КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ/ CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION (CIIP)

DOI: 10.18372/2225-5036.30.18603

SOCIOCYBERPHYSICAL SYSTEM WIRELESS AIR NETWORK TOPOLOGY SYNTHESIS MODEL

Nataliia Dzheniuk, Serhii Yevseiev, Stanislav Milevskyi, Natalya Voropay, Roman Korolov

National Technical University "Kharkiv Polytechnic Institute", Ukraine

Nataliia DZHENIUK, Associate Professor
Date and place of birth: 1960, Dzhankoj, AR Krym.
Education: Kharkiv Polytechnic Institute, 1983.
Position: associate professor of department of information systems named after V. O. Kravets, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: network, cybersecurity.
Publications: more than 40 scientific publications, including monographs, text-books, articles and patents.
E-mail: natalidzh16@gmail.com.
Orcid ID: 0000-0003-0758-7935.

Serhii YEVSEIEV, Doctor of Technical Science, Professor
Date and place of birth: 1969, Khartsyzsk, Donetsk region.
Education: Kharkov Military University, 2002.
Position: Head of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: protection of information resources, post-quantum cryptography, security in socio-cyber-physic.
Publications: more than 300 scientific publications, including monographs, text-books, articles and patents.
E-mail: serhii.yevseiev@gmail.com.
Orcid ID: 0000-0003-1647-6444.

Stanislav MILEVSKYI, Candidate of Economic Sciences, Associate Professor
Date and place of birth: 1979, Murom, Volodymyr region.
Education: Kharkiv National University of Economics, 2001.
Position: associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: information protection in sociocyberphysical systems.
Publications: more than 60 scientific publications, including monographs, text-books, articles and patents.
E-mail: milevskiysv@gmail.com.
Orcid ID: 0000-0001-5087-7036.

Natalya VOROPAY, Candidate of Technical Sciences, Associate Professor
Date and place of birth: 1984, Alushta, Crimean region.
Education: National Technical University "Kharkiv Polytechnic Institute", 2008.
Position: associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.
Scientific interests: protection models in sociocyberphysical systems.
Publications: more than 30 scientific publications, including monographs, text-books, articles.
E-mail: voropay.n@gmail.com.
Orcid ID: 0000-0003-1321-7324.

Roman KOROLOV, Candidate of Technical Sciences, Associate Professor
Date and place of birth: 1974, Krasnyi Luch, Luhanska oblast.
Education: Kharkov Military University, 1999.
Position: associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine
Scientific interests: information protection in socio-cyberphysical systems.
Publications: more than 80 scientific publications, including monographs, textbooks, articles and patents.
E-mail: korolevrv01@ukr.net.
Orcid ID: 0000-0002-7948-5914.

Abstract. *The subject of study is the process of building a Cyber-Physical System mobile communication network. The goal is to develop recommendations for the construction of a CPS mobile communication network – a system that works effectively in a complex interfering electromagnetic environment. The development is based on the technology of ultra-broadband signals that circulate in control and communication channels with the integration of elements of artificial intelligence into its structure. The task is to ensure stable and safe operation of the CPS wireless mobile communication network. Techniques used: Analytical, Time-Position-Pulse Coding, and Fuzzy Logic Inference techniques for network handover decision making. The following results were obtained. Recommendations for building a wireless mobile communication system have been developed. It is shown that in order to obtain high interference resistance of control and communication channels and to protect information from interception, ultra-broadband communication technology should be used, which allows providing large volumes and speeds of information transmission. Moreover, it is recommended to use the results of data processing in a fuzzy decision-making system during service transfer between mobile network nodes in conditions of interference. Conclusions. The use of channels with an ultra-wide frequency band makes it possible to practically increase the number of control and communication channels in a wireless mobile CPS. Predistribution between channels of orthogonal codes realizes the process of control and communication without interception of information and mutual interference. Thus, the use of the method of temporal position-pulse coding prevents the occurrence of intersymbol distortions of encoding ultra-short pulses. At the same time, the level of distortion of information signals, which is caused by its multipath propagation, also decreases, which guarantees the security of information in the system. The use of a fuzzy system during decision-making in the case of service handover between mobile network nodes makes it possible to dynamically change the topology of the CPS network in real time and maintain high quality of service.*

Keywords: *sociocyberphysical systems, mobile wireless network, cyber security, ultra-broadband technology, fuzzy system.*

Introduction

The term "cyber-physical systems" appeared around 2006 when it was proposed by Helen Gill at the National Science Foundation in the United States. [1]. Cyber-Physical Systems (CPS) are complex distributed systems that are controlled by computer algorithms and perform computational procedures in their distributed environment with feedback. CPS is an information technology concept that involves the integration of computing resources into any physical objects. It is a technology that connects the physical world with the informational world and focuses on the fundamental intellectual problem of combining the engineering traditions of the cyber and physical worlds [1].

The structural model of the CPS system is shown (fig. 1). Social disintegration brought a decisive shift to the worldview and social culture of electronic communication.

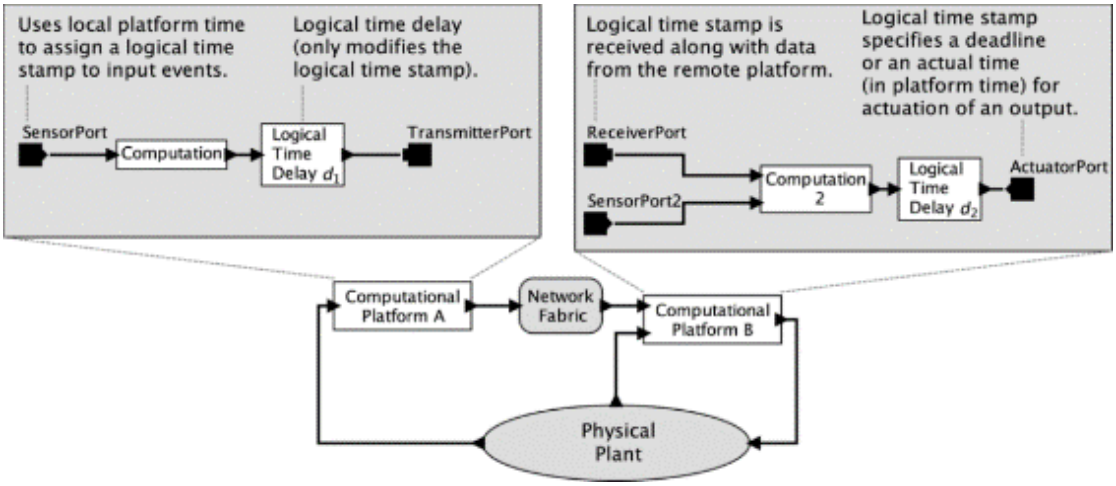

Fig. 1. Structural model of CPS [1]

The use of intellectual means in traditional life leads to the separation of reality and mind, which makes human reality itself virtual, which is under the uncontrolled domain of virtuality. Technological change is leading to uncontrolled confusion and widespread access to digital telecommunications. Cyber security is becoming an

increasingly versatile field, where a whole range of aspects, including beliefs, social influence, emotions in decision-making, and determines the related human vulnerability. These vulnerability mechanisms and attack methods are used to justify the success of attacks on socio-cyber-physical systems [2].

Thus, an attack on socio-cyber-physical systems is a type of attack in which an attacker uses human and/or software vulnerability to breach cyber security [2]. In this way, socio-cyber-physical systems turn into a permanent universal security threat (fig. 2). The model (program) and the hardware it runs on are mixed, so the intended behavior does not occur in the model, but rather occurs in its implementation. Advanced methods of socio-cyber-physical systems have revolutionized data and information management. However, for their implementation, more efficient means for data processing, interpretation and reuse should be used.

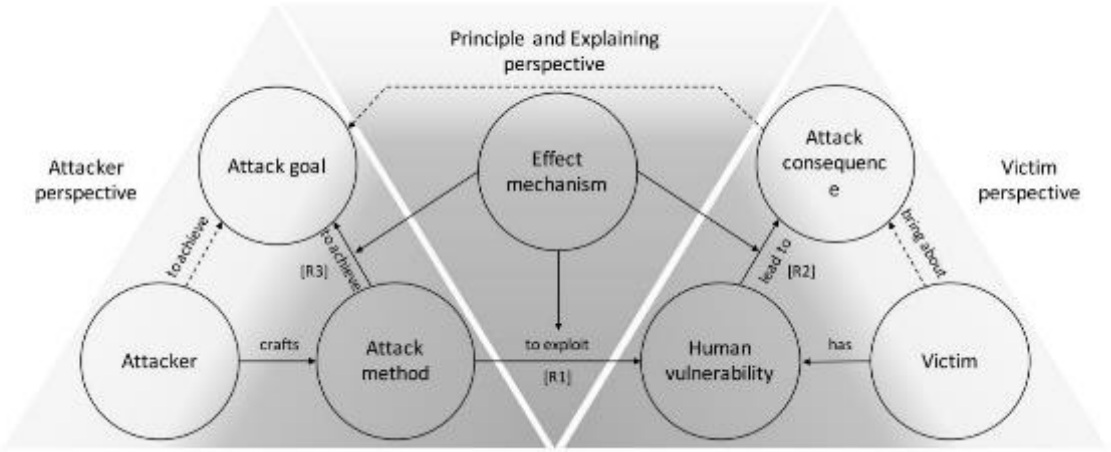

Fig. 2. Conceptual model of CPS attack

Because the data transmitted from CPS and the information obtained from the processing results often generate different forms of data that require different levels of security.

The security pyramid, created in 2013 by security expert David J. Bianco, explains the problems of CPS threats (fig. 3).

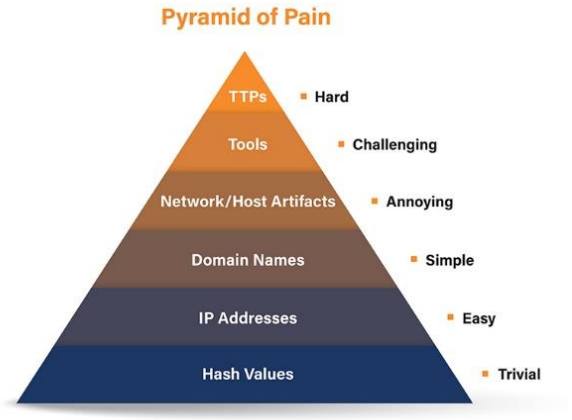

Fig. 3. Conceptual model of CPS attack

It ranks, in ascending order, the list of indicators used to determine the actions of attackers, as well as the effort and complexity of finding each indicator for security analysis. The closer we are to the top, the harder it is to identify and turn that information into something actionable.

The main part of the study

From the point of view of security of CPS, the most vulnerable is the wireless mobile network, which is its main link. 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 the CPS.

Existing terrestrial wireless mobile communications technologies are unable to meet the stringent Quality of Service (QoS) standards expected of terrestrial networks. An alternative solution for expanding the coverage area and improving the quality of service is the deployment of several unmanned aerial vehicles (UAVs), each of which has a switching module, thanks to which they coordinate and interact with each other. Moreover, to fully ensure global communication in the next-generation wireless air network, it should be combined with terrestrial networks. This creates a hybrid wireless network that is capable of providing users with quality services anywhere and anytime. The basis of the hybrid wireless network is the aerial mobile peer-to-peer network FANET (Flying Ad Hoc Network) [3], which is a set of UAVs connected to each other by communication channels, external ground-based control points and ground mobile base stations yakuza At the same time, each UAV is able to directly broadcast information from the source to the user. A distinctive feature of this system is the concentration in a limited space of a large number of sources of electromagnetic radiation, which have a diverse amplitude-frequency range. The presence of such a complex electromagnetic situation complicates the high-quality operation of the network, causing failures in control systems and communication channels. At the same time, there is a real possibility of unauthorized access to information circulating in the network, and the probability of unauthorized interception of the UAV control channel also increases. The purpose of the work is to develop recommendations for the construction of a CPS wireless mobile communication network - a system that functions effectively in the conditions of a complex electromagnetic environment.

CPS network operation features in the complex electromagnetic environment conditions

According to the classification of the international standard IEC 61000-2-13, the interference electromagnetic

environment, which in free space exerts a destabilizing electromagnetic influence on the control and communication channels of the UAV, is more than 100 v/m of the electric component or 0.27 A/m of the magnetic component [4].

Connecting individual devices to the FANET network turns it into a complex dynamic system that functions in conditions of significant a priori uncertainty and randomly organizes the interaction of its various components. Due to the high mobility of UAVs in the FANET network, the fulfillment of electromagnetic compatibility requirements becomes a critical factor. At the same time, their movement in three-dimensional space complicates the mobility problem, since the movement leads to the disconnection of current users and requires updating the locations of all nodes in the network. Each UAV must know the location of other devices in real time, which requires the need to obtain reliable and stable communication between devices to maintain an appropriate level of quality of service (QoS) and quality of experience (QoE) [5].

Analysis of the network functioning makes it possible to determine the following features of it, in particular, the possibility of automatic movement of UAVs according to a pre-set program and interception of information in digital radio channels.

Moreover, the use of UAV housings made of composite materials makes them practically invisible to radar stations. At the same time, the presence of a complex of tools for controlling UAVs and potentially vulnerable places in data transmission protocols, software of control systems, data transmission and navigation creates a threat to the security of the wireless network. It depends on the structure of the network and its location in space, the location of users, the length of the access line, the physical and geographical conditions of the area, as well as the possibility of providing the user with several information transmission routes at the same time.

CPS Network Security

The most widespread means of ensuring the integrity of information are methods of tamper-resistant coding and concealment of the transmission fact.

The interference immunity of the UAV control system and communication channel means the maximum level of electromagnetic interference at which it maintains the proper quality of work. Coding in information and control channels helps to increase immunity. In the presence of external influencing factors, the use of well-known algebraic, cascade, convolution and other codes, as well as their decoding methods, requires redundancy, which leads to a decrease in the speed of information transmission. At the same time, the need to increase the speed of control signals transmission in wireless channels requires the use of the widest possible frequency range. Thus, known methods of encoding information and control signals in UAV wireless channels do not provide the necessary immunity, which requires the development of new approaches to solving this problem. The physical limitation of the frequency spectrum led to the need to use ultra-broadband communication technologies [6-8].

In wireless control and communication channels, the transmission medium is the physical path between the transmitter and the receiver. At the same time, the characteristics of the information transmission medium are less important than the bandwidth of the radiation signal. The most common and optimal range is the range from 1 to 10 GHz.

This is due to the fact that at frequencies less than 1 GHz there is significant interference from various industrial electronic devices. At the same time, at frequencies higher than 10 GHz, there is a large absorption of the useful signal by the transmission medium.

When using ultra-broadband information transmission, relatively narrow-band information signals with an effective spectrum width Δf are deliberately converted to an ultra-wideband signal (UWS) with an effective spectrum width ΔF under the conditions of preservation of the total energy E of the signal. In this case, the spectral energy density of the channel signal is deliberately reduced by $\Delta F/\Delta f$ times and will be $\Delta E/\Delta F$. And the base of the channel signal also increases accordingly by $\Delta F/\Delta f$ times. The basis of an ultrashort pulse signal is the product of the duration of the signal by the width of its spectrum. The most simple and convenient method of expanding the signal base is the direct expansion of the frequency spectrum. At the same time, the higher the frequency of use, the higher the potential data transfer rate.

Thus, ultra-wideband communication technologies consist in the transmission of low-power coded pulses in a very wide frequency band without a carrier frequency. Usually, not a harmonic oscillation is emitted, but an ultrashort pulse, the duration of which is within 0.2 - 2.0 nS, and the period of the pulse sequence is 10 - 100 nS. Usually, such signals have the form of idealized Gaussian monocycles, the main part of the radiation spectrum of which is located in the frequency range from 1 to 10 GHz. Thus, the use of 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 the control and communication channels, information is coded by time-positional-pulse modulation. Thus, the shift of the pulse relative to its reference position in the sequence forward sets a zero bit, and backward - one, and the shift time does not exceed a quarter of the duration of the pulse. One information bit is encoded by a sequence of many pulses (chips) per bit. To separate information communication channels, the location of each pulse is additionally shifted by a time proportional to the current value of some pseudo-random sequence. Moreover, the shift time is one or two orders of magnitude higher than the shift during time modulation. Each of the communication channels is assigned its own expanding code combination, the elements of which make up the orthogonal basis and set the channel code. And the restoration of the information message is carried out only if the receiver and transmitter use the same channel code, which increases the immunity of signals in the wireless control and communication system. Extraction of the useful signal against the background of noise and interference is carried out by correlating the received and reference signals. The correlator performs convolution of the received signal with the reference signal. It is an ideal detector for determining the time shifts of the received pulses relative to the reference ones. Thus, when accepting a unit, the correlation function is equal to +1, and when accepting a zero, it takes the value –1. In all other

cases, the correlation function is equal to 0. Given that one information bit is represented by, for example, 200 ultrashort chips, when they coincide, they are accumulated in the integrator of the receiver. Thus, the information bit will be detected even if 99 chips out of 200 are lost. The useful signal is removed from the noise, which in this case significantly exceeds its level in the signal-to-noise ratio. Thanks to this method, the very fact of transmission is concealed. In addition, the use of a series of ultrashort pulses to encode an information bit makes it possible to get rid of intersymbol interference. This is due to the fact that before the approach of the next ultrashort pulse from a series of coding chips, the energy of the previous chip has time to completely dissipate.

UAV trajectory optimization in the CPS network

The combination of indicators of the mobility level, the direction of movement of the UAV, the bandwidth of the communication channels and the indication of the strength of the received signal make up an integral indicator for making a decision on the transfer of services between devices. Thus, it is advisable to apply an intelligent method of information transmission and service due to the integration of artificial intelligence elements into a wireless mobile network [9].

The optimal routing algorithm provides support for the necessary indicators of immunity and quality of information transmission and UAV control functions. A feature in solving the problem of improving the immunity of a wireless network is the method of controlling the trajectories of individual UAVs in order to create a network configuration that minimizes the impact of radio-electronic interference. In the implementation of this method, in particular, the organization of the exit of individual network elements from the interference zone is provided for the transmission of information to the base station on terrestrial networks. The basis of the organization of a wireless network is the creation of a network resistant to the effects of radio-electronic interference both within the network and by external ground-based control points. At the same time, they realize the possibility of direct information interaction in the middle of the network and external ground control points with the use of NSS signals.

The limitation regarding the formation of the optimal route of information transmission in the middle of the network is not to exceed the permissible value of the probability of error in the transmission of information between the subscriber and the user along the appropriate route using ultra-broadband technologies.

The network topology model is a graph, which is represented by a number of vertices - communication nodes. A communication channel directly connecting network nodes i and j creates a branch $\beta^{(i,j)}$. The quality of data transmission by the network branch $\beta^{(i,j)} \in M$ characterizes the probability of an error in the transmission of information in the network:

$$P^{(i,j)} = P_a^{(i,j)}(0)\, P_{fa}^{(i,j)} + P_a^{(i,j)}(1)\, P_{ms}^{(i,j)}, \qquad (1)$$

where $P_a^{(i,j)}(0)$, $P_a^{(i,j)}(1)$ - a priori probabilities regarding the presence and absence of a signal; $P_{fa}^{(i,j)}$ and $P_{ms}^{(i,j)}$ - corresponding false alarm and missed signal probabilities.

By ordering the set of edges included in the route, $\boldsymbol{\mu}(i, j) = (\beta_1, \beta_2, \ldots \beta_R)$ between subscriber i and user j, we get the probability of an error on the route $\boldsymbol{\mu}(i, j)$:

$$P[\boldsymbol{\mu}(i, j)] = 1 - \Pi^{R}_{r=1}(1-P(\beta_r)), \qquad (2)$$

where R – the number of branches of the graph included in the route $\boldsymbol{\mu}(i, j)$; $P(\beta_r)$ – the probability of an error in the transmission of information along an edge β_r.

At the same time, the compliance of the probability of an error in the transmission of information along the route with the necessary permissible value is used as an indicator of the efficiency of the network.

$$P[\mu(i, j)] \le P^{ep}, \qquad (3)$$

where P^{ep} – the assumed value of the error probability.

The high mobility of elements of the CPS network increases the delay in the transmission of information and complicates the decision-making process of connecting the device to the current or another access point and creating an optimal route by transferring service to communication channels with higher quality.

The criterion for making a handover decision is usually the strength of the received signal. However, this single criterion for routing information in a network can lead to service failures because it can direct the route to a congested part of the network with low bandwidth. Thus, for a guaranteed continuous connection and quality of service in a mobile wireless network, a complex criterion should be applied, which additionally takes into account both the direction and speed of UAV movement, the bandwidth of communication channels, and the level of their battery charge. Applying a fuzzy system to handover decision making with a logical inference system allows evaluation and generation of input for decision making. In fuzzy systems, results are classified between 0 and 1. A value of 0 means absolute impossibility, and a value of 1 means full correlation. The output of the fuzzy system indicates the probability that the mobile device is starting the handover process. In the general case, if the user has high mobility and a high level of received signal strength, the process of switching to another route will not occur.

An additional means of increasing the level of network immunity in this case is the management of the trajectories of individual UAVs in order to create a network configuration that minimizes the impact of interference. At the same time, it is advisable to choose the UAV most suitable for transferring control to it during movement with the organization of the exit of individual elements of the network from the zone of influence of radio-electronic interference for the transmission of information to the ground network.

In view of the application in the communication channels of the CPS network of UWS broadband technologies, when the useful signal is below the noise level, the quality criterion of the communication channel becomes simply the level of electromagnetic radiation, which, according to the developers of radio-electronic countermeasures systems, should exceed the useful signal by 30 dB [4]. Due to the high mobility of UAVs in the CPS network, the location update of all network nodes is a critical factor. Network devices need to know the locations of other elements in real time. Thus, in addition to using GPS, which sends information about its location on average once per second. UAVs must send their location data at intervals shorter than GPS, which requires high-bandwidth communication channels.

Conclusions. The use of signal processing technology in the control and communication channels of the CPS network allows to obtain a number of advantages that cannot be obtained by traditional methods. In particular, this applies to the improvement of the quality indicators of wireless network channels. The expansion of the communication channel bandwidth and the transition to broadband channels allows for an almost unlimited increase in the number of communication channels. Having previously distributed the modulation codes between the channels, their operation is carried out without intercepting the UAV control, information and mutual interference. An important criterion characterizing the effectiveness of wireless mobile communication systems is a high potential specific density of data and information transmission. It is determined by the value of the total speed of data transmission per one square meter of the working area, which is currently of the order of 1 Mbit/s/m2. The use of short information pulses-chips avoids intersymbol distortions due to the dissipation of the energy of the received pulse until the arrival of the next one. At the same time, the level of distortion of information signals caused by its multipath propagation also decreases.

A characteristic feature inherent in control and communication systems based on UWS is the low probability of detecting both the very fact of temporarily establishing communication channels and the impossibility of distorting information\ and intercepting UAV control channels. It is also possible for both traditional narrow-band communication systems and systems with UWS to work simultaneously without interference in the same frequency range. This is due to the fact that the levels of information and control signals do not exceed the noise level in the working frequency range. At the same time, reducing the power and radiation level of electromagnetic fields makes it possible to guarantee the fulfillment of electromagnetic compatibility requirements at all stages of development and implementation of a wireless CPS mobile network.

Automatic control of the individual UAVs trajectories allows to dynamically create a network configuration in real time that minimizes the impact of interference. At the same time, in real time, the most suitable UAV is automatically selected and control is transferred to it, with the organization of its exit from the zone of radio-electronic interference influence in order to transmit information to the terrestrial network.

References

[1]. Lee E. A. (2015). The past, present and future of cyber-physical systems: a focus on models. Sensors (Basel, Switzerland), 15(3), 4837-4869. https://doi.org/10.3390/s150304837.

[2]. Z. Wang, L. Sun, H. Zhu, Defining Social Engineering in Cybersecurity, IEEE Access, vol. 8, pp. 85094–85115, 2020, https://doi:10.1109/access.2020.2992807.

[3]. Ayass T, Coqueiro T, Carvalho T, Jailton J, Araújo J, Francês R. Unmanned aerial vehicle with handover management fuzzy system for 5G networks: challenges and perspectives. Intell Robot 2022;2(1): 20-36. https://dx.doi.org/10.20517/ir.2021.07.

[4]. Kravchenko V. I., Serkov O. A. Radio-electronic countermeasures, strangulation and forceful injury: monograph / V. Kravchenko, O. Serkov. H.: "View. "Drukarnia Madrid", 2022. 422 p. fig. 108., tab. 15. ISBN 978-617-8254-00-1.

[5]. Unmanned Aerial Vehicles: Control Methods and Future Challenges / Zongyu Zuo, Cunjia Liu, Qing-Long Han, Jiawei Song // IEEE /CAA Journal of Automatica Sinica, Vol. 9, No/ 4/ Fhril. 2022 pp. 601-614.

[6]. Ultra-Wideband Signals in Control Systems of Unmanned Aerial Vehicles / Serkov A., Kravets V., Yakovenko I., Churyumov G., Tokariev V., Namnan W. // (DESSERT'2019), pp. 25-28, Leeds, United Kingdom, June 5-7, 2019, doi:10.1109/DESSERT.2019.8770039.

[7]. Security Improvement Techniques for mobile applications of Industrial Internet of Things / A.A. Serkov, B.A. Lazurenko, K.A. Trubchaninova, A.E. Horiushkina // IJCSNS International Journal of Computer Science and Network Security. VOL, 20 No. 5, pp. 145-149. http:// paper.ijcsns.org/07_book/202005/20200519.pdf.

[8]. Serkov O.A., Lazurenko B.O., Pevnev V.Ya., Tkachenko V.A., Kharchenko V.S. The method of transmitting information over wide space pulse signals // Patent of Ukraine for winemaking No. 123519 U IPC H04B 1/69, H04B 7/00, Publ. 04/14/2021, Bull. No. 15.

[9]. Method of Increasing Security of Spatial Intelligence in the Industrial Internet of Things Systems / Trubchaninova K., Serkov A., Tkachenko V., Kharchenko V., Pevnev V., Doukas N. // 24th International Conference on Circuits, Systems, Communications and Computers (CSCC'2020), Platanias Chania Grete Island, Greece, July 19-22, 2020, pp. 283-289. doi:10.1109/CSCC49995.2020.00058.

УДК 004.056:004.7:004.9

Дженюк Н., Євсеєв С., Мілевський С., Воропай Н., Корольов Р. Модель синтезу топології соціокіберфізичної системи бездротової повітряної мережі

***Анотація**. Предметом дослідження є процес побудови мережі мобільного зв'язку кіберфізичної системи. Мета – розробити рекомендації щодо побудови мережі мобільного зв'язку CPS – системи, яка ефективно працює в складному електромагнітному середовищі, що створює перешкоди. В основі розробки лежить технологія ультраширокосмугових сигналів, що циркулюють по каналах управління та зв'язку з інтеграцією в її структуру елементів штучного інтелекту. Завдання – забезпечити стабільну та безпечну роботу мережі бездротового мобільного зв'язку CPS. Методи, що використовуються: аналітичний, часово-позиційно-імпульсний кодування та методи нечіткої логіки для прийняття рішень щодо передачі мережі. Були отримані наступні результати. Розроблено рекомендації щодо побудови системи бездротового мобільного зв'язку. Показано, що для отримання високої перешкодостійкості каналів управління та зв'язку та захисту інформації від перехоплення необхідно використовувати технологію надширокосмугового зв'язку, яка дозволяє забезпечити великі обсяги та швидкості передачі інформації. Крім того, рекомендується використовувати результати обробки даних у нечіткій системі прийняття рішень під час передачі послуг між вузлами мобільної мережі в умовах*

перешкод. Висновки. Використання каналів з надширокім діапазоном частот дозволяє практично збільшити кількість каналів управління та зв'язку в бездротовій мобільній CPS. Попередній розподіл між каналами ортогональних кодів реалізує процес управління та зв'язку без перехоплення інформації та взаємних перешкод. Таким чином, використання методу часового позиційно-імпульсного кодування запобігає виникненню міжсимвольних спотворень кодування ультракоротких імпульсів. При цьому також знижується рівень спотворення інформаційних сигналів, який викликається його багатопроменевим поширенням, що гарантує безпеку інформації в системі. Використання нечіткої системи під час прийняття рішень у разі передачі послуг між вузлами мобільної мережі дає можливість динамічно змінювати топологію мережі CPS у режимі реального часу та підтримувати високу якість обслуговування.

***Ключові слова**: соціокіберфізичні системи, інформаційна безпека, кібербезпека, безпека інформації, класифікатор інформаційних загроз соціокіберфізичних систем, багатоконтурна система захисту інформації.*

Дженюк Наталія Володимирівна, доцент кафедри інформаційних систем імені В. О. Кравця, Національний технічний університет «Харківський політехнічний інститут», Україна.
Nataliia Dzheniuk, associate professor of department of information systems named after V. O. Kravets, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Євсеєв Сергій Петрович, доктор технічних наук, професор, завідувач кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут», Україна.
Serhii Yevseiev, doctor of technical science, professor, head of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Мілевський Станіслав Валерійович, кандидат економічних наук, доцент кафедри кібербезпеки Національного технічного університету «Харківський політехнічний інститут», Україна.
Stanislav Milevskyi, candidate of economic sciences, associate professor of cybersecurity department National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Воропай Наталія Ігорівна, кандидат технічних наук, доцент кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Україна.
Natalya Voropay, candidate of technical sciences, associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Корольов Роман Володимирович, кандидат технічних наук, доцент кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», Україна.
Roman Korolov, candidate of technical sciences, associate professor of cyber security department, National Technical University "Kharkiv Polytechnic Institute", Ukraine.

Отримано *3 лютого 2024 року,* затверджено редколегією *1 квітня 2024 року*