UDC 330.46
DOI: 10.15587/2312-8372.2017.117593

Kondiloglu A., Bayer H., Celik E., Atalay M.

INFORMATION SECURITY BREACHES AND PRECAUTIONS ON INDUSTRY 4.0

Дане дослідження присвячене вивченню вразливостей і заходів інформаційної безпеки в Industry 4.0. Пропонується план безпеки, який пропорційний організаційним структурам ідентифікації протоколів кібербезпеки для Industry 4.0. Завдяки запропонованому підходу може бути забезпечена безпека інформації, а цінна інформація захищена від атак.

Ключові слова: *Четверта промислова революція (Industry 4.0), інформаційна безпека, безпека кібер-системи, управління ризиками.*

1. Introduction

Industrial revolutions: the first has been the discovery of mechanical workbenches that allow more efficient use of water and steam power. The second has been Henry Ford's production band design and the use of electricity in mass production. The third has been the introduction of programmable machines, which in 1970 caused mechanical and electronic technologies to leave their place in digital technology. The fourth has been in today's industrial revolution [1]. Industry 4.0 has been an industrial strategy plan that is supposed to launch the fourth industrial revolution. On the one hand, there is a trend about the digital communication of smart factories and objects, and on the other hand, a tendency has begun to aim to bring production back to human touch. This inclination is called «Industry 4.0» or collaborative (human and robot association) industries [2].

It seems that in the first stage of the industry 4.0 strategy, the passing of the software and hardware department is not going to be a problem. This is because there will be no problem as the energy to be used for hardware and software is thought to be low and the sixth version of the Internet protocol opens up the way to connect billions of devices to the Internet with IPv6 [3]. But it seems that it is not easy to adapt and program all of the machines to be used in production processes to the standards of Industry 4.0. In the process of converting IPv4 to IPv6; there may be disagreements between companies and stakeholders who do not want to have risks, change can be expensive and financial problems can arise, problems to protect the integrity of production processes may be solved in a long time but the process of digitization as a long way to go to in spite of all these strategies, this way can be covered in a fast way by cooperating [4].

The first industrial revolution has come from the use of machinery, steam and water in factories; the second has based on electricity and serial production; the third has been due to the introduction of computers that allow for improved automation of manufacturing. The fourth industrial revolution has been a blend of technologies that lead to the creation of a 'smart' and versatile 'cyber-physical' production environment. The various intelligent sensors have depended on personal configuration robots, 3D printers, large data analysis and communication channels that send data to large data collectors. With these innovations, privatized products will be promoted faster and at a lower cost, making supply lines more efficient. An obvious challenge for introducing such smart factories is to represent the cypher safely [5]. The technologies, concepts and protocols that make up the industry collectively have been designed with extreme connectivity that can be found wherever they are. It is at the beginning of this innovation period, as it is in the first, second and third revolutions, risks are very high. In each of the previous industrial revolutions, new technologies have been introduced at higher speeds, in larger volumes, at higher temperatures, in more difficult environments, and so on. It means that it is possible to produce things. In this case it carries industrial risk levels. Measures must be taken to prevent or mitigate these risk breaches [6].

The fact that factories work day after day with no incident has been a sign that the technologies used are mature and reliable. Steam engines have broken out from time to time and they have been made reliable. Today, large corporations have been doing things with high risk of fear of large-scale data breaches [7]. The cost of high-profile cyber-attacks on Sony Pictures is huge. However, in the case of cyber-physical systems, the potential damage caused by a computer attack may be even greater. If malicious hackers try to do as much damage as possible by targeting a large chemical plant, it's out of the catastrophic scale. The tendency of everything in the neighbourhood becomes smart. Nevertheless, engineers who design innovative devices must consider the safety implications of their work. Scientists who are looking for solutions to Internet problems are actively involved in developing solutions for industrial IT security and set the standard on a global scale [8].

2. The object of research and its technological audit

The object of research is fourth industrial revolution.

The fourth industrial revolution term was first used at the Hannover Fair in Germany in 2011. Industry 4.0 has been one of the strategies in this area, which was came up on to continue competitive advantages among the increasingly competitive conditions in Germany. The fourth industrial revolution has been a blend of technologies that lead to the creation of a «smart» and versatile «cyber-physical» production environment. It has included various intelligent sensors, personal configuration robots, 3D printers, communication channels that is used for large data analysis and large data collecting. These communication channels have too many risks in terms of personal or public information security. In the fourth industrial revolution, the risks of cyber security devices protecting smart factories from the risks and hazards has become an important issue. At the beginning of this innovation period, legal regulations and standards have been ignored just as in the first, second and third revolutions. Cyber security has not operated in full capacity today because the technologies, concepts and protocols that used for the operations of industry have not been connected to each other. With these innovations, it has been predicted that the privatized products would be promoted faster and at a lower cost, making supply lines more effective.

3. The aim and objectives of research

The aim of this research is ensuring the system's continuity and the complete operation of the existing order, which was emerged with forth industrial revolution's smart factories, or a new order. To achieve this aim, it is necessary to solve the following tasks:

1. To propose the new approaches in the identification of information security and cyber security protocols in Industry 4.0.
2. To determine system vulnerabilities of Industry 4.0 and to remove the deficits.
3. To determine what to do in case of any violation in terms of information security.

4. Research of existing solutions of the problem

According to research, due to the nature of Industry 4.0, where all devices in manufacturing technologies are interconnected, exchanging data and information with each other, broadens the cyber-lands horizons for cyber-criminals to exploit them in their interest. This study makes reference to the industrial control system's modern history and provides information on key technologies, i. e. Internet of Things and cyber-security. Then real case studies are presented and suggestions for effective cybersecurity are presented [9].

According to the scientists, the procedural model for a Cyber-Security analysis based on reference architecture model industry 4.0 and the VDI/VDE guideline 2182 is exemplary shown for the use case of a Cloud-based monitoring of the production. The derived procedure supports the identification of protection demands and allows a risk-based selection of suitable countermeasures [10].

In the article, the impacts of rapid technology development of the fourth industrial revolution present huge challenges for the society and for policy makers. We facing reduction of employment by automation rendering human work force uncompetitive with machines. New fields of employment industry 4.0, new types of jobs can compensate for the loss of traditional labour market requirements [11].

According to researchers, industry 4.0 is a comparatively new method of managing production processes. In the area of risk management, as a result of new approaches, modified frameworks, more complex information technology infrastructure and so on, new types of risks may occur. In this study is conducting research on Industry 4.0 related to key aspects and presentation of a design of framework to implement risk management for the industry 4.0 concept [12].

In study, joining volume, variety and velocity of data, with industry 4.0, makes the opportunity to enhance sustainable innovation in the Factories of the Future. In this, the collection, integration, storage, processing and analysis of data is a key challenge, being Big Data systems required to link all the entities and data require of the factory. In this work, all the data lifecycle, from collection to analysis, is handled, taking into consideration the different data processing speeds that can exist in the real environment of a factory [13].

A process model is developed, which consults Reference Architectural Model Industry 4.0 (RAMI 4.0) and well-established core elements of safety and IT security considering the standards IEC 61508 and IEC 62443. A use case driven approach is developed with the goal to demonstrate the functionalities and validation of the process model. In different iterations, the dynamic change of the system by mapping information technology security requirements on system assets and processes will be presented. The purpose of the developed process model is assigning a security measures to vulnerabilities and threats of a system for Industry 4.0 [14].

Scientists propose a practical approach to establish a security viewpoint in the Cyber-physical Production Systems (CPPS) reference architecture model, based on the draft standard of RAMI 4.0. Scientists have investigated the feasibility of using an architecture modelling tool to implement the concept and leverage existing work on models of layered architecture [15].

The paper propose to modify Privilege Management Infrastructure (PMI) to achieve a scalable access rule management system, with enhancement by introducing trust levels for PMI, associated with extended Attribute Certificates (AC). Using a Privilege Management Infrastructure (PMI) is basis to achieve the security objectives [16].

In this article, scientists exploit the innovative Software Defined Networking (SDN) paradigm to introduce improvements in managing the network infrastructure of industrial networked systems, as this can help in reducing the management costs and complexity. In particular, enhanced SDN functionalities are adopted, which are able to provide security support in additions to their native switching/routing functionalities. The study also shows how this approach can overcome some limitations of many current industry 4.0 systems security architectures [17].

This study examines how the cloud-based applications can meet the industry 4.0 requirements concerning security, communication, self-configuration, reliability, and asset administration shell. The use of cloud computing in an industrial automation domain in order to offer on-demand services, such as alarm flood management or control as a service, is a promising solution [18].

In this study, the implications of functional safety for industry 4.0 are explored. Integrated circuits are fundamental in the implementation of functional safety and therefore to industry 4.0. The implications include requirements for networks, security, robots and software and the semiconductors used to implement these features [19].

This paper develops a systematic methodology for designing intrusion detection systems (IDS) specially tailored to address the cyber and physical dimensions of industry 4.0 systems. The approach is aimed at reducing the number of monitored parameters by adopting a three-phase design strategy embracing sensitivity analysis, cross-association, and optimal IDS design [20].

5. Methods of research

In terms of information security and cyber security in Industry 4.0; the analysis of the existing system, the transformation of the establishment and operation of the new system are carried out by the following methods:

– by the way of comparison; the comparison of the previous industry revolutions with the current industrial revolution and the principles of information security;
– by grouping method; the grouping of industry 4.0 system vulnerabilities, threats and violations;
– by analysis method; the analysing of industry 4.0's existing risks and hazards.

5.1. Security breaches in industry 4.0 and precautions in case of a breach. Violation is the failure to enforce a rule to be applied. Problems in the existing order or a new order to be regulated will affect the continuity of the system and ensure that it is maintained incorrectly or incompletely. It has been so important that the continuity of any company's existing order or the order it is trying to create is as it should be.

It is the responsibility of all personnel to fill in the infringement form created in order to indicate this wrong or incomplete order in case of any infringement, that is to say, in case of a problem in a proper operation performed or in case of incomplete operation. Examples of violation incidents include entering prohibited sites during working hours, leaving the company without completing the permission form, disrupting any department's tasks, and not applying the necessary procedures even though the notification is made [21].

The management of information security incidents is the responsibility of the Information Security Representative. All staff has been immediately report to the Information Security Manager when they become aware of information security breaches and weaknesses. If the violation is personnel based, the process has been carried out according to the disciplinary order. If the supplier is based, the transaction has been started according to the provisions of the bilateral confidentiality agreement. If it is customer based, the provisions of business and confidentiality contracts have been evaluated. The decision on the execution of legal procedures belongs to the General Directorate [22].

Violations and weaknesses have been assessed at least twice a year to identify trends. Measures to be taken, if any, have been passed on at the oversea meeting depending on the risk assessment. The information security breaches in Industry 4.0 and the precautions to take are proposed below. These are:

– The physical security of the computer or information devices used by users has belonged to the user himself/herself. The user's responsbility of password security has started after the user first logs in to the system and then changes the password. Before that, the responsblity has belonged to the Information Security Administrator.
– The user who enters the system for the first time should change his/her password according to the general security regulations within the appropriate protocols and shall not tell anyone. The password security of the in-house logistics software is the responsibility of the user after logging into the system for the first time, before that the responsbility has belonged to business developmetn specialist.
– If the password is invalid or the password is forgotten, the user should contact the relevant system administrators as soon as possible and communicate the situation.
– Avoid unnecessary repetitions that would create a security breach on the wrong password.
– After entering the computer, the user should take the computer in lock mode to avoid a security breach if the computer has been left short or long.
– The company's internal e-mail address should be used only for business purposes, and unnecessary e-mails or spam e-mails or spam should be destroyed immediately by the Information Security Administrator Representative.
– A standard computer user can access the specific knowledge that standard users previously defined in the network environment have. This file can not do anything to access peripheral devices, such as a document or printer, except for rights from the group in which the users are defined. If the user does not have access to the relevant file or document, he/she should contact the network administrator to request access.
– If the user has access to folders, files or network shares outside his authority, he is responsible for notifying the Information Security Administrator Representative as soon as possible. Otherwise it would be a violation of security. The Information Security Administrator is responsible for preventing the user from accessing unauthorized areas or for identifying access to the user.
– In the system, each computer has a different physical address (Mac Address) and network IP address (Internet Protocol). Users can connect properly to the required network resources and access the necessary information and shared resources.
– It is not appropriate for users to enter sites that are banned on the internet and use resources they are not confident about on the internet because of security violations.
– Users who are entering inappropriate or illegal internet sites are monitored and detected by network monitoring devices. Detected users are warned first. Repeated violations are followed by the requirement of internal discipline regulation.
– After accessing the printer, file, or document that the user has access to and performing the necessary operations, the user should disconnect the source and not engage the network unnecessarily. Thus, information security is not violated.
– User should not receive documents or files that are sent by unknown people in the virtual environment according to the «Safety Instruction» and user should not disclose company information within the confidentiality of the company.

– It is strictly forbidden for unauthorized personnel or users to behave in contradiction to general security and instruction such as installing, updating and deleting programs.

– Users should not use data storage disks (USB memory) and other computers in the company unless they are compelled to do so without informing the Information Security Administrator Representative according to security instructions.

– With the approval of the Information Security Administrator, USB or external drives that need to be used internally must be scanned automatically by the antivirus program that is used in the system every time they are used.

– Users should remember that computers are corporate, all music and picture files must be restricted. Music, pictures, etc. can not be available on computers. If there are files like that, they should be deleted. The system is manageable from the center, after a while these things will be done automatically by the system.

– Employers should not buy anything in compliance with unwanted e-mails and donate to charitable institutions.

– Users should not forward chain e-mails. We may be exposed to unsubstantiated news or viruses, because we can not control who can see the e-mails.

– The size of the e-mails to be sent must not exceed 10 MB at a time. It is important to be extremely careful that large e-mails from this size will cause slowness in the system and at the same time cause mail quotas to be filled.

– No unlicensed program installation should be performed on computers in any way. Unlicensed installations can cause even imprisonment in the legal sense for the person who installs.

– If the problems related to the computers or software in the company are very important and serious, they should be notified to the related department by e-mail.

– Computers or computing equipment must not be provided at home for any use in the absence of information from the Information Security Administrator.

– Employees should not keep or disclose company documents containing usb memory, cd, dvd, floppy disks, external harddisk or confidential information at the end of the shift according to general security of system and data processing.

– Management is jointly responsible for the computing devices and their security used within the company, the confidentiality of internal information, and the actions to be taken in violation of information security. These include: detections of virus, intrusion, Trojan, spyware etc., system server service problems, hardware failures, network problems, data loss, unauthorized access to information, theft, loss, burning, breaking, etc. situations, people who has inappropriate behaviours and who do not obey rules, attacking over the network.

5.2. Breaches and dangers against mobile devices of companies and precautions for them. As Cybercrime continues to increase, it is necessary to think not only of personal computers but also of mobile devices that need to be protected. All mobile devices managed by the company or brought by employees must be taken into account in the security plans of the enterprises. It should not be forgotten that employees of the company may have less control over their phones [23].

One of the biggest threats facing open network operators is the use of free Wi-Fi networks to avoid using mobile data payments or avoiding expensive roaming charges. Open and password-free Wi-Fi does not contain enough encryption and it allows hackers to access almost all the information on a user device [24]. For instance, man-in-the-middle attacks can be done. In this type of attack, the device steals can be realized between the device and the wireless connection it is connected to, so that when the user is left unattended, attacker can receive information from the device. At least some of this threat can be decreased by educating the employers about the hazards that arise using unsafe Wi-Fi [25]. In addition, if you educate employees about controlling whether the website uses the HTTPS protocol and accessing encrypted data storage or not, it helps protect valuable corporate information from unsecured Wi-Fi. It is important to consider where employees store data and what applications they use on their devices. Potentially confidential data pose risks to businesses as they are entrusted to third parties' security protocols [26]. For example, employees who store data on mobile phones and Dropbox must trust their passwords to protect it, rather than robust, reliable end-to-end encryption. Using appropriate channels to store information, such as an encrypted Virtual Private Network for employees' mobile devices, is a step toward protecting business assets. While most app stores scan malicious apps, the user may download applications that appear harmless from third-party stores, but contain malware. Once downloaded, they will have the potential to upload malicious software or do other activities. On managed devices, companies can impose restrictions on which applications can be downloaded. By creating a separate enterprise application store through an enterprise mobile management platform, information technology departments can ensure that only approved applications can access corporate information, despite the freedom to download everything employees want to use in their devices [27].

Mobile devices like mobile computers are vulnerable to malware attacks. HummingBad or HummingWhale malware is an example of malware that affects mobile users on Android devices. Incorporating itself into versions of encrypted and trusted applications, it deploys applications that generate fraudulent advertising revenue and collect personal data to be sold along the way. The key here will be prevention rather than treatment [28]. There are many anti-adware, anti-virus, anti-malware and security wall products that can be deployed to a range of enterprise devices to protect against the latest threats in the market. In order to avoid sacrificing infections, fraudulent information can reduce risk and protect institutional data by creating a «firewall» around it [29]. In the meantime, robust security policies can be implemented without invading the privacy of an employee's personal phone, or without enforcing control over an oversight of an employer on a personal device. None of them provide 100 % protection, but training of employees should be a priority.

6. Research results

Phishing and e-mail vectors are suspected for harmful codes designed to disturb the industrial control systems of public services and supply networks of computer viruses that thought to have entered systems over the Internet. Regardless of the form of access, governments and other institutions strive to make the industry more aware of the threats and consequences, but many of today industrial networks are vulnerable to cyber-attacks and protection measures should be taken.

The benefits of industry 4.0 in terms of «smart factories», «Internet of Things» and «big data» could cause that future networks will be much clearer and therefore at an improved risk for a cyber-attack. Smart factories will not only include intelligent machines, called storage systems, but also all kinds of separate production facilities and physical production systems. Industry 4.0 inspiration practices of the physical production system will require base integration of end-to-end information technologies in production systems, from factory floor automation to production execution systems; moreover, they will be subject to extensive web and third party cloud based systems, so it is important to deal with the threat of attack. Potential risks that arise after late deliveries or party inconsistencies go beyond perceived threats such as intellectual property, trademark damage, financial loss, customer complaints, safety of manufacturing staff and even the safety of manufactured products.

7. SWOT analysis of research results

Strengths. If you secure the information in industry 4.0, it is possible to protect the confidential and personal information of the business against attacks and increase the efficiency of production.

Weaknesses. Information security in industry 4.0 can be affected from hardware, software and human factors so its weak points make it complex.

Opportunities. In industry 4.0, robot and human cooperation can contribute to the saving of material resources by increasing productivity.

Threats. There is a possibility that various attacks can be organized to businesses' online and offline security.

8. Conclusions

The authors of the article came to the following conclusions.

1. In industry 4.0, computer users have limited access to the network environment. Security is provided for cyber threats with user authentication protocol or network administrator's permission to access documents or peripheral devices. When the user first enters the system, user must change the password for the security instructions with the appropriate protocols. The user might have a high level security protocol if he or she determines his own password according to mathematical equations. The use of devices containing company information such as corporate phone, computer, memory card, etc. in the free internet (Wi-Fi) environment poses a danger and risk. Pirates can access confidential company information by listening at free internet access points. At this point the user needs to establish a secure connection to the internet. The company can reduce the dangers and risks by using encrypted VPN for all types of data storage devices or complying with firewall protocols.

2. In industry 4.0 there is no problem in entering the system with wrong password. The repeated entry of this incorrect password will force the system and create vulnerability. Destroying this vulnerability has increased the performance of information security. If any unnecessary, commercial, unspecified source and spam mails received via e-mail is blocked or destroyed by the system administrator, the vulnerability in the system will be destroyed. In addition, if system deficits are detected, information security is provided by scanning with anti-virus program or by making operating system updates.

3. In industry 4.0, leaving the computer after logging in to the computer will cause a security breach. In this case, controlling by computer locking or remote access will provide information security. If the computer user can access contents without authority on the network, it will violate the security of information. In this case, if MAC and IP address of the users are tracked with the LOG files, it can ensure effective and instant information security. Entering banned or illegal sites will cause security breaches. This user is identified with network monitoring devices and its internet access will be stopped to prevent information security violations.

References

1. Petro, V. Industry 4.0 and information communication technologies [Text] / V. Petro // 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo). – IEEE, 2017. doi:10.1109/ukrmico.2017.8095359
2. Santos, K. Opportunities Assessment of Product Development Process in Industry 4.0 [Text] / K. Santos, E. Loures, F. Piechnicki, O. Canciglieri // Procedia Manufacturing. – 2017. – Vol. 11. – P. 1358–1365. doi:10.1016/j.promfg.2017.07.265
3. Langmann, R. A PLC as an Industry 4.0 component [Text] / R. Langmann, L. F. Rojas-Pena // 2016 13th International Conference on Remote Engineering and Virtual Instrumentation (REV). – IEEE, 2016. doi:10.1109/rev.2016.7444433
4. Benesova, A. Requirements for Education and Qualification of People in Industry 4.0 [Text] / A. Benesova, J. Tupa // Procedia Manufacturing. – 2017. – Vol. 11. – P. 2195–2202. doi:10.1016/j.promfg.2017.07.366
5. Trstenjak, M. Process Planning in Industry 4.0 Environment [Text] / M. Trstenjak, P. Cosic // Procedia Manufacturing. – 2017. – Vol. 11. – P. 1744–1750. doi:10.1016/j.promfg.2017.07.303
6. Rennung, F. Service Provision in the Framework of Industry 4.0 [Text] / F. Rennung, C. T. Luminosu, A. Draghici // Procedia – Social and Behavioral Sciences. – 2016. – Vol. 221. – P. 372–377. doi:10.1016/j.sbspro.2016.05.127
7. Baena, F. Learning Factory: The Path to Industry 4.0 [Text] / F. Baena, A. Guarin, J. Mora, J. Sauza, S. Retat // Procedia Manufacturing. – 2017. – Vol. 9. – P. 73–80. doi:10.1016/j.promfg.2017.04.022
8. Bauer, W. Transforming to a Hyper-connected Society and Economy – Towards an «Industry 4.0» [Text] / W. Bauer, M. Hammerle, S. Schlund, C. Vocke // Procedia Manufacturing. – 2015. – Vol. 3. – P. 417–424. doi:10.1016/j.promfg.2015.07.200
9. Benias, N. A review on the readiness level and cyber-security challenges in Industry 4.0 [Text] / N. Benias, A. P. Markopoulos // 2017 South Eastern European Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM). – IEEE, 2017. doi:10.23919/seeda-cecnsm.2017.8088234
10. Flatt, H. Analysis of the Cyber-Security of industry 4.0 technologies based on RAMI 4.0 and identification of requirements [Text] / H. Flatt, S. Schriegel, J. Jasperneite, H. Trsek,

H. Adamczyk // 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA). – IEEE, 2016. doi:10.1109/etfa.2016.7733634

11. Rajnai, Z. Labor market risks of industry 4.0, digitization, robots and AI [Text] / Z. Rajnai, I. Kocsis // 2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY). – IEEE, 2017. doi:10.1109/sisy.2017.8080580
12. Tupa, J. Aspects of Risk Management Implementation for Industry 4.0 [Text] / J. Tupa, J. Simota, F. Steiner // Procedia Manufacturing. – 2017. – Vol. 11. – P. 1223–1230. doi:10.1016/j.promfg.2017.07.248
13. Santos, M. Y. A Big Data system supporting Bosch Braga Industry 4.0 strategy [Text] / M. Y. Santos, J. Oliveira e Sa, C. Andrade, F. Vale Lima, E. Costa, C. Costa, B. Martinho, J. Galvao // International Journal of Information Management. – 2017. – Vol. 37, No. 6. – P. 750–760. doi:10.1016/j.ijinfomgt.2017.07.012
14. Wang, Y. Concept and use Case Driven Approach for Mapping IT Security Requirements on System Assets and Processes in Industrie 4.0 [Text] / Y. Wang, O. Anokhin, R. Anderl // Procedia CIRP. – 2017. – Vol. 63. – P. 207–212. doi:10.1016/j.procir.2017.03.142
15. Ma, Z. Security Viewpoint in a Reference Architecture Model for Cyber-Physical Production Systems [Text] / Z. Ma, A. Hudic, A. Shaaban, S. Plos // 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). – IEEE, 2017. doi:10.1109/eurospw.2017.65
16. Wallis, K. Adaption of a Privilege Management Infrastructure (PMI) Approach to Industry 4.0 [Text] / K. Wallis, F. Kemmer, E. Jastremskoj, C. Reich // 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). – IEEE, 2017. doi:10.1109/ficloudw.2017.71
17. Cheminod, M. Leveraging SDN to improve security in industrial networks [Text] / M. Cheminod, L. Durante, L. Seno, F. Valenza, A. Valenzano, C. Zunino // 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS). – IEEE, 2017. doi:10.1109/wfcs.2017.7991960
18. Khan, W. A. Analysis of the requirements for offering industrie 4.0 applications as a cloud service [Text] / W. A. Khan, L. Wisniewski, D. Lang, J. Jasperneite // 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE). – IEEE, 2017. doi:10.1109/isie.2017.8001413
19. Meany, T. Functional safety and Industrie 4.0 [Text] / T. Meany // 2017 28th Irish Signals and Systems Conference (ISSC). – IEEE, 2017. doi:10.1109/issc.2017.7983633
20. Haller, P. Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection Systems in Industrial Cyber-Physical Systems [Text] / P. Haller, B. Genge // IEEE Access. – 2017. – Vol. 5. – P. 9336–9347. doi:10.1109/access.2017.2703906
21. Romanovs, A. Invited speech security in the Era of Industry 4.0 [Text] / A. Romanovs // 2017 Open Conference of Electrical, Electronic and Information Sciences (eStream). – IEEE, 2017. doi:10.1109/estream.2017.7950303
22. Saldivar, A. A. F. Self-organizing tool for smart design with predictive customer needs and wants to realize Industry 4.0 [Text] / A. A. F. Saldivar, C. Goh, W. Chen, Y. Li // 2016 IEEE Congress on Evolutionary Computation (CEC). – IEEE, 2016. doi:10.1109/cec.2016.7748366
23. Toro, C. A Perspective on Knowledge Based and Intelligent Systems Implementation in Industrie 4.0 [Text] / C. Toro, I. Barandiaran, J. Posada // Procedia Computer Science. – 2015. – Vol. 60. – P. 362–370. doi:10.1016/j.procs.2015.08.143
24. Witkowski, K. Internet of Things, Big Data, Industry 4.0 – Innovative Solutions in Logistics and Supply Chains Management [Text] / K. Witkowski // Procedia Engineering. – 2017. – Vol. 182. – P. 763–769. doi:10.1016/j.proeng.2017.03.197
25. Grabia, M. Design of a DASH7 low power wireless sensor network for Industry 4.0 applications [Text] / M. Grabia, T. Markowski, J. Mruczkiewicz, K. Plec // 2017 IEEE International Conference on RFID Technology & Application (RFID-TA). – IEEE, 2017. doi:10.1109/rfid-ta.2017.8098904
26. Bonavolonta, F. Enabling wireless technologies for industry 4.0: State of the art [Text] / F. Bonavolonta, A. Tedesco, R. S. L. Moriello, A. Tufano // 2017 IEEE International Workshop on Measurement and Networking (M&N). – IEEE, 2017. doi:10.1109/iwmn.2017.8078381
27. Poonpakdee, P. Decentralized Network Building Change in Large Manufacturing Companies towards Industry 4.0 [Text] / P. Poonpakdee, J. Koiwanit, C. Yuangyai // Procedia Computer Science. – 2017. – Vol. 110. – P. 46–53. doi:10.1016/j.procs.2017.06.113
28. Karimireddy, T. Guaranteed timely delivery of control packets for reliable industrial wireless networks in industry 4.0 Era [Text] / T. Karimireddy, S. Zhang // 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN). – IEEE, 2017. doi:10.1109/icufn.2017.7993826
29. Petrasch, R. Cloud storage hub: Data management for IoT and industry 4.0 applications: Towards a consistent enterprise information management system [Text] / R. Petrasch, R. Hentschke // 2016 Management and Innovation Technology International Conference (MITicon). – IEEE, 2016. doi:10.1109/miticon.2016.8025236

ИССЛЕДОВАНИЯ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕРЫ ПРЕДОСТОРОЖНОСТИ В INDUSTRY 4.0

Данное исследование посвящено изучению уязвимостей и мер информационной безопасности в Industry 4.0. Предлагается план безопасности, который пропорционален организационным структурам идентификации протоколов кибербезопасности для Industry 4.0. Благодаря предлагаемому подходу может быть обеспечена безопасность информации, а ценная информация защищена от атак.

Ключевые слова: Четвертая промышленная революция (Industry 4.0), информационная безопасность, безопасность киберсистемы, управление рисками.

***Kondiloglu Adil,** Lecturer, Department of Computer Science, Vocational School of Technical Sciences, Giresun University, Turkey, e-mail: adil.kondiloglu@giresun.edu.tr, ORCID: https://orcid.org/0000-0002-2729-7532*

***Bayer Harun,** Lecturer, Department of Computer Science, Akcadag Vocational School, Inonu University, Turkey, e-mail: harun.bayer@inonu.edu.tr, ORCID: https://orcid.org/0000-0003-3839-647X*

***Celik Enes,** Lecturer, Department of Computer Science, Babaeski Vocational School, Kirklareli University, Turkey, e-mail: enes.celik@klu.edu.tr, ORCID: https://orcid.org/0000-0002-3282-865X*

***Atalay Muhammet,** Assistant Professor, Department of Quantitative Methods, Faculty of Economics and Administrative Sciences, Kirklareli University, Turkey, e-mail: atalay@klu.edu.tr, ORCID: https://orcid.org/0000-0003-3960-500X*