69, H04B 7/00, Published on 14.04.2021, Bulletin No. 15.
29. Panchenko, S.V., Lazurenko, B.O., Serkov, O.A., Trubchaninova, K.A. and Goryushkina, A.E. (2020), *Method of receiving digital binary signals in noise conditions*, Patent of Ukraine for utility model No. 145319 U IPC H04B 1/06, published on 25.11.20, Bulletin No. 22.
30. Panchenko, S.V., Serkov, O.A., Trubchaninova, K.A., Kurtzev, M.S. and Lazurenko, B.O.(2019), *Ultra-wideband antenna with flickering polarisation and a method of its excitation*, Patent of Ukraine for invention No. 126475 U IPC H01Q 21/06, H01Q 13/08, Published on 13.10.22, Bulletin No. 41, application No. a 2019 08720 dated 19.07.2019.

Надійшла (received) 30.08.2023
Прийнята до друку (accepted for publication) 26.10.2023

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Дженюк Наталія Володимирівна –доцент кафедри “Системи інформації ім. В.О. Кравця”, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Nataliia Dzheniuk –Associate Professor of Department of Information Systems named after V. A. Kravets, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: natalidzh16@gmail.com; ORCID ID: https://orcid.org/0000-0003-0758-7935.

Євсеєв Сергій Петрович – доктор технічних наук, професор, завідувач кафедри кібербезпеки, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Serhii Yevseiev – Doctor of Technical Science, Professor, Head of the Department of Cybersecurity, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: serhii.yevseiev@gmail.com; ORCID ID: https://orcid.org/0000-0003-1647-6444.

Лазуренко Богдан Олександрович – аспірант кафедри “Системи інформації ім. В.О. Кравця”, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Bogdan Lazurenko – postgraduate of Department of Information Systems named after V. A. Kravets, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: torroloco789@gmail.com; ORCID ID: https://orcid.org/0000-0002-1914-7091.

Серков Олександр Анатолійович – доктор технічних наук, професор, професор кафедри “Системи інформації імені В.О. Кравця”, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Oleksandr Serkov – Doctor of Technical Science, Professor, Professor of Department of Information Systems named after V.A. Kravets, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: Oleksandr.Serkov@khpi.edu.ua; ORCID ID: https://orcid.org/0000-0002-6446-5523.

Касілов Олег Вікторович – кандидат технічних наук, доцент, професор “Системи інформації імені В.О. Кравця”, Національний технічний університет "Харківський політехнічний інститут", Харків, Україна;
Oleg Kasilov – Candidate of Technical Sciences, Associate Professor, Professor of Department of Information Systems named after V. A. Kravets, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine;
e-mail: oleg.kasilov@khpi.edu.ua; ORCID ID: https://orcid.org/0000-0002-8524-2345.

Спосіб захисту інформації в кіберфізичному просторі

Н. В. Дженюк, С. П. Євсєєв, Б. О. Лазуренко, О. А. Серков, О. В. Касілов

Анотація. Предметом дослідження є процеси забезпечення надійності та безпеки інформації в кіберфізичному просторі. **Мета** – розробити рекомендації щодо впровадження методу захисту інформації в кіберфізичному просторі. В основі розробки лежить технологія надширокосмугових сигналів, що циркулюють по бездротових каналах зв'язку. Завдання полягає в тому, щоб забезпечити стабільну та надійну роботу мережі бездротового мобільного повітряного зв’язку, яка є основною складовою кіберпростору та його найбільш вразливою ланкою до дестабілізуючих впливів. **Використані методи**: методи аналітичного моделювання та часопозиційного імпульсного кодування. Були отримані **наступні результати**. Показано, що для забезпечення високої якості роботи бездротової мережі необхідно розширити її смугу пропускання, яка обмежена фізичним ресурсом радіочастотного спектру. Це протиріччя вирішується застосуванням технології надширокосмугових сигналів, база яких набагато більша за одиницю, при цьому інформаційний сигнал випромінюється без несучої частоти одночасно у всій смузі частот за умови, що рівень сигналу нижче шуму. рівень. У цьому випадку використовується метод позиційно-часового кодування, при якому кожен біт інформації кодується сотнями надкоротких імпульсів-чіпів, які подаються в певній послідовності. У таких бездротових системах зв'язку пропонується використовувати автокореляційний прийом модульованих надширокосмугових сигналів. Порівняльний аналіз показав, що найкраща надійність і завадостійкість досягається в бездротовій мережі, де використовується часове розділення опорного та інформаційного сигналів. Таким чином, протягом першої половини бітового інтервалу комутатор закриває вихід передавача безпосередньо на генератор надширокосмугового сигналу, формуючи опорний сигнал. У середині бітового інтервалу комутатор перемикає вихід в одне з двох можливих положень в залежності від сигналу «нуль» або «одиниця», формуючи інформаційну частину сигналу. **Висновки.** Системи з автокореляційним прийомом і роздільною передачею опорного та інформаційного сигналів забезпечують високий рівень приховування структурного сигналу, а також надійну передачу цифрової інформації, особливо за наявності перешкод.

Ключові слова: кіберфізичний простір; кібербезпека; технологія ультраширокосмугового сигналу; мобільна бездротова мережа.