РОЗДІЛ 9
НОВІТНЯ ПАРАДИГМА І ПРАКТИКА АУДИТУ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

УДК 658:004.946.056]:005.334(477)

Bulkot Ganna Victorivna,
PhD in Economics, Associate Professor Department of Audit,
Fadina Yelyzaveta Konstantinovna,
applicant for higher education at the second (Master's) level,
State higher educational institution
«Kyiv National Economic University named after Vadym Hetman»,
Kyiv, Ukraine

THE RISK MANAGEMENT FEATURES OF ENTERPRISES' CYBERSECURITY IN UKRAINE

In the conditions of economic transformation under the influence of the introduction of digital technologies and global digitalization, the probability of periodic crisis is constantly increasing.

Therefore, the establishment of an effective system of risk management of enterprises' cybersecurity in Ukraine, taking the implementation of digital technologies, it should take place in the context of national approaches to guaranteeing national security and be based on best foreign practices.

In the matter of cybersecurity, it can be said that it is the process of applying security measures to ensure the data availability confidentiality, and integrity.

Cybersecurity – is a new round of information security, which is aimed at the digital environment [1]. In which we are actually with you, so cybersecurity means not only the protection of information itself, but also the protection of the entire system in the information field, in the IT field (the field of computer technology) in general.

For these reasons, cybersecurity risk management – is the foundation for any security action, whether implementing systems or tools, or building processes and implementing rules and policies.

Risk management projects are often underestimated and not decoupled [2]. Whereas precisely competent identification and management of cybersecurity risks allows you to rationally allocate the budget for cybersecurity and competently prepare for attacks and threats in advance.

Therefore, prerequisites for formalizing cybersecurity risk management processes are: digitization (or «digitalization») of modern business [6]. There are almost no industries left that are not involved in cyberspace, and the size of enterprises no longer matters; getting the person himself to cover the application of cybersecurity risks.

Man, himself is already an information asset that must be protected; increasing dependence of security areas on each other. For example, physical security from the Internet of Things; the need of top managers for a simple and clear tool for security assessment and development.

It is advisable to pay attention to the methods of protection the information security management system, namely: determine the methodology for assessing cybersecurity risk management; implement risk processing procedures; create a report on the assessment of cybersecurity risk management in the information security system; create statements on the applicability of cybersecurity risk management; create cybersecurity risk management processing plans.

Then, it is essential: determine the cause of the loss of confidentiality, integrity and accessibility; identify risk owners; determine the criteria for assessing the consequences and probabilities; determine how the value of risk will be calculated; determine the criteria for risk acceptance.

But the methods of protection cybersecurity risk management in enterprises are: identify the risk of information security; analyze the risk of information security; visualize (eg. risk map) and / or rank analyzed information security risk is estimated (or level).

Therefore, the process of managing cybersecurity risks of enterprises includes the following key issues: 1. Has the company developed a strategy for the development of information security (cybersecurity)? 2. Were changes made to the strategy for the development of information security (cybersecurity) during the reporting period? 3. What structural units of the enterprise are determined to be responsible for achieving the goals of the information security (cybersecurity) strategy? 4. Does the company use cloud technologies? 5. Is there a program to raise awareness / training of employees, which deals with information security (cybersecurity)? 6. Is there a periodic control over the level of awareness of employees on information security (cybersecurity)? 7. Has the enterprise developed an information security policy? 8. Has the company developed a methodology for assessing and handling information security / cyber risks? 9. Is there an information security / cyber risk management process in place? 10. Has an information security / cyber risk assessment of critical business processes been performed? 11. Has the company developed internal documents (applicability provisions, information security / cyber risk management plan) for risk management? 12. Has the management of the enterprise approved a list of measures to reduce the likelihood of identified risks and / or reduce their impact on the functioning of critical business processes of the enterprise (name, details of the document)? 13. Has the effectiveness of the implemented risk mitigation measures been assessed? 14. Does the control activity carried out by the enterprise within the functioning of the internal control system cover the issues of control over information security and information exchange? and many others.

Therefore, summarizing all the above, it is possible for us to draw a conclusion, that further development of enterprises' cybersecurity risk management in Ukraine will reduce the number of errors, violations and abuses and reduce the

level of financial risks, and will contribute to increasing economic stability, improving investment attractiveness and achieving other goals.

References:

1. Cybersecurity risk assessment of information systems resources. URL: http://vrkadry.rada.gov.ua/uploads/documents/31132.pdf (access date: 19.11.2021).

2. Demchishak N.B., Shkirya A.S., «Risk management in the financial sector of Ukraine in the context of cyber threats and post-pandemic economic recovery». Innovative economy. Scientific journal № 3-4, 2021.C. 19-27.

3. Aleksieiev, M.M. (2019), «Analysis of methodological approaches to the application of risk management technology in the field of cybersecurity», Protyborstvo u kibernetychnomu prostori, no. 1(34), pp. 109-114. (Ukraine).

4. Bratiuk, V.P. (2015), «The essence of cybercrime and insurance protection «against cyber risks in Ukraine», Aktualni problemy ekonomiky, no. 9, pp. 421-427. (Ukraine).

5. Vinnikova, I.I. and Marchuk, S.V. (2018), «Cyber risks as one of the types of modern risks in the activities of small and medium-sized businesses and their management», Skhidna Yevropa: ekonomika, biznes ta upravlinnia, no. 5(16), pp. 110-114. (Ukraine).

6. «Cyber risks: how to understand and manage. URL: https://10guards.com/ua/articles/cyber-risks/ (access date November 20, 2021). (Ukraine).

7. The Verkhovna Rada of Ukraine (2018), The Law of Ukraine «On National Security» dated 21.06.2018 no. 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (access date November 20, 2021). (Ukraine).

8. The Verkhovna Rada of Ukraine (2018), The Law of Ukraine «On the basic principles of cybersecurity of Ukraine» dated 05.10.2017 no. 2163-VI. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (access date November 20, 2021, 2021). (Ukraine).

9. Canalys: Cybersecurity investment grows in 2020, but organizations face record data breaches, 2020. URL: https://www.canalys.com/newsroom/cybersecurity-investment-2020 (access date November 20, 2021).

10. Mark Reeves. Top 5 Security Practices for Financial Institutions to Defeat Online Identity Attacks. URL: https://www.entrust.com/top-5-security-practices-financial-institutions-defeat-online-identity-attacks/ (access date November 20, 2021).

УДК 330.15:332.12

Богуславська Світлана Іванівна,
д.е.н., доцент,
доцент кафедри менеджменту та економічної безпеки,
Черкаський національний університет ім. Богдана Хмельницького,
м. Черкаси, Україна

ВПРОВАДЖЕННЯ ГЕОГРАФІЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОГО АУДИТУ ТА МЕНЕДЖМЕНТУ РЕГІОНАЛЬНИХ СОЦІАЛЬНО-ЕКОНОМІЧНИХ СИСТЕМ

Єдина технічна база, уніфікована структура та функції географічних інформаційних систем (ГІС) з автоматизованими картографічними системами є фактором, що зумовлює їх інтеграцію в майбутньому. На початкових етапах джерелами поповнення та розвитку ГІС були бази інформаційно-пошукових