IT Students about Risks and Security of Industrial Internet of Things

Marina S. Chvanova[1], Alexey E. Popovich[2]
Department of Information Systems and Technologies
K.G. Razumovsky Moscow State University of technologies and management (the First Cossack University)
Moscow, Russia
[1]tmbtsu@gmail.com, [2]popovichae@mgutm.ru

Maria S. Anurieva[3], Anastasia V. Frolova[4], Karapet A. Alekyan[5], Dmitry A. Makarov[6]
Department of Mathematical Modeling and Information Technologies
G.R. Derzhavin Tambov State University
Tambov, Russia
[3]anuryeva@mail.ru, [4]fr.anastasia.vit@gmail.com, [5]alekyan188@gmail.com

***Abstract*. The article provides a brief overview of the state and prospects of Industrial Internet of Things (IIoT) development in Russia and all over the world. Presents the results of survey of IT student youth to understand the problems of IIoT, its risks and security. The survey showed that the awareness of the youth audience about the risks and safety of IIoT is insufficient, and the competencies are largely intuitive. The content of training in this field is not systematically formed due to the novelty of the subject matter for Russia.**

***Keywords:* IIoT, IoT, data security.**

I. INTRODUCTION

One of the most important areas in the field of information technology nowadays is the development of the "Internet of Things", a system of integrated computer networks and connected physical objects (things) with embedded sensors and software for data collection and exchange, with the possibility of remote monitoring and control in an automated mode, without human intervention [1]. The B2B direction of industrial Internet of things is of particular interest. This includes M2M solutions, big data, cloud, robotics, etc. From the point of view of its application, IIoT can be used in all sectors: agriculture, transport industry, financial sector, extractive industries, urban infrastructure, medicine, etc. [2]. This is a completely new form of work organization and business models of service delivery. According to the most progressive scenario, the implementation is fully digitized and automated production is controlled by intelligent systems in real time mode, without human intervention, going beyond the boundaries of one enterprise, with the prospect of uniting into a global industrial network of things and services [1]. With regard to dynamic development of this area, it is important to pay attention to the training of computer science students in this filed, since it has its own characteristics and risks. To this end, it seems necessary to understand the state of the situation by interviewing the students themselves for information and the formation of individual ideas. This is useful because of the need to choose a further strategy for training students.

II. RESEARCH

Industrial Internet of Things (IIoT) in Russia and all over the world. Review of the state and development prospects.

2011 is considered the starting year of the development of the Internet of things industry, it was the year when the number of connected physical objects in the world exceeded the number of connected people [2]. One of the key factors that gave impetus to the development of the Internet of things in Russia is state interest. The "Digital Economy of the Russian Federation" program, which was approved in the summer of 2017, has adjusted the industry and the public sector to digitalize.

According to Global Market Insights, the global IIoT market in 2017 reached $ 312.79 billion. During the period from 2017 to 2023 it will grow at an average annual rate of 14.36%. By 2023, its volume will be 700.38 billion dollars. According to forecasts of another agency, Machina Research, by 2025 the global market for industrial Internet of things (equipment, including sensors, software and platforms, services) will reach 484 billion euros [3].

Overall production growth will be a powerful accelerator of the IIoT market in Russia. Experts say that tendencies to this growth against the background of Western sanctions can be traced now [4]. However, there are also constraints to the development of the Internet of things: state of the economy, sanctions, lack of specialized networks for IIoT, lack of investment, lack of specialists, low level of production automation.

According to TAdviser estimates, the Russian IIoT market in 2017 amounted to 93 billion rubles and is expected to grow to 270 billion by 2020. Industrial enterprises, focused in our research, provided about 20% of the market volume (their share will grow to 25% by 2020). The degree of the IIoT penetration in Russia depends largely on the level of state support. Technological solutions replenish the market, and from both international and Russian suppliers, but customers still lack the use of technology scenarios that produce tangible results [5].

Experts call promising ways to use the IIoT in industrial enterprises: the ability to implement complex end-to-end, fully automated business processes, remote monitoring and on-time

maintenance, as well as the provision of new service business models. At the same time, according to IBM research, studying the use of IoT will help global organizations to prevent incidents and increase employee safety. Data collected from sensors is combined with innovative cognitive capabilities and indicators obtained from other external sources (for example, meteorology) [3].

The role of student youth awareness of IIoT for dynamics of its development.

It is important to organize targeted training of students in the field of IIoT. Thus, IIoT Samsung Academy held summer educational program on the Internet of Things, where students gained theoretical knowledge in the field of the Internet of things, as well as practical experience in creating prototypes of IIoT solutions. Participation was attended by 15 students who passed through competitive selection process and 8 teachers from MIPT and MIREA. The program was held in July 2018 on the basis of the Fiztech School of Applied Mathematics and Computer Science [6].

This shows that the state is interested in training of highly qualified personnel in the field of information technologies that can develop, implement and maintain a system of any scale, complexity and functionality.

Based on the above, it is reasonable to conduct a survey of users on the Web, which can help identify awareness of IIoT, risks and security of these technologies.

Student youth survey for understanding IIoT issues, risks and safety.

The general population of our research is made up of Internet users in Russia, who considered as a homogeneous population, represented on the basis of "access to the Internet and the use of Internet resources". We have previously considered questions of features and properties of youth communication in the Internet space [7]. In this study, during the process of developing the topic of communication with Internet users, we conducted an online survey, using the target probability sample. A random selection of respondents from the general population was made by sending out invitations to participate in an online survey and posting a link in social networks to online questioning. Thus, the so-called "method of self-selection" was used. As a result, the total number of respondents was 153 people. The time of the survey is October 2018.

The questionnaire is based on Google Forms cloud technologies. In this case, the object to subject field defines Internet users as the general population and the sample population is composed of this category of citizens, which allows to say about the sufficient objectivity of collected data.

The overwhelming majority of those surveyed are young people between the ages of 19–25 years (76.5%). Only 7.8% of respondents aged 26–35 years took part in the study. The survey showed that the majority of respondents live in cities (71.4%). A small proportion of respondents are from villages (12.2%) and urban-type settlements (10.2%). Based on the processed data and taking into account the goal of the study on maximum indicators, we can say that the hypothetical social portrait of the respondent in our sample is represented by a young man from 19 to 25 years old who lives in a city.

Most respondents are familiar with the term IIoT, it is clear that the respondents studied this question in educational institutions and independently using the Internet. It is also clear that 43% of respondents have never heard of IIoT (Fig. 1).

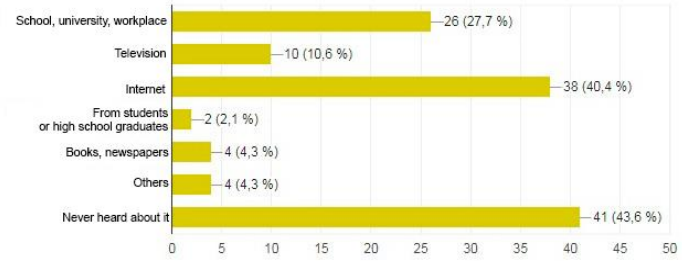

Fig. 2. Answers to the question about the knowledge of the term IIoT

Distribution of answers to the next question showed that the majority of respondents are interested in finding out how the Internet of Things can be used to improve the quality of everyday life of ordinary people (almost 60%), a quarter of the surveyed audience are interested in how IIoT can affect science or electronics (Fig. 2).

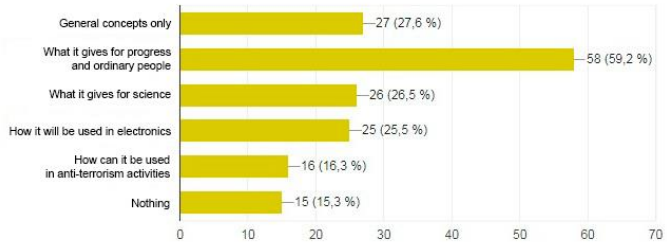

Fig. 3. Answers to the question "What would you like to know about the Internet of things?"

A significant part of respondents believe that the media reviews IIoT on the positive side, the rest of them find it difficult to answer this question (Fig. 3).

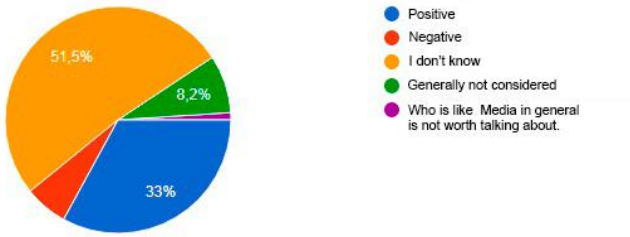

Fig. 4. Answers to the question "Opinion of respondents about the relation of mass-media to the IIoT from a negative or positive point of view"

It is necessary to consider the risks and safety of IIoT. According to the study by Kaspersky Lab [8], incidents with IoT devices are among the top three threats with the greatest financial damage to companies today. This applies to companies of all sizes: small and medium businesses, and large corporations. Realizing these risks, more and more companies

are taking steps to solve the problem of IoT security. More than 100 individuals who make decisions from companies in various industries were interviewed as part of the study "What prevents IoT managers from sleeping at night in 2018", conducted by IoT World. 72% of respondents guaranteed that their enterprises provide all the necessary measures for IoT security. At the same time, 43% of respondents do not test their IoT devices for vulnerabilities at all, which is an alarming signal, and less than half of the respondents have organized an inventory of connected devices. The reformative ability of IoT can be realized only when the safety of the entire ecosystem is priority [9]. Also, in the field of industrial cyber security, Kaspersky Lab experts identify one of their main problems - the lack of uniform standards for ensuring cyber security of industrial enterprises, including the security standards of industrial IoT devices [10].

At the same time, the tendency of Internet of things spread in everyday life of citizens carries not only material risks for society and individuals. Problems of preserving the confidentiality of personal data, reliable storage of large volumes of data using cloud technologies, which also ensure their integrity and availability, are becoming urgent. Today, IoT is one of the most vulnerable areas of information technology in security. Experts note that a safe IoT ecosystem does not exist today [11]. IoT in the context of the spread of targeted attacks is practically unprotected: attackers, interested in something, can effortlessly penetrate the private sector of life with the help of their IoT devices.

Thus, from the point of view of IIoT devices data security, each implementation in an enterprise infrastructure can provoke significant material losses; therefore, information security is crucial in this case. If we consider IoT devices, there is a high risk of interception of confidential data, which can lead to theft of money from bank accounts, as well as unauthorized access of intruders to personal information.

However, the survey showed that a little more than half of the respondents independently (without the suggested response options) found it difficult to determine the possible security risks that bear the active use of the Internet of things. At the same time, 74% of respondents fear leaks of their personal data (Fig. 4).

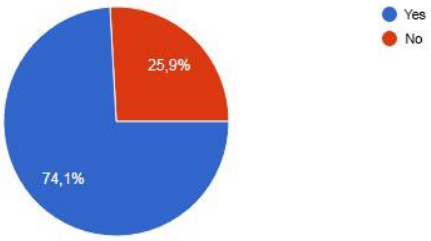

Fig. 5. Diagram showing the opinion of respondents about the risks of personal information loss in IIoT

The following diagram (Fig. 5) shows that the majority of respondents (81%) considers the risk of losing their personal information in the IIoT environment real.

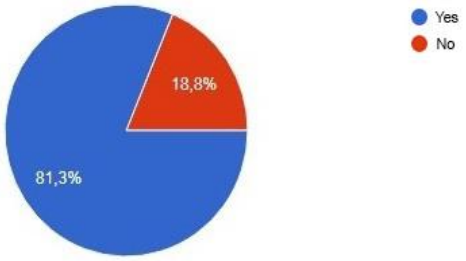

Fig. 6. Answers to the question about the risks of losing information in the Internet of Things environment

III. RESULTS OF THE STUDY

The survey showed that most of the respondents basically have an idea about IIoT (56.4%), a significant part of them learned about it from the Internet (40.4%) and in university (27.7%). The survey results revealed that the majority of respondents (59.2%) are interested in the question of how IIoT influences on progress and directly on society, 26.5% are interested in the potential of IIoT for science, 63.3% believe that IIoT can influence their daily life, but 36.7% believe the opposite.

A significant part of respondents find it difficult to answer what the safety of IIoT may be. However, 74.1% fear personal data leakage during the development of IIoT. The vast majority of respondents (81.3%) understand that there are risks of losing information in IIoT technologies.

Thus, it can be concluded that the awareness of the youth audience about the risks and safety of IIoT is insufficient, and the competencies are largely intuitive. Most likely, as the study showed, this topic is just beginning to be discussed at conferences and summer schools of students. Educational disciplines, one way or another, connected with IIoT have not yet been fully developed at universities. This topic is currently discussed fragmentary, there are practically no discussions of the problem in professional community with students. And announced sections at international conferences on this topic are often not filled with reports with students' participation. These arguments indicate the need to attract an attention of student audience to understanding of processes and problems of IIoT, as well as involvement of students in project activities on these issues.

Certain aspects investigated and the corresponding results obtained with financial support of the Russian Foundation of Basic Research for the project "Pedagogical basics of youth students' socialization in Internet space and their implementation in educational system", No. 17-36-00039, 2017-2019.

IV. REFERENCES

[1] Индустриальный (промышленный) Интернет вещей в мире и перспективы развития в Россиии. [Industrial Internet of Things in the world and prospects for development in Russia] // Analytics ICT and Digital Media. URL: http://json.tv/ict_telecom_analytics_view/mirovoy-opyt-vnedreniya-proektov-v-sfere-industrialnogo-promyshlennogo-interneta-veschey-i-perspektivy-ih-realizatsii-v-rossii--20160919061924.

[1] Индустриальный Интернет вещей в Росии и мире. Обзор состояния и перспективы развития.[Industrial Internet of Things (IIoT) in Russia and the world // Portal on modern technologies of mobile and wireless communications]. URL: http://1234g.ru/novosti/iiot-v-rossii-i-mire.

[2] Промышленный Интернет вещей в России. Исследование TAdviser и ГК «Ростех» [Industrial Internet of Things in Russia. Research TAdviser and Rostec GK]. URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:IIoT_2018:_%D0%A0%D1%8B%D0%BD%D0%BE%D0%BA_%D0%BF%D1%80%D0%BE%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_%D0%B2_%D0%A0%D0%BE%D1%81%D1%81%D0%B8%D0%B8.

[3] Промышленный Интернет вещей в России [Industrial Internet of Things in Russia]. URL: http://www.tadviser.ru/index.php/.

[4] TAdviser: Российский рынок промышленного Интернета в 2017 году достиг 93 млрд рублей [TAdviser: the Russian market of industrial Internet of things in 2017 reached 93 billion rubles. URL: http://www.cnews.ru/news/line/2018-05-21_tadviser_rossijskij_rynok_promyshlennogo_interneta.

[5] Студенты представили прототипы IoT-систем в летней школе Samsung [Students presented prototypes of IoT systems at Samsung Summer School]. URL: https://mipt.ru/news/studenty_predstavili_prototipy_iot_sistem_v_letney_shkole_samsung.

[6] Chvanova M.S., Shlenov Yu.V., Molchanov A.A. et al. New forms of young students' socialization in the Internet space // Quality Management, Transport and Information Security, Information Technologies. 2017. P. 648–651.

[7] Иванов А. Разработаны рекомендации по обеспечению безопасности IoT-устройств. [Ivamov A.Developed safety guidelines for IoT devices]. URL: https://www.anti-malware.ru/news/2017-12-26-1447/25175.

[8] Вайтчерч Г. Главные проблемы для безопасности Интернета вещей [Whitechurch G. Top issues for the security of the Internet of Things]. URL: https://iot.ru/promyshlennost/glavnye-problemy-dlya-bezopasnosti-interneta-veshchey.

[9] Панков Н. Еще один шаг к защите промышленного IoT [Pankov N. Another step towards industrial IoT protection standards]. URL: https://www.kaspersky.ru/blog/enisa-recomendations/19376/.

[10] Информационная безопасность Интернета вещей (Internet of Things). [Information security of the Internet of Things]. URL: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9_(Internet_of_Things).