Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chişinău, Moldova

CYBERSECURITY RISK

Serghei OHRIMENCO

PhD Habilitat, Professor,
Academy of Economic Studies of Moldova, Moldova,
ORCID 0000-0002-6734-4321
E-mail: osa@ase.md

Valeriu CERNEI
PhD Student,
Academy of Economic Studies of Moldova,
Partner, IT Audit & Advisory BSD, Management SRL, Moldova,
ORCID 0000-0003-3300-334X
E-mail: valeriu.cernei@bsd.md

Abstract: *This paper presents the multifaceted field of cyber risks, their structure and composition, exploring the challenges posed by the rapid evolution of digital technologies. It highlights the prevalence of cyber risks as a set of activities performed in various sectors of human life, revealing the vulnerabilities faced by individual and collective users, commercial organisations, governments and individuals in today's hyper-connected landscape. The paper emphasises the importance of robust risk management strategies, highlighting the dynamic and persistent nature of cyber threats. A host of relevant international standards, frameworks and cyber risk management techniques to mitigate potential losses are reviewed. Approaches to defining the category of cyber risk are analysed. Daily attack techniques are reviewed. Risk analysis based on a set of reports from leading computer firms has been carried out. The structure of cyber security threats affecting the level of risk is determined. Despite the existing scientific and practical achievements in the field of cyber security, the ever-changing tactics of cyber criminals require constant adaptation of organisational and technical actions and the adoption of a set of proactive measures. Cyber risk management strategies are discussed, which include the selection of possible approaches, taking into account factors such as the level of cyber maturity, available resources, required skills and experience in cyber risk management. The article identifies the most prominent risk management tools, suggests some risk management strategies and advocates a comprehensive approach to cyber security that recognises the inevitability of cyber attacks and the need to build resilience in the face of emerging threats.*

Keywords: *threat, risk, cyber, risk management, risk strategy.*

UDC: *004.056.53:330.131.7*

JEL Classification: *D74 D81 F52.*

INTRODUCTION

Currently, the digital world embeds everyone as they use platforms, applications, data, services, and communication tools. It is almost impossible to find an area of activity where modern achievements in information and communication technologies and applications are not used. In this regard, ensuring the security of users' activities is of crucial importance to protect people, organizations, the environment, and infrastructure. We manage risks every day and everywhere and technology brings many specific risks that may have a critical impact on our lives. By the other side, related to technology, a complex of specific solutions based on developments and achievements in artificial intelligence, "zero trust" model, etc., is being used to counteract these risks.

The ongoing and dynamic confrontation between groups of malicious software (malware) developers and information security tools reflects the ratio of achievements in theory and practice. As threats change and increase qualitatively and quantitatively, risks

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chişinău, Moldova

also change. Digital threats require increased vigilance and determination to adequately respond to the constantly expanding risk cycle. The landscape of cybersecurity risk management is rapidly changing, and experts expect the emergence of new developments from official regulators and standards aimed at developing cyber risk management strategies as well as organizational-technical plans to mitigate the consequences of incidents.

It should be kept in mind that cybersecurity breaches are inevitable, and there are objective reasons for this. Among security and risk management experts, there is an opinion that preventing all hacks and information leaks is practically impossible, despite serious investments in the protection system. One cannot minimize risks to a "zero absolute". It is essential to focus efforts on the resilience of the information security system, treating breaches as incidents and building a learning and resistance system based on their knowledge base.

Information security specialists know and understand that nothing ever works without disruptions for an extended period. Any internal or external threat or risk can lead to a state where a well-functioning management object loses its competitive advantages, faces disruptions, etc. There is a constant hope that information security specialists will establish processes that allow for a systematic analysis of risks, threats, hazards, and issues and provide a list of economically efficient measures to reduce the risk to an acceptable level.

RISKS AND RISKS MANAGEMENT

Literature review

There are quite a few literary sources that address the issues of managing cyber risks. Among the main ones, we should mention the following: " Cyber-Risk Management" [1], "Optimal Spending on Cybersecurity Measures: Risk Management" [2], "Managing Information Risks: Threats, Vulnerabilities, and Response Measures" [3], "Managing Risks of Organizational Incidents" [4], "Cyber Risk, Intellectual Property Theft, and Cyber Warfare: Asia, Europe, and the USA" [5], and others.

First of all, let's point out the book by Karl Young, " Cybercomplexity: A Macroscopic View of Cybersecurity Risk" [6]. This book examines the issue of IT environment complexity, or "cyber entropy," which is usually considered a primary source of cybersecurity risk. The complexity is defined and simplified for analysis, assuming a probabilistic approach to security risk management. Then, a simple model of cyber entropy based on Shannon's entropy, a fundamental concept in information theory, is proposed. Key factors of cyber entropy emerge from this model, where these drivers reveal the dependence of cybersecurity risk on scale and explain why macroscopic security measures are necessary to eliminate cybersecurity risk on an enterprise scale. The book also discusses significant operational consequences of cyber entropy, thus providing both theoretical foundation and practical guidance for addressing this longstanding issue in cybersecurity risk management.

The goal of managing cyber security risks is to identify and eliminate factors that compromise information or disrupt business related to information by applying security measures in accordance with the organization's risk tolerance [6, p.153].

A fundamental aspect of security risk management is that all threat scenarios are equivalent when viewed from a sufficiently high level. This equivalence partially explains why the risk assessment process is universal. However, equivalence is not the same as identity. It is evident that all threat scenarios are not identical, explaining why the experience required for security risk management depends on the details of the scenario.

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chişinău, Moldova

Another source of interesting information on cyber risks is the book by the collective authors David Insua, Caroline Baylon, Jose Vila, "Security Risk Models for Cyber Insurance" [7]. The authors propose a "model solution" [7, p.56-60], the essence of which is as follows: to determine a rational distribution of resources for the protection object (the so-called "cybersecurity portfolio," which is a combination of security products, security management and control tools, and recovery and insurance products (cyber insurance)), several steps are required:

- The problem of risk management should be considered from the perspective of the "defender" and the model of their preferences (i.e., their utility function) regarding the optimal distribution of resources, considering alternative solutions among different types of security products (portfolio of security control means and portfolio of recovery control means) and insurance options, as well as conditional probabilities of various threats or impacts.
- To determine the conditional probabilities of threats from the "attacker," it is necessary to investigate the risk management problem from the perspective of the "attacker" or adversary – their strategic thinking. It is necessary to create influence diagrams of the attacker and build a model of preferences (utilities) regarding the conduct of targeted attacks. It should be noted that the actions of the attacker are constrained by various factors, including the probability of detection, the consequences of the attack, the existence of alternative types of targeted attacks, etc. Then, the probability of an attack by the "attacker" on the "defender" should be modelled.
- Optimization is carried out to maximize the expected utility of the defender's actions, taking into account the strategic thinking of the attacker. We also consider the probability that the "defender" may be attacked by one or more "adversaries." Each possible case is matched with a potential cybersecurity portfolio that maximizes expected utility and demonstrates the optimal choice of a cybersecurity portfolio to protect against adversaries.

Simultaneously, it is necessary to understand the defender's challenge, which involves viewing the risk management problem from the defender's perspective and modelling their preferences, i.e., their utility function. This includes determining the optimal distribution of resources considering alternative security product solutions, such as portfolios of security control measures and portfolios of recovery control measures, along with insurance options.

There are numerous relevant international standards, frameworks and methods for managing cyber risks and helping answering the defender’s questions. Some most popular include [8] - [15]:

ISO/IEC 31000: Contains principles and general recommendations for risk management. The standard is not specific to any industry or sector; it can be applied to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services, and assets. It should also be applied to any type of risk.

ISO/IEC 27005: Provides recommendations for information security risk management. These recommendations are based on ISO/IEC 31000. This standard supports the general concept of ISO/IEC 27001 regarding the requirements for managing information security systems. ISO/IEC 27032 offers cybersecurity recommendations with a focus on the virtual world and virtual intangible assets. According to ISO/IEC 27002:2022 , "information related to information security threats must be collected and analyzed to obtain information about threats."

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

CRAMM (CCTA Risk Analysis and Management Method): Developed by the British government agency CCTA (Central Communications and Telecommunications Agency), now renamed the Office of Government Commerce (OGC).

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité): Developed by DCSSI (Central Directorate for Information System Security, under the Prime Minister) in France. EBIOS is designed to adapt to the specific characteristics and needs of French organizations and has some cultural and legal specificities.

Mehari Methodology: Developed in 1995 by CLUSIF (Club for Information Security and Freedom of Communications). Mehari focuses on assessing information security and IT resource risks in organizations, providing a structure for analyzing and managing these risks. One significant difference is that Mehari was developed by an independent organization, and specific approaches and tools may vary.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): Developed by Carnegie Mellon University in the United States, providing a sophisticated risk modeling methodology with a focus on identifying and assessing operational risks and security practices.

FAIR (Factor Analysis of Information Risk): A framework for analyzing and managing risks in information security and operational risks. It is a quantitative and model-based approach designed to help organizations understand, analyze, and quantitatively assess risks associated with information in financial terms.

NIST IR 8441 (Cybersecurity Framework Profile 20 for Hybrid Satellite Networks): A profile of the cybersecurity framework for hybrid satellite networks. This profile serves as a practical guide for organizations and stakeholders involved in designing, acquiring, and operating satellite buses. Using this profile provides protection of services, self-assessment in accordance with cybersecurity principles, detection of cybersecurity-related disruptions, timely and effective response to service anomalies, and recovery to normal operation after a cybersecurity incident.

It is worth mentioning that organizations and countries, aiming to minimize risks, issue and recommend the use of guidance documents, best practices, and specialized literature to systematize and more effectively manage them. In this regard, ISO 19600 introduces compliance risk assessment, consolidating individual compliance management and risk management standards, with processes closely aligned with ISO 31000. This standard aids in evaluating how legislative acts, guiding documents, and best practices have been implemented and maintained in terms of managed risks. Among them, notable standards and directives include Basel III, NIS (II) Directive, European Union Cybersecurity Act, Federal Information Security Management Act (FISMA), Payment Card Industry – Data Security Standard (PCIDSS), Sarbanes Oxley Act (SOX), and others [16].

It is also worth mentioning the models considered by the authors, which contribute to the development and improvement of the CCSMM model - The Two-Dimensional CCSMM and The Three-Dimensional Model for a Community. It is the latter version of this model that allows for research at practically all levels, from the individual level, organization, to the state and nation. The model takes into account five levels of coverage, from initial to advanced. This model demonstrates the thesis that society consists of individual personalities and organizations, and their maturity influences the overall cybersecurity maturity of society. The three-dimensional model, in particular, has expanded the possibilities for researching cybersecurity issues, providing flexibility and scalability in the analysis of processes.

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

Analysts argue that this model serves as a roadmap for improving cybersecurity for individuals, organizations, communities, states, and nations.

Threats and Risks

Let's present several definitions of risk. "Risk is the probability of an incident occurring and its consequences for the object" as defined by [1, p.9]. The "classic" risk management approach is based on the threat. Several definitions are used, among which the following is considered relevant: "A threat is the point of interaction and convergence of people, the Internet, and computers. The threat arising from interaction can result from an error or a malicious influence. An error can be eliminated by increasing the awareness of the importance of handling, for example, confidential information. In this regard, a malicious strike is different." [2, p.19]. The author associates information security threats with the activities of criminal groups and transnational organized crime (TOC). Criminal networks and organized groups operate in many countries, planning their activities and achieving their business goals. Their activities may include a multitude of heinous crimes - human trafficking, sexual exploitation of adults and children, drug trafficking, violent crimes, corruption, arms trafficking, and even the sale of human body parts and representatives of flora and fauna under threat of extinction. Unfortunately, it should be noted that TOC was the first to appreciate the benefits and implement modern information technologies and communications, as well as reliable security systems.

The goal of cybersecurity risk management is to identify and eliminate factors that compromise information or disrupt business by applying security measures in accordance with the organization's risk tolerance [3]. "We can define risk analysis as a set of knowledge (methodology) that assesses and determines the probability of adverse effects on an agent (chemical, physical, or other), industrial process, technology, or natural process," as stated [4].

In cybersecurity, risk is the probability of an adverse event occurring. Thus, risk includes two key parameters: the probability that the event will actually occur and the impact it will have, which can be assessed based on the probable seriousness of the event. In mathematical terms, risk can be expressed as a deviation or variation from the expected result. That is why in financial markets, high-risk investments may be more preferable than low-risk investments, as there is at least a chance of very high returns. However, in the field of computer security, it is usually necessary to create an environment with a low level of risk, where threats and the damage they can cause are actively minimized [5, p.16].

According to the "Global Risks" report for 2023 prepared by the World Economic Forum [17], global risks, ranked by severity in the short term (up to 2 years) and long term (10-year period), include several directions, including the technological sector. In particular, for short-term and long-term forecasts, the value "Widespread cybercrime and lack of cybersecurity" is ranked 8th. The report states that technologies will exacerbate digital inequality, while risks associated with cybersecurity will remain a constant problem. The technological sector will be the main target for industrial policy and expanded government intervention. Government aid, military budgets, and private investments will ensure high rates of development and research in new technologies over the next decade, with a focus on areas such as artificial intelligence, quantum computing, and biotechnology.

For some countries, this will be a partial solution to a range of emerging crises (healthcare, food security, and the consequences of climate change). For some countries, digital inequality and divergence will grow. In all economies, technologies bring risks as disinformation increases, and uncontrolled turnover occurs among both workers and "white-collar" workers. Along with the growth of cybercrime, an increase in attacks on

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

critical infrastructure objects is forecasted, including agriculture, water supply systems, financial systems, public safety, transportation, energy, and communication infrastructure (space and underwater). Technological risks will be associated not only with fraudsters. Big data analysis will allow the abuse of personal information; weaken individual digital sovereignty, and the right to privacy.

The map of interconnections in the landscape of global risks in the report for the technological group includes adverse consequences of advanced technologies, concentration of digital power, digital inequality, disruption of critical information infrastructure, widespread cybercrime. In other words, a low level of cybersecurity.

In most cases, when it comes to risk management, the main threat is hackers' activity and cyberattacks. Due to the extremely rapid development of technology (technical and software), a significant part of hackers' activity has radically changed. From individual acts of vandalism and theft, an underground industry has grown, well-organized and excellently equipped with the latest innovations [18]. There has been a rapid growth and leap from individual hacking cases to the creation of specialized structures whose activities range from extracting financial benefits to achieving political goals [19].

The seriousness of this activity is confirmed by information on events from September 16 to 30, 2023, recorded by the website https://www.hackmageddon.com [20]. Computer analyst Paolo Passeri presents the results of the study for this period: information on 165 events was collected and processed, or 11 events per day. The total number of cases consists of 119 cases (72%) of cybercrime, 23 cases of cyber espionage (13.9%), 8 cases of hacktivism (4.8%), and no data in 15 cases (9.1%). The techniques of daily attacks are characterized by the following data: malware 58 cases (35.2%); unknown 32 (19.4%); vulnerability exploitation 26 (15.8); targeted attacks 24 (14.5%); account takeover 11 (6.7%); DDoS attacks 8 (4.8%); scams or fraudulent schemes 4 cases, cross-site scripting 1, attacks through publicly available container images 1.

Experts have detected several large-scale organizations operating in the financial technology sector which had been compromised. For example, the company Mixin Network lost an amount equivalent to 200 million dollars. This case became the largest hack in 2023.

Risk aspects are also noted in the Hiscox report on cyber readiness for 2023 [21]. The report identifies several significant changes in cyberspace that should be noted by anyone involved in combating cybercriminals. Cyber technologies remain the number one issue for business, but timid sprouts of optimism are beginning to appear. The top ten business risks are listed in the following table 1.

Table 1. Top 10 major risks (%)

№	Name	2023	2022
1	Exposure to a cyber attack	40	45
2	Losses due to economical issues e.g. inflation	38	40
3	Emergence of new competitor	36	36
4	Skills shortage	35	40
5	Reputational damage e.g. negative press	35	37
6	Regulatory or legislative changes	34	37
7	Pandemic or infectious diseases	33	42
8	Geopolitical conflicts disrupting operations	33	-
9	Fraud and white-collar crime	32	38
10	Extreme weather and natural disasters	29	33

Source: Hiscox Cyber Readiness Report 2023.

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

The structure of cybersecurity threats that impact the risk is as follows [22, p.28-29]:

- ✓ *Phishing Attacks*: These attacks involve the use of fake emails or messages to trick people into providing confidential information or clicking on malicious links, often leading to the theft of confidential information or malware infection.
- ✓ *Ransomware Attacks:* Ransomware is a type of malware that encrypts an organization's data and demands payment in exchange for a decryption key. These attacks can result in significant disruptions to business operations and substantial financial losses.
- ✓ *Malware Attacks:* Malware is any type of software designed to harm a computer system or network. This category may include viruses, worms, and trojans, among others.
- ✓ *Insider Threats:* These threats originate from within the organization, such as employees or contractors who intentionally or unintentionally misuse their access to confidential information or systems.
- ✓ *Advanced Persistent Threats (APTs):* APTs are targeted attacks carried out over an extended period by experienced attackers seeking unauthorized access to confidential data or systems.
- ✓ *Internet of Things (IoT) Attacks:* As the number of Internet-connected devices increases, IoT devices become more vulnerable to cybercriminals who can exploit vulnerabilities to gain access to networks or cause disruptions.
- ✓ *Cloud Security Risks*: Cloud services have become an integral part of modern business operations, but they also introduce new security risks, including data leaks, service interception, and unauthorized access.
- ✓ *Social Engineering Attacks:* These attacks involve manipulating individuals into disclosing confidential information or taking actions that harm security, often using psychological tactics.
- ✓ *Distributed Denial of Service (DDoS) Attacks:* DDoS attacks involve overwhelming a system or network with traffic to make it unavailable to users. These attacks can be used to disrupt business operations or extort organizations.
- ✓ *Cyber Espionage*: Cyber espionage involves the theft of confidential information to obtain advantage by organizations and / or States.

Strategies for managing cyber risks

Strategies for managing cyber risks involve choosing possible approaches, considering factors such as the level of cyber maturity, available resources, necessary skills, and experience in managing cyber risks [23]. Various literature sources present different models for responding to identified risks. The authors have analyzed and summarized well-known models, as presented în the table further.

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

Table 2. Risk management strategies

№	Risk Strategy	Description
1.	Terminate	Applied when the risk level is high, and it's not possible to apply measures to minimize it, or the cost of implementing measures is too high
2	Control	The most effective measure, involving the implementation or reinforcement of control measures. It is also the most common approach in IT and cybersecurity
3	Transfer	Applied when the risk impact is assessed as high, but the probability of occurrence is low. Transferring risk to a third party can be either complete or partial
4	Contingency	A response measure for risks with high impact and low probability, involving the implementation of backup mechanisms or technologies
5	Take More	Used when both the impact and probability of the risk are low, exploring solutions to optimize resources or new investment directions
6	Tolerate/Accept	Risks with low impact and probability can be considered insignificant and accepted without any specific measures
7	Communicate	A stage in the risk management process related to risks with high impact and medium or low probability. When implementing security control measures cannot reduce risks to an acceptable level, it is recommended to communicate the existence of the risk to all stakeholders, indicating that the risk exists and may affect goal achievement. This aspect is often overlooked
8	Research	Applied in organizations with a mature risk management process, involving a more in-depth study, including impact assessment, probability analysis, comparative analysis, etc. This is typically used by large companies developing products (e.g., antivirus software)
9	Consult	For some risks with a high impact and high probability, more effective measures may be suggested by specialized companies rather than by internal risk management personnel
10	Compliance	Often overlooked, this measure focuses on areas where control is critical to minimize compliance risks and includes checking the effectiveness of control

Source: authors

These strategies provide a framework for organizations to respond effectively to cyber risks based on their specific circumstances and risk profiles.

CONCLUSIONS

In conclusion, the evolving landscape of cyber risks poses significant challenges to organizations, governments, and individuals. The interconnected nature of digital technologies in cyberspace creates both, opportunities and threats. The opportunities provided by widely interconnected digital technologies in cyberspace come with costs, including the creation of possibilities for crime and espionage.

Today, every sector of the economy, every government, and virtually every citizen are constantly exposed to cyber attacks. Most of them suffer from persistent malware infections. Cybercriminals infiltrate quickly and remain unnoticed for months.

Defenders have learned a lot about modern cyber threats, including the types of organizations that cause the most damage, their resources, how they operate, and their motives. We have studied best practices and ways to enhance protection, significantly complicating success for adversaries. The risk can be reduced. However, we also understand that adversaries will be persistent and catch us off guard, regardless of how strong our defence is.

Despite advancements in understanding and implementing cybersecurity measures, the persistent and sophisticated tactics employed by cybercriminals demand constant vigilance. It is important to adopting comprehensive risk management strategies,

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

acknowledging the inevitability of cyber attacks, and the need for continuous adaptation to emerging threats. As technology continues to advance, a proactive and adaptive approach to cybersecurity remains crucial in mitigating the impact of cyber risks and ensuring the resilience of digital ecosystems.

BIBLIOGRAPHY

1. REFSDAL, Atle, et al. *Cyber-risk management*. Springer International Publishing, 2015. p. 33-47.
2. KISSOON, Tara. *Optimal Spending on Cybersecurity Measures: Risk Management*. Routledge, 2021.
3. TAPLIN, Ruth. *Cyber Risk, Intellectual Property Theft and Cyberwarfare: Asia, Europe and the USA*. Routledge, 2020.
4. REASON, James. *Managing the risks of organizational accidents*. Routledge, 2016.
5. SAFFADY, William. *Managing information risks: threats, vulnerabilities, and responses*. Rowman & Littlefield Publishers, 2020.
6. YOUNG, Carl S. Complexity and Cybercomplexity. In: *Cybercomplexity: A Macroscopic View of Cybersecurity Risk*. Cham: Springer International Publishing, 2022. p. 79-87.
7. INSUA, David Ríos; BAYLON, Caroline; VILA, Jose (ed.). *Security Risk Models for Cyber Insurance*. CRC Press, 2020.
8. MCCARTHY, James, et al. Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN). *National Institute of Standards and Technology, NIST Interagency or Internal Report (IR) NIST IR*, 2023, 8441.2023: 28.
9. SCHREIDER, Tari. *Cybersecurity Law, Standards and Regulations*. Rothstein Publishing, 2020.
10. Information Security Forum. *Standard of Good Practice for Information Security* [online] 2020. [viewed 9 November 2023]. Available from: <https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security-2020/>
11. MALEH, Yassine, et al. *IT governance and information security: Guides, standards, and frameworks*. CRC Press, 2021.
12. Peltier T. R. Information security risk analysis. – CRC press, 2005.
13. WHITE, Gregory B. The community cyber security maturity model. In: *2011 IEEE international conference on technologies for homeland security (HST)*. IEEE, 2011. p. 173-178.
14. Hafiz Sheikh Adnan Ahmed. *A Guide to the Updated ISO/IEC 27002:2022 Standard.* Part 1. [online]. 2023. [viewed 6 December 2023]. Available from: <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-7/a-guide-to-the-updated-iso-iec-27002-2022-standard-part-1>
15. YOUNG, Carl S. Complexity and Cybercomplexity. In: *Cybercomplexity: A Macroscopic View of Cybersecurity Risk*. Cham: Springer International Publishing, 2022. p. 79-87.
16. SCHREIDER, Tari. *Cybersecurity Law, Standards and Regulations*. Rothstein Publishing, 2020.

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

17. World Economic Forum. *Global Risks Report 2023*. [online]. 2023. [viewed 29 November 2023]. Available from: < https://www.weforum.org/reports/global-risks-report-2023>
18. OHRIMENCO, Serghei; BORTA, Grigori; CERNEI, Valeriu. Estimation of the key segments of the cyber crime economics. In: *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*. IEEE, 2021. p. 103-107.
19. OHRIMENCO, Serghei; ORLOVA, Dinara; CERNEI, Valeriu. Cyber Threats Modeling: An Empirical Study. *Business Management/Biznes Upravlenie*, 2023, 3.
20. PASSERI, P. Hackmageddon. *Cyber Attacks Timeline. 16-30 September 2023*. [online] 2023 [viewed 28 November 2023]. Available from: <https://www.hackmageddon.com/2023/11/28/16-30-september-2023-cyber-attacks-timeline/>
21. Hiscox. *Cyber Readiness Report 2023*. [online]. [viewed 11 December 2023]. Available from: https://www.hiscoxgroup.com/sites/group/files/documents/2023-10/Hiscox-Cyber-Readiness-Report-2023.pdf
22. WATTERS, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.
23. ULSCH, MacDonnell. *Cyber threat!: how to manage the growing risk of cyber attacks*. John Wiley & Sons, 2014.