Information Security System in Provision of the Economic Security and Risk Management of the Enterprise

Euvgenia Nosova[1], Lyudmyla Anisimova[1], Tetiana Murovana[1], Yulia Sviatiuk[1], and Olena Iafinovych[1]

[1] *Taras Shevchenko National University of Kyiv, 60 Volodymyrska str., Kyiv 01033, Ukraine*

Abstract

The development of technology and digitalization mean that every year the economic security of enterprises becomes more and more dependent on information security. As the number of hacking attacks increases it can result in loss or withdrawal of confidential or enterprise-sensitive information. This requires significant financial resources for building a system of information security management, implementation of risk management to identify existing and potential threats to information security, as well as to conduct an information security audit to identify weak spots in the existing information security system. Information security threats are divided into external and internal threats. The first are caused by the actions of counterparties, hackers and other actors who cooperate or are interested in gaining access to the company's information, and the last are caused by the actions and behaviour of the employees of the company and lead to information security breach in about 80% of cases. Information security management system must perform such functions as prevention of the occurrence of threats, their detection, disable and recovery of information. The employees of the organization must be aware of the procedures for ensuring information security to perform all these functions at all stages. Information security management system is based on the following principles: responsibility and accountability, awareness of the existing corporate culture, compliance with the current legal acts and constant audit.

Keywords

Economic security, information security, information security management system, information systems, information security audit.

1. Introduction

Changes in the external and internal environment of enterprise functioning lead to the need for constant review of the components of economic security and their replenishment, since new challenges arise, which pose threats to enterprises.

At the present stage of economic development success of the functioning of enterprises is becoming increasingly determined by such a non-material asset as information. Its protection is more complicated issue compared with the protection of the existing material assets of the company, which determines its value and importance for the legal entity. Therefore, it is necessary to create risk management system of such a component of economic security as information security.

Development of digitalization in the world and in Ukraine, among others, leads to the fact that information security is gaining more and more importance in ensuring the economic security of the enterprise. This is due to the fact that enterprises are switching to electronic document management, are using cloud technologies, various software, computers are constantly connected to the Internet. The efficiency of the activities of the enterprises increasingly begins to depend on the security of their information systems. Information, which concerns the activities of the enterprise, requires protection

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine

EMAIL: euvgenianosova@knu.ua (E. Nosova); anisimova@knu.ua (L. Anisimova); murovana@knu.ua (T. Murovana); sviatiuk@gmail.com (Y. Sviatiuk); olenayafinovych@knu.ua (O. Iafinovych)
ORCID: 0000-0001-9678-269X (E. Nosova); 0000-0001-6285-7681 (L. Anisimova); 0000-0002-7975-0984 (T. Murovana); 0000-0001-8343-1890 (Y. Sviatiuk); 0000-0002-6804-0848 (O. Iafinovych)

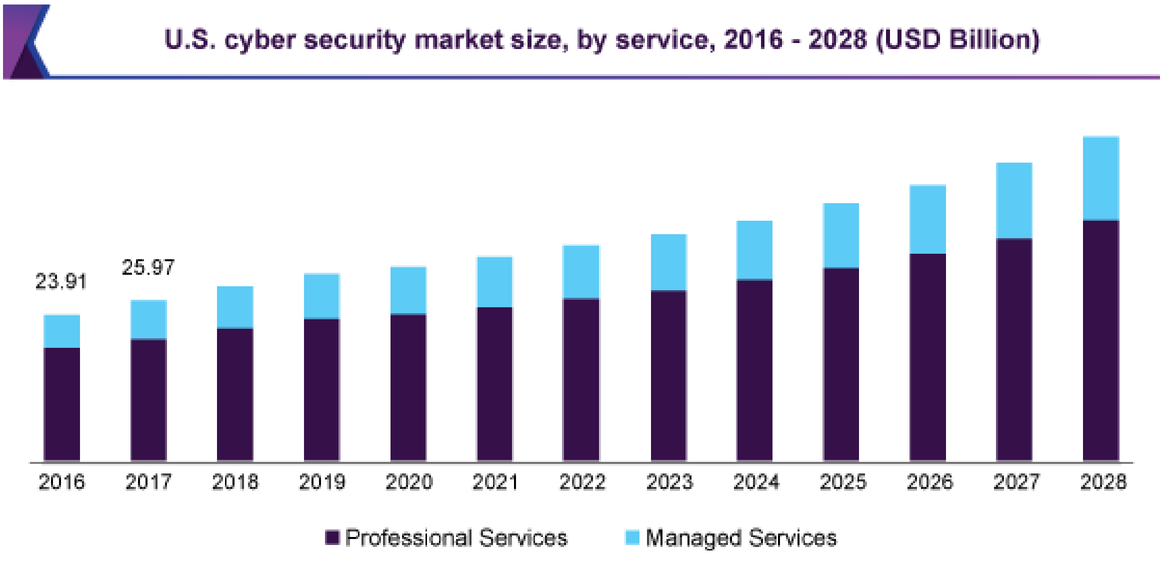
against unauthorized access, modification, disclosure and ensuring timely withdrawal. Security of information must be ensured at the stage of its receiving, storage and transfer. Nowadays, the information component of economic security is a vital element and an integral part of the management process of the enterprise and its economic security.

The growing number of cyber-attacks, which are becoming successful due to the presence of weak spots in the system of information security and occurring on the background of rapid technology development, confirms the topicality and relevance of the research topic. Each year it becomes more and more difficult to protect the data, and also the requirements to ensure the confidentiality of information preserving its accessibility and integrity are increasing.

The paper is organized as follows: first, the importance of information security in the context of increasing number of cyber-attacks is reviewed, which is confirmed by statistical data. Further are defined the essence of information security, current threats, systems and models of protection of information, which determines the necessity of building a system of information security management. This requires defining the stages of building an information security management system, the processes of its provision and management, the functions and principles that are at the basis of the system.

2. Cyber Security Market Trends

Under current conditions of the worldwide spread of the Covid-19 coronavirus infection, ensuring information security of enterprises in the context of a growing number of transactions via the Internet and the use of cloud-based resources for data storage becomes even more important. The global market of information security products is growing steadily, and it is predicted that by 2022 it will reach 170.4 billion dollars (Fig. 1).



Source: www.grandviewresearch.com

Figure 1: The volume of the market of cyber security, 2016–2028 [1]

Among the total number of cyber security violations approximately 95% of them are caused by human error [1]. Top managers of leading companies will be forced to redesign business processes at their enterprises in order to increase information security and awareness of existing threats and cyber attacks, and the company's activity should be focused on solving more complex threats.

The researchers at the Clark School at the University of Maryland are among the pioneers in providing a quantitative assessment of the number of hacker attacks over the Internet. On average, every 39 seconds a hacker attack occurs. Most attacks are aimed at stealing user names and passwords, which are used by individuals and legal entities [2]. Among all attacks targeting enterprises, 43% of cyber attacks were against small businesses. Meanwhile, companies spend an average of $7.68 million to mitigate security risks associated with cyber attacks [3].

For state-owned companies the cost is much higher, because they face a greater number of threats, the average data breach at a state-owned enterprise is estimated at $116 million. Moreover, the most common methods used to acquire personal and corporate data are: harmful programs (34%), fraud (25%), unauthorized access (20%) and incorrect configuration (12%). Moreover, 43% of the companies that were attacked were unable to identify these attacks [4].

In line with the trends of the last few years, not only the number of data leakage is growing, but also their scale.

3. Information Security of the Enterprise

Information security plays a key role in ensuring the long-term and successful functioning of the business as it contributes to its protection from the external and internal threats, which are related to the disclosure of information, allows the enterprise to preserve its reputation and its value for potential investors, owners and counterparties. On the one hand, information security can be ensured by the introduction of the enterprise technical service, which will be responsible for information technology and information protection. On the other hand, the effective management of information security is impossible without the support of the senior management, who will understand the importance of this issue and will contribute to the development of the enterprise appropriate policies and procedures for ensuring information security, as well as understand the importance of funding information protection at the required level. Furthermore, it must be clearly defined which division has the information to be protected, who is exactly responsible for its preservation, so there should be organized cooperation between the specific divisions.

At the enterprises there is a direct connection between the level of information security, corporate governance and compliance with the corporate culture and code of ethics, a part of which is the use of the information available to employees on various aspects of the activities of the company. Responsibility for the preservation of information should be a part of corporate management and corporate culture, which should be determined by the senior management and communicated to each individual employee. This will facilitate protection and prevent the leakage of confidential information and, thus, allow to protect the interests of the enterprise. The management should motivate employees to comply with the corporate culture, including the usage of the information, imposing the responsibility for violation of the established rules, creating such a team morale, which does not allow for unethical behavior. This will allow to prevent unauthorized information leakage and minimize the existing weaknesses in terms of information security, as the employees will clearly understand the importance of information security and will be aware of all the relevant policies and procedures that need to be followed to ensure this security.

3.1. The Sources of Threats to Information Security

The sources of threats to Information Security are divided into internal and external. External include competitors, counterparties, criminal groups, hackers and other individuals who are interested in the information that is in the possession of the enterprise. Internal threats can be caused by a human factor (intentional or negligent disclosure of information by the management of the enterprise, employees, including IT-specialists, its leakage or unauthorized access to sources) or by technical means used at the enterprise (software, electronic mail, other means of communication).

The ratio between internal and external threats is approximately 80 to 20. Unauthorized possession of information occurs in the result of:

- Its disclosure as a result of an excessive communication of employees, which makes it possible to obtain confidential information at a very low cost or free of charge (30%) without any effort by the intruder.
- Unauthorized access through bribery of employees by competitors and other interested parties—24%.
- Lack of proper control over information security at the enterprise—14%.
- Exchange of operational experience between the competing structures—12%.

- Uncontrolled use of information systems—10%.
- Disclosure of information as a result of conflict situations between the management and employees—8% [5].

Therefore, it is necessary to take great efforts to create an effective system of information security at the enterprise, for which it is necessary to identify the existing internal and external threats, perform their constant monitoring and take measures to prevent the leakage of information or unauthorized access to it.

3.2. System of Information Protection

Another component of information security is building a comprehensive system of information protection, the functioning of which will allow to protect it from any accidental or purposeful intrusion, which can lead to its damage, loss or editing and, as a result, to the emergence of additional costs for its renewal or incurrence of losses caused by the leakage of the confidential information.

The main methods of information protection in electronic form include:

- Means of identification and personalization of users, when the administrator limits the access rights according to the employee's responsibilities, as well as the ability to review his actions in the system.
- Encryption means of information stored on computers and transmitted through the networks, which complicates the process of interception of the information transmitted by the electronic mail, through the system of electronic payments or by means of electronic communications.
- Antivirus protection means.
- Systems for detecting network vulnerabilities and network attack analyzers.
- Network firewall and virtual private networks [6].

3.3. Models of Protection of Information Systems

The results of the conducted analysis allowed to systematize information about existing models of protection of information systems at enterprises:

1. Universal models, which are based on using the process of investigation, i.e. methods, based on the search for answers to corresponding questions that are set in the process of economic activities and monitoring measures.
2. Models oriented to the use of measures to eliminate information security vulnerability (Diamond, MITRE ATT & CK, PICERL).
3. Models aimed at building an information security system (Defense in Dept, Cyber Kill Chain, Pyramid of Pain, PICERL, CVSS3).

The worldwide spread of the coronavirus Covid-19 infection has led to all business entities using electronic commerce tools and cloud-based information exchange. In view of this, more and more attention is paid to the analysis and improvement of existing models of information systems protection, as well as the implementation of effective tools for their management. Increasingly popular are approaches of the integration of several different methods of information systems protection, in order to eliminate their vulnerability and build an effective system of information security at the enterprise.

Thus, the diamond model, combined with the intrusion process phasing, for example, according to the Kill Chain model, provides an excellent framework for describing the attack process. The process of linking is based on the following principle: what was a threat or an opportunity in one attack can become the basis for introducing additional actions in the next one. These events can belong to one phase or be carried out sequentially or in parallel (Fig. 2). Besides, it is suggested to describe the entities and their connection by vectors (the elements can be in the form of numerical data or a fixed verbal indicator). This process is possible due to clustering of incidents to find answers to any question in the course of business activities of the enterprise.

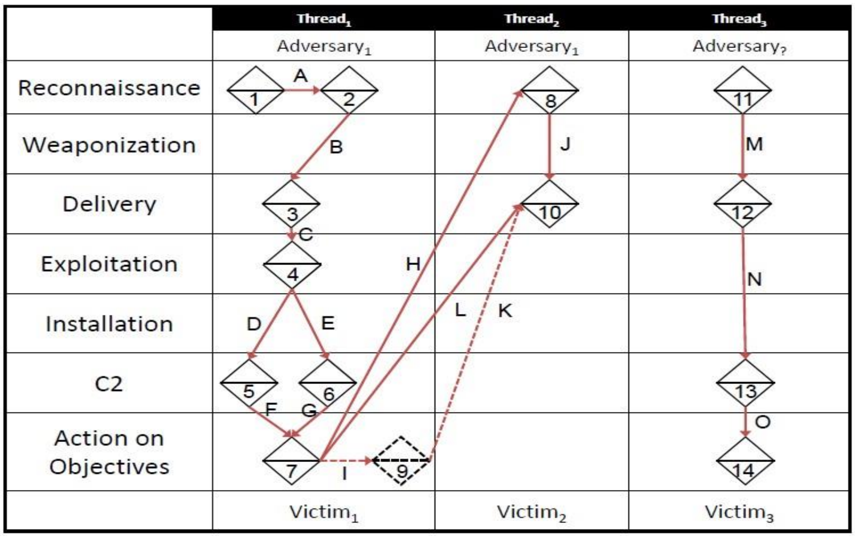


Figure 2: An example of the diamond model combined with the phasing of the invasion process by the Kill Chain model [7]

4. The Information Security Management System

Since the importance of information security is growing day by day, the development of a system of its management becomes a strategic task of the enterprise. This requires increased attention and support from the management and motivation of all stakeholders who can influence it – both the technical control service, and all parties who have access to the information related to the enterprise. Information security management is aimed to identify and manage the risks associated with the possibility of information leakage, control over the collection, storage and dissemination of information, the division of information into confidential, restricted and open, the identification of users and the responsibility for its disclosure.

According to ISO 27001: 2013, the information security management system is an integral part of an enterprise management system based on a risk-oriented approach and is designed for the creation, implementation, operation, monitoring, analysis, maintenance and improvement of information security of the enterprise. It includes processes of information security management, staff responsible for ensuring the functioning and management of information security, range of documented policies and procedures, mechanisms for ensuring information security. When building an information security management system, it is necessary to identify how processes and subsystems of information security are interconnected, who is responsible for them, what financial and human resources are necessary for its effective functioning [8].

Enterprises have to implement the information risk management system in their activities, namely to identify risks, perform their assessment to develop and implement measures to minimize or eliminate them. Studies show that risk management system is used by large enterprises, and more than three quarters of medium and small enterprises determine risks on the basis of intuition [9], which often leads to their underestimation due to the lack of knowledge of management in the field of information security and current cyber threats. This creates a significant risk not only for sustainable development, but also threatens their existence on the market.

4.1. Development of the Information Security System

Building an information security management system includes the following stages:

1. Defining the requirements for the construction of the system:

- Definition or specification of the scope of the ISMS.
- Analysis of business processes of the organization and their impact on the ISMS based on previously collected data.

- Inventory of the company's assets that are included in the scope of the ISMS, identifying their owners, the value for the company and their cost.
- Carrying out an initial assessment of the ISMS for compliance with existing standards (e.g. ISO 27001:2013) [8] and accepted management mechanisms.
- Development of information security policy taking into account the peculiarities of the enterprise, namely its location, resources and available technology.

2. Assessment of the risks of information security:

- Identification of risks and their assessment (provisions of ISO 27005:2011 can be used for this purpose) [10].
- Selection of risk control objectives and mechanisms, taking into account the possibility of their use at the enterprise.
- Development of a risk management plan that defines the actions of the company's management, resources, responsibility and existing priorities.

The results of this stage are reflected in the Declaration on the Application of Control Mechanisms.

3. Development of an information security management system:

- Documentation of information security management processes, namely policies, procedures, records.
- ISMS design, which includes the development of a technical specification.

4. Implementation of an information security management system:

- Training and professional development of personnel in the field of information security.
- Putting the ISMS into operation.
- Automation of information security management processes.

To create an effective system of information security, it is necessary to identify the range of information that must be protected and the existing factors that could threaten its confidentiality, namely the potential and real possibilities of its unlawful possession. When developing a system of information security of the enterprise it is necessary to distinguish between open information and information with restricted access, which, in its turn, is divided into confidential, private and information for internal use only.

The introduction of an internal control system at enterprises within the framework of corporate management has led to the fact that the responsibilities of top managers began to include the maintenance of information security. Thus, the managers have to develop the rules and perform control to provide accountability, responsibility, integrity and transparency. Since the peculiarities of corporate governance are related to the specific nature of the enterprise, the vision of the future, the mission and goals, the system of information security management for each enterprise is unique, and only due to its existence sustainable development can be achieved in the future.

4.2. Information Security Management and Provision

According to the ISO 27001:2013 [8] information security management processes include:

- Inventory and classification of information.
- Management of incidents related to breaches of information security.
- Internal audit of information security.
- Monitoring of information security management system performance.
- Records and document management.
- Analysis of the information security management system by management.
- External audit of information security.
- Improvement of the information security management system.

The implementation of these processes enables the management of information security risks.

Information security is provided by using the following processes:

- Management of vulnerabilities.
- Management of access to such an asset as information.
- Providing information security when working with staff.
- Continuous management of IT operations.

- Protection against malicious software.
- Network security management.
- Control of compliance with information security requirements.

Control over the information security is carried out by means of measuring, monitoring and reporting.

The information security management system comprises three levels – strategic, tactical and operational. Strategic management involves creation of information security policy, identification and assessment of potential risks and threats to information security. Tactical management includes the building and implementation of an information security system that complies with the developed policy. The operational level is to maintain and monitor the performance of the information security system.

4.3. Functions of the Information Security System

The information security system of the enterprise must be built taking into account four functions:

- Prevention – the networks must be protected from unauthorized intrusions. Usually this is done through the use of firewalls.
- Detection is the process of detecting attacks that are carried out through the Internet. The easiest way is to install anti-virus software.
- Disable – the system must be designed to defeat the attack if it is detected.
- Renewal – the system of permanent archiving of information or creating backups from which it can be renewed in case of complete or partial damage as a result of an attack.

The concept of information security is a protective mechanism, and therefore the system must be built before its breach occurred. System users need to know exactly how to react to various threats in order to detect them as quickly as possible and remove them with minimal negative consequences. To do this, the organization must develop a culture of information security management. The ISS must perform all four functions, but the more effective it is, the more rarely the last three have to be used. If any of them is weak, the information security of the company will be endangered.

4.4. Principles of the Information Security System

The information security management system has to comply with the following principles:

1. Responsibility and accountability – it should be defined for what information each of the employees is responsible for, their role in ensuring information security; interrelation of information security with the enterprise objectives, which must be specified in the company's information security policy along with the necessary procedures.
2. Awareness of the existing corporate culture at the enterprise, which will allow to build relationships based on mutual trust and thus eliminate the existing risks in the information security sphere. All employees of the enterprise have to be aware of the existing ethical rules and rules of information circulation at the enterprise.
3. Compliance with the current legal acts, which allows to ensure information security at the level of the enterprise without violating the national or intergovernmental requirements. The last one can concern the disclosure of public information, as well as the disclosure of information relating to the enterprise's counterparties or allows to protect its interests, if the counterparties disclose information about it.
4. Constant audit of the current information security system and assessment of its compliance with the organization's goals, which permits to reveal existing weaknesses in the procedures used to improve its efficiency by eliminating existing problems and oversights. Therefore, the audit can be carried out by the internal control service of the enterprise, as well as by external auditors.

The creation of an ISS requires significant financial costs, and therefore it is necessary to follow the principle of cost-effectiveness, which means that the costs incurred must be lower than the possible consequences of an unauthorized information leakage. Confidential information leakage leads to the loss of competitive positions on the market, and also affects the ability of the company to generate income and its value. This requires accurate identification of threats to information security of a particular company and the sources of the threats. Afterwards it is possible to proceed to the design and creation of the information security system. Modernization of the system should be carried out only after the changes in sources of risk are thoroughly studied.

4.5. Information Security Policy

According to the needs of the organization, an information security policy should be developed. It should be written in a comprehensible language to the user. In the context of Covid-19, while telecommuting and home-based work are increasingly common, this is a particularly urgent issue. Moreover, the current pace of life means that employees can work at contractors' offices, in public places and being out of work. Information security policy must be checked for feasibility in a particular organization, its validity and reviewed when conditions change.

Information security policy must describe:

- The employee's awareness of restrictions on the use of information upon recruitment.
- Procedure for providing access to information to employees.
- Level of access and distribution of information flows among divisions.
- Procedure for setting and changing passwords.
- Restriction of remote access.
- Restriction of corporate wireless network use.
- Use of the Intranet, etc.

It should not be forgotten that the introduction of any control system leads to a reduction in work productivity, as employees have to:

- Spend time learning existing safety measures and constantly update this knowledge through continuous improvement of the system.
- Have some restrictions on exchanging and transmitting information that slows down this process.
- Use passwords to prevent unauthorized access.
- Contact the system administrator when problems arise, etc.

5. Information Security Audit

Information security of the company could be ensured through an audit by independent companies or professionals who have the appropriate qualifications. They allow to identify whether the system of information security of the enterprise meets the current requirements and current practices of their construction: whether there are splinter elements of the system, which part of it is infected, whether there is a damaged code, which is located all over the information systems, etc. This is extremely important because hacker attacks are difficult to monitor and visually detect, and are mostly unnoticeable to users. However, when this fact is revealed, it means that the system has been penetrated, the equipment is infected and its use for someone else's interests has begun. In contrast to a corporate employee, who is responsible not only for ensuring information security but also for the operation of the information system, the independent auditor will be able to look at its operation and related threats from the outside.

When choosing a contractor, care should be taken to ensure that he has no interest in implementing his product, e.g. anti-virus software, other software or hardware, and its staff must have valid certificates confirming their qualifications and that they correspond to the level of a particular enterprise information system.

There are three main types of certificates in the field of enterprise information security [11]:

1. Certificates which cover various aspects of current information security technologies and are not linked to any particular product:

a) certificates in audit, consulting and management:

- Certified Information System Security Professional (CISSP) – the independent certification for information security by the non-profit organisation System Security Certification Consortium, in operation since 1991.

- System Security Certified Practitioner (SSCP) – a simplified version of the CISSP, suitable for information security specialists, administrators, IT specialists.
- Certified Information System Auditor (CISA) in Information Systems Audit and Control Association (ISACA) – the training programme for external information systems auditors and information security auditors has been in operation since 1976.
- Certified Information Security Manager (CISM) – certification of information security managers, which has been granted ANSI accreditation and is recognised at the state level in many countries around the world, has been in operation since 2002.

b) certificates in the field of testing and offensive security:

- Certified Ethical Hacker (CEH) – certification on the theoretical fundamentals of the ethical hacker.
- Offensive Security Certified Professional (OSCP) – certification for a specialist in detecting security offense in the virtual network.

2. Certificates which are related to a specific information security product or solution offered by some company (CCNA, CCNP, CCIE Security), Microsoft (MCSA, VCSE), Rad Hat (RHCSA, RHCE) and other. The advantages are: the possibility of getting a job with a company that issues a certificate; recognition by the professional community and a better chance of finding a job that requires the appropriate qualification.
3. Mixed certification systems.

6. Conclusions

The research shows that in the modern world great attention must be paid to ensuring information security. Information security is a complex of organizational, managerial, technical and preventive measures that are aimed at protecting the information environment of the organization from internal and external threats. The problem of information security of the corporate system is often handled on two fronts: firstly, the formal criteria are considered, which must meet the requirements of protected information technology, and secondly, the practical aspect – a specific set of measures to protect the information system and ensure information security. An important role in this plays the top management, because the managers determine the allocation of financial resources and the existence of a system of information security management at the enterprise.

Practice shows that the vast majority of enterprises, especially small and medium enterprises, do not properly established a system of information security. That leads to the loss or leakage of information, which has negative consequences for the functioning of the enterprise in the future. Employees are the main source of information threats and great care must be taken to raise their awareness of how to handle the information they have access to, the rules for using the Internet, gateway-free networks, mail, setting passwords, etc.

Building an effective information security system requires clear identification of the internal and external factors that could lead to information leakage or loss. The system functioning must be oriented on preventing intrusion, be able to detect and neutralize it immediately if it has occurred. In addition, the system must provide a backup mechanism through which the information can be restored with minimal losses.

The company must have a full-time employee or service specialising on information security to ensure uninterrupted functioning of the information system. In addition, an information security audit will reveal existing threats and test the system for resilience. Taking into account the constant emergence of new threats, technological progress and an increase in hacker attacks, great attention must be paid to the qualification of specialists who provide information security for the enterprise. Their qualification is confirmed by previous work experience and appropriate certification, which corresponds to the peculiarities of the information system of the enterprise. As the knowledge in this area quickly becomes outdated, continuous professional development must be an additional requirement.

7. References

[1] 15 Alarming Cyber Security Facts and Stats, 2020. URL: https://www.cybintsolutions.com/cyber-security-facts-stats/.

[2] Hackers Attack Every 39 Seconds, 2017. URL: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds.

[3] Overview: 30 Small Business Cyber Security Statistics, 2020. URL: https://www.fundera.com/resources/small-business-cyber-security-statistics.

[4] A. Nicodemus, Report: Average data breach costs public companies $116, 2020. URL: https://www.complianceweek.com/cyber-security/report-average-data-breach-costs-public-companies-116m/29037.article.

[5] O. Baranovsky, Financial Security in Ukraine (Assessment Methodology and Mechanism of Security Provision): Monograph, Kyiv, KNTEU, 2014, 759 p.

[6] G.V. Solomina, Ensuring Financial and Economic Security of the Enterprise: Tutorial, Dniepr, Dnipropetrovsk State University of Internal Affairs, 2018, 234 p.

[7] Models in information security, 2019. URL: https://habr.com/ru/post/467269/.

[8] ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements. URL: https://www.iso.org/standard/54534.html

[9] A. Ključnikov, L. Mura, D. Sklenár, Information security management in SMEs: factors of success, Entrepreneurship and Sustainability Issues 6(4) (2019) 2081-2094. doi: http://doi.org/10.9770/jesi.2019.6.4(37).

[10] ISO/IEC 27005:2011 Information technology. Security techniques. Information security risk management. URL: https://www.iso.org/standard/56742.html

[11] The 29 Most Valuable IT Certifications, 2021. URL: https://www.roberthalf.com/blog/salaries-and-skills/which-it-certifications-are-most-valuable

[12] O. Ali, A. Shrestha, A. Chatfield, P. Murray, Assessing information security risks in the cloud: A case study of Australian local government authorities, Government Information Quarterly (2020), Elsevier. URL: https://wroya.com

[13] Ad ́ele da Veiga, Liudmila V. Astakhova, Ad ́ele Botha, Marlien Herselman, Defining organisational information security culture, Perspectives from academia and industry, Computers & Security 92 (2020). doi:10.1016/j.cose.2020.101713

[14] M Brunner, C Sauerwein, M Felderer, R Breu, Risk management practices in information security: Exploring the status quo in the DACH region, Computers & Security 92 (2020), Elsevier. doi:10.1016/j.cose.2020.101776

[15] R. Contu, D. Kish, Ch.Canales, S. Deshpande, E. Kim, D. Gartner, Forecast Analysis: Information Security, Worldwide, 2Q18 Update, 2018. URL: https://www.gartner.com/en/documents/3889055.

[16] Cyber Security Market Trends & Growth Report, 2021-2028. URL: https://www.grandviewresearch.com/industry-analysis/cyber-security-market.

[17] B. Wang, Yu Liu, S. Parker, How does the use of information communication technology affect individuals? A work design perspective, Academy of Management Annals 14 (2020). doi:10.5465/annals.2018.0127.

[18] A. Jeyaraj, Y. Dwivedi, Meta-analysis in information systems research: review and recommendations, International Journal of Information Management 55 (2020). doi:10.1016/j.ijinfomgt.2020.102226.

[19] F. Nabi, X. Tao, J. Yong, Security aspects in modern service component-oriented application logic for social e-commerce systems, Social Network Analysis and Mining 11 (2021). doi:10.1007/s13278-020-00717-9.

[20] R. Algharabat, N. Rana, Social Commerce in Emerging Markets and its Impact on Online Community Engagement. Information systems frontiers, 2020. doi:10.1007/s10796-020-10041-4.

[21] J. Pool, S. Akhlaghpour, F. Fatehi, Health Data Privacy in the COVID-19 Pandemic Context: Discourses on HIPAA. Studies in health technology and informatics 279 (2021), pp.70-77. doi:10.3233/SHTI210091.

[22] A. Manoharan, A. Ingrams, D. Kang, H. Zhao, Globalization and Worldwide Best Practices in E-Government, International journal of public administration 44 (2020) 465-476. doi:10.1080/01900692.2020.1729182.

[23] S. AlGhamdi, A. K. T. Win, D. E. Vlahu-Gjorgievska, Information Security Governance Challenges and Critical Success Factors: Systematic Review, Computers & Security 99 (2020). doi:10.1016/j.cose.2020.102030.

[24] S. Schinagl, A. Shahim, What do we know about information security governance? "From the basement to the boardroom": towards digital security governance, Information and Computer Security 28 (2020). doi:10.1108/ics-02-2019-0033.

[25] N. Musa, A conceptual framework of IT security governance and internal controls, Proceedings of the 2018 Cyber Resilience Conference (CRC), 2018. doi:10.1109/cr.2018.8626831.

[26] W. Zeng, M. Koutny, Modelling and analysis of corporate efficiency and productivity loss associated with enterprise information security technologies, Journal of Information Security and Applications 49 (2019). doi:10.1016/j.jisa.2019.102385.

[27] D. Mandal, C. Mazumdar, Towards an Ontology for Enterprise Level Information Security Policy Analysis, Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP), 2021, pp. 492-499. doi:10.5220/0010248004920499.

[28] G. White, Strategic, tactical, & operational management security model, Journal of Computer Information Systems, Spring 2009, pp. 71-75. URL: http://130.18.86.27/faculty/warkentin/securitypapers/Leigh/White2009_JCIS49_3_ManagementandSecurity.pdf