Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society

Valeriy Dudykevych[1], Galyna Mykytyn[1], Taras Stosyk[1], and Pavlo Skladannyi[2]

[1] *Lviv Polytechnic National University, 12 Stepan Bandera str., Lviv, 79000, Ukraine*
[2] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine*

Abstract

This work proposes a platform for the safe intellectualization of society's infrastructure "objects—technologies—security" in the functional space "selection—information exchange—processing—management" by profiles—confidentiality, integrity, accessibility for "smart ecological monitoring", "smart education", "smart grid", "smart transportation system" and other subject areas. The platform of safe intellectualization of objects is revealed by the concept of a multilevel security system of cyber-physical systems, which is the basis for building a paradigm of security of physical space, communication environment, and cyberspace. A system model of security of the three-layer architecture of the Internet of Things based on the concept of "object—threat—protection" was built. An adaptive model of security of wireless communication environment of cyber-physical systems for segments of society's infrastructure was analyzed. The presented common methodology of security of intellectualization processes allows to implementation of complex security systems of technologies for the safe functioning of objects of the infrastructure of society.

Keywords

Intellectualization, information security, platform, cyber-physical system, security concept, internet of things, system model, adaptive model.

1. Introduction

Formulation of the problem. The world is unfolding processes of intellectualization in the space of Industry 4.0, which include: the introduction of intelligent technologies in various segments of the infrastructure of society, as a tool for the functioning of intellectual objects; and the development of security methodologies [1, 2]. Cyber-Physical Systems (CPSs) and the Internet of Things (IoTs) in their composition, as the main technologies of the fourth industrial revolution, provide a life cycle of information in automated processes of industrial facilities from selection and exchange, analysis, and processing to intelligent decision support for facility management in smart city infrastructure [3].

Analysis of the latest research. The literature [4–7] discusses approaches to ensuring the security of cyber-physical systems, in particular, as technologies for the functioning of critical infrastructure. The effectiveness of the processes of intellectualization of the infrastructure of society is determined by the functioning of the Internet of Things three-layer architecture [8], each layer of which is characterized by a different set of threats [9–10]. The functionality of the layer of perception is supported by a set of devices and sensors that extract information from the objects of physical space. For example, MEMC sensors—2JCIE-BL, BPS240, and BME680 are used to extract information from physical objects in intelligent technologies for ecological monitoring of environmental components. The network layer transmits information for further processing. Application layer—implements data processing and user interaction. Many scientific publications are devoted to the security of wireless communication technologies, and

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL: vdudykev@gmail.com (V. Dudykevych); cosmos-zirka@ukr.net (H. Mykytyn); taras.r.stosyk@lpnu.ua (T. Stosyk); p.skladannyi@kubg.edu.ua (P. Skladannyi)
ORCID: 0000-0001-8827-9920 (V. Dudykevych); 0000-0003-4275-8285 (H. Mykytyn); 0000-0001-7896-9792 (T. Stosyk); 0000-0002-7775-6039 (P. Skladannyi)

especially sensor networks, particularly in [11–12] the authors covered: aspects of information protection in wireless communication technologies GSM, CDMA, WiMAX, and LTE based on the system model; features of Zigbee, Wi-Fi, and Bluetooth wireless sensor security technologies based on the "object—threat—protection" concept and the OSI model; security features of CPS "Wi-Fi—Bluetooth—cloud computing—IoT;" specifics of the complex security system of CPS on "iPhone—Wi-Fi, Bluetooth—sensors." Foreign works [13—16] have developed modern trends in information security in wireless technologies. In particular, architecture, protocols, threats, and approaches to solving security problems, including elements of applied cryptography [17].

Development of approaches to the security of intellectualization technologies based on the structure "objects—CPSs—threats—protection" which will ensure the safe functioning of objects in the space "information selection—exchange—processing—management."

The purpose of the work is to create a single platform for the safe intellectualization of society's infrastructure based on the concept of a Complex Security System (CSS) of cyber-physical systems and system security of the Internet of Things.

2. A Platform for the Safe Intellectualization of Society's Infrastructure Based on Cyber-Physical Systems

The global challenges of the "Horizon Europe" program and the main directions of Ukraine's development in the space of the National Industry Strategy 4.0 allow for identification segments of implementation of intelligent technologies—ecological monitoring of environmental components, education, energy systems, transportation systems that interact and systematically form "smart infrastructure" of the country with such characteristics as interoperability, virtualization, decentralization, real-time, service orientation, modularity. In the context of "smart ecology," an important aspect is the system of local and global dynamic ecological monitoring of environmental parameters, in particular research ecological monitoring "program—IT—a methodology for assessing water quality", which is introduced in the case of accidental pollution when control and operational monitoring do not meet the needs of ecological objectives aimed at normalizing the state of environmental components.

To monitor the quality of environmental components, such as water objects, intelligent systems for measuring their parameters have been implemented, including intelligent geographic information systems and remote sensing of the Earth using the Landsat-8 satellite to obtain multispectral images of the surface water layer in the thermal infrared channel, and, on this basis, determining its temperature as one of the main indicators of quality [18]. Highly mobile laboratories of ecological monitoring are effectively used for monitoring complex parameters of water, soil, and air, the main components of which are: an intelligent information system for express measurement of basic parameters of the state of the environment; a set of autonomous instruments for measuring specific environmental parameters; equipment for sampling water, soil, air; measuring drone; GPS positioning system; GSM wireless communication system; laboratory management system [19]. The National Informatization Program in Ukraine directs the development of information support centers for higher education institutions and the introduction of secure information and communication technologies, including servers, personal computers, websites, virtual learning environments, electronic archives, and wireless communication technologies.

The concept of digital transformation of education and science in Ukraine provides for the consideration of foreign experience and implementation through the following areas: (1) effective use of digital technologies in the educational process; optimization of management, regulation, and monitoring processes, which involve the creation of a digital educational environment equipped with computers, multimedia hardware, modern communication technologies; (2) professional development of research and teaching staff of educational institutions in the context of digital competencies; development of a system of standards in the field of digital technologies and standards of higher education, which are harmonized with international ISO standards. Smart grid and "smart transportation systems" are very relevant segments of the country's

industrial infrastructure today, which include the implementation of secure intelligent cyber-physical systems and the use of cryptographic means to securely exchange information in wireless communication technologies, including efficient encryption algorithms to ensure the security of information resources of users.

Consider a platform for the safe intellectualization of society's infrastructure, which is based on the CPS and the concept of "object—threat—protection", and is multilevel (Fig. 1). The first level is functional, which ensures the operability of the system "components of the infrastructure—operating technologies/"smart objects" ($O_{1\text{-}N(R,S,T)}$)—Cyber-Physical Systems ($CPS_{1\text{-}N(R,S,T)}$)" according to the segments: N—"Smart Ecology" (SEc), R—"Smart Education" (SEd), S—"Smart Energy" (SEn), T—"Smart Transportation System" (STS). The second level is the integration of the CPS levels "Internet of Things ($IoT_{1\text{-}N(R,S,T)}$)—Wireless Technologies ($WT_{1\text{-}N(R,S,T)}$)—Information Systems ($IS_{1\text{-}N(R,S,T)}$)" and integration of one-tier components. The third level—processes of "Information Selection ($S_{1\text{-}N(R,S,T)}$)/control—Transmission/Reception ($T_{1\text{-}N(R,S,T)}/R_{1\text{-}N(R,S,T)}$)—Processing Information ($P_{1\text{-}N(R,S,T)}$)/Management ($M_{1\text{-}N(R,S,T)}$)". The fourth level—threats to information security at the structural and functional level of the CPS ($a_{1\text{-}N}$–$b_{1\text{-}N}$ –$c_{1\text{-}N}$ (SEc); $d_{1\text{-}R}$–$e_{1\text{-}R}$–$f_{1\text{-}R}$ (SEd); $g_{1\text{-}S}$–$h_{1\text{-}S}$ –$i_{1\text{-}S}$ (SEn); $k_{1\text{-}T}$–$l_{1\text{-}T}$–$m_{1\text{-}T}$ (STS)). Fifth level—hardware and software security technologies in the profiles "confidentiality—integrity—accessibility" ($A_{1\text{-}N}$–$B_{1\text{-}N}$ –$C_{1\text{-}N}$ (SEc); $D_{1\text{-}R}$–$E_{1\text{-}R}$–$F_{1\text{-}R}$ (SEd); $G_{1\text{-}S}$–$H_{1\text{-}S}$–$I_{1\text{-}S}$ (SEn); $K_{1\text{-}T}$–$L_{1\text{-}T}$–$M_{1\text{-}T}$ (STS)). In Fig. 1, the structure of the safe intellectualization platform is shown only for the "smart ecology" segment.

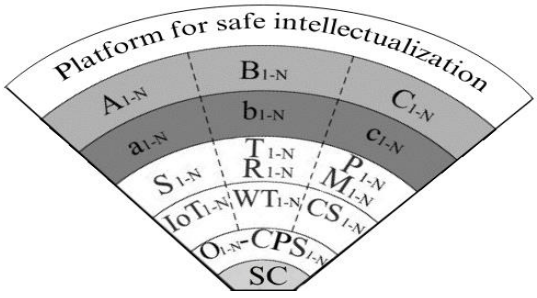

Figure 1: Structure of the platform of safe intellectualization of infrastructure based on CPS

3. The Concept of a Complex Security System of Cyber-Physical Systems

Consider a multilevel cyber-physical system and the concept of multilevel information security. The multilevel hierarchical structure of CPS is presented in Fig. 2: Physical Space (PS)—the Internet of Things that interacts with physical objects/devices in which sensors are built; Communication Environment (CE)—wireless and wired communication technologies, cloud technologies; Cyberspace (CS)—information systems, information resources, information processes.

The multilevel structure of the CPS operates at the plane of two channels—measuring and control. A network of sensors based on MEMS technologies that combine microelectronic and micromechanical systems, as well as actuators in the process of monitoring infrastructure objects generate information (selection, measurement, registration) about the status of their parameters, which is transmitted wirelessly from the physical space of CPS for storage, processing, analysis and management. In cyberspace, based on the analysis of processed information, comparison with the normalized parameters of the object, and detection of deviations, the computer system decides to manage the state of the object through the communication environment and physical space of the CPS.

The concept of a complex security system of the CPS is based on the paradigm of "multilevel CPS—multilevel information security" and a system approach, which consists of applying the principles of hierarchy, structure, and integrity, which provide grounds for creating a CSS of cyber-physical systems in the segment of optimal combination of regulatory, organizational, informational, hardware and software at the stages of the safe life cycle of information.

The concept of a complex security system is determined by the structure: classification of threats—the formation of security criteria—the creation of a model of multilevel CSS of CPS—the choice of method for assessing the security of the cyber-physical system. The basis for building a multilevel CSS is universal platform "threats—profiles—tools"; information protection model in CPS "CPS level—STRIDE threat—security profile—security technology"; normative document ND TZI 3.7-001-99 "Methodical instructions on development of the technical task on the creation of the complex system of protection of the information in the automated

system", which regulates: requirements for the CSS in terms of protection against unauthorized access; requirements to the CSS in terms of protection against information leakage through technical channels.

The complex security system of the PS, connected to the Internet of Things, is based on the concept of "object—threat—protection" according to the segments: physical devices, in particular MEMS sensors (IEEE 2700-2014), and built-in actuators.

The complex security system of the CE is created based on the concept of "object—threat—protection" according to the segments: wireless communication technologies (ZigBee, Wi-Fi, Bluetooth, WiMAX, LTE, etc. (DSTU ISO/IEC 7498)); cloud technologies (DSTU ISO/IEC 17788:2017, NIST); wired communication technologies (networks based on coaxial (DSTU EN 50117) and fiber-optic cables (DSTU IEC 60794)).

The complex security system of the CS is formed based on the concept "object—threat—protection" by the segments—information resources: accidental, intentional threats—hardware and software protection; information systems: accidental, intentional threats—hardware and software multilevel protection; information processes: accidental, intentional threats—hardware, software protection (DSTU ISO/IEC 15408).

The IS management of a multilevel CPS is based on the methodology of applying methods, in particular, basic (ISO/IEC TR 13335-3:2007) and IS management models, including the "plan-perform—check—act" model (ISO/IEC 27001: 2010) to adjust the structure of the complex security system and ensure the effectiveness of information protection.

The concept of a complex security system of the CPS is universal in the space of functional tasks of safe intellectualization of infrastructure objects—monitoring, forecasting, diagnostics, interpretation, identification, etc.

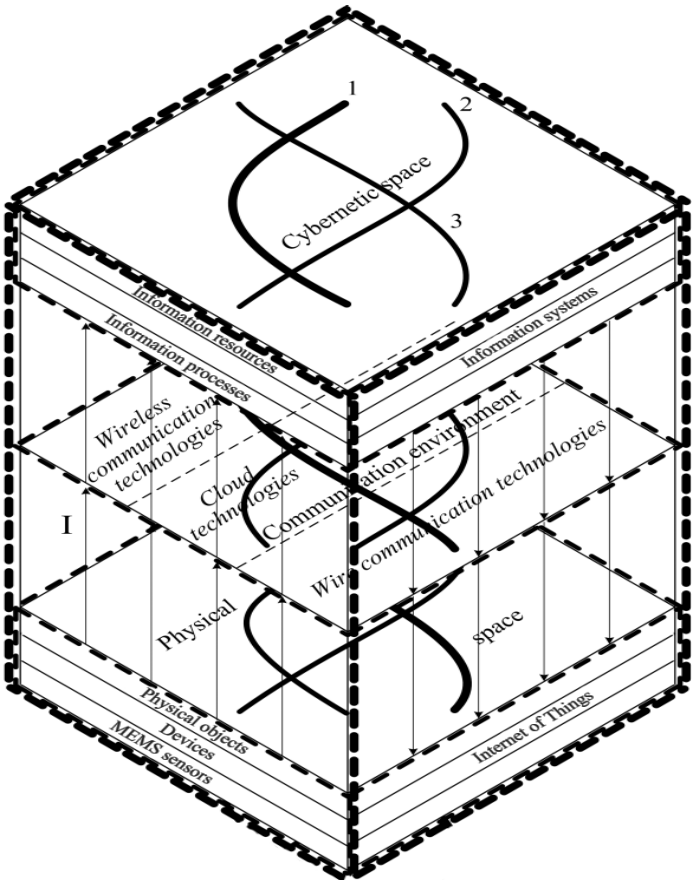

Figure 2: The structure of the concept of CSS of cyber-physical system in the context of integration levels

4. System Model of Security of the Three-Layer Architecture of the Internet of Things

One of the approaches to the safe functioning of the Internet of Things is to create a system model based on the concept of "object—threat—protection" and system principles—integrity, hierarchy, and structure.

The structure of the system model (Fig. 3): (1) at each layer of the architecture of the Internet of Things there are types of threats, which are also unfolded by their subcategories; (2) according to the layers of perception, network, application—the types of security technologies are presented and also unfolded by their subcategories. According to this structure, we give examples for each layer of the IoT: one threat and the variety of its subcategories; one security technology, deploying its functional implementation with a variety of tools [20].

Perception layer. This layer is characterized by the highest number of threats to the main security profiles (DSTU ISO/IEC 15408), as it is exposed to a set of threats related to the functional security of devices and sensors that interact with physical objects. Main threat—attacks on nodes (sensors and other devices that interact with the physical environment). Subcategories—destruction of the node (dealing damage to the device until its complete failure to disrupt the system and interrupt the process of collecting information), capture (usually carried out to gain access to sensitive information that can be stored on the device, and to be able to replicate node), cloning (replacement of the original device with third-party, programmed by an attacker and intended for unauthorized access to the network and transmission of false data) and jamming of the node (generating interference to prevent the transmission of information from the node to the network). At this layer, the key method of information protection is to ensure the physical security of the nodes, which is achieved by placing devices within the controlled area.

Network layer. Threat—network eavesdropping (interception of communications between devices in the network). Subcategories—passive (without direct intervention and change of information), active (attack "man in the middle", editing transmitted information), traffic analysis (listening to network communications without compromising data, to determine the location of nodes, routing structure). An important security technology is the use of Intrusion Detection Systems (IDS), which can be presented by Network (NIDS), Host (HIDS), and even Intrusion Prevention Systems (IPS).

Application layer. Threat—malware. Subcategories—common on the Internet of Things ransomware, spyware, trojans, and worms. One of the methods of protection of this layer is the organization of secure software development, which is implemented by three technologies: secure coding, static and dynamic code analysis, and explicit error checking of all internally developed software [21].

The criterion for selecting IS threats of the three-layer architecture of the Internet of Things presented in the system model is the degree of violation of functional security of infrastructure objects (systems), which makes it impossible to ensure their warranty and causes the functioning of systems in the space of their information and technical conditions: partially operational device (safe), inoperable (safe), inoperable (dangerous) (SOU-N NSAU 0060:2010). The criterion for choosing security technologies is the optimal effectiveness of counteracting the number of threats and their subcategories at each layer of the IoT [22].

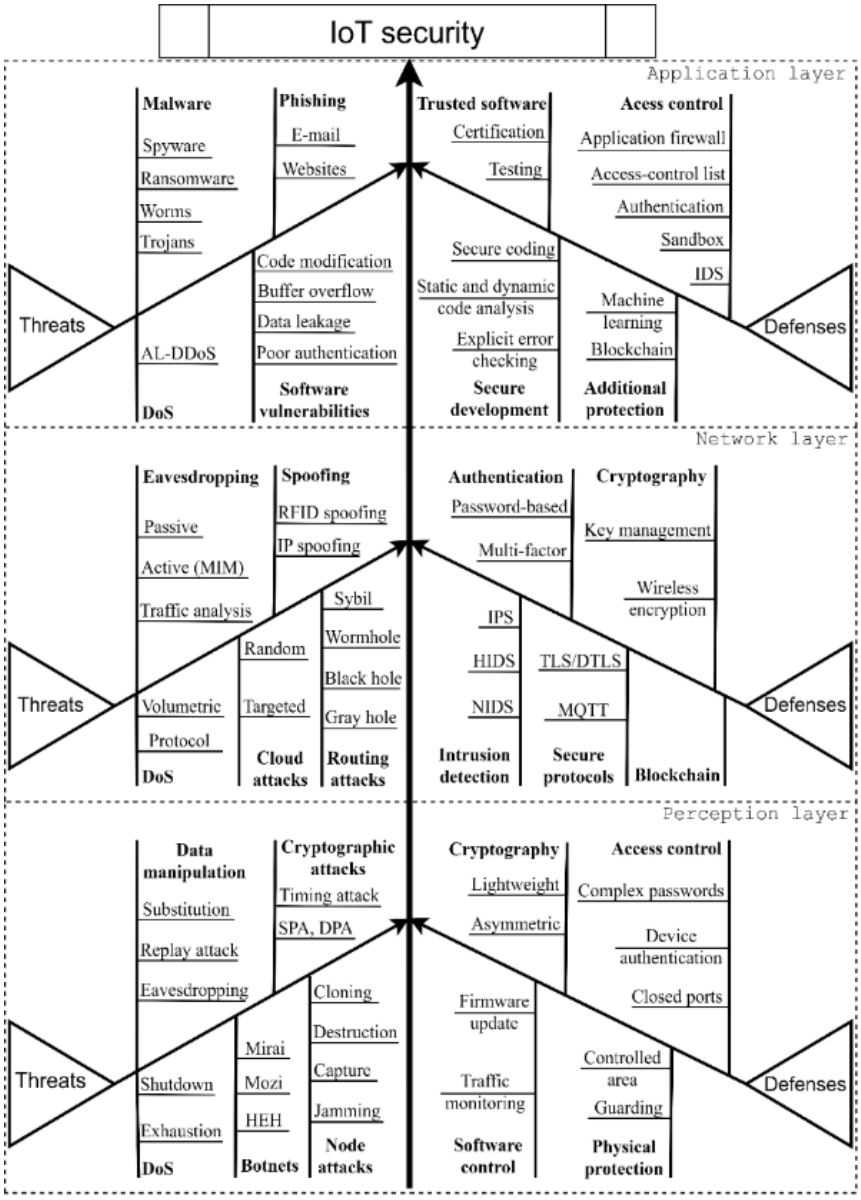

Figure 3: System model of security of the three-layer architecture of the Internet of Things

The system model of the IoT security is the basis for the formation of a complex security system, which can transform into different variants depending on the object of infrastructure, the types of threats, and information security technologies [23].

5. Adaptive Security Model of Wireless Communication Technologies

In the context of the development of IS technologies wireless sensor networks are relevant: (1) methods of modeling the functioning of sensor networks, in particular, the parameters of signals of information nodes as components of networks in anti-attack modes; (2) study of vulnerabilities of sensory subnets of the architecture of the Internet of Things under the influence of a set of attacks [24]. Current security trends for wireless sensor networks are developed in approaches based, in particular, on the use of RSA cryptosystem for secure exchange, three-factor authentication protocol, and machine learning algorithms [25, 26].

In the platform of infrastructure intellectualization (Fig. 1) wireless communication technologies are one of the functional levels of CPS, which is designed to exchange information between physical space (Internet of Things) and cyberspace (information system) in the process of

extracting information from physical objects and state management based on data processing, analysis and decision-making.

In the concept of a complex security system of multilevel CPS (Fig. 2), wireless communication technologies are a segment of a secure communication environment. To ensure the secure exchange of information in the multilevel CPS, the adaptive model of security of wireless communication technologies is relevant (Fig. 4), which is also related to the system model of IoT security at the network layer (Fig. 3).

The adaptive model is characterized by: 1) a single functional structure of information protection—external security, internal security, and information security policy; 2) a specialized structure of the CSS based on the concept "object—threat—protection", due to a set of threats to the infrastructure of society: "smart environment", "smart education", "smart energy", "smart transportation system".

The external level of security of wireless technologies is provided by the system of protection of the perimeter of the object of intellectualization, which has the appropriate protection criteria and degree of complexity. The main perimeter security technologies aimed at counteracting the threat of unauthorized access to the resources of the object of intellectualization are video surveillance cameras, access control systems, electronic locks, and biometric recognition systems. The internal level of security of wireless technologies is determined by the categories of threats, classified according to various criteria, including threats by the nature of occurrence: objective (natural), and subjective (artificial); among the subjective threats are accidental and intentional. The main tasks of IS of intelligent technologies are connected with counteraction to intentional (targeted) threats.

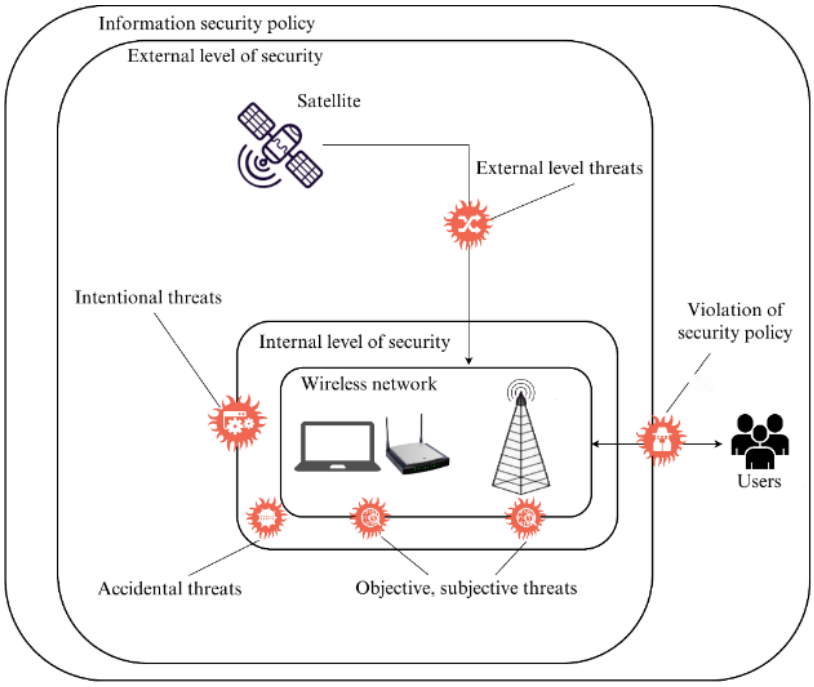

Figure 4: Adaptive security model of wireless communication technologies

6. Conclusions

A platform for the safe intellectualization of society's infrastructure is proposed, which is the basis for creating a conceptual approach to the safe selection of information, secure data exchange; safe handling, and condition management. The concept of CSS of the cyber-physical system—a tool for the intellectualization of objects, which is the basis for building security models of technologies of physical space, communication environment, and cyberspace under the influence of threats to confidentiality, integrity, and accessibility was created. The Internet of Things and wireless technologies security was developed at the level of system and adaptive models by probable threats, which ensures secure information exchange in a multilevel cyber-physical system.

References

[1] K. Schwab, The Fourth Industrial Revolution, Crown Publishing Group, (2017).

[2] B. Gajdzik, S. Grabowska, S. Saniuk, A Theoretical Framework for Industry 4.0 and Its Implementation with Selected Practical Schedules, Energies 14(4) (2021). doi: 10.3390/EN14040940.

[3] F. Khan, et al., Cyber Physical Systems: A Smart City Perspective, Int. J. Electrical Comput. Eng. 11(4) (2021) 3609–3616. doi: 10.11591/IJECE.V11I4.PP3609-3616.

[4] J.-P. Yaacoub, et al., Cyber-Physical Systems Security: Limitations, Issues and Future Trends, Microprocessors and Microsystems, 77 (2020) 103201. doi: 10.1016/j.micpro.2020.103201.

[5] H. Sandberg Cyber-Physical Security, Encyclopedia Syst. Control. (2020). doi: 10.1007/978-1-4471-5102-9_100112-1.

[6] I. Opirskyy, I. Tyshyk, V. Susukailo, Evaluation of the Possibility of Realizing the Crime of the Information System at Different Stages of TCP/IP, 4th International Conference on Advanced Information and Communication Technologies (AICT) (2021) 261–265. doi: 10.1109/AICT52120.2021.9628936.

[7] V. Maksymovych, et al., Simulation of Authentication in Information-Processing Electronic Devices Based on Poisson Pulse Sequence Generators, Electronics, 11(13) (2022). doi: 10.3390/electronics11132039.

[8] M. Lombardi, F. Pascale, D. Santaniello, Internet of Things: A General Overview between Architectures, Protocols and Applications, Information 12(2) (2021) 87. doi: 10.3390/info12020087.

[9] C.–K. Wu, Internet of Things Security, Advances in Computer Science and Technology, Springer (2021).

[10] N. Gupta, U. Garg, A Proposed IoT Security Framework and Analysis of Network Layer Attacks in IoT, Soft Computing: Theories and Applications. AISC 1380 (2021) 85–95. doi: 10.1007/978-981-16-1740-9_9.

[11] H. Mykytyn, Complex Security System of Cyber-Physical System "iPhone—Wi-Fi, Bluetooth—Sensors", Information Processing Systems 2(148) (2017) 84–87.

[12] V. Dudykevych V. B. ZigBee, Wi-Fi and Bluetooth Wireless Sensor Networks in Cyber-Physical Systems: the "Object—Threat—Protection" Concept Based on the OSI Model, Information Processing Systems 2(157) (2019) 114–120.

[13] W. Osterhage, Wireless Network Security: Second Edition, CRC Press (2018). doi: 10.1201/9781315106373.

[14] K. Sako, N. Tippenhauer, Applied Cryptography and Network Security, ACNS, Springer (2021). doi: 10.1007/978-3-030-78372-3.

[15] M. Chakraborty, et al., Trends in Wireless Communication and Information Security, LNEE 740, Springer (2021). doi: 10.1007/978-981-33-6393-9.

[16] R. Nazir, et al., Survey on Wireless Network Security, Arch. Comput. Methods Eng. (2021). doi: 10.1007/s11831-021-09631-5.

[17] V. Astapenya, et al., Last Mile Technique for Wireless Delivery System using an Accelerating Lens, in: 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (2020). doi: 10.1109/picst51311.2020.9467886.

[18] V. Zatserkovnyi, et al., Use of Technologies of Geographic Information Systems and Remote Sensing of the Earth for Monitoring of Water Objects, Science-Based Technologies 1(33) (2017) 78–88.

[19] V. Kropyvnytskyi, M. Pavlyshyn, V. Chumak, Highly Mobile Environmental Monitoring Laboratory. URL: https://ns-plus.com.ua/2017/06/13/vysokomobilna-laboratoriya-ekologichnogo-monitoryngu

[20] F. Kipchuk, et al., Investigation of Availability of Wireless Access Points based on Embedded Systems, in: 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (2019). doi: 10.1109/picst47496.2019.9061551.

[21] Z. Hu, et al., Bandwidth Research of Wireless IoT Switches, in: IEEE 15th International Conference on Advanced

Trends in Radioelectronics, Telecommunications and Computer Engineering (2020). doi: 10.1109/tcset49122.2020.2354922.

[22] V. Sokolov, et al., Method for Increasing the Various Sources Data Consistency for IoT Sensors, in: IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (2023) 522–526. doi: 10.1109/PICST57299.2022.10238518.

[23] I Kuzminykh, et al., Investigation of the IoT Device Lifetime with Secure Data Transmission, Internet of Things, Smart Spaces, and Next Generation Networks and Systems, vol. 11660 (2019) 16–27. doi: 10.1007/978-3-030-30859-9_2.

[24] M. Aleksander, et al., Information Security in the Environment of Wireless Sensor Networks: A Monograph, Publishing House Ivan Puluj TNTU (2016).

[25] S. Awan, et al., Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks, Sensors 22(1) (2022) 411. doi: 10.3390/s22020411.

[26] L. Zhu, H. Xiang, K. Zhang, A Light and Anonymous Three-Factor Authentication Protocol for Wireless Sensor Networks, Symmetry 14(1) (2022) 46. doi: 10.3390/sym14010046.