Paradigm of Safe Intelligent Ecological Monitoring of Environmental Parameters

Yuriy Bobalo[1], Valeriy Dudykevych[2], Galyna Mykytyn[3], Taras Stosyk[4]

[1,2,3,4] *Lviv Polytechnic National University, Stepana Bandery St, 12, Lviv, 79013, Ukraine*

Abstract

In the context of the development of the 7-year European Union scientific research initiative "Horizon Europe", the paradigm of ecological monitoring of the environment "intellectualization – information security" is proposed. The multilevel paradigm of safe ecological monitoring “intelligent cyber-physical systems (CPS) – integration of CPS levels – information processes of selection, processing, management – threats to information security (IS) – hardware and software security technologies” is a universal in structure and specialized in functionality for the natural environment “water – air – soil – forest”. The universal paradigm is revealed by the improved complex model of research monitoring of ecological parameters of water “program – intelligent technology (IT) and IS – methodology”. The informational security model of the three-layers structure of the Internet of Things based on the concept “object – threat – protection” provides secure interaction between sensors and devices for ecological monitoring of environmental parameters with computer systems. The created paradigm is the basis for the development of approaches to safe intellectualization of ecological monitoring of environmental components using intelligent systems and technologies to ensure basic safety profiles.

Keywords

Intellectualization, information security, ecological monitoring, intelligent cyber-physical system, paradigm, water, complex model of monitoring, Internet of Things, informational security model.

1. Introduction

Problem formulation. In the conditions of technological development of civilization, the complex of global problems of planetary scale is evolving. One of them is the safety of human life under the influence of natural and man-made threats. Public safety, in particular, is determined by the vector of information and technical condition of critical infrastructure, the disruption of which can lead to impacts on natural ecosystems and losses. The quintessence of solving this problem is the structure “intellectualization – information security – ecological monitoring” within the basic principles: Ukrainian strategy Industry 4.0, Concept of information security of Ukraine, European Union scientific research initiative “Horizon Europe” (2021 – 2027) [1, 2, 3]. The safety of environmental components – water, air, soil, forests – is ensured by the implementation of models of safe ecological monitoring based on intelligent CPS.

Analysis of recent achievements and publications. The strategy of the state ecological policy of Ukraine is aimed at the implementation of: comprehensive ecological monitoring of the condition of the environment and improvement of

III International Scientific And Practical Conference “Information Security And Information Technologies”, September 13–19, 2021, Odesa, Ukraine

EMAIL: rector@lpnu.ua (A. 1); vdudykev@gmail.com (A. 2); cosmos-zirka@ukr.net (A. 3); taras.r.stosyk@lpnu.ua (A. 4)
ORCID: 0000-0001-9185-7074 (A. 1); 0000-0001-8827-9920 (A. 2); 0000-0003-4275-8285 (A. 3); 0000-0001-7896-9792 (A. 4)

the system of information support of the management decision-making process [4].

In this regard, the relevant segment is the use of intelligent ecological monitoring systems of environmental components and the implementation of information security technologies, which comprehensively form the tools of environmental security, which is a component of national security of Ukraine and the vector of sustainable development of Ukraine.

Intelligent informational measuring systems are effectively used for ecological monitoring [5], as well as geo-information and aerospace technologies, which carry out: registration of ecological parameters of environmental components, rapid analysis, processing, preservation, identification, intelligent decision support [6].

The principles of construction of wireless sensor networks (WSN) for ecological environmental monitoring are developed. In paper [7] WSNs, based on the method of coordinate routing, which takes into account the interaction of sensor nodes and intellectualization of decision-making processes at OSI levels and management functions, were developed.

Progressive are the scientific and technical developments of the National Academy of Sciences of Ukraine in the field of creating sensors for ecological research, intelligent systems for monitoring of environmental parameters [8].

The development of tools for intellectual ecological monitoring at the international level continues. The paper [9] presents trends in the use of IT for monitoring air, water, radiation pollution, including sensors, IoT, machine learning methods.

IoT based smart water quality monitoring system is presented in [10] structurally: sensor for measuring water parameters (temperature, pH, turbidity), Zigbee WSN for data transferring, central processing unit, main data storage module, displaying information for users. Also in this paper known sensors for the environmental water monitoring system were analysed and the permissible limits of drinking water parameters according to the recommendations of the WHO and the Environmental Protection Agency (WHO/USEPA) were highlighted.

The publication [11] considers the structure of smart ecological monitoring of water, air, soil based on IoT platform according to the IEEE 1451 standard and data flow modeling.

Intelligent technologies of ecological monitoring of the environment must be dependable – to meet the requirements of functional and information security by the standard SOU-N NSAU 0060:2010.

The goal of the work. The aim of the work is to create a paradigm of ecological monitoring “intellectualization - information security”, which is the basis of safe research monitoring of water quality “program – IT – IS – assessment methodology” and information model of security of the three-layer architecture of IoT.

2. Paradigm of ecological monitoring: “intellectualization – information security”

The multilevel paradigm of ecological monitoring of the environment “intellectualization – information security” created on the basis of the concept “object – threat – protection” is the development of methodological principles of monitoring components – water, air, soil, forests. (Fig. 1).

The first level – functionality of the structure “component of the environment – operating technologies” / “objects ($O_{1-N(R,S,T)}$) – cyber-physical systems ($CPS_{1-N(R,S,T)}$)” according to the components – water (W), air (A), soil (S), forests (F). The second level – integration of the levels of the CPS “Internet of Things ($IoT_{1-N(R,S,T)}$) – wireless technologies ($WT_{1-N(R,S,T)}$) – computer systems ($CS_{1-N(R,S,T)}$)”. The third level – processes of “information selection ($S_{1-N(R,S,T)}$)/ monitoring – transmission/reception ($T_{1-N(R,S,T)}$/$R_{1-N(R,S,T)}$) – information processing ($P_{1-N(R,S,T)}$) / management ($M_{1-N(R,S,T)}$)”. The fourth level – IS threats at the structural and functional levels of the CPS a_{1-N} – b_{1-N} – c_{1-N} (water monitoring); d_{1-R} – e_{1-R} – f_{1-R} (air monitoring); g_{1-S} – h_{1-S} – i_{1-S} (soil monitoring); k_{1-T} – l_{1-T} – m_{1-T} (forest monitoring). Fifth level – hardware and software security technologies in the profiles “confidentiality – integrity – accessibility” A_{1-N} –B_{1-N} – C_{1-N} (W); D_{1-R} – E_{1-R} – F_{1-R} (A); G_{1-S} – H_{1-S} – I_{1-S} (S); K_{1-T} – L_{1-T} – M_{1-T} (F) according to DSTU ISO/IEC 15408.

Secure data collection by intelligent sensors or sensors that interact with objects as components of the environment and the exchange of information in intelligent ecological monitoring technology are carried out by the Internet of Things (CPS physical space) and wireless technologies (CPS communication environment).

The computer system (CPS cyberspace) provides data storage, analysis, processing, identification, forecasting and, on this basis, management of the state of the environment.

The paradigm of safe intellectualization of ecological monitoring of environmental components is the basis for building comprehensive security systems for intelligent systems based on the concept of "object – threat – protection".

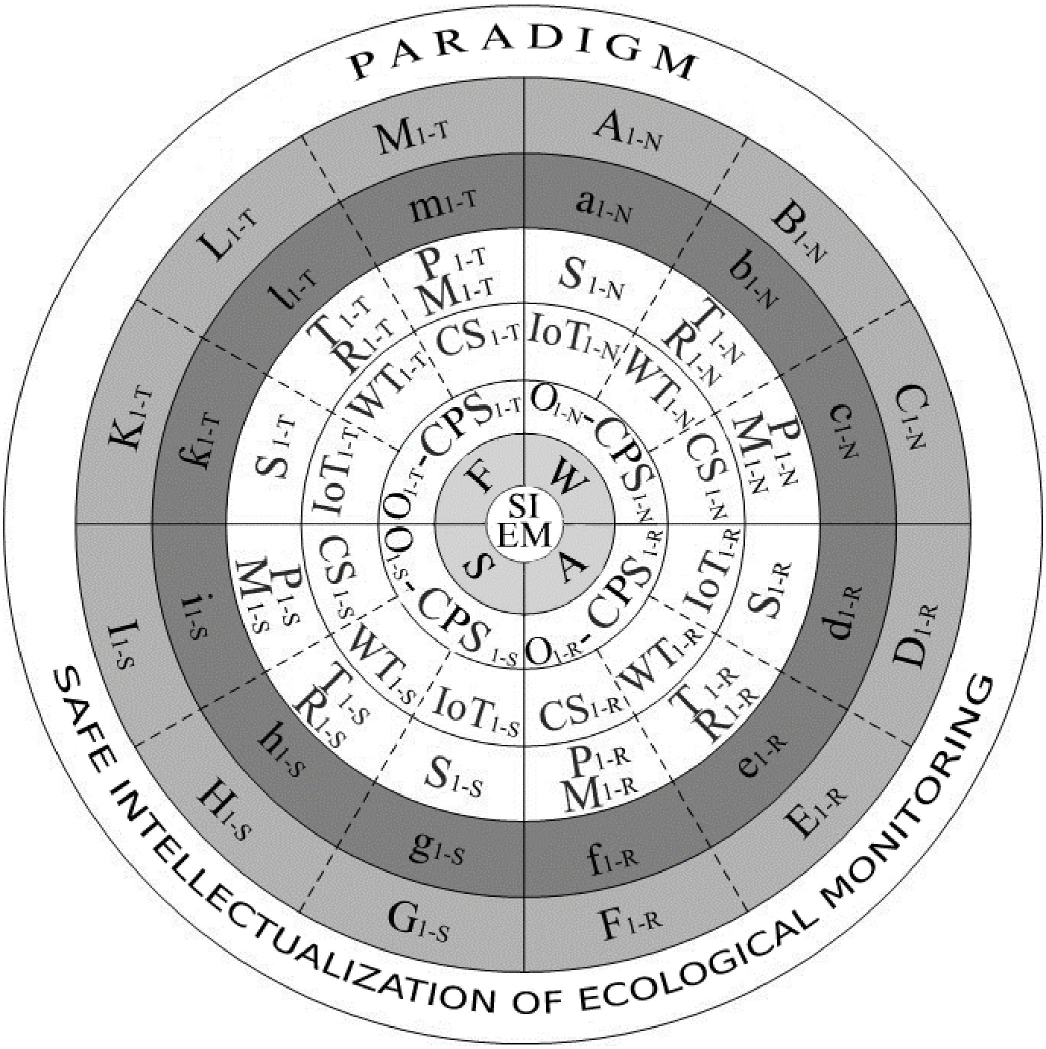

Figure 1: Paradigm of safe intellectualization of ecological monitoring

2.1. Research ecological monitoring of water: complex model "program – IT – IS – methodology"

According to DSTU 3041-95, water monitoring is an observation of the state of natural water and its evaluation. In order to ensure water quality and apply the model of environmental management system, Ukraine has implemented standards DSTU 7525: 2014 and DSTU 14004: 2016, which respectively establish requirements and methods of drinking water quality control and a systematic approach to ecological management in sustainable development and environmental management. The methodological approach to assessing the current state of water quality provides appropriate methods and tools for ecological monitoring: determination of water parameters (registration / measurement), assessment of ecological characteristics of water, forecasting and management decisions on the state of the water. Standardized technologies are used to monitor the set of water parameters, in particular the standard DSTU ISO 15923-1: 2018 describes the use of discrete analysis systems to determine individual environmental parameters. Water quality control with the use of IT ecological monitoring, secure cyber-physical systems, is important and relevant. In order to assess the set of drinking water parameters, research monitoring has been developed at the level of a comprehensive model "program – IT – IS – methodology". In terms of intelligent technologies and information security, a comprehensive model of research monitoring includes: 1) MEMS sensors (microelectromechanical systems), integrated into intelligent informational measuring systems, which are designed for remote sampling of water and its environmental parameters and wireless transmission (DSTU-P CEN/CLC/ETSI/TR 50572:2020) and, on this basis, the creation of databases, information processing and decision-making; 2) security technologies of intelligent systems under the influence of threats to confidentiality, integrity, accessibility, in particular at the IoT level, which provides algorithmic and software interaction between sensors and devices with computer systems (Fig. 2) [12, 13, 14].

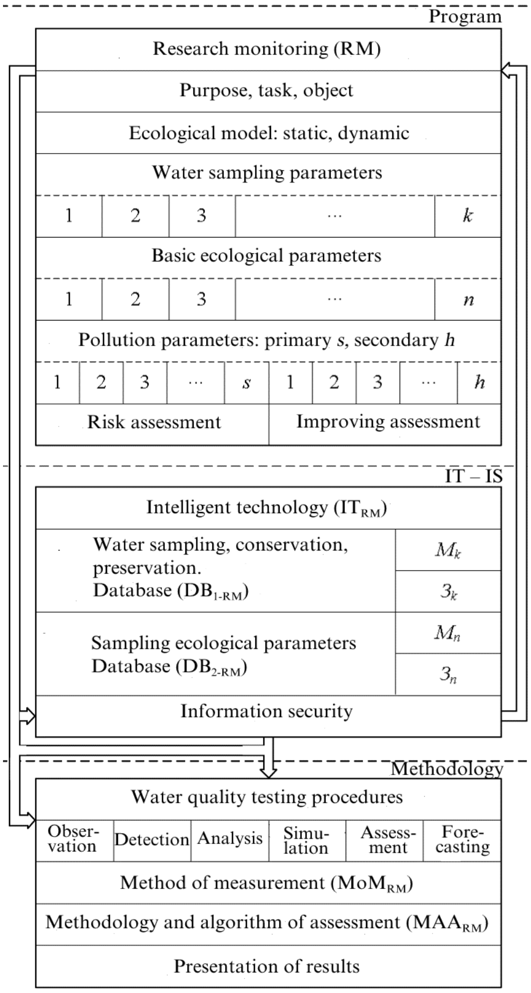
Program
Research monitoring (RM)
Purpose, task, object
Ecological model: static, dynamic
Water sampling parameters
1
2
3
…
k
Basic ecological parameters
1
2
3
…
n
Pollution parameters: primary s, secondary h
1
2
3
…
s
1
2
3
…
h
Risk assessment
Improving assessment
IT – IS
Intelligent technology (IT_RM)
Water sampling, conservation, preservation.
Database (DB_1-RM)
M_k
3_k
Sampling ecological parameters
Database (DB_2-RM)
M_n
3_n
Information security
Methodology
Water quality testing procedures
Observation
Detection
Analysis
Simulation
Assessment
Forecasting
Method of measurement (MoM_RM)
Methodology and algorithm of assessment (MAA_RM)
Presentation of results

Figure 2: Research monitoring of drinking water parameters

The approach to the assessment of physicochemical and biological properties of drinking water under man-caused influence is determined by the system of regulations:

Standards: DSanPiN 2.2.4-171-10, GOST 27384-2002, DSTU 4808:2007, DSTU 3831-98, DSTU 10260:2007, GOST 8.556-91, GOST R 52180-2003, GOST R 52181-2003, DSTU GOST 18294-2009, DSTU ISO 9377-2:2015.

Experimental conditions:

1. taking into account the system of factors influencing drinking water;
2. water sampling, transportation, canning, storage.

Methodology – method, means, technique:

1. measurement of water parameters, processing, presentation of results;
2. methods and tools for selection of physicochemical and biological parameters of water:

- methods – selective, multicomponent (atomic emission, X-ray, spectral analysis, chromatography), etc.;
- tools: conductometers, pH-meters, ionometers, ORP-meters, photoelectric colorimeter, gas chromatographs, automated natural water quality control systems (DSTU 3831-98), laser measuring systems, intelligent informational measuring systems, intelligent geoinformational systems.

3. the result of measuring N-standard:

- maximum allowable concentration of harmful substances in water (MAC_H);
- maximum allowable concentration (MAC);
- maximum allowable emissions (MAE);
- maximum allowable discharges (MAD);
- measurement error Δ, range Δ_U, Δ_L; P;
- for physicochemical: P = 0,95; for biological: P = 0,9;
- accuracy: $S_L + \Delta_U < MAC$, S_L – device sensitivity threshold.

4. technologies for restoring the properties of water: filters, activators, magnetohydrodynamic systems, biotechnology, etc.

2.2. Informational model of security of three-layer architecture of the Internet of Things

The Internet of Things is one of the intelligent technologies for ecological monitoring of the natural environment. The Internet of Things consists of a large number of different devices, networks and technologies that are sometimes difficult to combine. Accordingly, today there is no single common IoT architecture. However, of all the proposed IoT architectures, the most widely recognized and widespread is the three-layer structure [15, 16]. Based on it, an informational model of Internet of Things security in intelligent ecological monitoring systems was built, according to standard ETSI TS 103 645 from European Telecommunications Standards Institute (Fig. 3).

The perception layer is the physical level of the IoT architecture. In the context of intelligent CPS-based ecological monitoring, the perception layer consists of sensors and external devices that collect information about the state of environmental components for further transmission. This level is the most vulnerable to attacks due to the possibility of gaining direct physical access to devices operating outside the controlled area. The main threats are node capture and fake node injection. To protect against those attacks security measures, such as asymmetric cryptography (does not allow to obtain a key from the captured node), physical protection and authentication of devices, are provided.

The network layer is responsible for transmitting and processing environmental information collected by sensors at the perception layer. The main threats at this level are DDoS attacks and eavesdropping, including man-in-the-middle. Security measures include multi-factor authentication, wireless encryption, traffic analysis using an intrusion detection system and the organization of a separate network.

The application layer is responsible for processing information received from the network layer, controlling devices and interacting with users. The key issue of information security at this layer is the vulnerability of the software and the implementation of malicious code. Countermeasures include the use of trusted software components, an application-level firewall, and an access control list (ACL).

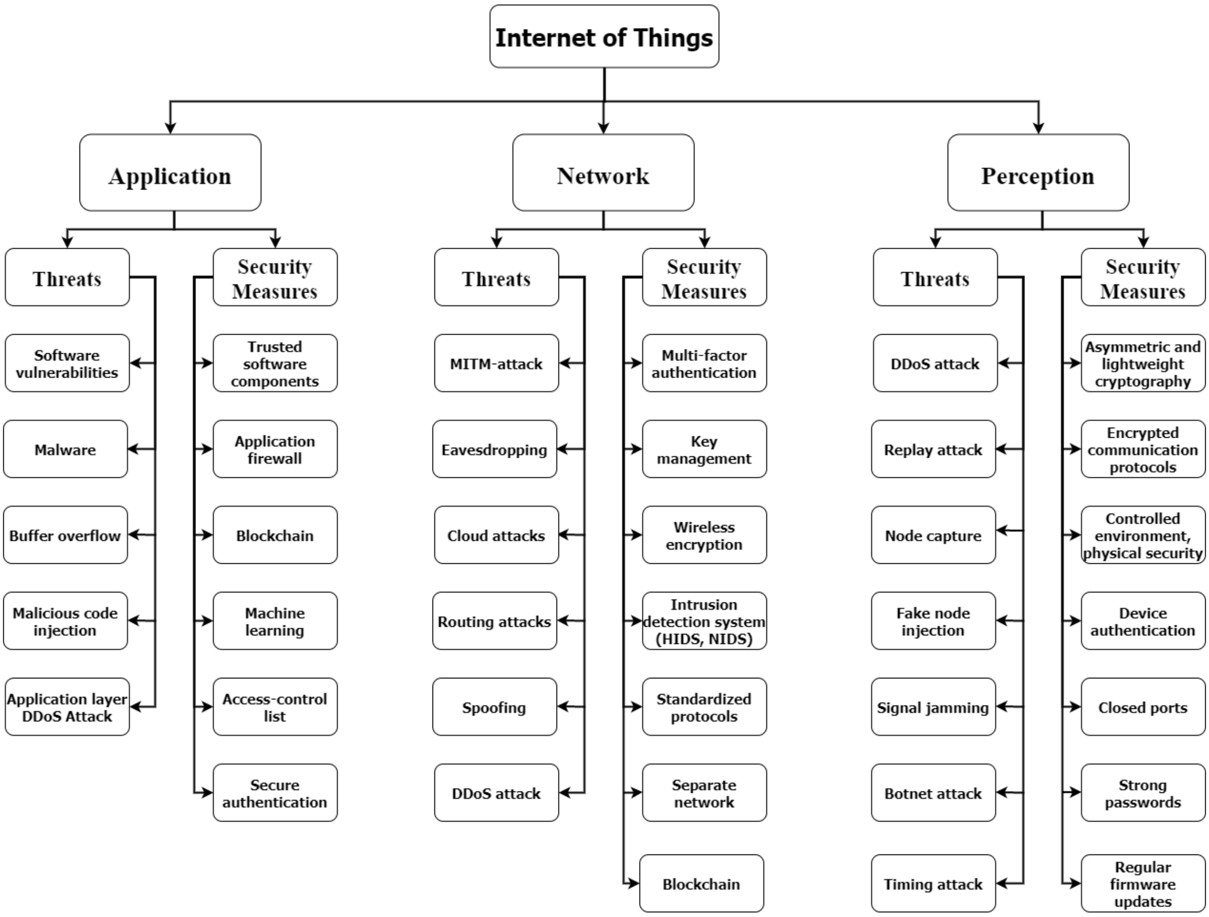

Figure 3: Informational model of security of three-layer architecture of the Internet of Things

3. Conclusions

The paper presents a single methodology for safe ecological monitoring of environmental components: 1) universal paradigm “intellectualization – information security”; 2) a comprehensive model of research monitoring of drinking water quality; 3) informational model of Internet of Things security, which allows the development of approaches and models for monitoring air, soil, forest on the basis of intelligent systems and the construction of integrated security systems by profiles – confidentiality, integrity, accessibility.

4. References

[1] Yurchak Oleksandr. Ukrayins'ka stratehiya Industriyi 4.0 – 7 napryamiv rozvytku [Elektronnyy resurs]. – Rezhym dostupu: https://industry4-0-ukraine.com.ua/2019/01/02/ukrainska-strategiya-industrii-4-0-7-napriankiv-rozvutku/.

[2] Proekt Kontseptsiyi informatsiynoyi bezpeky Ukrayiny. – [Elektronnyy resurs]. – Rezhym dostupu: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf.

[3] Horizon Europe. The next eu research & innovation investment programme (2021–2027). URL: https:// ec.europa.eu /info/sites/default/files/research_and_innovation/strategy_on_research_and_innovation/presentations/horizon_europe_en_investing_to_shape_our_future.pdf.

[4] Pro osnovni zasady (ctratehiyu) derzhavnoyi ekolohichnoyi polityky Ukrayiny na period do 2030 roku. – Zatverdzheno Zakonom Ukrayiny vid 28 lyutoho 2019 roku # 2697 – VIII. – [Elektronnyy resurs]. – Rezhym dostupu: https://zakon.rada.gov.ua/laws/show/2697-19#Text.

[5] Kropyvnytskyi V., Pavlyshyn M., Chumak V. Vysokomobil'na laboratoriya ekolohichnoho monitorynhu – [Elektronnyy resurs]. – Rezhym dostupu: https://ns-plus.com.ua/2017/06/13/vysokomobilna-laboratoriya-ekologichnogo-monitoryngu/.

[6] Trysniuk V.M., Okhariev V.O., Trysniu T.V, Smetanin K.V., Holovan Yu.M. Stvorennya systemy mobil'noho ekolohichnoho monitorynhu // Ekolohichna bezpeka ta zbalansovane resursokoryt·stuvannya. – №2 (18). – 2018. – S. 118 – 125.

[7] Lysenko O.I. Rozrobka pryntsypiv pobudovy bezprovodovykh sensornykh merezh iz samoorhanizatsiyeyu dlya monitorynhu parametriv navkolyshn'oho seredovyshcha. – [Elektronnyy resurs]. – Rezhym dostupu: https://report.kpi.ua/uk/0115U000269.

[8] Perspektyvni naukovo-tekhnichni rozrobky NAN Ukrayiny. – Ekolohiya ta okhorona dovkillya. – [Elektronnyy resurs]. – Rezhym dostupu: https://www.nas.gov.ua/RDOutput/UA/book2017/Pages/sd.aspx?SRDID=02.

[9] Silvia Liberata Ullo, G. R. Sinha. Advances in Smart Environment Monitoring Systems Using IoT and Sensors // Sensors 2020, 20(11), 3113. doi:10.3390/s20113113.

[10] Farmanullah Jan, Nasro Min-Allah, Dilek Düştegör. IoT Based Smart Water Quality Monitoring: Recent Techniques, Trends and Challenges for Domestic Applications // Water 2021, 13(13), 1729. doi: 10.3390/w13131729.

[11] Tércio Filho, Luiz Fernando, Marcos Rabelo, Sérgio Silva, Carlos Santos, Maria Ribeiro ,Ian A. Grout, Waldir Moreira, Antonio Oliveira-Jr. A Standard-Based Internet of Things Platform and Data Flow Modeling for Smart Environmental Monitoring// Sensors 2021, 21(12), 4228. doi: 10.3390/s21124228.

[12] Stvorennya mikroelektronnykh datchykiv novoho pokolinnya dlya intelektual'nykh system / Ya. I. Lepikh, Yu. O. Hordiienko, S. V. Dziadevych [et al.]. – Odesa: Astroprint, 2010. – 256 s.

[13] Intelektual'ni vymiryuval'ni systemy na osnovi mikroelektronnykh datchykiv novoho pokolinnya / Ya. I. Lepikh, Yu. O. Hordiienko, S. V. Dziadevych [et al.]. – Odesa: Astroprint, 2011. – 351 s.

[14] Vashpanov Yu. O. Suchasni sensory avtomatychnykh system: navch. posib. / Yu. O. Vashpanov – Odesa: VMV, 2014. – 240 s.

[15] Miao Wu, Ting-Jie Lu, Fei-Yang Ling, Jing Sun and Hui-Ying Du, “Research on the architecture of Internet of Things,” 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), 2010, pp. V5-484-V5-487, doi: 10.1109/ICACTE.2010.5579493.

[16] Quandeng Gou, Lianshan Yan, Yihe Liu. Construction and Strategies in IoT Security System. Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing, 2013, pp. 1129-1132.