The 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
21-23 September, 2017, Bucharest, Romania

Internet of Things: Hierarhy of Smart Systems

Dmitry Maevsky [1], Andriy Bojko [1], Elena Maevskaya [1], Oleksandr Vinakov [1], Lyudmila Shapa [1]
[1] Odessa National Polytechnic University, 1, Shevchenko ave., 65041, Ukraine
Dmitry.A.Maevsky@opu.ua, a.o.boyko@opu.ua, E.J.Maevskaya@opu.ua, afvinakov@opu.ua, l.n.shapa@opu.us

***Abstract*—This paper is the first attempt to carry out the system analysis of Internet of Things as a global and booming object. The hierarchical IoT division into subsystems has been made. The main function executed by certain subsystem is chosen as a criterion of division. The scale of degrees of risks, which can emerge because of negative factors, arising in each of the subsystems is offered. The scale of degrees of risks allows to assess the own risks and cross risks in IoT subsystems. According to the experts involved in the process of assessment the scale is able to indicate the risks emerging at all IoT hierarchy levels. The authors show that the biggest risks emerge in the highest-level system – the one of Internet of Things as a global and planetary object. The directions of the further research of IoT system risks are formulated.**

Keywords—IoT; smart systems; hierarcy; risk; risk analysis

I. INTRODUCTION

The fact is that a human being is a system containing a set of systems in himself and surrounded by systems. Throughout his life a continuous interaction of these systems occurs. One can say that life itself is a system interaction process. As Genrich Altshuller [1] has showed all systems a human is surrounded with can be classified into two types. The first type includes the ones, which were created by the nature without human activity, and function according to the laws of nature. Such kind of systems are called “natural (inartificial) systems”. The second one embraces artificial systems created by a human to satisfy his needs. They were created for a specific purpose. This purpose determines a so-called “main function” of artificial systems. All artificial systems unlike the natural ones possess necessarily their main function.

Among a huge variety of artificial systems one should allocate the so-called Intelligent Systems (IS), which are able to solve problems traditionally considered to be the creative ones and referred to some specific subject area, and the knowledge of the area are stored in this system memory [2]. In recent years, such types of systems have been widely spread especially due to the rapid development of Internet of Things (IoT). It is they which control traffic flows, nuclear and thermal power plants, and medical equipment at present. From year to year the mankind becomes more and more dependent on IS entrusting more and more functions to them.

Naturally the risks associated with IS malfunctioning or stopping their functioning [3] increase significantly. Moreover, an unauthorized access to such kind of systems allows a malefactor to receive tangible benefits. This fact increases the risks of illegal target influence on IS even more. That is why the task to analyze such types of risks and the effects of illegal target influence on IS is actual and timely.

In the given article, the fragmentation of IS IoT into levels in accordance with the main system function is offered. In addition, the developed risk scale and the performed evaluation of risk effects for different IS levels, which are used in functioning the current IoT systems, are presented.

II. STATE OF THE ART

Internet of Things in general and the problem of its safety and security in particular is a relatively new line of research. However, in recent year the significant growth of amount of articles dealing with IS reliability and safety can be observed. All researchers understand that widespread IS IoT implementation in the modern society can have risky consequences for its existence. The virus attack on uranium enrichment plants in Iran in 2010 [4] was without radiation leakage and human victims only by chance.

But this attack has shown that a potential target of terrorists can become the objects the destruction or disruption of which will influence catastrophically on the human habitat.

The complete analysis of literature on the problem of IS IoT safety and security is impossible within a short article since only the “Internet of Things security” keyword search in e.g. IEEE Xplore Electronic Library shows more than 2700 items. A similar search for the words "Internet of Things safety" gives 525 items.

That is why we will consider only the main trends in this mass of information and present the latest articles as the examples.

In [5] the analysis of approaches to the detection of risks caused by data and IoT device interaction is made. Here the authors propose to use the so-called “social graphs” to detect risks. It is social graphs which commonly help to trace the interaction of users in the social networks. But in the given article a slightly different approach to a social graph construction is offered. As graph nodes, the IoT resources are taken and

its edges are the data, which are transferred between these resources. Such kind of approach allows to apply mathematical apparatus of the social graph theory to the analysis of risks in IoT.

The authors of [6] give their attention to one of the particular issues – IoT system safety used in the field of public health. The real scheme of storing and processing the data concerning chronic diseases of the elderly is taken as the basis. In the article the heuristic approaches are proposed to analyze the risks arisen in storing the personal information in this system.

In [7] the analysis of components of such concepts as "safety" and "security" is made. The authors argue that these concepts contradict each other quite often when they are used for complex industrial control systems. Nevertheless, in order to decrease the risks in operating the industrial control systems one should consider these concepts only in the combination with each other. According to the authors' opinion, it is the methods of system engineering proposed in this article which are able to be useful.

The narration of the previous article subject is continued in [8], in which privacy issues of personal information in IoT systems as well as the risks associated with the breach of confidentiality are considered. The methods of counteraction to these risks are proposed.

The important topic of Maritime safety is touched upon in [9]. The authors note that on the vessels with high risk level such as cruise ships and tankers the monitoring and detailed analysis of its individual systems is required except for the general ship condition monitoring. To solve this problem the IoT sensor pairing system, which was introduced by the authors, capable of transmitting different data of ship sounding to the coastal system is considered.

Article [10] contains question in its title "Is the IoT a tech bubble for cities?"

The concept "a tech bubble" is more economic than technical. The authors mean, that the neoteric and violently developed branches are very much invested in order to get a big profit. Investment of capital in its turn leads to greater growth of these branches which increases the profit got by the investors. And this in its turn increases the investments. In technology, such a phenomenon is called a positive feedback. A "bubble" is formed, which is inflated with money. A "dotcom bubble" has become the biggest "bubble" of such type, which included a huge number of companies trading online. It burst in March 2000 and led to the collapse about 50% companies marketing through Internet [11].

In [10] the authors show the apprehension that the technological project "Smart city" will become such kind of technological bubble. The thing is that the widespread Internet use is supposed in this project as it was in the case with trading online. However, in both cases Internet is just the means only of communication. In the project "Smart city" sensors and executing mechanisms as well as the intellectual system of decision making are to play the main role. And the correctness of the smart city system operation as a whole is dependent on the correct running of all these devices. And the risks of incorrect operation of this system as will be demonstrated further are able to far exceed the expected benefits.

Article [12] deals with the analysis of safety and risks arising in the so-called "Fog of Things" (FoT). The origin of FoT concept is associated with "Internet of things" development. After Internet of things introduction many objects surrounding humans have built-in microprocessors capable of solving the computational problems. Smart phones, "smart watch", "smart spectacles", etc. can be referred to such kinds of objects. This in its turn allows distributing the calculation problems solved by humans among these devices. Such type of parallelism permits to greatly increase the speed of problem solution and simultaneously relieve the load of cloud servers. The computer processing the data can perform their processing not on account of the load on cloud but on account of the neighboring "smart" devices, which are situated near the computer. Thus, the cloud "descends" to an end user and its components are the "smart" devices surrounding a user. Such a descending cloud forms "Fog of Things". And besides the devices, which form the fog, do not necessarily belong to that exact end user! Any of them can be switched off and shifted to solving another problem any moment. E.g. if your neighbor runs his own data processing on your smart phone without your (and his) knowledge but at IoT server will then you can switch your smart phone off and interrupt this processing any moment. If this situation is not correctly approached to the risks of data loss are possible. Article [12] is devoted to the analysis and simulation of such risks.

In [13] the risks of widespread introduction of "smart homes" are considered.

Article [14] concerns the security issues of multimedia content, which is stored and processed in a user's "smart" devices. What is more according to [12] the part of this content can be processed in "Fog of Things" as well.

In [15] an attempt to systematize not individual special cases of IoT implementation but separate components the IoT is constructed. A set of standard criteria evaluating the extent of safety of these or those structures and the method of safety evaluation of all IoT system formed based on these structures have been developed.

One more particularistic direction namely the risks of usage of IoT devices, connected to Smart TV, is considered in [16]. The authors note that such devices fulfill the private information collection about an owner even without his knowledge and consent.

In [17] the authors create the taxonomy of attacks on IoT devices. Four types of network attacks are distinguished and their negative consequences are

analyzed. The attack taxonomy in IoT networks is formed to assist the IoT developers to better understand risks for safety and use more reliable means of protection.

Of all the analysis of articles presented here we have come to the two important conclusions.

Firstly, introducing the IoT technology in human life, we face along with the obvious advantages, the serious threats of technological and social nature. At that, these threats can potentially emerge actually in all directions of IoT implementation.

Secondly, in order to decrease the risks in operating the IoT systems one should together consider both concepts – safety and security.

At last, we should note that the authors in their majority aim at the researches of risks and harmful consequences of comparatively particularistic fields. However, at present there is no research of IoT system risks in general. After all each of the directions considered in this analysis cannot exist and function apart from the others. All of them are connected with each other and form a system. That is why outside the analysis presented in the articles the risks remain, which emerge in interacting the individual subsystems united in one common system called "IoT".

In the given article, an attempt is made to carry out exactly such kind of colligating system analysis and risk evaluation.

III. Hierarchy of Smart Systems

The attempts to construct various hierarchical IoT models were made repeatedly [18, 19, 20]. The basis for the hierarchy construction in [18] is the architecture of IoT construction (sensors, network, applications). In [19] the five-layered (five levelled) model is offered: edge technology layer (level), access gateway layer (level), internet layer (level), middleware layer (level) and application layer (level). In [20], three layered model (three levelled) is suggested. This model has sensing extension layer, network layer and application layer. Sensors and physical devices take part in sensing extension layer. Network layer and application layer fulfills similar task to other models.

The variety of hierarchical models is completely justified because IoT is a multifaceted object and each of the hierarchies is one if its facets. Hereinafter the authors will suggest one more approach to the hierarchy construction based on IoT fragmentation into subsystems based on the main function executed by them. It is true, IoT is an artificial system made by a Moreover, as we already know from [1] every artificial system necessarily possesses its own main function.

According to the type of the main function, the IoT can be represented in the form of hierarchical structure consisting of nine levels:

1. The system of "Internet of things"
2. Smart state
3. Smart area (region, state, federal district, etc.)
4. Smart city
5. Smart district of the city
6. Smart house (apartment house)
7. Smart apartment (dwelling)
8. Smart room (workplace)
9. Smart device.

At the first highest level of hierarchy the IoT system itself exists as a whole phenomenon of the planetary scale. The system functions at this level is to organize the interstate cooperation to solve the problems of civilization survival as a whole. This can be achieved on the account of optimum and timely solutions of environmental, demographic, raw materials and other international problems of modernity.

At the second hierarchical level there is a smart state. Its main function is to ensure the rights and freedoms of citizens on the account of the optimum governing and close interconnection of all state structures.

The third level is the one of a smart region as an independent territorial association in the state. The main IoT function at this level is to organize the sustainable operation of the region's infrastructure.

At the fourth level of the hierarchy a smart city exists as a part of region. We should stress that the word combination "smart city" means not only a modern metropolis with several million inhabitants. City is a territorial unit with its own borders within which some amount of residents' lives. In this aspect, the word "city" means just such a territorial formation. "City" in IoT system is both a metropolis and a small village. The main function of this territorial formation depends on its size, geographic position and natural resources. The main IoT function at this level is the optimum governing of all processes providing vital activity of the city and its connections with other cities.

The fifth level of IoT system is a smart city district. City district is a strictly territorial unit, boundaries of which are conditional. The main IoT function at this level is governing and controlling the systems providing normal conditions of vital activity and interconnections of objects existing in the district territory.

The sixth and seventh IoT levels are devoted to smart house and smart apartment. We are integrating both of these concepts because one can sometimes draw a clear line between them but they are sometimes united in one whole. E.g. if we are speaking of an apartment house these concepts are different. However, if we mean a private house in a cottage village then the concepts "house" and "apartment" are different.

The main function of a smart apartment (or private house) is comfortable conditions of habitation of some small separate group of people – a family as well as its security and energy saving. IoT function in an apartment house is accounting and controlling the resources consumed by a separate apartment.

The eighth IoT level is a smart workplace, the role of which a separate room plays more often in the apartment

or private house. The main function at this level is the provision of comfortable working and rest conditions of one or a few persons.

The last, ninth level consists of strictly speaking smart things that have termed the whole direction – Internet of things. A smart thing is e.g. TV, fridge, washer, microwave, etc. These are things surround a modern person at present but they become more and more intellectual every year. Even now a smart TV is capable of recording the necessary program in the absence of a host independently, and a smart slow cooker – making dinner by his (a host) returning. All this determines the main function of smart things – to meet the specific human needs at a specific time.

As we have seen in transiting from the lowest level to the highest ones of this hierarchy the globalization of the main function occurs, and it becomes more and more common and multipronged. However, IoT is a technical system, in which various accidents and damages are possible. Any accident or damage is ultimately the function execution discontinuation by a subsystem. That is why the evaluation of risks for vital activity of a person, which arise in stopping the main function execution at each of the nine levels of the Internet of things system is a very important and interesting problem.

IV. Risk Assessment Scale

In this article the term "risk" will further preserve its classical definition as the characteristic of situation which has an uncertain outcome in the obligatory presence of adverse effects. To assess the risks the product of probability of an adverse event occurrence by the quantitative assessment of damage from such event is commonly used. However, this approach to the risk assessment is lately criticized. For example, Nassim Nicholas Taleb in the book "Black Swan" notes that events the probability of which is "in the tails of Gaussian curves" have as rule not only adverse but also catastrophic effects. Besides the quantitative damage caused by an event is still open to question. How one can count, for example, a human life in money? Uncertainty of evaluation can be seen especially clear in risk assessment in heterogeneous systems. E.g. in terms of money the fire damage in an apartment and the one in an ammunition depot cannot be compared to each other. However, from the viewpoint of a host of the apartment his personal damage is catastrophic while he is not sensitive to the fire damage somewhere far away in an ammunition depot.

The intellectual subsystems of IoT system distinguished in section III are just such kind of heterogeneous subsystems. That is why in the given article in order to assess the risks in IoT the relative risk evaluation is applied, which is indicated based on negative consequences of some event for this very subsystem.

We will assess the risks arising in smart IoT subsystems on a twelve-point scale the basis of which is the extent of negative effect of risk factor on the main function execution by appropriate subsystem. Let us consider the risk degree scale.

Degree 0 – risk is fully absent.

Degree 1 – there is the most minimal risk the consequences of which are negligible for system functioning, i.e. risk factor may not be eliminated.

Degree 2 – there is a risk the consequences of which are noticeable but do not impact on the main function execution.

Degree 3 – the risk with tangible consequences; risk factor should be eliminated but not immediately.

Degree 4 – the risk with tangible consequences, which have to be eliminated immediately.

Degree 5 – the risk with significant consequences interrupting the main function execution in the acceptable period.

Degree 6 – risk with the consequences interrupting the main function execution in the period close to critical one but not exceeding it.

Degree 7 – risk interrupting the main function execution in the period equal to critical one.

Degree 8 – risk interrupting the main function execution in the period of time, which is more than critical but on eliminating the factor the main function can be restored.

Degree 9 – risk in which the restoring of system functioning is unlike but possible.

Degree 10 – the restoring of functioning is impossible but a system (its elements) is kept.

Degree 11 – complete and irreversible destruction of all of the system elements.

The fact that this scale is based on the main function execution of a subsystem allows applying it in two cases. Firstly, it allows assessing the extent of risk arising from the effect of some negative factor, which emerges in the given subsystem, on the subsystem itself. Secondly, we are able to assess the so-called "cross risks" which arises from the effect of some negative factor, emerging in the given subsystem, on the of the main function execution by the other subsystems. Wherein we can create a risk matrix of the following form: along the main diagonal the own risk assessments are placed, and on the sides – the ones of cross risks. This is especially valuable for IoT system, the subsystems of which are closely integrated one in another.

V. Risk Assessment in Smart Systems

For the quantitative risk assessment with the help of this scale a method of expert evaluation is applied. The authors of this article and the other disinterested specialists in IT field participated as the experts. In all, seven experts were involved for risk assessment. All the experts were implied to have equal qualification. The

results of risk assessment in IoT subsystems are presented in table 1.

The table contains nine lines and nine columns, in which the mean arithmetic assessments of risk given by all experts are registered. The numbers of lines and columns corresponds to the ones of subsystems allocated in section 2.

TABLE I
RESULTS OF RISK ASSESSMENT FOR IOT SMART SYSTEMS

SubS	1	2	3	4	5	6	7	8	9
1	8,5	5,3	4,5	3,3	2,3	0,8	0,0	0,3	0,0
2	7,0	7,0	5,0	3,3	2,5	1,5	0,3	0,0	0,5
3	5,8	5,0	6,0	3,8	2,5	1,3	0,5	0,0	0,5
4	5,0	4,5	5,0	4,5	4,0	2,0	0,8	0,3	0,0
5	3,5	3,5	4,0	4,0	3,8	2,0	1,3	0,5	0,0
6	2,5	2,5	3,3	3,3	3,5	3,5	2,0	1,3	0,8
7	1,8	1,8	2,5	2,3	2,3	3,3	3,0	3,0	2,0
8	0,8	0,5	1,8	1,0	1,5	2,0	3,0	3,0	2,0
9	0,3	0,3	0,8	0,8	1,0	1,5	1,8	2,3	5,3

The table contains nine lines and nine columns, in which the mean arithmetic assessments of risk given by all experts are registered. The numbers of lines and columns corresponds to the ones of subsystems allocated in section 2. In the cells with the similar numbers of line and column (situated on the main diagonal) the degrees of risk arising from the effect of some negative factor, which emerges in the given subsystem, one of the main function execution by this exact subsystem are presented. In the cells with line number i and column *j* the degrees of risk arising from the effect on the subsystem with number *i* from a negative factor, which emerges in the subsystem with number *j* (cross risks) are given.

In order to facilitate the analysis, we should consider several curves, which are created based on the data of table 1.

In Fig. 1 a curve of dependence of the degree of risk for the main function execution by IoT system as a whole (level 1 of the hierarchy) on the negative factors, arising at all other levels, is presented. The numbers of these levels are given along the axis abscissa of the curve.

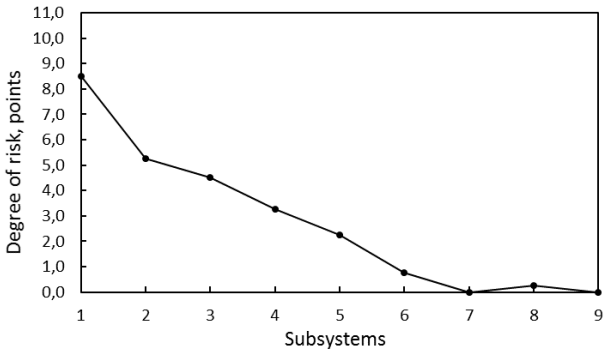

Fig. 1. The degrees of risks for IoT system (level 1)

As we can see in Fig. 1 the highest risk for IoT system corresponds to the global negative factors arising in this very system. In transiting to the lower levels of the hierarchy the risk degree drops fast. A negative factor arising in a subsystem of level 9 (a separate sensor in a workplace) does not effect on the main function execution by a smart house system.

In Fig. 2 the dependence of the degree of risk for the main function execution by a subsystem of level 4 (smart city) on the negative factors, which emerges at all other levels, is shown. To make the comparison of the degrees of risk more suitable the scale of the axis ordinate is similar to the one in Fig. 1.

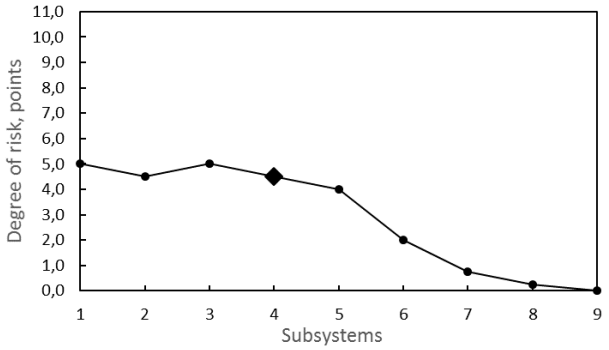

Fig. 2. The degrees of risks for IoT system (level 4)

All experts have come to one and the same conclusion: the risks arising at the “smart city” level (in the subsystem of lower level of the hierarchy) are generally lower than for IoT system. At this level the trend of lowering the risk degree in rising the subsystem hierarchy level persists as well. Indeed all risks for subsystems 5, 6, etc. are lower than the degree of the own risk (marker emphasized with a rhomboid in the curve).

Along with this, the negative factors arising in the higher-level subsystems are simultaneously the most dangerous for the functioning of “smart city”. However, the risks, which emerge in the subsystem of level 9 (“smart things”) do not effect on the “smart city” functioning at all.

However, at the level of the “smart city” subsystem (level 6 of the hierarchy) the degree of risks changes (Fig. 3).

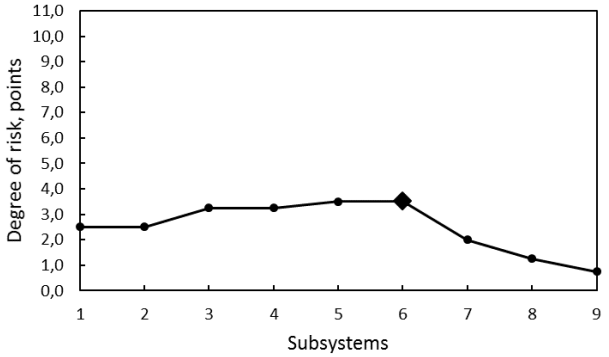

Fig. 3. The degrees of risk for the “smart house” system (level 6)

Firstly, the mean value of risk degree is lower here as a whole than in subsystems of the higher hierarchy level. Secondly, unlike the subsystems considered earlier the negative factors, emerging in the subsystems of higher hierarchy levels, effects more and more on the "smart house" subsystem functioning. And, thirdly, effects of risks, arising from the malfunction of "smart things", on the "smart house" subsystem functioning cannot be negligible.

In Fig. 4 the dependence of the degree of risk for the main function execution by the subsystem of the lowest level (level 9 – "smart things") on negative factors which emerge at all the levels, is shown.

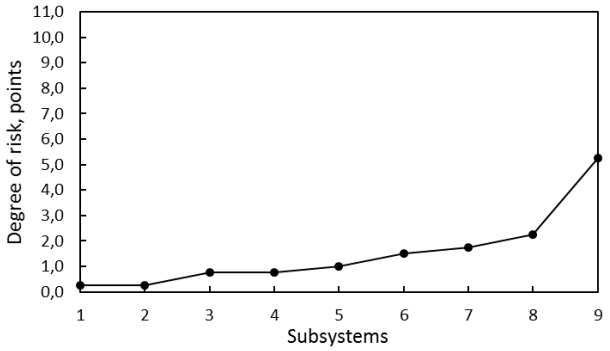

Fig. 4. Degrees of risk for the system "smart thing" (level 9)

The nature of the risk degree changes is completely different here. The "smart things" functioning impacts on all the subsystems. The lower is a subsystem in the hierarchy the more is the effect. And certainly, the greatest danger for a "smart thing" functioning are risk factors inherent in this exact "smart thing".

VI. CONCLUSIONS

If an observer is inside a system, and even more, if he himself is a part of this system he is not able to understand the system functioning. For example, if a person is inside a vehicle and operates it he cannot understand completely how it is arranged. To do it he has to stop first, then get off the vehicle and raise the hood. That is, he should be outside the system or over the system. The articles mentioned in Section II can be called the attempts to understand the vehicle operation without leaving it..

The presented article is the first attempt to have a look at Internet of Things from outside. Here we show IoT structure researched and links between the elements of this structure. On the foundation of these links the following conclusions of the degrees of risks emerging at each of the structure levels have been made:

1. Each of the subsystems emphasized in our paper effects on risks, which are global for all IoT system;
2. The total degree of risks decreases as the subsystem level lowers.
3. The risk factors arising in the given subsystem do not lead to the biggest risk for this exact subsystem in all cases. It can be numerically seen in table 1, in which the maximal number is not always along the main diagonal. The examples of such kinds of subsystems are "smart city", "smart district of the city" and "smart apartment".
4. The biggest risks emerge in the highest-level system – the one of Internet of Things as a global planetary object. At present IoT is not still planetary. But its fast growth shows that the humankind has not a lot of time to analyze the probable global risks and to develop the means to counteract these risks.

According to the authors the issues mentioned in the given article are of great importance. And certainly, we cannot claim here that we are completely covering the problem. That is why the further research directions will be and have to be the following ones:

– more clear determination of the main function of each of the IoT subsystems and more clear distinction of these subsystems;

– further risk scale improvement and particularization;

– to involve as maximal as possible amount of qualified experts in order to assess the risk degrees.

REFERENCES

[1] G. S. Altshuller, *Creativity as an exact science*. Moscow, Soviet Radio, 1979, 174 p. (in Russian)

[2] R. Pfeifer; C. Scheier, "Principles of Intelligent Systems," in *Understanding Intelligence* , 1, MIT Press, 2001, 297 p.

[3] T. Frühwirth, L. Krammer and W. Kastner, "Dependability demands and state of the art in the internet of things," in *2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*, Luxembourg, 2015, pp. 1-4.

[4] E.Nakashima and J. Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say," *The Washington Post*, June 2, 2012

[5] O. Johny, S. Sotiriadis, E. Asimakopoulou and N. Bessis, "Towards a Social Graph Approach for Modeling Risks in Big Data and Internet of Things (IoT)," in *2014 International Conference on Intelligent Networking and Collaborative Systems*, Salerno, 2014, pp. 439-444.

[6] R. M. Savola, P. Savolainen, A. Evesti, H. Abie and M. Sihvonen, "Risk-driven security metrics development for an e-health IoT application," in *2015 Information Security for South Africa (ISSA)*, Johannesburg, 2015, pp. 1-6

[7] M. StJohn-Green, R. Piggin, J. A. McDermid and R. Oates, "Combined security and safety risk assessment — What needs to be done for ICS and the IoT," in *10th IET System Safety and Cyber-Security Conference 2015*, Bristol, 2015, pp. 1-7.

[8] W. Xi and L. Ling, "Research on IoT Privacy Security Risks," in *2016 International Conference on Industrial Informatics - Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII)*, Wuhan, 2016, pp. 259-262.

[9] D. Y. Kim, K. Y. Kim, G. K. Park and J. S. Jeong, "A Study on the Implementation of Intelligent Navigational Risk Assessment System with IoT Sensor," in *2016 Joint 8th International Conference on Soft Computing and Intelligent Systems (SCIS) and 17th International Symposium on Advanced Intelligent Systems (ISIS)*, Sapporo, 2016, pp. 328-333.

[10] P. Valerio, "Is the Iot a tech bubble for cities?: With more cities joining the smart city revolution and investing in sensors and other iot devices, the risk of a new tech bubble is rising," in *IEEE Consumer Electronics Magazine*, vol. 5, no. 1, pp. 61-62

[11] D. Howard, "Welcome to the post-dotcom era," netWorker 5, 2 (June 2001), 26-31.

[12] D. Nunes et al., "FoTSeC — Human Security in Fog of Things," *2016 IEEE International Conference on Computer and Information Technology (CIT)*, Nadi, Fiji, 2016, pp. 743-749.

[13] J. Bugeja, A. Jacobsson and P. Davidsson, "On Privacy and Security Challenges in Smart Connected Homes," *2016 European Intelligence and Security Informatics Conference (EISIC)*, Uppsala, Sweden, 2016, pp. 172-175.

[14] A. Shifa, M. N. Asghar and M. Fleury, "Multimedia security perspectives in IoT," *2016 Sixth International Conference on Innovative Computing Technology (INTECH)*, Dublin, 2016, pp. 550-555.

[15] M. Irshad, "A Systematic Review of Information Security Frameworks in the Internet of Things (IoT)," *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Sydney, NSW, 2016, pp. 1270-1275.

[16] R. L. Rutledge, A. K. Massey and A. I. Anton, "Privacy Impacts of IoT Devices: A SmartTV Case Study," *2016 IEEE 24th International Requirements Engineering Conference Workshops (REW)*, Beijing, 2016, pp. 261-270

[17] M. Nawir, A. Amir, N. Yaakob and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," *2016 3rd International Conference on Electronic Design (ICED)*, Phuket, 2016, pp. 321-326.

[18] F. Jammes, and H. Smit, "Service-oriented paradigms in industrial automation," *IEEE Transactions on Industrial Informatics*, 2005, pp. 62-70.

[19] Y. Bo, H. Guangwen, "Supply chain information transmission based on RFID and internet of things," *ISECS International Colloquium on Computing, Communication, Control and Management*. 2009, 4, pp. 166-169.

[20] S. Chen, Y. Hu, L. Zheng, and S. Xiang, "Research of architecture and application of Internet of Things for smart grid," *International Conference on Computer Science and Service System*, 2012.

[21] N. N. Taleb, The Black Swan: The Impact of the Highly Improbable, Penguin Random House, USA, 2007.