I. J. Education and Management Engineering, **2023, 2, 18-26**
Published Online on April 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijeme.2023.02.03

Cyber-physical Systems: Security Problems and Issues of Personnel Information Security Culture

Rasmiyya Sh. Mahmudova
Institute of Information Technology/Training-Innovation Center, Baku, AZ1141, Azerbaijan
E-mail: rasmahmudova@gmail.com
ORCID iD: https://orcid.org/0000-0002-5816-9373

Received: 09 September, 2022; Revised: 31 October, 2022; Accepted: 27 December, 2022; Published: 08 April, 2023

Abstract: Cyber-physical systems (CFS) have already become an integral part of our lives. Starting from the energy sector, production and transport, to healthcare, trade, and financial spheres, these systems have been widely applied everywhere. The realization of threats to the information security of such systems can cause very serious disasters, human casualties, financial loss, as well as damage the image of the companies that use these systems.

From this point of view, it is very important to investigate the issues of ensuring information security of KFS.Security problems of cyber-physical systems are analyzed. At the same time, the role and importance of the human factor in ensuring the information security of cyber-physical systems are explained. The difficulties faced by enterprises in informing employees about information security and forming a culture of information security in them are analyzed. Appropriate training methods are explained and recommendations are given to develop employees' necessary knowledge and skills related to information security.

Index Terms: Information Security, Information Security Culture, Attack Cyberphysical Systems, İnformation Security of Cyberphysical Systems, Human Factor, Cyber Training

1. Introduction

As cyber-physical systems (CPS) combine information technology with physical processes and the interaction of objects, their use is becoming more widespread and the demand for these systems is growing. It should be noted that there is still no single definition of CPS in the scientific literature. CPS was first proposed as a term in 2006 to refer to complexes consisting of natural objects, artificial subsystems, and controllers [1]. At the same time, the popularity of this term is associated with the Industrial 4.0 project, which is based on the industrial application of these systems [2]. Typically, CPSs include [3]: production management systems; internet of things; "smart home"; robotic systems; unmanned aerial vehicles; unmanned vehicles; military systems.

The development of digital technologies, the application of cyber-physical systems, and the use of artificial intelligence are causing an increase in the living standards of certain groups of the population and economic growth in many sectors of the economy. At the same time, it leads to the cessation of several activities dominated by physical labor. The latest technologies are designed to provide humanity with everything it needs, including the security of the individual, society, and the state. CPS is another type of technology that is actively used in some areas of public life. Today, it is difficult to imagine not only production but also daily human life without them. Their safe operation is not only ensured by technical, organizational, and physical means. States set specific tasks for the CPS to take comprehensive measures to combat cyber threats [2].

Previously, there was an opinion that the development of powerful software and technical methods is enough to prevent unauthorized access to information resources. However, it is not possible to ensure information security only by software and hardware.

It is known that information security encompasses technology, processes, and people. From this point of view, the solution to information security problems also depends on people's culture and their behavior about the information.

It should be noted that the majority of security violations are the result of human error. An enterprise needs to train its employees better to increase the level of its information security and increase the resistance of employees to cyber threats. At the same time, human errors, their types, the causes of these errors, and ways to reduce them should be investigated and analyzed. One of the important measures to ensure the information security of CPSs is to increase the awareness of employees about information security and the formation of a culture of information security. Also, taking

into account the innovations brought by the IV industrial revolution, the pace of development of information technology, and the training of employees to deal with new information threats should be a continuous process.

The role of the human factor in the information security of cyber-physical systems has not been sufficiently investigated. The purpose of the article is to show the importance and complexity of human factor management in information security.

2. The Essence of Cyber-Physical Systems

CPS are engineering systems built and dependent on the perfect integration of computing and physical components. Just as the Internet changes people's interactions with information, so do KFS technologies change people's interactions with engineering systems. The new, smart CPS promotes innovation and competition in several applications, including agriculture, aeronautics, building design, energy, environmental protection, health, personalized medicine, manufacturing, and transportation.

The first scientific sources on cyber-physical systems appeared in 2006. At the same time, its popularity as a term is associated with the Industry 4.0 project. Typically, cyber-physical systems include the following systems:

- Industrial Management Systems;
- Internet of Things;
- "Smart home" systems;
- Unmanned vehicles;
- Robotics systems;
- And so on.

A cyber-physical system is considered to be both relatively small objects (for example, an unmanned aerial vehicle, a system of smart room devices) and large-scale objects: factories or even entire cities (smart city systems).

It should be noted that there is no universally accepted definition of cyber-physical systems in the scientific literature. There are different approaches to explaining the nature of cyber-physical systems in different sources. The National Institute of Science and Technology under the US Department of Commerce, which studies CPS, defines them as technically interconnected intelligent systems that combine physical and computational components in a complex way [4]. At the same time, another study conducted by this institute states that this system has the following important features [5]:

- it is a hybrid system because it integrates physical processes with computing;
- CPS combines computing and communication capabilities with the ability to monitor and manage objects in the physical world;
- CPS consists of physical objects, sensors, and information systems.

In one study [6], a cyber-physical system is considered to be a complex technical system that combines sensory technology, computing technology, communication (contact), and control. The hardware and software of the system are closely connected through the network, forming four processes: data collection, data analysis, decision-making, and implementation. In the source [7], the concept of cyber-physical space is used to describe the conventional environment in which physical objects and their information nature are inextricably linked. In another source, the concept of a cyber-physical system is presented as a convenient concept for representing technological systems as a result of the integration of physical processes and the information environment.

The European Strategy for the Development of CPS consists of computational, communication, and control components that are closely related to physical processes of various natures (mechanical, electrical, and chemical). CPS can be explained by the following characteristics: "related", "understandable" and "controlled". These features correspond to three aspects of the system: the physical world is connected using network technologies and integrated into cyberspace through sensors and control [Security and Privacy 2018].

The authors conclude that the cyber-physical system can be explained as the integration of three elements: physical objects, software, and communication networks [5]. The authors conclude that the cyber-physical system can be explained as the integration of three elements: physical objects, software, and communication networks [5]. Depending on the different criteria, CPS is divided into different types and covers a wide range of technical means and their combination. For example, cyber-physical systems include the Internet of Things, industrial Internet, "smart" cities, as well as individual physical objects (gadgets, vehicles, drones, robotic surgeons, buildings, etc.) controlled by computer programs.

If we look at the main technological trends that form the basis of cyber-physical systems, we can see that they are already used in different areas, but when integrated, they change the existing relationships between manufacturers, suppliers, and buyers, as well as between man and machine [2].

The main components of any cyber-physical system are:

- physical layer of the system (objects of the real physical world);
- digital layer of the system (a set of data about the system - algorithms for managing physical objects, algorithms for processing information, etc.);
- interface for interaction between the digital and physical layers (various sensors, control mechanisms, etc.);
- interface of interaction between the digital and physical layers with a person (various augmented reality technologies).

These components interact with each other in time and space, forming a single ecosystem aimed at solving a specific task. Cyber-physical systems are the next step in the evolution of systems with a large scale of granularity. In other words, such a system itself consists of many other complex systems.

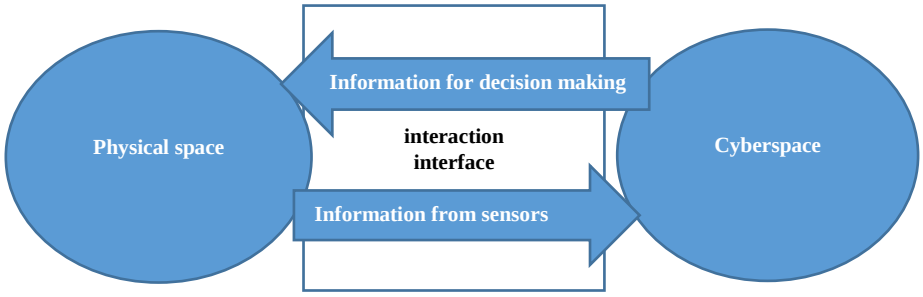

Fig. 1. Conceptual diagram of a cyber-physical system

3. Information Security Issues of Cyber-Physical Systems

The use of KFS in various areas of human life causes various risks, including the risk of human physical integrity, the risk of violation of privacy, unauthorized access to information, the risk of changing or deleting information, the risk of increasing electronic waste, etc. refers to [8]. The most pressing issue at the moment is the risk of a cyber attack. Carrying out a cyber attack on KFSs can lead to data leakage, equipment malfunction or complete shutdown. Cyber-attacks are likely to occur for many reasons, such as the imperfection of KFS's software.

Information security of a cyber-physical system means ensuring the integrity, confidentiality, and accessibility of processed data, infrastructure, and related physical processes. At the same time, the information security of a cyber-physical system means the protection of information and information resources of this system from various types of threats (illegal access to information, alteration, deletion of information, and disruption of the system).

The authors [9] analyzed the attackers of cyber-physical systems according to various characteristics and classified them according to the type of access to the system, level of knowledge, purpose, available resources for the attacker, and method of access to the system.

For example, in [9,10], attacks are grouped according to the method of affecting information security objects as follows: information - unauthorized access to information, copying, and theft, violation of information processing technology; software - the use of errors and vulnerabilities in the software, the spread of malware, the installation of bookmarks; physical - the destruction of system devices, theft of memory media, theft of cryptographic means of data protection and keys; radio-electronic - the capture of information in communication channels, interception, decryption, change and destruction of data in communication channels; organizational and legal - violation of the law, acquisition of outdated programs and facilities.

The problem of protecting cyber-physical systems - Industrial Control Systems - from cyber attacks, which are mostly used in industry today, is very relevant. Industrial Control System (ICS) including Supervisory Control And Data Acquisition (SCADA), Distributed Management Systems (DCS), systems based on programmable logic controllers, etc. is a general term used to describe several types of control systems. All of these systems are used in industrial environments and contain critical infrastructure. Ensuring the security of ICS means, first of all, protecting them from any intentional or unintentional interference that could disrupt the system.

Threats to modern IMS come in many forms. There are both external and internal threats to management systems. They can be intentional, that is, premeditated or accidental threats. Typical external threats are the actions of hackers, business competitors, or competing organizations/states. Internal threats often include wrongdoing, failure to respond properly to any current event, retaliation from dissatisfied employees, and so on.

More needs to be done to protect against external threats than to improve the security of the network itself. At the same time, it is not possible to avoid all internal threats simply by strengthening internal procedures or information policy. Optimal security of ICS can be achieved both through strengthening network security and through an approach to implementing the right policies and procedures.

Previously, ICSs were autonomous, however, these systems are already vulnerable to external threats, mainly due to their use of standard and commercially available technologies and their widespread networking. Internal threats, as in the past, arise primarily due to employee misconduct or errors in the organization of the management system.

Critical infrastructure facilities are those facilities, the disruption of which can lead to loss of control, destruction of infrastructure, weakening or destruction of the country's economy, and a significant deterioration in the security of the country's population. Critical infrastructures include energy, transport, emergency services, the banking and financial sector, the telecommunications sector, and other vital resources [11].

Modern enterprises in the energy sector are increasingly relying on automated production process control systems in their work, which leads to malicious cyber attacks. One of the most important tasks of any developed state is the production, transmission, and distribution of critical infrastructure, including electricity and energy carriers, ensuring the information security of enterprises.

In the European Union, the term "core services operator" has been adopted to mean "a public or private entity that provides a service and is essential for supporting other important services or economic activities". The list of main service operators includes electricity generation, transmission and distribution enterprises, oil production, oil refining and treatment plants, oil storage and transportation operators, natural gas distribution, and transmission and storage operators.

Oil and gas companies occupy an important place among the companies that own and manage the main critical infrastructure assets that are vital for the economic and military well-being of the country. The extraction, processing, and transportation of raw materials are the most important objects of cyber-attacks by aggressors for a variety of motives - from personal gain to industrial espionage and economic disruption. Due to the critical importance of these assets, oil and gas companies also face serious cybersecurity requirements.

The oil and gas sector has always been a target of criminals. Previously, the likelihood of a major incident due to a cyber-attack was very low, as enterprises usually operated in isolation, without integration into other enterprise systems.

At present, the situation has changed with the advent of the Internet of Things (IoT) and the penetration of new technologies in all areas. For a long time now, industrial facilities such as oil and gas fields, pipelines, oil refineries, and gas stations have come under cyber attack.

Industrial Control Systems (ICS) and Operational Technologies (OT) are used to manage industrial operations and allow monitoring and control throughout the value chain. The process of automating and digitizing the life cycle of production and distribution of products leads to increased productivity and reduced costs.

However, these processes also pose several risks. [12] distinguishes the following types of attacks in the classification of attack actions in SCADA systems: weakening of network perimeters using backdoors, exploitation of gaps in the protocols used, control of individual devices of the system, database malfunctions, interception and alteration of network data, changing the system time to stop the protection.

In one of the sources [13], attacks on cyber-physical systems are grouped as in table 1:

Table 1. Attacks on cyber-physical systems

Attacks	Purpose
Attacks on sensors	Use of physical processes for sensor malfunction, equipment failure, power outage
Attacks on computing processes	Deleting, altering, or falsifying data using viruses, trojans, or worms;
Feedback attacks	Violation of data integrity, seizure of control;
Attacks on the data transmission environment	Data deletion, alteration, replacement or falsification, data loss;
Attacks on actuators (execution mechanisms)	Deletion, alteration, or falsification of data, power outages, hardware, and software modifications.

A prerequisite for addressing security issues is a comprehensive approach. The establishment of a comprehensive security management system should take into account the identification of potential threats and their consequences, and assess and reduce the likelihood of their impact by significantly minimizing the risks of cyber incidents. It is extremely important to create a stable, reliable, and integrated information security system to prevent serious cyber threats.

In addition, all countries of the world accept that the ICT environment is interdependent and interconnected. If in the past the concepts of information security and cybersecurity were differentiated (information security includes information and humanitarian aspects along with information and technical aspects), in recent years they have become closer. The threat of the impact of information, for example, on the public consciousness, is now highlighted in the context of cybersecurity, and cybersecurity is increasingly being discussed as a separate issue within the concept of information security.

4. The Human Factor in Ensuring the Information Security of Cyber-Physical Systems

The human factor is the biggest problem in ensuring information security, and at the same time, the most reliable defender of the organization is the person. Many years of experience have shown that the most successful attacks often "break" users, not software. Most of the incidents are the result of individual mistakes. That is, the threat vector is often - the enterprise, the enterprise's IT services, and users.

Despite years of training, a multi-page security policy, and mandatory annual training, most information security professionals consider employee negligence to be a major threat.[14].

In [15] it is shown that the provision of information security depends on the behavior of employees, along with technical and organizational factors. "Kaspersky Labs and B2B International conducted research on more than 5,000

campaigns worldwide to investigate this. It was found that 52 percent of the campaigns consider the internal threat, that is, the human factor, as the main threat [16]. Their employees put their company at risk, either intentionally or due to their own negligence or lack of knowledge.

Even a report by the IBM company states that more than 95 percent of internal security breaches occur as a result of human error [17].

The cause of technical and social gaps in the organization's information security is the human factor and the organizational factor [18]. The types of attacks that occur due to human factor loopholes are common. These include: online fraud; drive by download; social engineering attacks; DDoS (Distributed Denial of Service) [19-21].

In the past, information security was often focused on technical and physical solutions. But now it is understood that it is impossible to solve the problem only by means of technical solutions, without taking into account the human factor. It is accepted that the problem of information security is a complex problem that depends on interrelated factors. It is noted that measures should be taken so that people are not part of the problem, but part of the solution. Let them stand in front of the line of defense against cyberattacks [21,22].

In this regard, people remain an important element of the organization's information security. Because they have a decisive role in the success or failure of information security management in organizations. Employees who are knowledgeable and trained in information security minimize cyber security violations. They play an important role in minimizing information security risks, protecting critical assets and intellectual property of the organization [23].

Despite the increasing number of accidents caused by personnel negligence, people do not change their behavior. According to a 2018 Verizon Data Breach report [24], an average of 4% of users open malicious links.

Using psychological methods to influence people's weaknesses, criminals persuade company employees to do what they need to do. For example, on May 7, 2021, there was a cyber attack on the operator of Colonial Pipeline, a huge US fuel pipeline. A phishing scheme was used to gain access to computer systems. One of the employees infected the company's information systems and gained access to the information by following the link in the e-mail sent by the criminals. As a result, the company was forced to pay $ 5 million to secure the data [25].

In December 2020, the data of 16,000 customers of Freedom Finance investment company, including qualified investors, were put up for sale on the Internet. The attackers attacked a segment of the company's internal network and stole some information from the local machines of several broker employees in the Russian Federation.

The attackers were online for more than two weeks, stealing 700 GB of files, including confidential information about patients and employees, contracts, financial statements, salary reports, etc. The criminals demanded $ 19.9 million to decrypt and delete the stolen data.

As can be seen, the protection of information resources cannot be limited to the use of technical methods or the adoption of organizational normative documents. The main and urgent problem here is the formation of a culture of information security for staff. Information security culture refers to a set of skills, habits, and attitudes that a person uses to protect various areas of his life and activities from information security threats.

Everyone should understand the value of information resources, and understand the reasons for taking concrete measures to ensure the security of information resources. Recognition of the importance of the formation of a culture of information security by European countries is associated with the publication in 2002 of the document "Guidelines for the security of information systems and networks: towards a culture of security." This document is the basis of the UN General Assembly Resolution 57/239 of December 20, 2002, "Creation of a Global Culture of Cybersecurity" [26]. The culture of information security must be formed at the initial stage of the creation and implementation of a centralized system to ensure the security of information resources. Having a culture of information security can significantly reduce the risk of information security threats, even if there are no technical and organizational measures to ensure information security.

The global cybersecurity culture requires all participants - government agencies, enterprises, and other organizations that create, maintain, manage and use information systems and networks, and individual users to follow the nine complimentary items, including the following:

1) *Responsibility.* Each participant is responsible for the security of information systems and networks by their roles. Participants should regularly review their policies, activities, measures, and procedures and assess their suitability for the environment in which they operate.
2) *Ethics.* Given the pervasiveness of information systems and networks in modern societies, participants need to respect the legitimate interests of others and recognize that their actions or inaction may harm others;
3) *Democracy.* Security should be implemented in a manner consistent with the values recognized by democratic societies, including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness, and transparency;

In the information security doctrines of NATO countries in 2017 and 2018, the issue of comprehensive teaching of the basics of information security to staff, employees, and ordinary citizens is reflected as a priority [27].

5. Methods of Developing a Staff Information Security Culture

Information security is a complex concept, it is determined not only by the number of qualified technical staff in this field but also by the level of knowledge and skills of all employees of the enterprise to ensure cyber security.

Being aware of the dangers is half the battle, first of all, it is necessary to understand what to do to avoid these dangers. Information security experts are still studying how to address vulnerabilities in user security. Admittedly, even the best professionals may not be able to organize this process properly.

Many companies buy online training videos and try to solve the problem with its help or their IT professionals give a lecture once a year to remind employees of the basic concepts. Experience shows that after a while, employees forget about this lecture.

Conducting information security training and exams for employees is an important part of ensuring the security of any organization. However, the ultimate goal should not only be to increase user awareness, but also to create a culture of security. First of all, people need to understand why this knowledge is needed and be able to apply it. Then knowledge must become a habit.

Pieces of training to ensure corporate information security should be regular, it is more appropriate to conduct training several times a year. In other words, instead of conducting a large training once a year, it can be divided into parts and put into short-term tasks. At the same time, it is possible to hold regular lectures and tests on cyber security.

Campaigns, companies around the world are adopting programs to increase the awareness of their employees about information security, their knowledge, and skills. However, research and surveys show that literacy programs in this area are not effective enough. Experts explain the ineffectiveness of information security training for the following reasons:

- It is tedious for users to read information security policies and other technical documents, sometimes not understanding the terms;
- Lack of motivation for employees to learn - they often think that they will not fall victim to bad people;
- Lack of involvement of senior management in the culture of information security;
- Focus on prohibitions rather than teaching what to do;
- Users accept the rules as restrictions and try to circumvent them;
- Difficult to assess the effectiveness of training.

To ensure the information security of the enterprise, it is important not only to increase the knowledge of employees but also to develop the necessary skills.

According to experts, traditional training methods are not effective in forming a culture of information security. The most effective training methods are cyber training (simulation of various life situations), banners and posters, micro-training, and educational games [28].

For example, Kaspersky Security Awareness, a project developed by Kaspersky Lab, uses game-type training to increase employees' awareness of information security. Kaspersky Security Awareness consists of several modules: Kaspersky Interactive Protection Simulation for senior management; Kaspersky CyberSafety Games for line managers and (or) middle managers; Online skills training platform for all company employees; Cybersecurity for IT Online to train IT professionals in cybersecurity skills.

Bysupplementing theoretical knowledge with experiential learning and interactive training (e.g., games, puzzles,scenarios) for general employees could provide a more practical hands-on training that looks at real situationalthreats (cyber-ranges). The cognitive learning can bring the foundations to the discussions and practicalsolutions for acquisition of skills, but also to design of training and education for cybersecurity professionals [29].

There are many studies that show that game-based training is a more effective way to increase the knowledge and skills of personnel in the field of information security in organizations. [30] examines games used to teach cybersecurity knowledge.

Augmented reality interfaces and specialized scenarios with content that reflects the context are in use ingaming, which may be very useful in forming required competences, skills and abilities; games may be theappropriate method of implementing skills frameworks into study programs [31].

The analysis of the literature suggests that the following methods may be more effective in informing employees about information security.

Use of memory books. In many cases, the effectiveness of training can be increased by using a manual or memory book to perform this or that operation. Instead of flipping through thick books about any specific situation and how to deal with it, an employee can use a pre-made booklet. For example, on a double-sided, laminated sheet of paper, you can write an illustrated picture and signs of a letter sent by e-mail with malicious code, and on the other three pages, you can describe the sequence of actions required by a simple block diagram.

Micro training. Micro training is a general concept in which learning material is given in relatively small doses. The pace of modern life is very fast and it is becoming increasingly difficult for people to devote time to any work,

including education. In micro-education, knowledge, skills, and habits can be transmitted to students in a variety of ways, for example, with the help of modern Education Management Systems. Micro training is a new and growing trend that meets the special needs of today's dynamic organizations and their employees. This method is very suitable for teaching special skills such as cybersecurity skills. Given the rapid growth of cyber threats, micro training can be held regularly. This allows employees to be educated about current security issues, develop the necessary skills and thus increase the overall level of security in the company. At the same time, the format of this training method allows you to study anywhere: on the subway, during a break from work, or waiting for your order in a restaurant. The main principle of this approach is to allow students to study whenever and wherever they want.

Game-based training. This method uses approaches that are typical for computer games in the learning process. The purpose of this method is to involve students in the learning process through entertaining tasks, and in some cases to create a competitive environment. By scoring points, upgrading their status, and gaining a foothold among the leaders, or through other game modes, users gain additional incentive to continue learning. Game-type organization of training can be carried out in different ways and at different levels. To increase the level of awareness of employees on information security issues, training can be carried out with the participation of gaming experts.

As can be seen, the formation of a culture of information security is a multifaceted and specific pedagogical process. There are many issues to study and research thoroughly.

6. Conclusion

Protecting your resources from information security threats is one of the main tasks of any enterprise. The list of traditional measures to ensure information security (legislative, moral, ethical, administrative, physical, hardware and software) should be supplemented as a separate item to inform employees about information security problems, and to form a culture of information security.

In areas where cyber-physical systems are applied, it is important to take many measures to form ERCs of employees, especially in the oil and gas industry:

- The formation of a culture of information security of employees by the management of the enterprise should be considered a high priority and should always be kept in mind.
- When developing a program, employees should be grouped (executives, IT specialists, ordinary users) and a list of knowledge and skills needed for them should be identified.
- The formation and development of a culture of information security should be a managed process. A budget should be allocated for this work, training should be planned, appropriate programs should be developed for different categories of employees by job requirements, training methods should be selected, knowledge should be assessed and certified, and the impact of training should be systematically studied.
- The training program should be constantly updated, taking into account the risks of information security.
- Given that the list of threats is constantly growing with the application of cyber-physical systems, and smart technologies, the process of forming a culture of information security must be continuous.

Information security policy plays a crucial role in shaping the culture of information security. It is important for the company that all employees are familiar with this policy. At the same time, they must comply with the existing laws of the country on information security, and the information security policy of the enterprise. Because the behavior of employees plays an important role here.

[19] considers the culture of information security as an integral part of human information culture. The authors also divide the information culture into general and professional information cultures. The same can be said for the culture of information security. Indeed, depending on the professional characteristics of professionals, the requirements for their knowledge and skills in the field of information security are also different. This factor should be taken into account in the process of organizing training to develop a culture of information security for employees within the enterprise.

The results of the study can be used as a resource by researchers of information securitu culture. At the same time, it can be useful for those responsible for developing the information security culture of the personnel.

Acknowledgment

This work is supported by the Science Foundation of the State Oil Company of Azerbaijan Republic (SOCAR) (Contract No. 3LR-AMEA).

References

[1] Baheti R., Gill H. Cyber-physical systems. The impact of control technology, 2011, vol. 12, no. 1, pp. 161–166.
[2] Klaus Schwab. The Fourth Industrial Revolution.Geneva: World Economic Forum. 2016.
[3] Zeqjda P.D., Poltavceva M.A., Lavrova D.S. "Sistematizaciya kiberfizicheskix sistem i ocenka ix bezopasnosti. Problemi informacionnoy bezopasnosti," *Kompyuterniye sistemi*. 2017, №2, pp. 127-138.
[4] Framework for Cyber-Physical Systems. Volume 1, Overwiew (2017) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf
[5] Kuteynikov D.L., Ijayev O.A., Zenin C.C., Lebedev V.A. "Kiberfiziceskiye, kiberbioloqiceskiye I iskustvenniye koqnitivniye sistemi: sushnost I yuridiceskiye svoystva," Rossiyskoe pravo: obrazovaniye, praktika, nauka, 2019, No.3, pp.75-81.
[6] Li Y., Li X., Wang L., Li Y. 'Limestone-gypsum wet flue gas desulfurization based on Cyber-Physical System', Chinese Control And Decision Conference (CCDC), 2019, pp. 473-477.
[7] Roqozinskiy Q.Q. "Multidomenniy podxod i modeli obyektov kiberfiziceskoqo prostranstva v zadacax otobrajeniya informacii", *Trudi ucebnix zavedeniy*, 2017, vol.3, No. 4, pp.88-93.
[8] Zhernova V. M. Problems of legal counteraction to cyber attacks on cyber-physical systems. Bulletin of the South Ural State University. Ser. Law, 2020, vol. 20, no. 4, pp. 104–108. (in Russ.) DOI: 10.14529/law200418.
[9] Levshun D.C., Qayfulina D.A., Ceculin A.A., Kotenko I.V. "Problemniye voprosi informacionnoy bezopasnosti kiberfiziceskix sistem", *Informatika i avtomatizaciya*. vol.19, No. 5, pp. 1050-1088. https://doi.org/10.15622/ia.2020.19.5.6
[10] Alekseyev D.M., Ivanenko K.N., Ubiraylo V.N. "Klassifikaciya uqroz informacionnoy bezopasnosti", *Simvol nauki*, 2016, No.9, pp. 18-20.
[11] https://controleng.ru/wp-content/uploads/7563.pdf
[12] Massel A.Q. "Metodika analiza uqrozi ocenki riska narusheniya informacionno-texnoloqiceskoy bezopasnosti enerqeticeskoy kompleksov", *Informacionniye I matematiceskiye texnoloqii v nauke I upravlenii*, 2015, pp. 186-195.
[13] Zhu B., Joseph A., Sastry S. A taxonomy of cyberattacks on SCADA systems, International conference on internet of things and 4th international conference on cyber, physical and social computing, 2011, pp. 380-388.
[14] Alguliyev R., Imamverdiyev Y., Sukhostat L. "Cyber-physical systems and their security issues", *Computers in Industry*, 2018, vol.100, pp. 212-223.
[15] Furnell S., Clarke N. Power to the people? The evolving recognition of human aspects of security. Comput. Secur., 2012, vol. 31, no. 8, pp. 983–988. DOI: https://doi.org/10.1016/ j.cose.2012.08.004
[16] Humans Factor in IT security: How Employees are Making Businesses Vulnerable from Within, «Kaspersky Labaratory» and B2B International, 2017, https://www.kaspersky.com/blog/the-human-factor-in-it-security/
[17] IBM 2015 Cyber Security Intelligence Index, https://informationsecurity.report/Resources/Whitepapers/fb170637-58b8-4580-9c7c-745d8adca24d_2015%20Cyber%20Security%20Intelligence%20Index%20for%20Retail.PDF
[18] ENISA threat landscape 2020: cyber attacks becoming more sophisticated, targeted, widespread and undetected. European Union Agency for Network and Information Security, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020
[19] Katsikas SK, López J, Backes M, Gritzalis S, Preneel B (Eds). Information security: 9th international conference, ISC 2006, Samos Island, Greece, August 30–September 2, 2006. Proceedings. Springer
[20] Bendovschi A. Cyber-attacks – trends, patterns and security countermeasures. Procedia Econ Finance, 2015, 28:24–31. https://doi.org/10.1016/S2212-5671(15)01077-1.
[21] Zimmermann V, Renaud K , Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. Int J Hum Comput Stud., 2019, 131:169–187
[22] Eminağaoğlu M, Uçar E, Eren Ş, The positive outcomes of information security awareness training in companies – A case study. Inf Secur Tech Rep, 2009, 14(4):223–229. https://doi.org/10. 1016/j.istr.2010.05.002
[23] Adèda Veiga NicoMartins, Defining and identifying dominant information security cultures and subcultures, Computers & Security, Volume 70, September 2017, Pages 72-94
[24] Insights from the Verizon 2018 Data Breach Investigation Report,https://delinea.com/blog/verizon-data-breach-report
[25] Dudley R., Golden D. The colonial pipeline ransomware hackers had a secret weapon: self-promoting cybersecurity firms. – 2021.
[26] https://digitallibrary.un.org/record/482184
[27] Vilkova A.V., Litvishkov V.M., Shvirev B.A., "Problemi neprerivnoqo obuceniya personala informacionnoy bezopasnosti", *Mir nauiki, kulturi obrazovaniya*, No.4(77), 2019, pp.29-31.
[28] Lopatina K. Formirovaniye i povisheniye kulturi kiberbezopasnosti. Opit Sberbanka, *Information Security*, https://www.itsec.ru/articles/formirovaniye-i-povysheniye-kultura-kiberbezopasnosti
[29] Aaltola, K., & Taitto, P. Utilising Experiential and Organizational Learning Theories to Improve Human Performancein Cyber Training. g. Information & Security: An International Journal 43, no. 2 (2019): 123-133.
[30] Hill, Winston Anthony Jr.; Fanuel, Mesafint; Yuan, Xiaohong; Zhang, Jinghua; and Sajad, Sajad, "A Survey of Serious Games for Cybersecurity Education and Training" (2020). KSU Proceedings on Cybersecurity Education, Research and Practice. 7.
[31] Skorenkyy, Y., Kozak, R., Zagorodna, N., Kramar, O., & Baran, I. (2021). Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education. Journal of Physics: Conference Series, 1840(1).
[32] Rasim M. Alguliyev, Rasmiyya Sh. Mahmudova, "Information Culture Formation as the Most Promising Direction of Individual`s General Culture", IJMECS, vol.7, no.3, pp.54-61, 2015. DOI: 10.5815/ijmecs.2015.03.08

Author's Profile

Rasmiyya Sh. Mahmudova graduated from Baku State University, Faculty of Applied Mathematics. In 2019, the Supreme Attestation Commission under the President of the Republic of Azerbaijan awarded him the degree of Doctor of Philosophy in Technical Sciences. His main research interests are information culture, digital skills, information security culture, knowledge, skills assessment problems, etc. includes. Since 2014, he is the head of the Training and Innovation Center of the Institute of Information Technology. He is the author of more than 50 scientific works.

How to cite this paper: Rasmiyya Sh. Mahmudova, "Cyber-physical Systems: Security Problems and Issues of Personnel Information Security Culture", International Journal of Education and Management Engineering (IJEME), Vol.13, No.2, pp. 18-26, 2023. DOI:10.5815/ijeme.2023.02.03