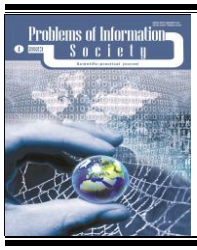

www.jpis.az

14 (1)
2023

Problems of evaluating the organization's information security culture

Rasmiyya Sh. Mahmudova

Ministry of Science and Education Republic of Azerbaijan Institute of Information Technology,
B. Vahabzade str., 9A, AZ1141 Baku, Azerbaijan

rasmahmudova@gmail.com

https://orcid.org/0000-0002-5816-9373

ARTICLE INFO

http://doi.org/10.25045/jpis.v14.i1.07

Article history:
Received 05 September 2022
Received in revised form
07 November 2022
Accepted 10 January 2023

Keywords:
Information security culture
Information protection
Organization's information security
Cyber security culture
Information security policy
Security awareness

ABSTRACT

Nowadays, digitization of all areas of human activity leads to an increase in the number of information security incidents in organizations. From this point of view, the problem of information security culture in organizations becomes very relevant in modern times. Obviously, the majority of incidents related to information security violations in organizations are associated to the human factor. To overcome this problem, the research in the field of the evaluation of information security culture is urgent. Measuring and evaluating information security culture can enable an organization to identify its weaknesses in this area and take measures to eliminate them. This article examines various approaches to the concept of information security culture, and analyzes the affecting factors within the organization (management's attitude towards information security, information security policy, information security awareness and employee's behaviors). It also studies the documents adopted in the field of development and evaluation of information security culture in the European Union countries and the United States, and implemented projects. It analyzes proposed methods for measuring the information security culture in the organization using various methods. Moreover, the article reveals existing problems in this field and provides certain recommendations for their elimination. The methods of analysis and synthesis, comparison, generalization and systematic approach are used in this research.

1. Introduction

Technology processes and people are the main components of an organization's information security. From this point of view, recognizing how important the employees' role is in ensuring information security, the development of personnel's skills in this field should always be in the focus. Along with compliance with the requirements for the technologies used and proper establishment of processes information security risks will always exist if employees' knowledge and skills in this area are not evaluated and developed.

Studying the problems of information security culture is becoming intensive in foreign countries. However, scholars believe that the range of research topics and methods is extremely limited and largely theoretical in nature. The analysis of the articles published in this field in 2010-2017 concludes that 40% of these publications are dominated by research conducted through interview and analytical methods, literature review [1]. Empirical analysis is mentioned in only one fifth of these materials.

Since the emergence of the concept of information security culture, there has been a need for its measurement. Measuring information security culture is important not only for scientific research in the field of information security, but also from a practical point of view. When an organization measures its information security culture, it obtains information about its employees' security behaviors, awareness of the importance of security, their knowledge, values, and other aspects of information security. Thus, measuring the information security culture can

help the organization identify its weaknesses in this area and take measures for their elimination.

The European Network and Information Security Agency (ENISA) makes special calls for measuring information security culture in terms of evaluating and improving the human factor related to security in organizations [2]. This document provides recommendations for the development and implementation of the information security culture program in organizations.

Accurate and reliable measurement of such a complex theoretical concept as information security culture is problematic, but possible. The presented article examines the organization's information security culture and its evaluation. The goal of this research is to examine the scientific literature on this topic and to reveal the problems by analyzing the studies conducted in the field of evaluating the organization's information security culture.

2. Approaches to the concept of information security culture

It is known that currently there are a number of threats to the protection of the vital interests of individuals, society and the state in the information space. Meanwhile, the number of these threats is increasing rapidly. Information security culture is very vital in preventing these threats.

The concept of information security culture is viewed from different aspects. Among these approaches, the technological approach prevails. Previously, there was an idea that to ensure information security, it is enough to create a strong software or technical protection system limiting undesirable access to digital information resources by outsiders. However, everyone already understands that this is not the right approach. Information security cannot be ensured only by technical means. To ensure information security, all participants of information processes must comprehend the importance of information security for society, take into account factors that threaten security, realize their responsibilities and roles in ensuring information security, and, if necessary, be able to take necessary measures in this field.

There are different approaches to the concept of information security culture in the scientific literature. Table 1 presents some of them.

Table 1. Approaches to information security culture

Begishev I.R.	The main component of information security culture is a set of information security policy, including ethical norms, rules, norms and standards for safe use of digital technologies [3].
Schlienger T., Teufel S.	Security culture includes all socio-cultural measures supporting technical security measures so that information security becomes a natural aspect of every employee's daily activities [4].
Helokunnas T., Kuusisto R.	Information security culture is a system comprising interconnected structures (standardization, certification and measurement of information security) and content components (people's attitudes, motivation, mental models of information security knowledge) [5].
Dhillon, G.	Information security culture is a set of human qualities such as behaviors, attitudes and values contributing to the protection of all types of information in a specific organization [6].
Mahmudova R.	Technical knowledge and skills on information security, knowledge and skills on information effects that are hazardous for a person's spiritual and psychological health and the methods of protection from them, compliance with legal and ethical norms when using information resources constitute the basis for a person's information security culture [7].

Schlienger and Teufel [4] also state that information security culture is a "sub-culture in terms of content". In other words, it is a part of the organizational culture. Overall, many studies view information security culture as one of the main elements of organizational culture or corporate culture. Corporate culture guides the activities of the organization and its employees by limiting the activities and behaviors of the employees, and determines what the organization and its employees should do, what they can or cannot do. Given that organizational culture affects employee's behavior and can be used to regulate employee's behavior in information security.

[7] views information security culture as the process of acquiring knowledge, skills and habits in the field of information security and their application.

In recent research, information security culture is viewed as a multidimensional concept covering awareness, knowledge, attitudes, behaviors, intentions, beliefs, values, and other relevant concepts.

3. Factors affecting the organization's information security culture

Enterprises and organizations are one of the important elements of the state and society. It is

no longer a secret to anyone that most of the incidents related to the violation of information security in organizations are associated to the human factor. Most organizations use various technologies (firewalls, antivirus programs, information resources access control systems, etc.) to ensure information security, prevent threats and attacks. However, if users are not aware of the policy of using these technologies, they will not be able to apply this technology effectively. As a result, the organization will suffer from this.

[8] mentions information and telecommunication technologies to have an important role in terms of sustainable economic development of the country, social welfare, stability of important infrastructure and national security. Therefore, it is extremely important to focus on cyber security education to protect the country's cyber sovereignty from malicious acts, build a sustainable cyber security ecosystem and support cyber sovereignty.

Security awareness refers to the user's comprehension about the potential problems related to information security and that he/she understands his/her mission [9]. The level of employee's awareness is one of the main challenges that organizations face in achieving an appropriate security level. When employees are aware of safety policies, and the safety policies are followed, then a safety culture develops [4]. Consequently, security awareness is a key factor leading to higher compliance with security requirements and the development of a security culture [10].

If employees realize the importance of protecting information, as well as their responsibilities, then employees can understand the security risks that may arise as a result of their actions. Accordingly, this increases security policy compliance and security awareness, thus leading to the creation of an information security culture.

Experts believe that compliance with information security is important for creating an information security culture. Adherence to security requirements is an indicator of the extent to which the behavior of employees conforms to the information security policy to reduce the number of security breaches occurring due to the wrong behavior of employees. [11] states that compliance with security requirements is important for information security management and creation of security culture.

The analysis suggests that the main factors affecting the organization's information security culture (Fig. 1) are: the management's attitude, the organization's information security policy, employees' awareness of information security, and employees' behavior.

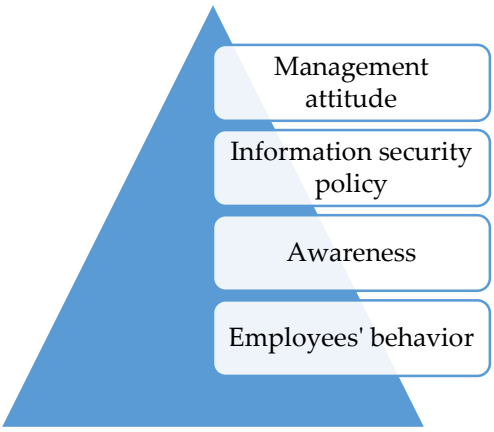

Fig.1. Factors affecting the organization's information security culture

3.1. Management's attitude

According to [12], the corporate information security policy is believed to describe the vision and goal of the management regarding information security. Correspondingly, the organization's leadership needs to appreciate where employees' security concerns come from and how each of the awareness or education options can help solve the problem.

The management of the enterprise must accept the importance of information security in order to increase the level of awareness of employees and implement training programs to be successful. If the management does not support this, and is not closely involved in the process of the information security culture formation, the set goal cannot be achieved. Because all documents related to ensuring information security should reflect this. No document can be approved without the signature of an authorized person.

Management should evaluate information security as a risk to be taken into account during the strategic planning of the organization's activities and development. In this regard, security should be considered not only as a cost, but also as a risk reduction factor. In this regard, clear priorities should be determined and brought to the attention of the persons responsible for ensuring information security, so that they take measures in accordance with the interests of the enterprise and existing risks.

3.2. Information security policy

One of the factors affecting information security culture possesses a written information

security policy. This policy ensures the purpose of information protection management in the organization and is the formal basis.

Information security policy plays an important role in managing the employees' behavior to protect information. Employees must know the requirements of the information security policy and recognize the importance of complying with these requirements for the secure information processing.

Possessing an information security policy is imperative for the enterprise. However, if employees have not read or understood it, it will not be possible to enforce their compliance with this policy.

Australian scientists believe that it is necessary for employees to know and follow the information security policy and their legal behavior in order to make a successful decision in the field of information security [13].

Information security culture is primarily defined by the information security policy. This is a high-level document for all measures related to information security and defines the main trends of ensuring information security.

3.3. Information security awareness

Information security awareness is defined as a level at which each employee comprehends the importance of information security, the level of information security appropriate to the enterprise, and his/her individual duty in the field of information security and acts accordingly.

Due to the lack of awareness, for example, the user does not know how to protect his/her personal data, as well as cannot control the intrusion of other users into his/her computer. They are unable to distinguish between spyware, spam emails, and cannot or don't know how to protect themselves from them.

Knowledge sharing improves information security awareness. Therefore, organizations should focus on the knowledge sharing in the field of information security. They should strive to make this knowledge available to anyone who needs it, ultimately improving information security across the organization.

Scientific literature includes a number of approaches related to the establishment of a knowledge management system in the sphere of information security to implement knowledge sharing among employees [14].

[15] defines the knowledge sharing as the overt or covert transfer of values, experience, expert judgments and contextual information from one person to another. This helps the person to grasp and evaluate new information and experience.

Researchers have studied the human factor in information security and conclude that human errors are mainly associated to lack of awareness and knowledge about information security [16]. The authors measure the awareness level of 500 employees through a questionnaire and conclude that employees with low security awareness expose their organizations to information security risks.

[17] proposes a two-dimensional model of end-user security behavior, the first being experience and the second being intention (good faith). People without knowledge in this category make simple mistakes, but the knowledge in this field leads to awareness and information security assurance.

A five-step model is proposed in [18] to evaluate the effectiveness of information security awareness raising measures. These levels include knowledge, attitude, normative belief, intention and behavior. Knowledge is considered to be the foundational pillar of the model here.

Another study conducts a comprehensive review to analyze the current state of cybersecurity awareness in the context of the Internet of Things in the industry: defining the concepts of cybersecurity awareness and information security awareness; methods adopted to raise cyber security awareness (e.g., serious games, online surveys); advantages of large-scale awareness raising campaigns in the field of cyber security [19].

3.4. Employees' behavior

Authors of [20] focus on the importance of developing and improving Information Security Culture through a structured model that takes into account employee's behavior. They believe that information security culture in any organization depends on how people behave in relation to information and its security. The procedures that employees themselves use in their daily activities can be the weakest link in the information security chain.

A number of international reports analyzing cyber-attacks also confirm that the main problem is caused by the behavior of employees. For example, employees opening phishing emails and unverified attachments, transferring confidential information during an attack through social engineering, etc. expose organizations to serious losses.

In this regard, organizations should monitor information security and punish those who do not

comply with the requirements of the information security policy so that they realize their responsibility.

The goal of forming an information security culture is that everyone within the enterprise, from a manager to an ordinary employee, takes responsibility for ensuring information security and understands that this is not case for only the employee responsible for information security, but everyone. Indeed, most employees believe that only the relevant department is responsible for ensuring information security. Therefore, everyone should recognize their role and responsibilities in relation to security and take responsibility for their behavior. If employees feel their obligations, it will positively affect their behavior.

4. International experience in the field of information security culture development and evaluation

Information security culture has not yet been widely studied, but the number of works published in the last decade suggests that active research is being conducted. However, the number of studies conducted in the field of information security culture assessment is limited. These studies are based on expert evaluation and opinion questionnaire methods.

Up to the early 2000s, developed European countries were not concerned about the unawareness of citizens in the field of network and information security, about the risks and threats in this field and how to protect themselves from them. However, in the end, the EU countries came to the conclusion that citizens and representatives of small and medium-sized enterprises using Internet-connected ICT devices without a certain culture and correct behavior in terms of information security pose a threat to the state.

In the European Union (EU), the information security skills are being developed out in a systematic and consistent way [2, 21]. Thus, everything was taken into account, including self-assessment, from the definition of the skills (competencies) model, from the development of training programs to the creation of skills assessment tools. One of the activities of ENISA, which was established in the EU in 2004, is to support education and training activities for the safe use of information and communication technologies in the EU member states, and to increase the level of preparation of citizens.

In 2010, the agency prepared a document "Guide for New Users: How to Raise Information Security Awareness." This is a practical guide for planning and implementing an information security awareness program.

The knowledge and skills required in this field are specified in the recommendations prepared by the EU for citizens in 2018. It focuses on cybersecurity threats to information and related risks (disinformation, cyber-bullying and radicalization risks). Violation of information security in the public administration system is noted as a critical risk.

Training and assessment on information security is performed within the framework of pan-European training "Cyber Europe". The training applies technologies developed by European cyber security experts and based on reality modeling.

The duties of the US government organizations to provide training on the fundamentals of information security to all employees have been determined at the legislative level. The Federal Information Security Management Act (FISMA), part III of "Electronic Government Act" of 2002, defines the duties related to raising the awareness of all employees working with information systems on information security issues. Employees are grouped as "information technology specialists" and "users" for the implementation and evaluation of information security competence development program. Verification of the effectiveness of the implementation of the information security policy and procedure and verification of knowledge are performed periodically. Requirements for improving awareness in the field of information security and their verification methods are represented in a special document [22].

In the United States, periodic knowledge assessments are an important component of the information security awareness program. In this case, tests are mainly used as a means of checking knowledge. Furthermore, additional inspection methods are applied, such as surprise inspections, use of specially prepared dispatches, violation of the accepted information security policy and rules, and monitoring of their registration.

The document "National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework" [23], adopted in 2017, includes a model for determining the degree required of information security specialists of various profiles who perform labor functions. The

document mentions 52 functional specializations involved in ensuring information security and provides a list of tasks for each of them and generates appropriate knowledge, skills and habits.

The evaluation method is selected according to the characteristics of the inspection area. Special tests are used to assess knowledge and the cases and simulation exercises to assess skills and habits.

5. Studies on the evaluation of information security culture

The concept of information security culture is relatively new. Thus, only since the early 21st century, information security culture has been recognized as an important factor in ensuring the security of information systems in the organization.

Researchers have already considered the human factor in information security from theoretical, organizational, methodical, pedagogical, sociological and economic, etc. aspects. The authors performed a general morphological analysis to define structure and analyze the national cyber security culture [24].

The authors believe that an ideal information security culture can help minimize people's threat to information security, thus preventing data breaches and other incidents in organizations. This study uses a mixed methods approach to understand how information security culture is defined in academic community and industry. Here, the factors required to have an ideal information security culture and the potential impact of an ideal information security culture are studied from both aspects [25].

[26] shows that because the auditing of people's behavior is extremely complex, to measure the information security culture, it is necessary to apply a step-by-step audit method, using a softer, informal approach, rather than being harsh on employees.

Scientists also evaluate the effectiveness of various tools and methods used to increase the level of information security culture based on psychological theories and models. At the same time, a method for measuring information security awareness in the organization is proposed [27].

The level of the organization's information security culture can be measured using various methods: for example, by analyzing the company's documents related to information security, by conducting a test of employees or by interviewing.

The model proposed by A. da Veiga et.al. [28] develops an evaluation tool, i.e., a questionnaire, developed by the authors Martins & Eloff [20] and Martins [29]. In the questionnaire developed for the evaluation of the information security culture, the questions are grouped into three blocks:

1) information about information security culture;
2) knowledge questions;
3) biographical questions.

The information about information security culture block evaluates the employees' understanding of 8 different aspects of information security: information security policy, governance, programs, leadership, asset management, user management, change management, and trust. A Likert scale ("Completely agree", "Agree", "Not sure", "Disagree", "Completely disagree") is used to confirm the answers to the questions.

The authors included a block of questions about knowledge in order to determine the extent to which employees are aware of information security, as well as whether the low level of information security culture is the result of educational problems or comprehension problems. In the block of questions about knowledge, the following types of questions are asked:

- The organization has a written information security policy.
- I have read the section of the information security policy relevant to my activity.
- I know what an information security incident is.

"Yes/No" scale is used to answer these questions.

The reason for including biographical questions in the information security culture questionnaire is to segment data and make comparisons across populations, such as by job title and department.

The research conducted by T. Schlienger and S. Teufel begins with the analysis of security policy [11]. The aim here is to examine in depth the official rules that should affect the safe behavior of the employees working in the enterprise. They use the communication model given in [30] to interpret policy and reveal norms and values. To verify the interpretation with the organization members, they interviewed the organization's security service manager.

The main goal of the prepared questionnaire is to find out the employees' attitude to the safety policy: do they know what this policy is and do they support it. The questions in the survey

measure employees' attitudes and perceptions of safety. Each question analyzes three different parts: 1) individual attitude (actual value), 2) perception of company attitude (formal value - information security policy), and 3) best solution.

Such an approach is useful in revealing the gaps between the understanding of information security culture by human and enterprise. There are ten questions, each directed at one of three different organizational levels: six at the employee level, two at the group level, and two at the organizational level. The last five questions refer to demographic aspects and the questionnaire itself. Demographic questions provide interesting information about different groups of employees.

The model proposed to evaluate the skills of civil servants on information security [31] takes the requirements for civil servants in the field of information security as the basis. These requirements include knowledge of the normative legal acts of the country and knowledge and skills in the field of information and communication technologies. However, since these requirements are not collected in a separate document and not divided by tasks, the authors had difficulty in systematically covering all requirements and developing an evaluation methodology for information security. Therefore, they based on the five-item digital skills evaluation model proposed within the framework of the G20 Summit in 2017. These items include: information literacy, computer literacy, media literacy, communicative literacy, and attitude to technological innovation.

The authors systematize the requirements (the list of required knowledge and skills) on the items of the model. Then they analyze the tasks to take into account the performance characteristics and the degree of responsibility of the employees in the information security requirements model. They are divided into two large groups: users and IT specialists. Each of these groups is divided into two subgroups. The group A is sub-grouped into A1 (managers of different levels) and A2 (ordinary employees of different levels by responsibility and information access).

B group of specialists is also divided into 2 groups according to specialization and type of activity: information technology (B1) and information security (B2) specialists. Here, the use of tests, cases, check-lists, interviews and simulations is proposed as the evaluation tools used for information security evaluation of different target groups.

Another model proposed for measuring information security culture [32] distinguishes the factors that make up the information security culture and the factors affecting information security. The authors use an open-ended interview method to develop an information security culture measurement model. They interviewed 8 different enterprises, ranging from small enterprises to large organizations, including both public enterprises and the private sector. They came to the conclusion that the factors that make up the culture of information security are awareness in the field of information security and responsibility for information security. The factors affecting information security are the involvement of general management in information security, the availability of an information security policy, and the organization of information security training.

A questionnaire is arranged by preparing questions characterizing the factors included in the two groups mentioned above:

- involvement of high management in information security (5 questions);
- application of information security policy (4 questions);
- organization of trainings on information security (3 questions);
- awareness in the field of information security (4 questions);
- responsibility for information security (3 questions).

The responses of the respondents are evaluated using a Likert scale, where it is required to choose one of two answers: "completely disagree" and "completely agree".

In the end, a correlation analysis is conducted to further investigate the relationship between the components of the factors affecting the information security culture and the factors constituting the information security culture. The results show that all the correlations between the factors affecting the security culture and the factors constituting the security culture are statistically significant. At the same time, experiments are conducted to verify the reliability of the proposed model.

A questionnaire is developed during a study to evaluate the information security culture of e-government [33] in the United Arab Emirates. This survey covers three broad areas: information security policy, information security compliance, and policy awareness.

The survey included 5 questions on information security policy, 7 on compliance and 5

on awareness. A questionnaire is developed to evaluate employees' opinions and attitudes. A Likert scale is used to measure the extent to which a respondent agrees or disagrees with other respondents. This is used to calculate the total scores appointed for each question. A Likert scale from 1 to 5 is also used in this study. Here, it is denoted as 1-Completely disagree, 2-Disagree, 3-Not sure, 4- Agree, 5- Completely agree.

There is also a number of studies on measuring and developing information security culture that are theoretically useful, but no evaluation tool is developed to measure information security culture. For example, [34] presents a conceptual model of the information security culture of the organization. Here, these components are taken as the structural elements of the information security culture: management's attitude towards information security, information security management, compliance with information security standards, information security awareness, and user behavior artifacts. At the same time, this study evaluates the national culture and corporate culture as external factors affecting information security culture. Another study [35] views information security culture as a component of information culture.

Despite the large number of studies on the topic, there is no comprehensive approach to measure information security culture for comprehensive evaluation of all its levels. First of all, this can be explained by the fact that the concept of information security culture itself is not sufficiently justified in terms of a comprehensive approach. Moreover, although there are different approaches to the structure of information security culture, there is no universally accepted approach. In order to evaluate the information security culture, the structure of each of the constituent elements included in its structure should be elaborated in a complex manner.

6. Conclusion

The main cause of threats to information security in organizations is the human factor. Therefore, organizations should provide their employees with quality training to resist cyber threats, and take measures to improve their information security culture. From this point of view, the mistakes made by employees, the types of these mistakes, the reasons for their occurrence, as well as the methods of reducing their number should be studied. It is now widely accepted that the management of the human factor in terms of information security depends on the creation and development of the information security culture of the organization.

Developing an information security culture can be achieved through the development and implementation of training programs within the organization, involving employees from all positions, including high management. However, to determine how effective these or other measures are, it is necessary to measure information security culture.

This study showed that the evaluation of the organization's information security culture was mainly implemented through opinion polls and questionnaire methods. The results of the study concluded that:

- Solution of the organization's information security problems depends on the level of information security culture of employees, along with technological methods and tools.
- Development of information security culture in organizations should be treated as one of the measures to ensure information security.
- Development of information security culture of personnel should be a controlled process, correspondingly, it should be regularly measured and evaluated.
- To measure information security culture, indicators should be developed, taking into account each of the factors affecting it.

Further studies are planned to be implemented on the development of indicators for measuring the culture of information security and the assessment of the level of culture of personnel in this area.

References

1. Astakhova, L.V., Lushnikova, S.S. (2019). Enterprise information security culture: a comparative analysis of foreign and Russian studies. Bulletin of the Ural Federal District. Information sphere security.1 (31), 37-47. (in Russian)
2. European Union Agency for Network and Information Security (ENISA, 2017). Cyber Security Culture in organisations, https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations/at_download/fullReport .
3. Begishev, I.R. (2021). Cyber-Security Culture: Psychological and Legal Aspects. Psikhologiya i pravo = Psychology and Law, 11(4), pp. 207-220. https://doi.org/10.17759/psylaw.2021110415 (In Russian).
4. Schlienger, T., Teufel, S. (2002). Information Security Culture. The Socio-Cultural Dimension in Information Security Management. Security in the Information Society. IFIP Advances in Information and Communication

Technology, 86, 191—201. https://doi.org/10.1007/978-0-387- 35586-3_46.
5. Helokunnas, T., Kuusisto, R. (2003). Information security culture in a value net. IEMC'03 Proceedings. Managing Technologically Driven Organizations: The Human Side of Innovation and Change. Albany, NY, USA (2–4 Nov. 2003). Chichester: J. Wiley and sons LTD. pp. 190–194.
6. Dhillon, G. (1999). Managing and controlling computer misuse. Information Management & Computer Security, 7(4), 171-175.
7. Mahmudova, R. (2013). Formation of information security culture in society. Problems of Information Society, №1 (7), s. 32-38. (in Azerbaijani)
8. Saleh AlDaajeh, Heba Saleous, Saed Alrabaee, Ezedin Barka, Frank Breitinger, Kim-Kwang Raymond Choo. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. Computers & Security, 119, 102754.
9. Da Veiga, A. and Eloff, J.H.P. (2010). A framework and assessment instrument for information security culture. Computers and Security, 29,196–207.
10. Wiley, A., McCormac, A., Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. Computers & Security, 88, 101640.
11. Schlienger, T., Teufel, S. (2003). Information security culture-from analysis to change. South African Computer Journal, 2003, 46–52.
12. Sherif, E. and Furnell, S. (2015). A Conceptual Model for Cultivating an Information Security Culture. International Journal for Information Security Research, 5(2), 565–573. https://doi.org/10.20533/ijisr.2042.4639.2015.0065.
13. Parsons, K.M., et al. (2015). The Influence of Organizational Information Security Culture on Information Security Decision Making. Journal of Cognitive Engineering and Decision Making, 9(2), 117—129. https://doi.org/10.1177/1555343415575152.
14. Lunacek, O. (2017) Knowledge system new tool of the security experts education. 6th International Conference on Military Technologies, p. 430–434.
15. Rocha Flores, V., Antonsen, E., Ekstedt, M. (2014) Information security knowledge sharing in organizations: A study of the impact of behavioral information security management and national culture. Computers and Security, 43, 90-110. (in Russian)
16. Parsons, K., Kalik, D, Pattinson, M., Butavichyus, M., McCormack, A., Zwaans, T. (2017). Human aspects of information security questionnaire: Two additional verification studies. Computers and Security, 66, 40-51. (in Russian)
17. Stanton, J., Stam, C., Mastrangelo, P., Jolton, J. A. (2005). Analysis of end user security behavior. Computers and Security, 2 (24), 124-133. (in Russian)
18. Khan, B., Alghathbar, K. S., Nabi, S. I., Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. African Journal of Business Management, 5 (26), 10862–10868. https://doi.org/ 10.5897/ajbm11.067.
19. Angelo Corallo, Mariangela Lazoi, Marianna Lezzi, Angela Luperto. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review, Computers in Industry, 137, 103614.
20. Martins, A. & Eloff, J.H.P. (2002). Information security culture. Security in the Information Society, pp. 203 214. IFIP/SEC2002. Boston, MA: Kluwer Academic Publishers.
21. Mahmudova, R. (2022). Analysis of international experience in the formation of a culture of information security in society. Problems of Information Society, 13(1), 75–82. https://doi.org/10.25045/jpis.v13.i1.10 .
22. Federal Information Security Management Act of 2022. (2022). 107-347, https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma.
23. National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework. (2017). https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf
24. Astakhova, L. V. (2018). From culture to the cultural resourse of an organization's information security. Bulletin of culture and arts, 3 (55), 85–101. (in Russian)
25. Adéleda Veiga, Liudmila V.Astakhova, Adéle Botha, Marlien Herselman. (2020). Defining organisational information security culture—Perspectives from academia and industry, Computers & Security, 92, 101713.
26. Vroom, C., Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security. 23 (3), 191–198. https://doi.org/ 10.1016/j.cose.2004.01.012.
27. Khan, B., Alghathbar, K. S., Nabi, S. I., Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. African Journal of Business Management, 5 (26), 10862–10868. https://doi.org/10.5897/ajbm11.067.
28. Da Veiga, A., Martins, N., Eloff, J.H.P. (2007) Information security culture – validation of an assessment instrument. Southern African Business Review, 11(1), 147–166.
29. Martins, A. (2002). Information security culture. MCom dissertation, Rand Afrikaans University, Johannesburg.
30. F. Schulz von Thun. (1992). Miteinander reden. Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag.
31. Sladkova, N.M., Ilchenko, O.A., Stepanenko, A.A., Shaposhnikov, V.A. (2021). Features of assessment of competences in information security of state and municipal employees. Issues of state and municipal management, 1, 122-149. (in Russian)
32. Alnatheer, Mohammed; Chan, Taizan; and Nelson, Karen. (2012). Understanding And Measuring Information Security Culture. PACIS 2012 Proceedings. 144. http://aisel.aisnet.org/pacis2012/144.
33. Ibrahim Al-Mayahi and Sa'ad P. Mansoor. (2013). Information Security Culture Assessment: Case Study. Third International Conference on Information Science and Technology, March 23-25, 2013, p.789-792; Yangzhou, Jiangsu, China.
34. Imamverdiyev, Y.N. (2015). Issues of information security culture in the e-government environment. Information technology problems, 1, 80-88. (in Azerbaijani)
35. Alguliev, R.M., Mahmudova, R.Sh. (2011). Structural Approach to the Formation of Information Culture of Individuals, Proceedings of the International Conference on Informatics Engineering and Information Science, Kuala Lumpur, Malaysia, part IV, 254, https://link.springer.com/book/10.1007/978-3-642-25483-3