Challenges and Solutions for Cybersecurity and Information Security Management in Organizations

Vladimer Svanadze[1], Maksim Iavich[2], and Sergiy Gnatyuk[3, 4, 5]

[1] *Business and Technology University, 82 Ilia Chavchavadze ave, Tbilisi, 0160, Georgia*
[2] *Caucasus University, 1 Paata Saakadze str., Tbilisi, 0102, Georgia*
[3] *National Aviation University, 1 Liubomyra Huzara ave, Kyiv, 03058, Ukraine*
[4] *State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, 3 Maksyma Zaliznyaka str., Kyiv, 03142, Ukraine*
[5] *Yessenov University, 32 microdistrict, Aktau, 130000, Kazakhstan*

Abstract

The rapid development of Internet technologies and the current global situation have accelerated the growing demand for digital transformation in organizations. The technological components of digital transformation make it easier for organizations to operate, but at the same time, it is essential to maintain a balance between technological innovation and cybersecurity, as much as possible to protect the activities of organizations in cyberspace. The process of introducing digital transformation involves high-level management of organizations, as well as information security managers, cybersecurity specialists, and representatives of other structural units. This is necessary as digital transformation is a complex process and such joint involvement facilitates the development of cybersecurity strategies and policies within digital transformation, with proper planning of the process in a given direction. Digital transformation is an innovative approach that ensures the full or partial digitization of organizations and, in turn, is a serious challenge to the process of introducing proper cybersecurity management in organizations, which must be in line with each direction of digital transformation. Given the increasingly complex conditions posed by threats, the introduction and development of effective cybersecurity management is a major challenge for many organizations. The paper analyzes the existing problems of cyber security systems management in organizations and offers an innovative and efficient cyber security management model.

Keywords

Internet technologies, digital transformation, cyber security, information security, innovative approaches, risk assessment, threat, standard, report, commitment, necessary resource.

1. Introduction

Security management is a process that allows to control of internal and external threats that prevent the normal functioning of organizations. Security management of organizations also means effective coordination of actions aimed at the maximum reduction of risks, which in turn ensures maximum security of organizations. All of this contributes to the safe transfer of information both inside and outside the organization and making appropriate decisions.

In addition, one of the main components of the security of organizations can be considered the responsibility of each employee, and security decisions should be made at all levels of management of organizations. For this, it is necessary that the top management correctly assess the risks so that the regulations and rules are properly implemented within the organizations [1, 2].

CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2024, Kyiv, Ukraine
EMAIL: svanadze@gmail.com (V. Svanadze); miavich@cu.edu.ge (M. Iavich); s.gnatyuk@nau.edu.ua (S. Gnatyuk)
ORCID: 0000-0001-4122-2536 (V. Svanadze); 0000-0002-3109-7971 (M. Iavich); 0000-0003-4992-0564 (S. Gnatyuk)

In general, in the direction of security, the problems that organizations face in the course of their activities should be considered, and those approaches that are suitable for the organization should be selected. This is important because the implementation of security processes does not mean that security will be fully ensured [3].

Security approaches should be consistent with the organization's governance and functioning, should be embedded in a unified governance system, and should function in a complex manner in harmony with other organizational-structural units. Along with all this, it is necessary for the security direction to assess both internal and external risks, that are a threat to the normal functioning of organizations, and, taking this into account, to implement the relevant rules and regulations, the fulfillment of which will be a necessary obligation for all levels of management [4, 5].

Otherwise, to avoid this or that threat, employees will try to act independently within the framework of an incompetent approach to the issue, which will ultimately harm the normal functioning of organizations.

There is no universal approach to the issue of security, because the approaches within organizations, which should ensure the safe functioning of organizations, are different. In particular, on the one hand, organizations may adopt a formalized approach to security with clearly defined roles and business processes, and on the other hand, organizations may choose a more informal management approach involving security control and decision-making [6–8]. Some questions need to be answered that help organizations determine how formal decisions and approaches should be, namely:

- How big is the organization and how difficult is its organizational and structural arrangement?
- What resources are available for effective security governance?
- In what field does the organization operate, what goals does it have and how important is security for the organization's activities and achieving the set goals?
- Are there any kind of external and internal requirements, be they agreements, normative or sectoral, or legal requirements?

In practice, correct approaches reveal the following:

- Security decisions must be taken.
- The person or groups of people who will implement the safety management process.
- Information necessary to make a correct and reasonable choice.

Regardless of the level of formality, the following factors should be considered during the effective management of organizations:

- All security measures must be in accordance and consistent with the goals and priorities of organizations.
- At all levels, a person or a group of people responsible for making safety decisions should be defined and allowed to carry out their activities.
- Ensuring responsibility for decisions.
- Provide feedback to decision-makers.
- Any approach to safety governance must be consistent with the wider system of governance of organizations. Security must be considered in the overall structure of the organization, along with other business priorities [9].

The ISO/IEC27001 standard (Fig. 1), developed by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), defines information technology governance as "a system by which an organization directs and controls security governance, defines an accountability structure, and provides oversight to ensure appropriate risk mitigation when management implements the necessary controls to reduce risks."

Given the increasingly complex threat landscape, implementing and developing effective cybersecurity governance is a challenge for many organizations [10, 11].

As research and organizational assessments reveal, many organizations struggle to address five fundamental cybersecurity and information security governance issues, namely:

1. Cyber security strategy and goals.
2. Standardized processes.
3. Enforcement and accountability.
4. Implementation of supervision and control at the high level.
5. Necessary resources.

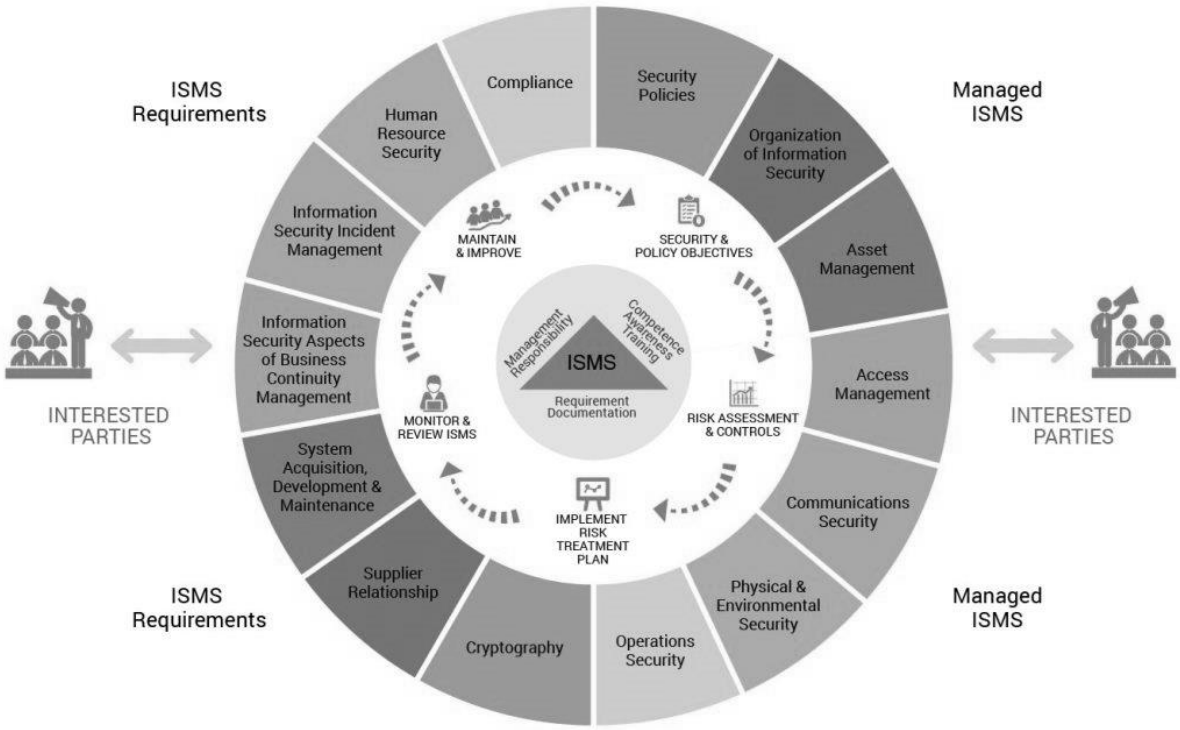

Figure 1: ISMS generalized scheme

2. Cyber Security Strategy and Objectives

To create an effective cybersecurity governance program, organizations must clearly define their risk management policies, strategies, and objectives. Before the strategy and objectives are defined, senior management must evaluate its approach to risk management. The strategy should be a high-level document that guides organizations in maintaining and improving risk management [12, 13]. Once the cyber security strategy and goals are finalized, implementation across the organization is essential.

The main components of an effective cyber security governance strategy are:

- Perceiving and understanding how cyber security risks are related to the organization's business process continuity and critical operations.
- Determination and development of strategic goals of the organization.
- Identifying the need for cyber security and developing goals.
- Determination of Key Performance Indicators (KPIs).
- Determination of resource needs.

Establishment of continuous monitoring.

3. Standardized Processes

Without the implementation of existing and approved standardized processes in organizations, organizations can't ensure normal functioning and achieve efficiency, quality, and consistency. The latter, consistency, is important in terms of common understanding and management of risks across organizations. A key factor in an organization's overall cybersecurity management program is the repeatable establishment of processes. In short, a cybersecurity management program that is ad hoc and inconsistent will eventually lead to deficiencies. An ineffective cybersecurity management program will lead to increased security breaches, compromises, and a dramatic increase in the number of attacks.

4. Enforcement and Accountability

It is necessary to have processes in place to help ensure compliance with requirements. Otherwise, cybersecurity programs will become irrelevant to common processes, and inconsistent, requests will be ignored, and system crashes will occur. There is a risk that those responsible for the implementation of the cyber security program in organizations, as

soon as they notice the lack of accountability and governance in the cyber security program, immediately start looking for ways to solve the problem, thereby disregarding the established norms and standards. This is already a serious problem for the entire system. Cybersecurity management must be measurable and enforceable, and responsibility for its protection must be held at all levels of staff.

The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) recommends a multi-layered approach to risk management throughout the Information Systems Development Life Cycle (SDLC) to help develop security and privacy capabilities. This approach can be implemented through continuous monitoring, as well as constant awareness of high-level management [14–16].

5. Supervision and Control Exercised by the Upper Echelon

Our Managing cyber security processes are the concern and prerogative of top management in organizations. The decision-making link and the well-being of the organization depend on their making the right decision. If the organization's e. year If "top management" does not promote and support the issue of proper management of cyber security, then risk management in organizations will fail and will experience complete collapse. Senior management should be involved throughout the "life" process, contributing not only to their high awareness of the issue but also to realizing their willingness and ability to manage cybersecurity processes at a high level [17–19]. The fifth section of ISO 27001 contains a list of leadership principles that are important in developing an effective cybersecurity management program, namely:

- It should be ensured that the information security policy is created and goals are set, which will be consistent with the activities of the organization's strategic direction.
- Ensuring the integration of information security management system requirements into the organization's processes.
- Provision of information security management systems with all necessary resources.
- Constant awareness of the importance of information security systems management efficiency and its requirements.
- Ensuring the achievement of the set goal of the information security management system.
- Staff support to increase the effectiveness of the information security management system.
- Promotion of continuous process improvement.

Senior management should create a cybersecurity policy that:

- Corresponds to the goals of the organization.
- Contains information security objectives, or the structure to be used for information security objectives.
- Contains the obligation to meet requirements related to information security protection.
- Includes the obligation of continuous improvement of the information security management system.
- Available as documented information.
- Distributed within organizations and accessible to all stakeholders when needed.

Let's represent the components of the cybersecurity management system with some variables and explain their significance:

ISMP: Information Security Management Policy.

ISMS: Information Security Management System.

G: Goals of the organization.

S: Strategic direction of the organization.

R: Integration of ISMS requirements into organizational processes.

Resources: Necessary resources for ISMS.

E: Efficiency of ISMS and its requirements.

Goal: The set goal of ISMS.

Staff: Staff support for increasing ISMS effectiveness.

P: Promotion of continuous process improvement.

Now, let's define some mathematical relationships:

ISMP should be consistent with the organization's goals *(G)* and strategic direction *(S):*

$$ISMP = f(G, S). \quad (1)$$

Integration of ISMS Requirements (R) into organizational processes is crucial:

$$R = g(ISMS). \quad (2)$$

Provision of necessary resources *(Resources)* for ISMS:

$$Resources = h(ISMS). \quad (3)$$

Constant awareness *(E)* of the importance of ISMS efficiency and its requirements:

$$E = i(ISMS). \quad (4)$$

Ensuring the achievement of the set goal (Goal) of ISMS:

$$Goal = j(ISMS). \quad (5)$$

Staff support *(Staff)* to increase ISMS effectiveness:

$$Staff = k(ISMS). \quad (6)$$

Promotion of continuous process improvement *(P):*

$$P = l(ISMS). \quad (7)$$

The cybersecurity policy *(ISMP)* should contain information security objectives and the obligation to meet the requirements:

$$ISMP = m(Objectives, Requirements). \quad (8)$$

The cybersecurity policy *(ISMP)* should include the obligation of continuous improvement of the ISMS:

$$ISMP = n(Continuous\_Improvement). \quad (9)$$

The functions *f, g, h, i, j, k, l, m,* and *n* are abstract and represent the relationships and dependencies between the components. The formulation of these functions can depend specific organization's structure, culture, and goals.

But we can represent the needed parameters as follows:

ISMP should be consistent with the organization's goals *(G)* and strategic direction *(S):*

$$ISMP = G+S. \quad (10)$$

Integration of ISMS requirements *(R)* into organizational processes is crucial:

$$R = 2 \times ISMS. \quad (11)$$

Provision of necessary resources *(Resources)* for *ISMS:*

$$Resources = 3 \times ISMS. \quad (12)$$

Constant awareness *(E)* of the importance of ISMS efficiency and its requirements:

$$E = 0.5 \times ISMS. \quad (13)$$

Ensuring the achievement of the set goal (Goal) of *ISMS:*

$$Goal = ISMS/2. \quad (14)$$

Staff support (Staff) to increase ISMS effectiveness:

$$Staff = ISMS+needed\_number. \quad (15)$$

Promotion of continuous process improvement (*P*):

$$P = ISMS \times calculated\_coefficient. \quad (16)$$

The cybersecurity policy *(ISMP)* should contain information security objectives and the obligation to meet the requirements:

$$ISMP = Objectives+Requirement. \quad (17)$$

The cybersecurity policy *(ISMP)* should include the obligation of continuous improvement of the *ISMS:*

$$ISMP = Continuous\_Improvement \times 2. \quad (18)$$

6. Necessary Resources

Top management must provide all necessary resources needed to effectively implement and comply with cybersecurity and information security management systems. Funding should be allocated taking into account the priorities for the protection of information and information systems that are adequate to the relevant risks [20, 21]. Allocated financial means should also consider qualified personnel and their training. Also, allocated resources should allow and ensure the ability to purchase the necessary tools and equipment, as well as ensure the continuity of the process.

The management of cyber security systems begins with the top management of the organization and all subsequent links, personnel have their role, and their share of responsibility in ensuring the protection of information and information systems in the organization. It is also necessary to take into account the fact that it is necessary to conduct cyber hygiene courses for the staff in the organization, which in turn further reduces the risks in the organization related to the provision of cyber security [22, 23].

Cybercriminals will become increasingly savvy and dangerous to organizations, taking advantage of the latest technological advances. The most dangerous is the fact that not only simple hackers are behind cyber-attacks, but entire criminal syndicates, and even more dangerous and alarming is the fact that organizations and companies are increasingly turning to the services of cybercriminals as part of corporate espionage to gain their advantages [24–26].

Below are some recommended steps that organizations can take to strengthen an effective cybersecurity and information security management system:

1. The Chief Information Security Officer (CISO) must report directly to the CEO, which in turn emphasizes the strategic importance of cyber security in the organization. Those responsible for the protection of information and information systems in organizations should discuss and agree on the issue of cyber security strategy and plans with the organization's senior management and the board of directors. The CISO should actively participate in board meetings and regularly provide them with updated information on threats, preparedness, and response plans.

2. Conducting internal cyber security policy review. It is necessary to conduct an independent objective assessment to ensure the validity of the cyber security policy and the measures taken. The board of directors and all internal stakeholders of the organizations should be involved in this process so that full support and agreement are achieved [27].

3. We must make sure that organizations' cyber security processes and control mechanisms are reliable. In particular, are security controls integrated, and is the organization compliant with the NIST Cybersecurity Framework?

4. It is necessary to be familiar with all legal and normative acts related to the circulation of information in organizations and its protection, as well as cyber security processes. At the same time, the obligation to disclose personal data to employees should not be violated, and GDPR requirements should be observed [28–30].

5. Correct, targeted, and sufficient budgeting of cyber security is necessary. As practice shows, it should be about 10–12 % of the total budget of the information technology direction of organizations. Organizations' boards of directors and senior management must be informed of existing risks, the cybersecurity landscape, and emerging threats to budget appropriately and plan for response. It should also be noted here that in the event of an increase in risks and threats, budgeting should be increased accordingly.

6. A comprehensive incident response strategy should be developed and regularly updated. This allows organizations' critical infrastructure to be on constant alert for cyber incidents. Also, in the development of response plans against incidents, the participation of other structural units of organizations and their active involvement is necessary [24, 31, 32].

7. It is necessary to have constant contact with partners, suppliers, and clients of organizations, to introduce and provide them with advanced methods of ensuring cyber security within the framework of this relationship, and it is also necessary to demand maximum compliance with established requirements and rules from their side. This will reduce risks and ensure better protection of organizations' infrastructure.

7. Conclusions

The rapid development of Internet technologies and the global situation have accelerated the increase in demand for the process of implementing digital transformation in organizations. The components of digital transformation make it easier for organizations to operate, but at the same time, it is necessary to maintain a balance between technological innovation and cyber security, in which both the board of directors, senior management, information security manager, and other structural units should be involved. This is a complex process and such joint engagement will help to develop a cyber-security strategy and policy within the framework of digital transformation and to properly plan the process.

The World Economic Forum noted in its annual risk assessment index that cyber-attacks and the resulting increased risks have become one of the most important challenges for corporations. The potential dangers associated with such attacks go beyond

monetary and data loss, as a cyber-attack on a victim can lead to customer attacks, reputational damage, and fines from regulatory authorities. All this can cause great damage to the business. At the global level, 2020 was a serious challenge in the direction of cyber security. The same report notes that in 2021, the threats and methods of cyber-attacks that existed in 2020 will remain.

Digital transformation is the innovative approach to the implementation of electronic services and governance, which ensures full or partial digitalization of organizations and, in turn, is a serious challenge for the process of introducing the correct management of cyber security and information security in organizations, which must be consistent and consistent with other directions of digital transformation. Therefore, it is obligatory to offer the cyber security management model for the organizations. The model offered in this paper considers the major part of the obligatory parameters.

Acknowledgment

This work was funded by the Shota Rustaveli National Foundation of Georgia (SRNSFG) (NFR-22-14060).

References

[1] F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021). doi: 10.1109/ picst54195.2021.9772181.

[2] H. Shevchenko, et al., Information security risk analysis SWOT, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 309–317.

[3] V. Buriachok, V. Sokolov, P. Skladannyi, Security Rating Metrics for Distributed Wireless Systems, in: Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education:" Modern Machine Learning Technologies and Data Science, vol. 2386 (2019) 222–233.

[4] V. Svanadze, Doctoral Thesis "Cybersecurity Policy and Strategy of Management," Georgian Technical University, 2023.

[5] V. Svanadze, The Impact of COVID-19 on the Future Development of Cybersecurity, Global Foundation for Cyber Studies and Research, July 2020.

[6] M. Iavich, et al., The Novel System of Attacks Detection in 5G, Lecture Notes in Networks and Systems, vol. 226 (2021) 580–591.

[7] V. Svanadze, Near Future of Cyber Security and New Trends in Cyberspace, Global Foundation for Cyber Studies and Research, Dec 2020.

[8] S. Gnatyuk, T. Zhmurko, P. Falat, Efficiency Increasing Method for Quantum Secure Direct Communication Protocols, Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS'2015), Warsaw, Poland, Sept. 24–26, vol. 1 (2015) 468–472.

[9] V. Svanadze, The Importance of Education in the Development of Cyber Security, Sci. Pract. Cyber Secur. J. 5(2) (2021) 39–44.

[10] P. Anakhov, et al., Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network, J. Theor. Appl. Inf. Technol. 100(22) (2022) 6635–6644.

[11] H. Hulak, et al., Dynamic Model of Guarantee Capacity and Cyber Security Management in the Critical Automated System, in: 2nd Int. Conf. on Conflict Management in Global Information Networks, vol. 3530 (2023) 102–111.

[12] The Global Risks Report 2021, 16th Edition of the World Economic Forum, In partnership with Marsh McLennan, SK Group and Zurich Insurance Group, 19 Jan., 2021.

[13] Guide to Good Governance in Cybersecurity, DCAF Business and Security Division, Directorate for Security Cooperation and Defence (DCSD) of the French Ministry of Europe and Foreign Affairs, 19 Jan., 2021.

[14] V. Svanadze, A. Gotsiridze, Cyber Defense. Major Players in Cyberspace.

Cyber Security Policy, Strategy and Challenges (Collection of Papers and Articles), Ministry of Defense of Georgia (2015).
[15] Z. Hu, et al., Method of Searching Birationally Equivalent Edwards Curves over Binary Fields, Advances in Intelligent Systems and Computing, vol. 754 (2019) 309–319.
[16] S. Gnatyuk, et al., Method of Algorithm Building for Modular Reducing by Irreducible Polynomial, Proceedings of the 16th International Conference on Control, Automation and Systems, Oct. 16–19, Gyeongju, Korea (2016) 1476–1479.
[17] M. Ekstedt, et al., Securi CAD by Foreseeti: A CAD Tool for Enterprise Cyber Security Management, in: 2015 IEEE 19th Int. Enterprise Distributed Object Computing Workshop, Adelaide, SA, Australia, (2015) 152–155, doi: 10.1109/edocw.2015.40.
[18] C. Schmittner, et al., A Preliminary View on Automotive Cyber Security Management Systems, in: 2020 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, France (2020) 1634–1639, doi: 10.23919/date48585.2020.9116406.
[19] N. Goderdzishvili, S. Khutsishvili, Cyber-crime in Georgia: Current Challenges and Possible Developments, PMCG Research Center, 2021.
[20] M. Antunes, et al., Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal. J. Cybersecur. Priv. 1 (2021) 219–238, doi: 10.3390/jcp1020012.
[21] F. E. Catota, et al., Cybersecurity Education in a Developing nation: The Ecuadorian Environment, J. Cybersecur. (2019) 1–19.
[22] I. Lee, Internet of Things Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet 2020, 12. doi: 10.3390/fi12090157.
[23] R. J. Raimundo, A. T. Rosário, Cybersecu-rity in the Internet of Things in Industrial Management. Appl. Sci. 2022, 12. doi: 10.3390/app12031598.
[24] O. Chebanyuk, O. Palahin, K. Markov, Domain Engineering Approach of Software Requirement Analysis, in: 12th Int. Conf. of Programming, vol. 2866 (2020) 164–173.
[25] J. Brown, Executive's Cybersecurity Program Handbook: A Comprehensive Guide to Building and Operationalizing a Complete Cybersecurity Program, Packt Publishing (2023).
[26] P. Prystavka, et al., Devising Information Technology for Determining the Redundant Information Content of a Digital Image, East.-Eur. J. Enterp. Technol. 6(2-114) (2021) 59–70.
[27] E. Y. Handri, P. A. W. Putro, D. I. Sensuse, Evaluating the People, Process, and Technology Priorities for NIST Cybersecurity Framework Implementation in E-Government, in: 2023 IEEE Int. Conf. on Cryptography, Informatics, and Cybersecurity (ICoCICs), Bogor, Indonesia (2023) 82–87, doi: 10.1109/icocics58778.2023.10277024.
[28] D. Kucherov, A. Berezkin, L. Onikienko, Detection of Signals from a LoRa System under Interference Conditions, in: Int. Scientific-Practical Conf. on Problems of Infocommunications: Science and Technology (2018) 437–441.
[29] T. Khodadadi, et al., Exploring the Benefits and Drawbacks of Machine Learning in Cybersecurity to Strengthen Cybersecurity Defences, 2023 IEEE 30th Annual Software Technology Conference (STC), MD, USA (2023). doi: 10.1109/STC58598.2023.00005.
[30] O. Chebanyuk, An approach to software assets reusing. In: Zlateva, T., Goleva, R. (eds.) CSECS 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 450 (2022) 73–83. doi: 10.1007/978-3-031-17292-2_6.
[31] K. Tharot, et al., Industrial Cybersecurity Game-Scenarios based on the MITRE ATT&CK Framework, in: 2023 Asia Meeting on Environment and Electrical Engineering (EEE-AM), Hanoi, Vietnam (2023) 1–4, doi: 10.1109/eee-am58328.2023.10395155.
[32] O. Oksiiuk, V. Chaikovska, A. Fesenko, Security Technique for Authentication Process in the Cloud Environment, in: Int. Scientific-Practical Conf. Problems of Infocommunications Science and Technology (2019) 379–382.