UDC 004.93

CONCEPTION AND APPLICATION OF DEPENDABLE INTERNET OF THINGS BASED SYSTEMS

Illiashenko O. O. – PhD, Associate Professor of Computer systems, networks and cybersecurity department, National aerospace university "KhAI", Kharkiv, Ukraine.

Kolisnyk M. A. – PhD, Associate Professor of Computer systems, networks and cybersecurity department, National aerospace university "KhAI", Kharkiv, Ukraine.

Strielkina A. E. – PhD, Assistant Lecturer of Computer systems, networks and cybersecurity department, National aerospace university "KhAI", Kharkiv, Ukraine.

Kotsiuba I. V. – PhD, Lead Project Engineer of Pukhov Institute for Modelling in Energy Engineering of National Academy of Sciences of Ukraine, Kyiv, Ukraine.

Kharchenko V. S. – Dr. Sc., Professor and Laureate of the State Prize of Ukraine in the field of science and technology, Honored Inventor of Ukraine, Head of Computer systems, networks and cybersecurity department, National aerospace university "KhAI", Kharkiv, Ukraine.

ABSTRACT

Context. The problem is in the design, development, maintenance and commisioning of interoperable dependable systems using on the Internet of Things based on von Neumann paradigm of "building reliable systems from unreliable components" for dependable service-oriented systems and infrastructures.

Objective. The goals of the paper are in the development of concepts and principles and assessment technologies for creation and maintenance of complex critical systems based on Internet of Things (IoT) as well as implementation of research in various domains.

Method. In the paper the concept of development of dependable systems on the basis of the Internet of things is described. The multisectoral analysis of methods and models of reliability and cybersecurity (dependability) evaluation of information and control systems of critical applications using the Internet of things has been performed for different domains: power, healthcare, industrial, etc. The analysis has shown that some software failures and malfunctions, cyberattacks and consequences of influence of attacks are identical for all domains, but there are specific features for each domain, which are necessary to consider at working out of methodology of maintenance of denepdability of reliability of systems of critical applications using the Internet of things.

Results. The developed conception, methods, tools and technologies for the creation and implementation of dependable information & control systems for critical applications based on the Internet of Things.

Conclusions. The paper proposes a conception that includes a set of scientific and applied tasks for the development of methods, tools and technologies for the creation and implementation of dependable information & analytical and information & control systems for critical applications based on the Internet of Things. The prospects for further research may include the detailing of the developed models, methods and technologies to ensure the dependability of complex information & control systems for critical applications based on the Internet of Things.

KEYWORDS: Information and control systems of critical applications, Internet of Things, dependability, cybersecurity, functional safety.

ABBREVIATIONS

DDoS – Distributed Denial of Services;

ICSIoT – Information & Control Systems based on Internet of Things;

ICT – Information and Communication Technologies;

IoT – Internet of Things;

LAN – Local Area Network;

USB – Universal Serial Bus.

NOMENCLATURE

λij is a failure rate or attack rate;

μij is a recovery rate;

$Pi(t)$ is a probability of finding the ICSIoT system in each of the states;

$AC(t)$ is an availability function.

INTRODUCTION

One of the promising areas of modern information and telecommunication technologies development is the IoT. The infrastructure of interconnected objects, people, systems and information resources together with intelligent services allowing them to process information, combine the physical and virtual world is a paradigm of IoT, which ensures the integration of any electronic device into the Internet environment. Areas of application of IoT are information & analytical and information & control systems of manufacturing, energy, defense, transport, construction, healthcare, smart cities and buildings.

IoT-based technologies are implemented both in everyday life, where they increase comfort and quality of life, and in the so-called critical systems, which must provide a high level of reliability, safety for long-term use, and meet strict national and international standards. Information & analytical and information & control systems of critical applications (energy, aerospace and transport complexes, medical equipment and communications) based on the ICSIoT are a separate class of such systems [1].

Failures of such systems are possible due to software design defects, physical defects of hardware, attacks on system vulnerabilities. Adverse effects and attacks on vulnerabilities in ICSIoT components, software, and databases can occur at each of these levels. The target of at-

DOI 10.15588/1607-3274-2020-4-14

tackers can be data, video and audio recordings, disabling hardware and software components.

It is important for ICSIoT to ensure the protection and tolerance of systems to failures of various natures, i.e. to ensure their dependability. Dependability is a complex property of the system to perform appropriate functions and provide services that can be justifiably trusted [2]. Dependability combines reliability, functionality and cybersecurity, which is very important in the requirements regulation, evaluation, creation and use of critical systems in general as much as systems based on the IoT in particular. It should be emphasized that systems based on IoT technologies consist of hardware, software, communication components of different reliability and security levels. Therefore, there is a contradiction between the requirements for dependability (reliability and safety) of ICSIoT and the level of characteristics of the dependability of their components in an aggressive physical and information environment, between the capabilities of appropriate technologies and inspiring methods and means of creating critical systems using IoT. Therefore, it is necessary to consider the concept of ensuring the dependability of critical systems based on IoT, which combines the principles, methods and tools of analysis, evaluation and ensuring the reliability, security and dependability of these systems as a whole.

1 PROBLEM STATEMENT

The purpose of the paper: development of concepts and principles, systematization of models and methods to ensure ICSIoT compliance with reliability and safety requirements, review of assessment technologies, creation and maintenance of such systems and implementation of research results of authors in creating ICSIoT in various domains.

The scientific novelty and applied task, which is solved in the work, is the development of methods, means and technologies of creation and introduction of capable information-analytical and information-control systems of critical application on the basis of the IoT.

In accordance with the purpose of the work the following tasks are solved:

1. The concept, principles of dependable ICSIoT are offered.
2. The normative profile of ICSIoT is developed, which takes into account and harmonizes the list and content of requirements of international and national standards for reliability, availability, functional and cybersecurity and modernization.
3. Mathematical models and methods for assessing the performance, availability, functionality and cybersecurity of ICSIoT, which take into account various types of failures and cyberattacks on systems, allow to analyze their functional behavior and formulate recommendations for the choice of hardware and software components, architecture, interaction protocols and more.
4. Methods of development of capable ICSIoT for various complexes (medical, power, industrial, communication, etc.) and maintenance of their reliability and safety at creation, modernization and use are offered.
5. Developed and implemented information technologies to support decision-making in the creation, modernization and maintenance of ICSIoT.

To solve the set tasks, it is necessary to create models and methods that will allow assessing the reliability, availability, and reliability of the system. The apparatus of Markov models has proven itself well in assessing ICSIoT system availability. The following assumptions were made when creating the models and simulations. Assumptions in Markov model development:

– current system hardware failures are subject to Poisson distribution;

– the flow of subsystem failures is governed by Poisson's distribution law because the results of monitoring and diagnostics, antivirus software testing have corrected a secondary error (the result of the accumulation of primary errors and defects, software bookmarks) and to correct software failures or failures, troubleshooting or consequences code, attacks on DoS – and DDoS – the number of primary software defects constantly. Therefore, it is true to assume that the flow of software failures is subject to Poisson propagation, the failure rate is constant;

– the model does not take into account that the elimination of software vulnerabilities and design errors change the parameters of the failure flow (and recovery). Markov's model theory is used to study the reliability of ICSIoT, because the failure rate of hardware and software and the presence of software vulnerabilities are constant.

The main parameters indicated on the graph of Markov model – the transition rates from one state to another: λij, μij. Several models are used to create the conception and application of dependable IoT based systems. The initial data for the models, which are used in conception, are different for different models. For the model, described in this paper, initial data are: $\lambda 1317=5,7\cdot10^{-4}$ 1/h; $\lambda 1517=1\cdot10^{-5}$ 1/h; $\lambda 1617=1\cdot10^{-6}$ 1/h; $\lambda 218=1\cdot10^{-5}$ 1/h; $\lambda 318=1\cdot10^{-5}$ 1/h; $\lambda 1320=1\cdot10^{-6}$ 1/h; $\lambda 1520=1\cdot10^{-6}$ 1/h; $\lambda 2017=1,14\cdot10^{-3}$ 1/h; $\lambda 120=1\cdot10^{-6}$ 1/h; $\mu 67=60$ 1/h; $\mu 141=0,125$ 1/h; $\mu 111=0,5$ 1/h; $\mu 32=40$ 1/h; $\mu 42=30$ 1/h; $\mu 52=30$ 1/h; $\mu 1513=50$ 1/h; $\mu 1613=60$ 1/h; $\mu 71=0,02$ 1/h; $\mu 87=2$ 1/h; $\mu 81=30$ 1/h; $\mu 101=1$ 1/h; $\mu 121=5$ 1/h; $\mu 181=1$ 1/h; $\mu 191=0,02$ 1/h; $\mu 91=1$ 1/h; $\mu 171=1$ 1/h; $\mu 188=60$ 1/h; $\mu 61=0,02$ 1/h; $\mu 2021=60$ 1/h; $\mu 221=20$ 1/h; $\mu 211=30$ 1/h; $\mu 1722=60$ 1/h; $\mu 201=40$ 1/h; $\mu 2113=20$ 1/h.

2 REVIEW OF THE LITERATURE

The analysis of known proceedings, projects and experience of such systems operation allows formulating the purpose and objectives of research conducted by the authors over the past 10 years. Currently, there are publications of many authors who have conducted research in the following areas: critical application systems reliability, IoT systems cybersecurity, Web-services dependability, critical application systems dependability, IoT systems, IoT systems dependability.

DOI 10.15588/1607-3274-2020-4-14

The issues of research and development of dependable systems were considered in the following scientific proceedings. In [1] the basic methods of modeling, design and evaluation, as well as providing dependable IoT systems described, their architecture and the particular implementation are introduced. In [2] the basic concepts of dependability are introduced, and it is shown that it combines the system's reliability and cybersecurity, the classification of different types of failures, threats and their attributes.

In [3] the modified taxonomic scheme of system dependability taking into account the changes of functional requirements, dependability requirements, computer systems environment characteristics, including an operating cycle and levels of maintenance of fault tolerance is offered, the taxonomy of multiversion calculations in dependable systems is generalized.

Study of the design and architecture of IoT systems and their dependability were considered in next scientific proceedings: in [4] the analysis and the classification of technologies, protocols and applications of IoT and their interaction with big data technologies and cloud and fog computing is performed. In [5] the depedability assessment of energy-efficient IoT devices is held.

In [6] Markov model of applications for ICT systems dependability is provied, taking into account redundancy.

In [7] the problem of applications of the IoT dependability regardless of their size and area of use is reseached. In [8] to ensure IoT system dependability it is adviced to use a simple formal "Mirror model" to transmit data from sensors in the IoT network, using the assets of the trust in blockchain.

In [9] a study of dependability of edge computing is conducted and challenges of deploying IoT systems in view of failures as hardware (crashing, hanging, and so on) and software, and vulnerabilities of IoT devices with decentralized control are included.

In [10] the methods and tools to predict dependability and improve the reliability of IoT are provided. The authors of this article propose the concept of creating dependable critical systems using IoT.

Thus, there is a large number of scientific publications that present the results of research, including analysis, evaluation and assurance of the reliability and cybersecurity of critical infrastructure systems, the dependability of these systems, as well as individual components of IoT systems. The known publications do not include generalized methodological results that would take into account certain contradictions between IoT capabilities and certain security deficiencies that may occur in their implementation in critical systems.

3 MATERIALS AND METHODS

The conception of interoperable systems based on the IoT is based on the well-known von Neumann paradigm of "building reliable systems from unreliable components" and its developed variants for dependable service-oriented systems and infrastructures [1].

For ICSIoT, it can be formulated as the construction of dependable IoT systems from insufficiently dependable (reliable and secure) nodes (embedded digital media, intelligent sensors, etc.), communications and cloud (server) resources in an aggressive environment with uncertain characteristics.

The scheme, which reflects the structure and interrelation of methodology elements of dependable systems, based design on the IoT, namely the concept, principles, models, methods, tools and technology, is shown in Fig. 1.

The conception of dependable systems based on the IoT is grounded on the next principles:

1. The principle of comprehensive consideration and assessment of various failure types of components, communications, services due to software defects and attacks on ICSIoT.

2. The principle of case-oriented formation and analysis and assessment of compliance with the requirements of ICSIoT dependability [11].

3. The principle of selection and implementation of measures to ensure dependability at all the life-cycle stges by the criterion – "acceptable risk – costs".

The conception and principles are implemented through the development of relevant models and methods of assessment and dependability implementation. In particular, the following groups of models have been developed:

1. Models of ICSIoT functional behavior, which are divided into:

a. distributed intellectual energy ICSIoT models;

b. dynamic ICSIoT based on cybergraphs model;

c. functional behavior of medical ICSIoT [12] model.

The use of models allows to get a clear idea of how the system works (ICSIoT subsystem) in different situations and under the influence of various factors, including cyberattacks.

2. Models of dependability which include:

a. theoretical-multiple model of dependability assessment [13];

b. ICSIoT dependability assessment under cyberattacks influence [14]–[16];

c. dependability assessment taking into account the power consumption modes of ICSIoT components [24].

The use of them allows a detailed assessment of the performance indicators of ICSIoT (availability functions, etc.) and its subsystems.

The models take into account two properties of dependability – cybersecurity and reliability of ICSIoT and its subsystems considering different types of cyberattacks.

3. ICSIoT reliability and cybersecurity models, including:

a. ontological ICSIoT cybersecurity assessment mo-del;

DOI 10.15588/1607-3274-2020-4-14

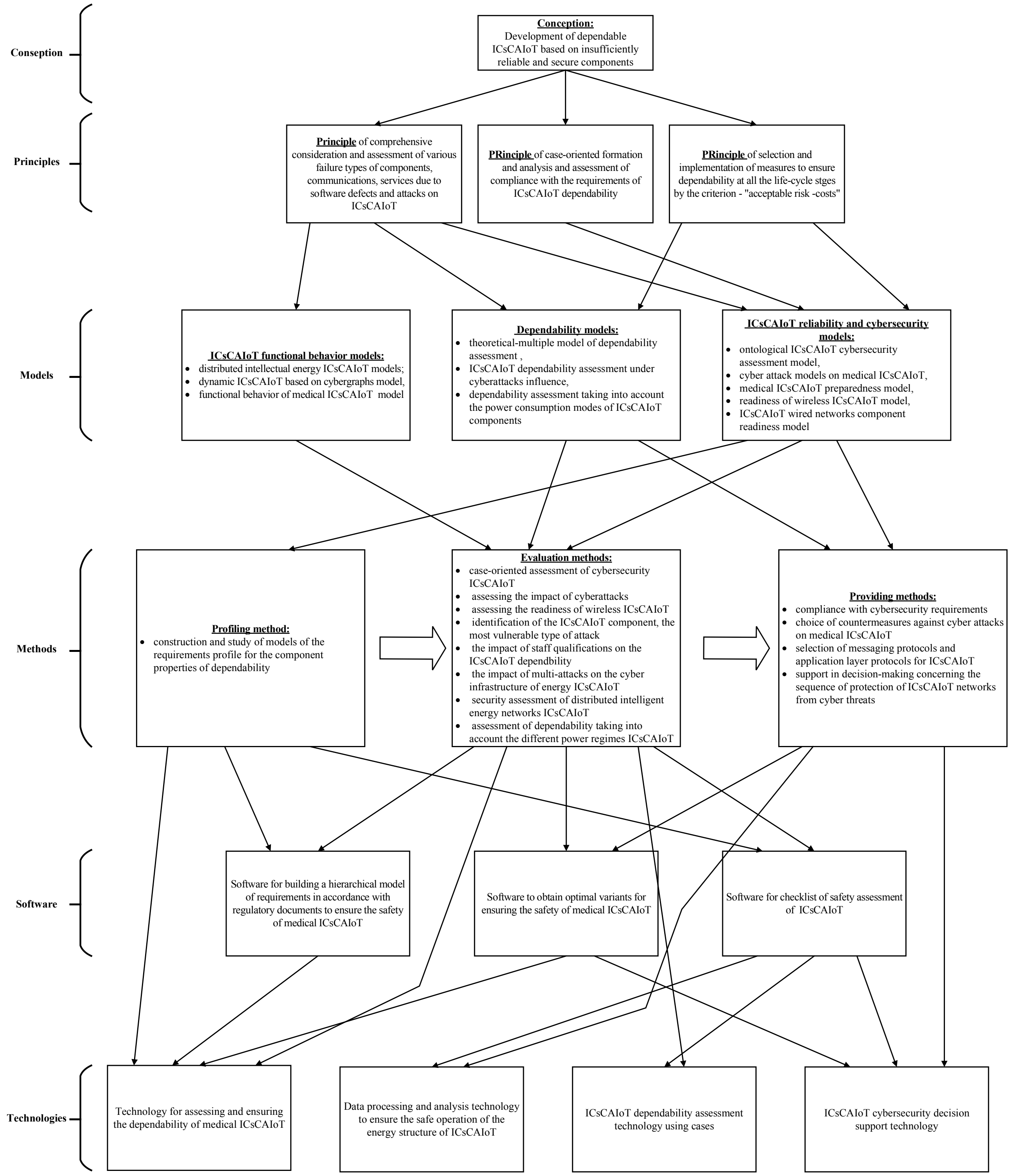

Figure 1 – Structure and interrelation of methodology elements of dependable systems, based design on the IoT

b. cyber attack models on medical ICSIoT [17], medical ICSIoT preparedness model, taking into account attacks on vulnerabilities of infrastructure components [18];

c. availability of wireless ICSIoT model taking into account the coverage factor;

d. ICSIoT wired networks component availability model [19].

These models allow to assess separately the reliability (coefficient or availability function) of ICSIoT and its subsystems, and separately the indicators of cybersecurity of ICSIoT and its subsystems.

Security models allow to identify the requirements for cybersecurity and assess the availability of ICSIoT under the influence of cyber attacks.

DOI 10.15588/1607-3274-2020-4-14

These security models are the basis for a number of profiling, evaluation and assurance of ICSIoT methods. The profiling method is based on the construction and study of models of the requirements profile for the component properties of dependability [20]. Evaluation methods are based on the development and study of models of all the above types. Methods of ensuring security are based on the use of models of dependability and models of reliability and cybersecurity for ICSIoT [21].

On the basis of the profiling and evaluation methods, software ools for constructing a hierarchical model of requirements in accordance with the normative documents to ensure the safety of medical ICSIoT [21] are proposed. Based on security methods and evaluation methods, the best options for cybersecurity for the entire range of attacks have been developed [18]. Based on the profiling method and assessment methods, the software is developed for the ICSIoT security checklist assessment [20, 21].

Developed software tools have been integrated into information technology. Based on the best cybersecurity options for the entire range of attacks and the construction of a hierarchical model of requirements in accordance with regulatory documents to ensure the safety of medical ICSIoT, as well as the above relevant models and methods, the technology for assessing and ensuring the dependability of medical ICSIoT [21] was obtained.

Basing on the usage of software to form options for cybersecurity for the entire range of attacks there were proposed:

a) data processing and analysis technology to ensure the safe operation of the energy structure of ICSIoT;

b) ICSIoT dependability assessment technology using cases [20].

In addition, ICSIoT cybersecurity decision support technology is proposed, which is based on the use of security methods and software for ICSIoT security assessment checklists to obtain optimal cybersecurity options for the entire range of attacks [21].

4 EXPERIMENTS

To create the concept of dependable systems of critical applications based on the IoT, several models for assessing the reliability of the system, models of the functional behavior of the ICSIoT, models of reliability and cybersecurity were developed by authors of this paper. For so many models, different assumptions apply, and their input to the simulation. Based on the proposed models, methods for assessment, functional behavior, reliability and cyber security have been developed. Let's consider several examples of simulation of the obtained models.

The Markov model (Fig. 2) [14] describes the states of ICSIoT, which takes into account the reliability of system's software and hardware, attacks on the system and different modes of power consumption of the server and router. The simulation results are shown in Fig. 3 and Fig. 4.

The Markov model considering DDoS attacks and server's and router's energy modes without patches on possible vulnerabilities, which has the following states: good-working state (1); the server is fully used with high power consumption S0 (2); the server is fully used, the hardware, that are not used, can enter the low-power mode S1 (3); sleep mode of the server with low power consumption, a computer can wake up from a keyboard input, a LAN network or USB device S2 (4); server appears off, power consumption is reduced to the lowest level S3 (5); server failure (6); switching to the backup server device after the server failure (7); restarting of the server after the software fail (8); successful DDoS attack on the server after the firewall failure (9); firewall software or hardware failure (10); attack on the power supply system after the firewall failure, that lead the failure of general power system (11); technical state of switch from the general power system after its failure on the alternative energy sources (solar, diesel generator, wind turbine) (12); router status active – sending packages with high power consumption (13); successful DDoS attack on the router (14); good-working state of the router with transmitting packets – normal idle (15); good-working state of the router without packet transmission low-power idle (16); router software or hardware failure (17); server software or hardware fail (18); router hardware or software fail (20); switching to the backup router device after the router failure (21); restarting the router software after the router software fail (22).

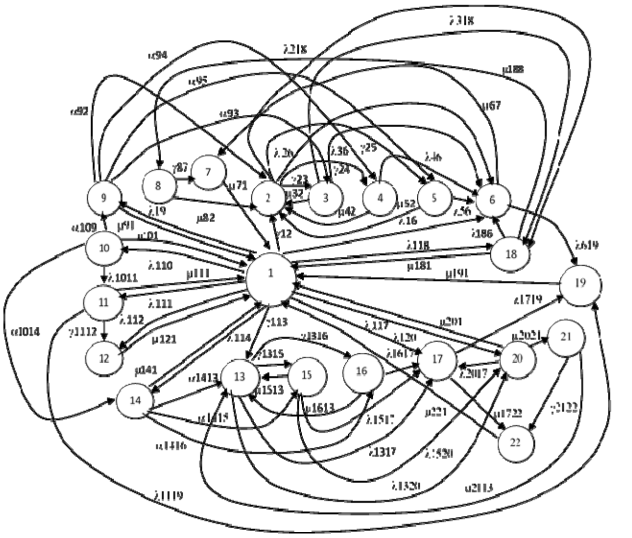

Figure 2 – Graph of the Markov model of the ICSIoT system states [14]

The model takes into account the rates to the states of the power consumption modes of the server and router (from state 2 to 3, 4, 5 and from states 14 to 13, 15, 16). Timely installation of a patch on firewall software vulnerabilities can reduce or stop the impact of DDoS attacks, which primarily affects the reliability of the ICSIoT server, router, and firewall (as a separate network device). When a DDoS attack affects ICSIoT subsystems, they cannot go into a state of reduced power consumption. For the Markov model (different variants of firewall software patching) the system of Kolmogorov-Chapman differential linear equations was presented and investigated, the

DOI 10.15588/1607-3274-2020-4-14

value of the availability function $AC(t)$ ICSIoT with normalization conditions was calculated and analyzed [14]:

$$AC(t) = P1(t) + P2(t) + P3(t) + P4(t) + P5(t) + P12(t) + \\ + P13(t) + P15(t) + P16(t) + P21(t),$$

where

$$\sum_{i=1}^{22} Pi(t) = 1; \quad P1(0) = 1.$$

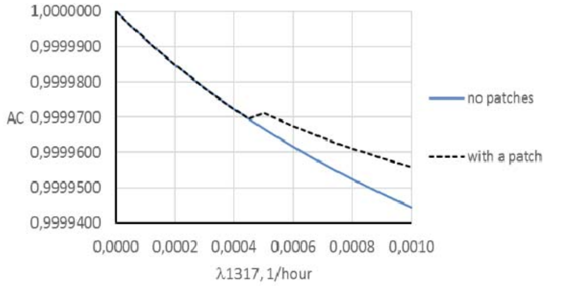

Figure 3 – Graphical dependences of AC ICSIoT on rate λ1317 for models with patching of firewall software vulnerabilities and without patches, if λ1317 = 0...1·10^{-3} 1/h [14]

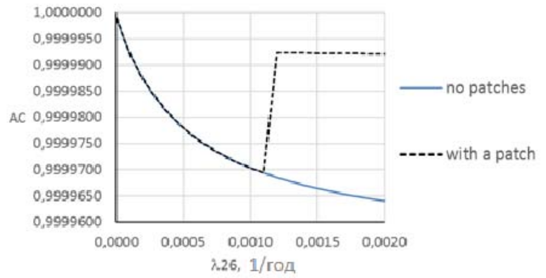

Figure 4 – Graphical dependences of AC ICSIoT on rate λ26 with patcherization of vulnerabilities in firewall software (*AC10*) and server and router firewalls (*AC*9_14), if λ26 changes values within 0... 2·10^{-3} 1/h [14]

5 RESULTS

If the transition rate λ26 changes from 0 to 0.001 1/h, the *AC* value decreases from 1 to 0.99997 for the unpatched model and to 0.9999925 for the model with the firewall software patch installed (Fig. 4) [14]. The *AC* value is decreased by 0.999945 for the model without patch. If the values of λ1317 change in the range of 0… 10^{-3} 1/h, the *AC* value for the model with the firewall software patch will decrease from 1 to 0.999957 (Fig. 3). Installing a patch on the firewall (Fig. 3) allows you to obtain the same *AC* values (1 ... 0.93) at λ1317 = 0 ... 10^{-3} 1/h, but this value is significantly higher than in the model without patches: *AC* = 1 ... 0.9999553 (Fig. 3).

If no patches are installed on the firewall software, then *AC* decreases from 1 to 0.9999553 at λ26 = 10^{-3} 1/h. Installing a patch on the server firewall does not significantly change the AC value. If you install a patch on the firewall software, the AC value increases compared to the case without patches, with the same initial data, from 0.9999553 to 0.9999925. If the transition rate λ26 changes from 0 to 0.001 1/h, the *AC* value decreases from 1 to 0.99997 for the unpatched model and to 0.9999925 for the model with the firewall software patch installed (Fig. 4).

The *AC* value is decreased by 0.999945 for the model without patch. If the values of λ1317 change in the range of 0… 10^{-3} 1/h, the *AC* value for the model with the firewall software patch will decrease from 1 to 0.999957 (Fig. 3).

Installing a patch on the firewall allows to obtain the same *AC* values (1 ... 0.93) at λ1317 = 0 ... 10^{-3} 1/h, but this value is significantly higher than without patches: *AC* = 1 ... 0.9999553.

If no patches are installed on the firewall software, then *AC* decreases from 1 to 0.9999553 at λ26 = 10^{-3} 1/h. Installing a patch on the server firewall does not significantly change the *AC* value. If you install a patch on the firewall software, the *AC* value increases compared to the model without patches, with the same initial data, from 0.9999553 to 0.9999925.

If the transition rate value λ26 is changed from 0 to 0.001 1/h, the *AC* value decreases from 1 to 0.99997 for the model without patching and to 0.9999925 for the case with the patch installed on the firewall.

Decrease in the *AC* value occurs 0.999945 for a model without a patch. If the values of λ1317 change within the range 0…10^{-3} 1/h, value of *AC* for the case with patch on firewall decrease from value 1 to 0.999957.

Establishing a patch on the firewall allows to obtain the same *AC* values (1…0.999553) at λ1317 = 0…10^{-3} 1/h, but this value is significantly higher than in the case without patch: *AC* = 1…0.9999553. If patches are not installed on the firewalls, then the AC decrease from value 1 to 0.9999553 at λ26 = 10^{-3} 1/h. Patch installation on server firewall not significantly changes the *AC* of ICSIoT value.

Under the influence of DDoS attacks, the server, which is in one of the energy-saving modes, will switch to the mode of increased power consumption.

6 DISCUSSION

It was researched and analyzed the function availability of ICSIoT, taking into account the reliability of components, recovery rates, and different kinds of energy modes of server and router OS, DDoS attacks on the router and the server, and setting patches on firewalls vulnerabilities. Therefore, it is necessary to analysis of graphical dependences of the AC on the change of values of transition rates from one ICSIoT state to another showed that timely introduction of patches on software vulnerabilities of ICSIoT components significantly increases the value of the *AC* of the whole system and allows to increase system availability.

Markov models of ICSIoT system operation, in contrast to the existing ones, take into account the power regimes of the router and server, the impact of DDoS attacks, failures and failures of software and hardware, patching vulnerabilities of router software.

DOI 10.15588/1607-3274-2020-4-14

The study results made it possible to develop and implement appropriate principles, methods, models and information technologies for assessing and ensuring the viability of ICSIoT in the fields of energy, medicine, mechanical engineering, aerospace, transport systems, etc.

The results of research of this proceeding are implemented on the follwoing enterprises (Table 1):

– at the enterprises of energy engineering (nuclear domain), RPC Radics LLC (Kropyvnytskyi, Ukraine) and PJSC SRPA Impulse (Severodonetsk, Ukraine);

– on the development of medical equipment, LLC “XAI-MEDICA” (Kharkiv, Ukraine);

– on the development of transport systems, LLC “SPC” Railwayautomatics” (Kharkiv);

– at machine-building enterprise, PJSC “FED” (Kharkiv);

– on the development of aerospace systems, scientific and technical design bureau “POLISVIT” (Kharkiv);

– on the development of state regulations by the State Service for Special Communications and Information Protection of Ukraine (Kyiv);

– on the development of methodological documents and requirements for the safety of critical infrastructure, PJSC “Institute of Information Technologies” (Kharkiv);

– in the educational process of the National Aerospace University “KhAI” (Kharkiv), Pukhov Institute for Modelling in Energy Engineering (Kyiv), Volodymyr Dahl East Ukrainian National University (Severodonetsk);

Table 1 – Summary of practical implementation of research and development results

Areas, enterprises (organizations), systems			**Results of research and development**							
			Models of non-functional characteristics			Methods of working with requirements			Automation technologies	
			Dependability models	Functional and behavior models	Reliability and cybersecurity models	Requirements profiling methods	Evaluation methods	Providing methods	Tools	Information technologies
Energy	RPC Radics LLC	ICSIoT components			+	+			+	
		Regulations			+	+				
	PJSC SRPA Impulse	ICSIoT components		+	+		+	+		
		Software								+
Medicine	LLC “XAI-MEDICA”	Telemedicine systems		+		+			+	
Transport systems	LLC “Scientific and Production Company” Railwayautomatics”	Microprocessor systems					+			
Engineering	PJSC “FED”	ICSIoT					+	+		
Aerospace systems	EDB “POLISVIT” SSPE “Kommunar Corporation”	Embedded systems				+	+	+		
State regulations	State Service for Special Communications and Information Protection of Ukraine	Critical Infrastructure Asset		+			+	+		+
	PJSC “Institute of Information Technologies”	Critical Infrastructure Asset				+	+	+	+	
Higher education	National Aerospace University “KhAI”, Pukhov Institute for Modelling in Energy Engineering, Volodymyr Dahl East Ukrainian National University	Learning process	+	+	+	+	+	+	+	+
International projects	TEMPUS international projects	MASTAC, SAFEGUARD, GREENCO, SEREIN, CABRIOLET	+	+	+	+	+	+	+	+
	ERASMUS+ international project	ALIOT	+	+	+	+	+	+	+	+
	FP7 scientific project	KhAI-ERA	+	+	+	+	+	+	+	+
	Horizon 2020 scientific project	ECHO, COST Action DigForAsp, SPEAR	+		+	+	+	+	+	+

DOI 10.15588/1607-3274-2020-4-14

– in the educational process of the universities of EU countries: Institute of Informatics and Technology Alessandro Faedo of the National Research Council of Italy ISTI-CNR (Pisa, Italy), Tallinn Technical University TalTech (Tallinn, Estonia), Leeds Beckett University LBU (Leeds, UK);

– within the implementation of international projects under the European programs TEMPUS MASTAC, SAFEGUARD, GREENCO, SEREIN, CABRIOLET, ERASMUS + (ALIOT), FP7 (KhAI-ERA) [22], Horizon 2020 (ECHO) [23], COST Action DigForAsp [24], SPEAR [25], as well as in the implementation of national projects commissioned by the Ministry of Education and Science, the National Academy of Sciences of Ukraine in 2010–2020.The implementation in RPC Radics LLC has reduced the risks of cybersecurity violations in the development and implementation of NPP information and management systems. The implementation in PJSC SRPA Impulse allowed increasing the competence of operational personnel to ensure the protection of components of distributed intelligent power systems from cyberthreats. The completeness of cybersecurity increases by 20–30 %. The implementation of the results in LLC "XAI-MEDICA" allowed automating the process of the medical device functional behavior modeling, to reduce the evaluation time and to provide recommendations for ensuring the warranty and selection of evaluation tools. The implementition in LLC "SPCompany" Railwayautomatics" allowed reducing the risks of cybersecurity violations during the development and implementation of the software and hardware set "TEMP". While using it in PJSC "FED" it was possible to reduce time costs, automate the process and increase the credibility of assessing the reliability of industrial IoT, to provide recommendations for ensuring the dependability and choice of assessment tools. The implementation of the research results in scientific and technical design bureau "POLISVIT" allowed reducing the time spent on assessing the security of systems, increasing the credibility of the assessment and confirming compliance with the requirements of technical and regulatory documentation. The implementation of the results at the PJSC "Institute of Information Technologies" has reduced the risks of cybersecurity violations in the development and implementation of cryptographic information security systems.

The use of research results at enterprises allowed obtaining technical and economic indicators that correspond to the level and exceed the best domestic and world counterparts.

The use of research results in the educational process and scientific work of the National Aerospace University "KhAI", Pukhov Institute for Modelling in Energy Engineering, Volodymyr Dahl East Ukrainian National University, Tallinn Technical University, Institute of Informatics and Technology "Alessandro Faedo" of the National Research Council of Italy ISTI-CNR (Pisa, Italy), Leeds Beckett University (Leeds, UK), as well as in the implementation of international projects of the European programmes TEMPUS and ERASMUS+, the seventh framework program to support research activities FP7, the framework program of the European Union for Research and Innovation "Horizon 2020" funded by the EU, as well as state budget projects allowed to increase the fundamentality, clarity and practical orientation of the educational process and scientific activity.

Further research of the authors is aimed at detailing the developed models, methods and technologies to ensure the dependability of complex ICSIoT.

Research currently continues withing the ECHO project (creation of the European Network of Cyber Security Centers and the Center of Competence for Innovation and Operations). The developed methods of ensuring the dependability of complex ICSIoT s form the basis for identifying intersectoral and transversal challenges and opportunities in cybersecurity in various sectors as health, transport, manufacturing, telecommunications, energy, finance, management, space, defense.

The results of the research, presented in this paper, will be further used and developed in the doctoral dissertation on "Methodology for ensuring the dependability of IIoT systems", in research projects under the funding program Horizon 2020 – ECHO and STARC and in public research proceedings commissioned by the Ministry of Education and Science of Ukraine.

CONCLUSIONS

The paper proposes a conception that includes a set of scientific and applied tasks for the development of methods, tools and technologies for the creation and implementation of dependable information & analytical and information & control systems for critical applications based on the Internet of Things. The following results were obtained:

1. The conception principles of ensuring the reliability of Information and control systems of critical applications based on Internet of Things, which are based on the development of von Neumann's paradigm of creating reliable and secure systems based on insufficiently reliable and secure components.

2. The normative profile of ICSIoT was developed, which takes into account and harmonizes the list and content of requirements of international and national standards, which allow to make decisions on compliance of such systems with requirements in terms of reliability, availability, functional and cybersecurity, as well as to take them into account during development and modernization of ICSIoT.

3. Mathematical models and methods for assessing the performance, availability, functional and cybersecurity of ICSIoT were developed and researched, taking into account different types of failures and cyberattacks on systems that allow to analyze their functional behavior, improve assessment accuracy and formulate recommendations for selection hardware and software components, architecture, interaction protocols, etc.

4. Methods of creating dependable I ICSIoT for various complexes (medical, energy, industrial, communica-

DOI 10.15588/1607-3274-2020-4-14

tion, etc.) and ensuring their reliability and safety in the development, modernization and use were developed.

5. Tools and information technologies to support decision-making in the creation, modernization and maintenance of ICSIoT for medical, energy, industrial, communication systems and complexes were developed and implemented.

In general, the authors obtained a number of technical and economic indicators, which are provided by the implementation of the results of scientific proceeding, correspond to the level and exceed the best domestic and world analogues.

The results of the presented study were implemented at eight enterprises of Ukraine in the fields of energy, medicine, mechanical engineering, aerospace industry, transport systems, as well as in the development of state regulations in the field of critical infrastructures. The obtained results are used in the educational process of three universities of Ukraine, two universities of the European Union (Estonia, Italy) and the University of Great Britain, as well as in the implementation of eleven international projects funded by the EU.

Some results of the study were also used in the development of draft regulations at the state level on the classification of critical information infrastructure by criticality and the criteria and procedure for classifying critical information infrastructure as critical. The implementation of the developed documents is an important step in building the Ukrainian state system of protection of critical information infrastructure.

ACKNOWLEDGEMENTS

The scientific and educational results obtained during the research have been implemented and supported by the project STARC (Methodology of SusTAinable Development and InfoRmation Technologies of Green COmputing and Communication) funded by the Ministry of Education and Science of Ukraine. These results were supported by the ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations) project which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no 830943. The authors very appreciated to scientific society of consortium and in particular the staff of the Department of Computer Systems, Networks and Cybersecurity of National Aerospace University «Kharkiv Aviation Institute» for discussing the results of the paper.

REFERENCES

1. Kharchenko V. (editor), Kor A-L., Rucinski A. Dependable IoT for human and industry modeling, architecting, implementation, *River Publishers Series in Information Science and Technology*. Denmark, 2019, 566 p.
2. Avizienis A., Laprie J. C., Randell B. et al. Basic concepts and taxonomy of dependable and secure computing [Text], *IEEE transactions on dependable and secure computing*, 2004, Vol. 1, №1, pp. 11–33. DOI 10.1109/TDSC.2004.2.
3. Fitzgerald J., Ingram C., Romanovsky A. Concepts of dependable cyber-physical systems engineering: model-based approaches [Electronic resource]. London, CRC Press, 2016, pp. 1–22. Access mode: https://eprint.ncl.ac.uk/230739.
4. Al-Fuqaha A., Guizani M., Mohammadi M. et al Internet of Things: A survey on enabling technologies, protocols, and applications [Text], *IEEE Communications Surveys & Tutorials*, 2015, Vol. 17, № 4, pp. 2347–2376. DOI: 10.1109/COMST.2015.2444095.
5. Henkel J., Pagani S., Amrouch H., et al. Ultra-low power and dependability for IoT devices (Invited paper for IoT technologies) [Text], *Design, Automation & Test in Europe Conference & Exhibition (DATE): proceedings*, 2017, pp. 954–959. DOI: 10.23919/DATE.2017.7927129.
6. Macedo D., Guedes L. A., Silva I. A dependability evaluation for Internet of Things incorporating redundancy aspects, *11th IEEE International conference on networking, sensing and control: proceedings*, 2014, pp. 417–422. DOI: 10.1109/icnsc.2014.6819662.
7. Ojie E., Pereira E. Exploring dependability issues in IoT applications, *The second international conference on internet of things, data and cloud computing – ICC'17): proceedings*, 2017, pp. 1–5. DOI:10.1145/3018896.3036364.
8. Bellini A., Bellini E., Gherardelli M., et al. Enhancing IoT data dependability through a blockchain mirror model [Text], *Future Internet,* 2019, Vol. 11, No. 5, pp. 1–9. DOI: 10.3390/fi11050117.
9. Bagchi S., Siddiqui M.-B., Wood P., et al. Dependability in edge computing [Text], *Communications of the ACM,* 2020, Vol. 63, No. 1, pp. 58–66. DOI 10.1145/3362068.
10. Boano C. A., Romer K., Roderick B., et al. Dependability for the Internet of Things – from dependable networking in harsh environments to a holistic view on dependability [Text], *Elektrotechnik und Informationstechnik,* 2016, Vol. 133, pp. 304–309. DOI: 10.1007/s00502-016-0436-4.
11. Illiashenko O., Potii O., Komin D. Advanced security assurance case based on ISO/IEC 15408, *Advances in intelligent systems and computing. International conference on dependability and complex systems DepCoS-RELCOMEX 2015 (June 29 – July3, 2015, Lwówek Śląski). Lwówek Śląski,* Poland. Theory and engineering of complex systems and dependability. DepCoS-RELCOMEX 2015. Springer, Cham: proceedings, 2015, Vol. 365, pp. 391–401. DOI: 10.1007/978-3-319-59415-6_7.
12. Strielkina A., Volochiy B., Kharchenko V. Model of functional behavior of healthcare Internet of Things device, *10th International conference on dependable systems, services and technologies (DESSERT): proceedings*, 2019, pp. 63–69. DOI: 10.1109/dessert.2019.8770020.
13. Strielkina A., Kharchenko V., Uzun D. Availability models of the healthcare Internet of Things system taking into account countermeasures selection, *Information and communication technologies in education, research, and industrial applications*, 2019, Vol. 1007, pp. 220–242. DOI: 10.1007/978-3-030-13929-2_11.
14. Kolisnyk M., Kharchenko V., Kharchenko V., Kondratenko Y., Kacprzyk J. (edits). A Markov model of IoT system availability considering DDoS attacks, patching and energy modes, *Green IT Engineering: social, business and industrial applications*. Springer International Publishing. Book, 2018, pp. 185–207. DOI: 10.1007/978-3-030-00253-4_9.
15. Kolisnyk M., Kharchenko V. Investigation of the smart business center for IoT systems availability considering attacks on the router, *Dependable IoT for human and industry. Modeling, architecting, implementation, dependable IoT for human and industry modeling, architecting, implementation*.

DOI 10.15588/1607-3274-2020-4-14

River Publishers series in information science and technology, Denmark, 2019, pp. 169–191.
16. Kolisnyk M., Kharchenko V., Piskacheva I. et al.; Kharchenko, V. (edits). Markov's model-based technique of IoT system availability considering DDoS attacks [Text], *Secure and resilient computing for industry and human domains. Techniques, tools and assurance cases for security and resilient computing*. Kharkiv, Department of education and science of Ukraine, National Aerospace University named after N. E. Zhukovsky "KhAI", 2017, 449 p.
17. Strielkina A., Uzun D., Kharchenko V., et al. Modeling and availability assessment of mobile healthcare IoT using tree analysis and queueing theory, *Dependable IoT for human and industry modeling, architecting, implementation*. River Publishers series in information science and technology. Denmark, 2019, pp. 105–126.
18. Strielkina A., Illiashenko O., Zhydenko M., et al. Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment [Text], *2018 IEEE 9th International conference on dependable systems, services and technologies (DESSERT): proceedings,* 2018, pp. 67–73. DOI: 10.1109/dessert.2018.8409101.
19. Kolisnyk M., Kharchenko V., Piskachova I., et al. Reliability and security issues for IoT-based smart business center: architecture and Markov model [Text], *The World conference IEEE: MCSI. 2016, Greece, Chania: proceedings*, 2016, pp. 313–318.
20. Illiashenko O. O., Kharchenko V. S., Kor A. Gap-analysis of assurance case-based cybersecurity assessment: technique and case study, *Advanced Information Systems*. Kharkiv, НТУ «ХПІ», 2018, Vol. 2. No. 1, pp. 64–68. DOI: 10.20998/2522-9052.2018.1.12.
21. Kharchenko V., Illiashenko O. Concepts of green IT-engineering: taxonomy, principles and implementation, *Studies in systems, decision and control*, 2017, Vol. 74, pp. 3–19. DOI: 10.1007/978-3-319-44162-7_1.
22. FP7 KhAI-ERA project website [Electronic resource]. Access mode: http://khai-era.khai.edu/.
23. Horizon2020 ECHO project website [Electronic resource]. Access mode: https://echonetwork.eu/.
24. DigForAsp project website [Electronic resource]. Access mode: https://digforasp.uca.es/.
25. Horizon 2020 SPEAR project website [Electronic resource]. Access mode: https://www.spear2020.eu/.

Received 20.06.2020.
Accepted 04.08.2020.

УДК 004.93

КОНЦЕПЦІЯ І ВПРОВАДЖЕННЯ ҐАРАНТОЗДАТНИХ СИСТЕМ НА ОСНОВІ ІНТЕРНЕТУ РЕЧЕЙ

Ілляшенко О. О. – кандидат технічних наук, доцент кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Колісник М. О. – докторантка, кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Стрєлкіна А. А. – доктор філософії, асистент кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Коцюба І. В. – кандидат технічних наук, головний інженер проекту Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова Національної академії наук України, Київ, Україна.

Харченко В. С. – доктор технічних наук, професор, Лауреат Державної премії України у галузі науки і техніки, Заслужений винахідник України, завідувач кафедри комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

АНОТАЦІЯ

Актуальність. Проблема проектування, розробки, обслуговування та введення в експлуатацію гарантоздатних систем, побудованих з використанням інтернету речей на основі парадигми фон Неймана про «створення надійних систем з ненадійних компонентів» для надійних сервіс-орієнтованих систем та інфраструктур.

Метод. В статті запропоновано концепцію побудови ґарантоздатних систем на основі інтернету речей, проведений мультисекторальний аналіз методів і моделей оцінки надійності та кібербезпеки (ґарантоздатності) інформаційно-керуючих системи критичного застосування на основі інтернету речей для різних доменів: енергетичного, медичного, індустріального та ін. Аналіз показав, що деякі відмови і збої технічних засобів і програмного забезпечення, кібератаки і післядія впливу атак однакові для всіх доменів, але існують специфічні особливості для кожного домену, які необхідно враховувати при розробці методології забезпечення ґарантоздатності інформаційно-керуючих системи критичного застосування на основі інтернету речей.

Результати. Розроблена концепція, методи, засоби та технології створення та впровадження гарантоздатних інформаційно-керуючих систем критичного застосування на основі інтернету речей.

Висновки. У статті запропоновано концепцію, яка включає набір наукових та прикладних завдань щодо розробки методів, засобів та технологій для створення та впровадження гарантоздатних інформаційно-аналітичних та інформаційно-керуючих систем критичного застосування на основі інтернету речей. Перспективи подальших досліджень можуть включати деталізацію розроблених моделей, методів та технологій для забезпечення надійності складних інформаційно-керуючих систем критичного застосування на основі інтернету речей.

КЛЮЧОВІ СЛОВА: інформаційно-керуючі системи критичного застосування, інтернет речей, ґарантоздатність, кібербезпека, функційна безпечність.

DOI 10.15588/1607-3274-2020-4-14

УДК 004.93

КОНЦЕПЦИЯ И ПРИМЕНЕНИЕ ГАРАНТОСПОСОБНЫХ СИСТЕМ НА ОСНОВЕ ИНТЕРНЕТА ВЕЩЕЙ

Ильяшенко О.А. – кандидат технических наук, доцент кафедры компьютерных систем, сетей и кибербезопасности Национального аэрокосмического университета им. Н.Е. Жуковского «Харьковский авиационный институт», Харьков, Украина.

Колесник М. А. – докторант, кандидат технических наук, доцент, доцент кафедры компьютерных систем, сетей и кибербезопасности Национального аэрокосмического университета им. Н.Е. Жуковского «Харьковский авиационный институт», Харьков, Украина.

Стрелкина А. А. – доктор философии, ассистент кафедры компьютерных систем, сетей и кибербезопасности Национального аэрокосмического университета им. Н.Е. Жуковского «Харьковский авиационный институт», Харьков, Украина.

Коцюба I. В. – кандидат технических наук, главный инженер проекта Института проблем моделирования в энергетике им. Е. Пухова Национальной академии наук Украины, Киев, Украина.

Харченко В. С. – доктор технических наук, профессор, Лауреат Государственной премии Украины в области науки и техники, Заслуженный изобретатель Украины, заведующий кафедрой компьютерных систем, сетей и кибербезопасности Национального аэрокосмического университета им. Н. Е. Жуковского «Харьковский авиационный институт», Харьков, Украина.

АННОТАЦИЯ

Актуальность. Проблема проектирования, разработки, обслуживания и ввода в эксплуатацию гарантоспособных систем, построенных с использованием Интернета вещей на основе парадигмы фон Неймана о «создании надежных систем из ненадежных компонентов» для надежных сервис-ориентированных систем и инфраструктур.

Метод. В статье предложена концепция построения гарантоспособных систем на основе Интернета вещей, проведенный мультисекторный анализ методов и моделей оценки надежности и кибербезопасности (гарантоспособности) информационно-управляющих систем критического применения на основе Интернета вещей для разных доменов: энергетического, медицинского, промышленного и др. Анализ показал, что некоторые отказы и сбои программного обеспечения, кибератаки и последействие влияния атак одинаковы для всех доменов, но существуют специфические особенности для каждого домена, которые необходимо учитывать при разработке методологии обеспечения гарантоспособности систем притического применения на основе Интернета вещей.

Результаты. Разработана концепция, методы, средства и технологии создания и внедрения гарантоспособных информационно-управляющих систем критического применения на основе Интернета вещей.

Выводы. В статье предложена концепция, которая включает набор научных и прикладных задач по разработке методов, средств и технологий для создания и внедрения гарантоспособных информационно-аналитических и информационно-управляющих систем критического применения на основе Интернета вещей. Перспективы дальнейших исследований могут включать детализацию разработанных моделей, методов и технологий для обеспечения надежности сложных информационно-управляющих систем критического применения на основе Интернета вещей.

КЛЮЧЕВЫЕ СЛОВА: информационно-управляющие системы критического применения, Интернет вещей, гарантоспособность, кибербезопасность, функциональная безопасность.

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Kharchenko V. (editor). Dependable IoT for human and industry modeling, architecting, implementation / V. Kharchenko, A-L. Kor, A. Rucinski // River Publishers Series in Information Science and Technology. – Denmark, 2019. – 566 p.
2. Basic concepts and taxonomy of dependable and secure computing [Text] / [A. Avizienis, J. C. Laprie, B. Randell, et al.] // IEEE transactions on dependable and secure computing. – 2004. – Vol. 1, № 1. – P. 11–33. DOI 10.1109/TDSC.2004.2.
3. Fitzgerald J. Concepts of dependable cyber-physical systems engineering: model-based approaches [Electronic resource] / J. Fitzgerald, C. Ingram, A. Romanovsky. – London : CRC Press, 2016. – P. 1–22. Access mode: https://eprint.ncl.ac.uk/230739.
4. Internet of Things: A survey on enabling technologies, protocols, and applications [Text] / [A. Al-Fuqaha, M. Guizani, M. Mohammadi, et al.] // IEEE Communications Surveys & Tutorials. – 2015. – Vol. 17, № 4. – P. 2347–2376. DOI: 10.1109/COMST.2015.2444095.
5. Ultra-low power and dependability for IoT devices (Invited paper for IoT technologies) [Text] / J. Henkel, S. Pagani, H. Amrouch, et al.] // Design, Automation & Test in Europe Conference & Exhibition (DATE): proceedings. – 2017. – P. 954–959. DOI: 10.23919/DATE.2017.7927129.
6. Macedo D. A dependability evaluation for Internet of Things incorporating redundancy aspects / D. Macedo, L. A. Guedes, I. Silva // 11th IEEE International conference on networking, sensing and control: proceedings. – 2014. – P. 417–422. DOI:10.1109/icnsc.2014.6819662.
7. Ojie E. Exploring dependability issues in IoT applications. / E. Ojie, E. Pereira // The second international conference on internet of things, data and cloud computing – ICC'17): proceedings. – 2017. – P. 1–5. DOI:10.1145/3018896.3036364.
8. Enhancing IoT data dependability through a blockchain mirror model [Text] / [A. Bellini, E. Bellini, M. Gher-

DOI 10.15588/1607-3274-2020-4-14

ardelli, et al.] // Future Internet. – 2019. – Vol. 11, № 5. – P. 1–9. DOI:10.3390/fi11050117.

9. Dependability in edge computing [Text] / [S. Bagchi, M.-B. Siddiqui, P. Wood, et al.] // Communications of the ACM. – 2020. – Vol. 63, № 1. – P. 58–66. DOI 10.1145/3362068.
10. Dependability for the Internet of Things – from dependable networking in harsh environments to a holistic view on dependability [Text] / [C. A. Boano, K. Romer, B. Roderick, et al.] // Elektrotechnik und Informationstechnik. – 2016. – Vol. 133. – P. 304–309. DOI: 10.1007/s00502-016-0436-4.
11. Illiashenko O. Advanced security assurance case based on ISO/IEC 15408 / O. Illiashenko, O. Potii, D. Komin // Advances in intelligent systems and computing. International conference on dependability and complex systems DepCoS-RELCOMEX 2015 (June 29 – July 3, 2015, Lwówek Śląski). Lwówek Śląski, Poland. Theory and engineering of complex systems and dependability. DepCoS-RELCOMEX 2015. Springer, Cham : proceedings. – 2015. – Vol. 365. – P. 391–401. DOI: 10.1007/978-3-319-59415-6_7.
12. Strielkina A. Model of functional behavior of healthcare Internet of Things device / A. Strielkina, B. Volochiy, V. Kharchenko // 10 th International conference on dependable systems, services and technologies (DESSERT) : proceedings. – 2019. – P. 63–69. DOI: 10.1109/dessert.2019.8770020.
13. Strielkina A. Availability models of the healthcare Internet of Things system taking into account countermeasures selection / A. Strielkina, V. Kharchenko, D. Uzun // Information and communication technologies in education, research, and industrial applications. – 2019. – Vol. 1007. – P. 220–242. DOI: 10.1007/978-3-030-13929-2_11.
14. Kolisnyk M. A Markov model of IoT system availability considering DDoS attacks, patching and energy modes / M. Kolisnyk, V. Kharchenko // Green IT Engineering: social, business and industrial applications / V. Kharchenko, Y. Kondratenko, J. Kacprzyk (edits). – Springer International Publishing. Book. – 2018. – P. 185–207. DOI: 10.1007/978-3-030-00253-4_9.
15. Kolisnyk M. Investigation of the smart business center for IoT systems availability considering attacks on the router / M. Kolisnyk, V. Kharchenko // Dependable IoT for human and industry. Modeling, architecting, implementation, dependable IoT for human and industry modeling, architecting, implementation. – River Publishers series in information science and technology, Denmark. – 2019. – P. 169 – 191.
16. Markov's model-based technique of IoT system availability considering DDoS attacks [Text] / [M. Kolisnyk, V. Kharchenko, I. Piskacheva et al.]; Kharchenko V. (edits). // Secure and resilient computing for industry and human domains. Techniques, tools and assurance cases for security and resilient computing. – Kharkiv : Department of education and science of Ukraine, National Aerospace University named after N. E. Zhukovsky "KhAI". – 2017. – 449 p.
17. Modeling and availability assessment of mobile healthcare IoT using tree analysis and queueing theory / [A. Strielkina, D. Uzun, V. Kharchenko, et al.] // Dependable IoT for human and industry modeling, architecting, implementation. – River Publishers series in information science and technology, Denmark. – 2019. – P. 105–126.
18. Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment [Text] / [A. Strielkina, O. Illiashenko, M. Zhydenko, et al.] // 2018 IEEE 9th International conference on dependable systems, services and technologies (DESSERT): proceedings. – 2018. – P. 67–73. DOI: 10.1109/dessert.2018.8409101.
19. Reliability and security issues for IoT-based smart business center: architecture and Markov model [Text] / [M. Kolisnyk, V. Kharchenko, I. Piskachova, et al.] // The World conference IEEE: MCSI. 2016, Greece, Chania: proceedings. – 2016. – P. 313–318.
20. Illiashenko O. O. Gap-analysis of assurance case-based cybersecurity assessment: technique and case study / O. O. Illiashenko, V. S. Kharchenko, A. Kor // Advanced Information Systems. – Kharkiv : НТУ «ХПІ». – 2018. – Vol. 2, № 1. – P. 64–68. DOI: 10.20998/2522-9052.2018.1.12.
21. Kharchenko V. Concepts of green IT-engineering: taxonomy, principles and implementation / V. Kharchenko, O. Illiashenko // Studies in systems, decision and control. – 2017. – Vol. 74. – P. 3–19. DOI: 10.1007/978-3-319-44162-7_1.
22. FP7 KhAI-ERA project website [Electronic resource]. – Access mode: http://khai-era.khai.edu/.
23. Horizon2020 ECHO project website [Electronic resource]. – Access mode: https://echonetwork.eu/.
24. DigForAsp project website [Electronic resource]. – Access mode: https://digforasp.uca.es/.
25. Horizon 2020 SPEAR project website [Electronic resource]. – Access mode: https://www.spear2020.eu/.

DOI 10.15588/1607-3274-2020-4-14