Information security and protection from cyber attacks as a component of the economic security system of the enterprise[⋆]

Sergiy Gnatyuk[1,†], Zarina Poberezhna[1,†] and Maksym Zaliskyi[1,*,†]

[1] *State University "Kyiv Aviation Institute", 1 Liubomyra Huzara ave., 03058 Kyiv, Ukraine*

Abstract

The paper deals with the issue of ensuring economic security of an enterprise in the context of growing cyber threats and digital transformation. The author proves that cyber security is a key element of an enterprise's information security, which is an integral part of its overall economic security. The authors summarize the main approaches to building a comprehensive system for protecting the economic interests of an enterprise, which includes both preventive and reactive measures to counter cyber threats. Attention is paid to the analysis of current trends in the field of information security: the increasing complexity of attacks, the use of malware and the importance of the human factor in the emergence of threats. The authors substantiate the importance of raising employees' awareness of the main cyber threats, since a significant part of incidents is related to the human factor. It is proved that an enterprise's cyber security strategy should include measures to identify potential risks, assess the vulnerabilities of information systems, and develop effective methods to counter threats. Attention is paid to the analysis of the experience of leading companies in the field of cyber security, which allows implementing best practices to ensure the long-term economic sustainability of the enterprise. It is concluded that it is necessary to develop adaptive models of cyber defense that can take into account the specifics of the enterprise, the speed of technology development and the constantly changing nature of cyber threats.

Keywords

economic security, information security, cyber security, cyber attacks, digital transformation, data protection, enterprise resilience, business sustainability

1. Introduction

Enterprises are the main link in the economy that combines productive forces and industrial relations, and operate in a fiercely competitive and unstable external environment. The management faces a difficult task not only to maintain the sustainability of the enterprise, but also to effectively manage the numerous challenges it faces on a daily basis. It is necessary to apply modern methods of assessing the competitiveness of the enterprise in terms of resource and market trends, namely, the assessment of the financial and resource status, which involves the development of indicators of financial stability, business activity, and net profit [1].

In today's operating environment, enterprises are particularly threatened by both internal and external factors that can lead to the loss of strategic stability, failure to achieve goals, and violation of economic security. One of the key threats today is cyber attacks, which can cause leakage of confidential information, disruption of operational processes, and lead to significant financial losses. In this regard, an urgent task for enterprises is to form a comprehensive economic security system that will ensure timely detection, assessment, and neutralization of threats aimed at the information and economic resources of the enterprise. An important aspect of ensuring economic security is the protection of information from cyber attacks, which includes the implementation of effective cyber security measures, risk monitoring and the development of incident response strategies [2–4]. Creating a reliable data protection system will allow businesses not only to prevent potential losses but also to ensure long-term stability and competitiveness in the market.

[⋆] *CSDP'2025: Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine*

[*] Corresponding author.

[†] These authors contributed equally.

✉ serhii.hnatiuk@npp.kai.edu.ua (S. Gnatyuk); zarina_www@ukr.net (Z. Poberezhna); maximus2812@ukr.net (M. Zaliskyi)

iD 0000-0003-4992-0564 (S. Gnatyuk); 0000-0001-6245-038X (Z. Poberezhna); 0000-0002-1535-4384 (M. Zaliskyi)

Thus, the implementation of measures to increase the level of economic efficiency by ensuring a high level of information security is one of the most important tasks for a modern enterprise in the context of digital transformation and growing cyber threats.

2. Literature review and problem statement

A significant contribution to the development of economic security of an enterprise is obtained in [5]. The information component of enterprise economic security is discussed in detail in [6–8]. Studies related to cyber security as one of the elements of enterprise information security are presented in [9–11].

In the context of the digitalization of the economy, businesses are increasingly experiencing the impact and consequences of cyber threats and incidents. Cyber terrorist attacks aimed at the functioning of payment systems, transportation, energy, and other government electronic platforms can have consequences in the form of unnecessary costs and a decrease in overall performance [12–14].

The main indicators that describe the economic security of an enterprise are determined by the frequency and significance of cyber incidents, the level of protection against cyber threats, and possible losses due to disruption of the normal functioning of the enterprise [15, 16]. Among the performance indicators, the modern literature considers the following: (a) the ratio of detected incidents to the cost of their detection, (b) financial stability, (c) probability of disruption of the enterprise's functioning, (d) digital vulnerability index, and others.

To maintain performance indicators at a given level, risk management technologies can be used, in particular those described in [17].

Research [18] identifies a list of critical factors for ensuring the cyber resilience of an enterprise. The authors propose to use the functionality of the enterprise to assess the level of its vulnerability to cyber threats. In this case, in the absence of cyber incidents, it is considered that the enterprise is normally functioning, and the emergence of a cyber threat reduces the functionality either to the minimum possible level at which the enterprise can still operate or to a complete loss of functionality (Figure 1).

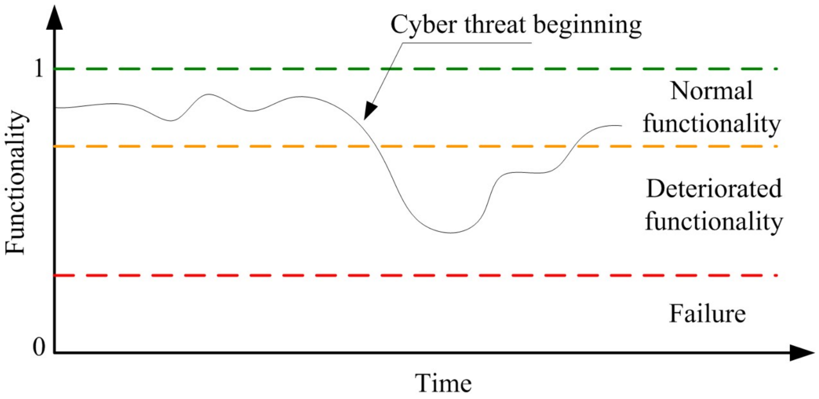


Figure 1: Enterprise resilience based on functionality

The relationship between functionality and enterprise performance indicators is presented in [19]. To simplify the model, this study assumes that normal operation is characterized by one hundred percent functionality. At the same time, the authors focus on the study of cumulative functionality in the form of the area under the curve (AUC) metric and the same normalized metric in relation to the case with no cyber incidents.

The fundamental concepts of enterprise resilience to cyber threats are analyzed in articles [20–22]. The authors of article [20] consider resilience to cyber incidents in three aspects: organizational, operational and cyber aspects. It is noted that resilience is a property that is able to withstand deliberate attacks, accidents or natural threats or incidents, as well as recover from them.

This property fits into the framework of The United Nations' 17 Sustainable Development Goals [21]. The key players in the process of ensuring the cyber resilience of an enterprise are not only the enterprise itself but also governments, individuals, threat actors, cyber security providers, and regulators [22]. At the same time, the authors of [22] identified the main features and consequences of various cyber threats to an enterprise, including viruses, worms, trojans, DDoS attacks, keyloggers, spam, logic bombs, and others. An analysis of possible countermeasures to these threats for enterprises in various industries is provided in [23].

Article [24] discusses the peculiarities of implementing preventive measures to reduce the risks of cyber threats at enterprises in Saudi Arabia. In general, the authors substantiated eleven hypotheses for improving the efficiency of enterprises in the face of cyber threats.

Usually, the moments of cyber threats and incidents are random in nature. Therefore, methods of probability theory, mathematical statistics, machine learning, and deep learning can serve as a classical mathematical tool for their detection and analysis [15, 25, 26]. In addition, the tasks of analyzing traffic in the event of various types of cyber attacks can be considered as tasks of detecting non-stationary trends. Therefore, the methods described in are appropriate [27, 28]. Regarding the peculiarities of restoring the functionality of the enterprise, technologies from related industries can also be applied, for example, those described in [29, 30].

If we consider aviation enterprises of Ukraine, we should note the increased risks of cyber incidents that accompany military operations [31].

Thus, the challenges of today require deepening theoretical knowledge and practical experience in the field of information security and protection against cyber threats in order to ensure the sustainability of the enterprise in the market.

The purpose of the paper is to substantiate the importance of integrating information security measures into the overall system of economic security of an enterprise, to identify current trends in cyber threats and mechanisms for their neutralization, and to develop an integrated approach to building a system of enterprise protection against cyber attacks, taking into account internal and external risks that affect its stability and competitiveness.

3. Materials and methods

In today's world, where the economy and digital technologies are interconnected, cyber security is becoming a key factor in ensuring the stability and reliability of economic systems. The deep integration of information technology into all areas of activity creates new challenges and threats to the economic security of both the state and business. Cyber attacks can cause serious damage, ranging from loss of confidence in business entities to direct financial losses and even destabilization of economic processes.

Economic security guarantees the ability of an enterprise to respond effectively to risks, adapt to changes in the external environment, and minimize losses while maintaining long-term profitability and reputation [5].

In this context, it is necessary to ensure the information security of the enterprise, which is aimed at protecting information and information systems of the enterprise from unauthorized access, cyber attacks, theft, destruction, modification or damage to data. It covers technical, organizational and legal aspects that ensure the confidentiality, integrity and availability of information. The main goal of information security is to ensure the safety of critical data, the smooth operation of systems and the reduction of risks associated with cyber threats [32].

Information security is an integral part of the economic security of the enterprise, its importance is as follows [33–35]:

- Protection of financial and strategic resources, since information security helps to protect financial transactions, trade secrets, intellectual property, which is one of the key assets of the enterprise.

- PROTECTION against cyber attacks makes it possible to reduce the likelihood of costs associated with data recovery, litigation and reputational losses.
- Ensuring business sustainability, the cyber security system allows the company to withstand external and internal threats, ensuring the continuity of operations and business processes.
- Information security increases the trust of partners, customers and investors in the company, which has a positive impact on its competitiveness and economic stability.

The change in society towards computerization and digital transformation has led to a rapidly increasing complexity of information security in both the public and private sectors due to the growing scale and coordination of cyber attacks targeting private or critical information infrastructure. The growing interest of foreign intelligence services in the information space of the country and individual business entities, in turn, increases the risk of using information technologies to undermine the sovereignty, territorial integrity, political, economic and social security of the state and individual business entities. Given the current knowledge of cyber threats, a typical forensic model of cyber attacks can be identified [36].

The main features of cyber attacks include [9]:

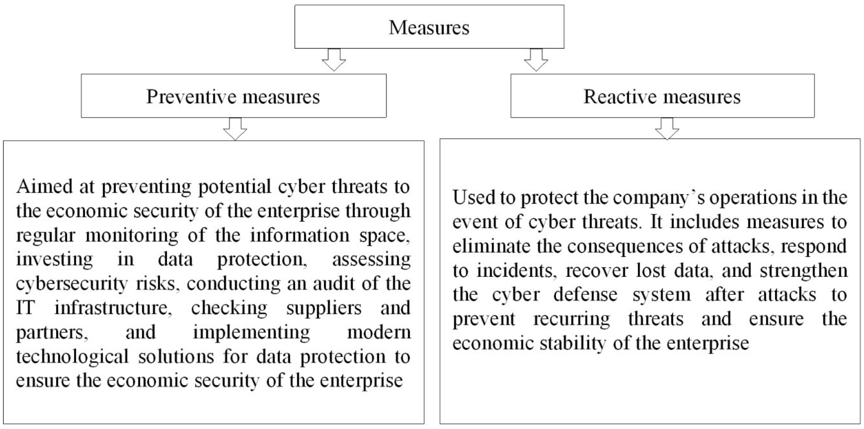
- The lack of personalization, conditional anonymity and decentralized structure of the Internet create significant difficulties in identifying perpetrators.
- The transnational nature of the network allows for long-distance attacks, causing significant financial and reputational damage.

Analyzing the methods of cyber attacks, we note that previously they were mainly understood as such types of attacks as DoS and DDoS, which usually consisted of denial of service and distributed denial of service resulting from sending a large number of false requests to the server, but today cyber criminals have significantly expanded and changed their content and format [10, 37]. Recently, cyber attacks using malware have become the most widespread. Such programs, after penetrating the system, spread independently by injecting their code into existing programs through software vulnerabilities. This allows them to spread rapidly and cause damage to the infrastructure of enterprises. Thus, cyber threats are becoming more complex and large-scale, requiring enterprises to take comprehensive approaches to ensuring information security in the economic security system of the enterprise [38].

Ensuring information security helps to minimize the risks of data leakage, economic losses, reputational damage, and business interruption caused by external and internal threats. An effective cyber security system allows businesses to withstand these challenges, ensuring the sustainability of their operations in the digital economy. The use of digital tools in management allows to find an individual approach to each client, which increases customer satisfaction and loyalty. This approach helps to increase sales and reduce customer losses [39].

Thus, given the digitalization of society, the definition of economic security of an enterprise can be clarified, which should be presented as a holistic set of tools, methods and measures aimed at effective protection of the interests of a business entity from external and internal threats, including threats in the field of information and cyber resources that may cause economic losses. The economic security system should be based on the principle of comprehensiveness, which implies taking into account all possible threats when building a protection system, including cyber threats, and ensuring the interconnection between all means and measures of protection. This approach allows for the creation of a single system that simultaneously ensures the stable functioning of the enterprise, effective risk management, and preservation of economic and digital resilience.

A comprehensive system for protecting the economic security of an enterprise from cyber threats includes preventive and reactive measures, as shown in Figure 2.



Aimed at preventing potential cyber threats to the economic security of the enterprise through regular monitoring of the information space, investing in data protection, assessing cybersecurity risks, conducting an audit of the IT infrastructure, checking suppliers and partners, and implementing modern technological solutions for data protection to ensure the economic security of the enterprise

Used to protect the company's operations in the event of cyber threats. It includes measures to eliminate the consequences of attacks, respond to incidents, recover lost data, and strengthen the cyber defense system after attacks to prevent recurring threats and ensure the economic stability of the enterprise

Figure 2: Measures to form a comprehensive system of economic security protection against cyber threats

The main purpose of such a system is to create conditions for economic sustainability, continuity of business processes and effective response to cyber attacks and other threats, thereby ensuring the long-term development of the enterprise. The specific objects of protection include the key resources of the enterprise: financial, material, information, human resources, as well as digital assets and information infrastructure, which are becoming critically important in the face of growing cyber threats. Particular emphasis is placed on the protection of information and cyber resources, since their compromise can cause significant economic losses and jeopardize the sustainability and development of an enterprise.

The authors proposed a model of an integrated system for the formation of economic security of an enterprise and protection against cyber threats (Figure 3).

This model includes key elements of ensuring the economic sustainability of an enterprise, takes into account current challenges in the field of cyber security and offers an integrated approach to protecting resources, managing risks and countering potential threats. After all, studies show that cyber attacks entail not only direct economic losses in the form of damage to assets and recovery costs, but also indirect losses, such as reduced consumer confidence, loss of market value, and increased borrowing costs. At the same time, investments in cybersecurity measures help to increase the level of technological readiness of the enterprise, stimulate the introduction of innovative solutions and increase market competitiveness. The development of cyber security systems at the enterprise level also contributes to the creation of new jobs in the field of information security, which has a positive impact on its overall economic sustainability and adaptation to modern challenges.

It should be noted that ensuring the sustainability of an enterprise in the digital economy directly depends on the effectiveness of cyber security measures, including both technological solutions and legal, organizational and educational ones. There is a two-way relationship between innovation and sustainable development. On the one hand, economic, social and environmental factors improve as a result of intensified innovation. On the other hand, these changes lead to the accumulation of funds, knowledge, and skills to spread innovation processes in the country [40].

When planning measures to ensure the economic security of an enterprise and its protection from cyber threats, it is first of all necessary to take into account the trends in the emergence of new security threats and mechanisms for their implementation at the present stage of development of information technologies (Figure 4).

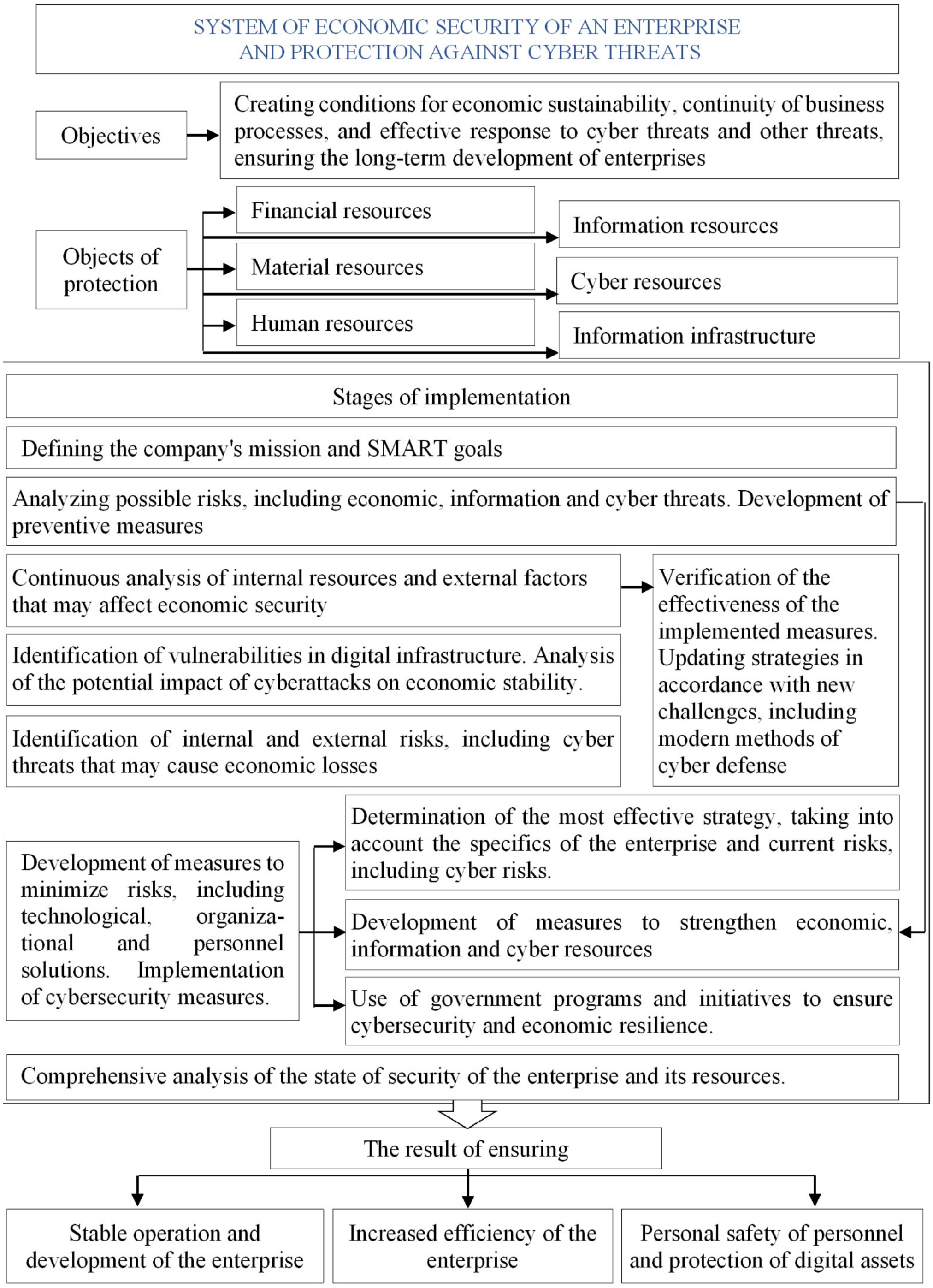
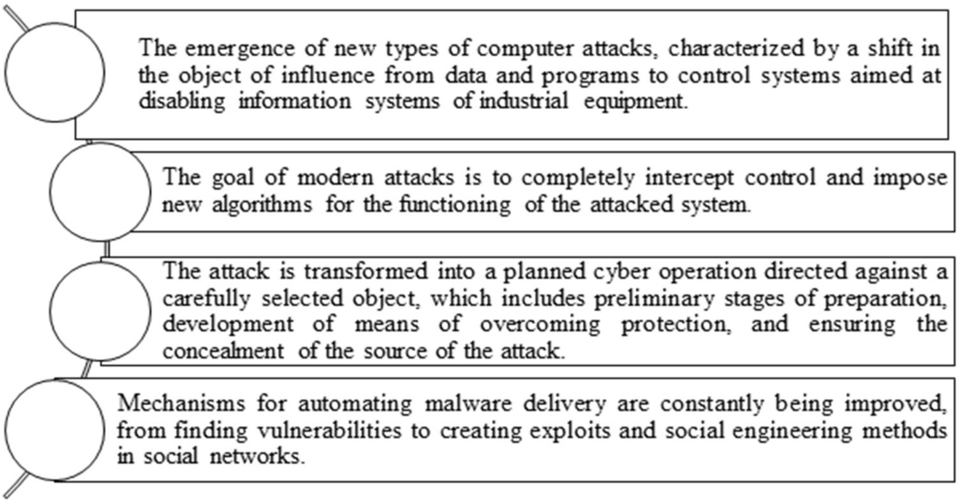

SYSTEM OF ECONOMIC SECURITY OF AN ENTERPRISE AND PROTECTION AGAINST CYBER THREATS
Objectives
Creating conditions for economic sustainability, continuity of business processes, and effective response to cyber threats and other threats, ensuring the long-term development of enterprises
Objects of protection
Financial resources
Material resources
Human resources
Information resources
Cyber resources
Information infrastructure
Stages of implementation
Defining the company's mission and SMART goals
Analyzing possible risks, including economic, information and cyber threats. Development of preventive measures
Continuous analysis of internal resources and external factors that may affect economic security
Identification of vulnerabilities in digital infrastructure. Analysis of the potential impact of cyberattacks on economic stability.
Identification of internal and external risks, including cyber threats that may cause economic losses
Verification of the effectiveness of the implemented measures. Updating strategies in accordance with new challenges, including modern methods of cyber defense
Development of measures to minimize risks, including technological, organizational and personnel solutions. Implementation of cybersecurity measures.
Determination of the most effective strategy, taking into account the specifics of the enterprise and current risks, including cyber risks.
Development of measures to strengthen economic, information and cyber resources
Use of government programs and initiatives to ensure cybersecurity and economic resilience.
Comprehensive analysis of the state of security of the enterprise and its resources.
The result of ensuring
Stable operation and development of the enterprise
Increased efficiency of the enterprise
Personal safety of personnel and protection of digital assets

Figure 3: Integrated system of enterprise economic security and protection against cyber threats

There is a close relationship between information security, corporate governance, compliance with corporate culture and code of conduct, which is related to the human factor. Incorporating information security into corporate governance and culture will help reduce risks, increase security and avoid confidential information leakage.

To create an effective information security system, it is necessary to determine the amount of information to be protected and assess the factors that threaten its confidentiality, including potential and actual risks of illegal use. When developing such a system, a distinction should be made between public information and restricted data, which are divided into confidential, private information and data for internal use.

The formation of an enterprise information security system and protection of economic security from cyber attacks is shown in Figure 5.



The emergence of new types of computer attacks, characterized by a shift in the object of influence from data and programs to control systems aimed at disabling information systems of industrial equipment.

The goal of modern attacks is to completely intercept control and impose new algorithms for the functioning of the attacked system.

The attack is transformed into a planned cyber operation directed against a carefully selected object, which includes preliminary stages of preparation, development of means of overcoming protection, and ensuring the concealment of the source of the attack.

Mechanisms for automating malware delivery are constantly being improved, from finding vulnerabilities to creating exploits and social engineering methods in social networks.

Figure 4: Trends in the emergence of new security threats and mechanisms for their implementation at the current stage of development of information technologies

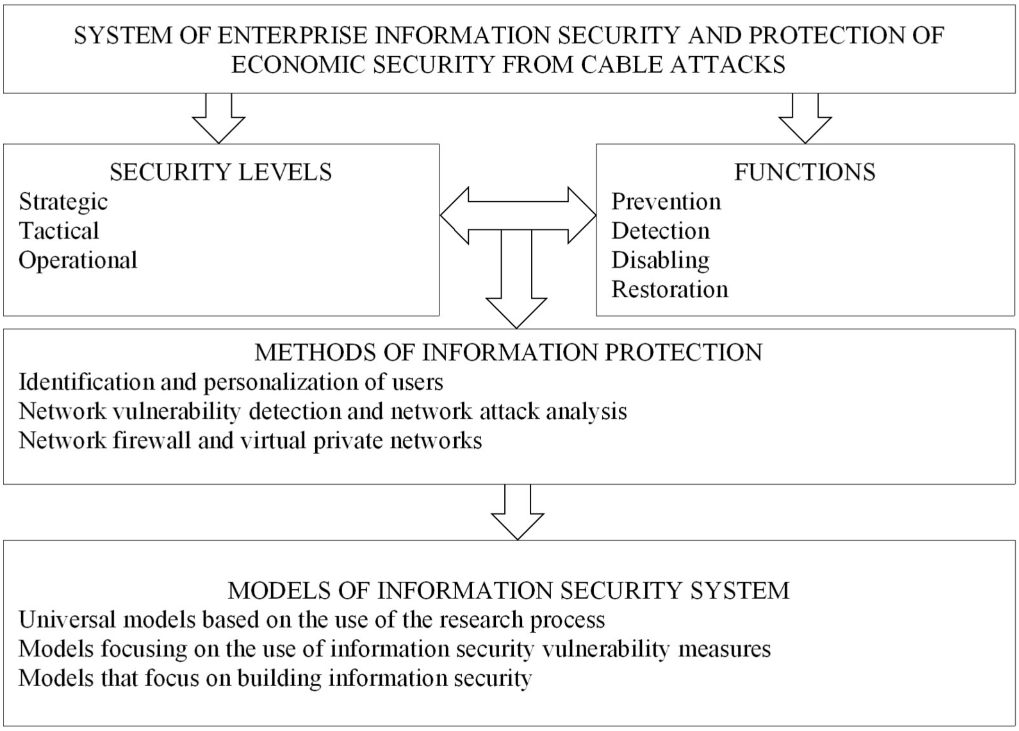

SYSTEM OF ENTERPRISE INFORMATION SECURITY AND PROTECTION OF ECONOMIC SECURITY FROM CABLE ATTACKS
SECURITY LEVELS
Strategic
Tactical
Operational
FUNCTIONS
Prevention
Detection
Disabling
Restoration
METHODS OF INFORMATION PROTECTION
Identification and personalization of users
Network vulnerability detection and network attack analysis
Network firewall and virtual private networks
MODELS OF INFORMATION SECURITY SYSTEM
Universal models based on the use of the research process
Models focusing on the use of information security vulnerability measures
Models that focus on building information security

Figure 5: Enterprise information security system and protection of economic security from cyber attacks

This information security management system combines three levels: strategic, tactical and operational. Strategic management includes the creation of an information security policy, identification and assessment of potential risks and threats to information security. Tactical management involves creating and implementing an information security system in accordance with the developed policy. The operational level is to maintain and monitor the functionality of the information security system. The enterprise under the influence of the external and internal environment, in the context of investment and security aspects, as well as the development of effective measures to prevent the risks of unstable activity [41].

The enterprise information security system should be built with the following functions:

- Prevention: networks must be protected from unauthorized intrusions, usually done with the help of firewalls.
- Detection: the process of identifying attacks carried out via the Internet.
- Disabling: the system should be designed in such a way as to be able to neutralize the attack in case of its detection.
- Recovery: a system of permanent archiving of information or backup of information from which it can be restored in case of full or partial destruction as a result of an attack.

A systematic analysis of cyber attacks taking place in the world practice and the experience of counteracting them allows to systematize the existing models of information security systems at enterprises [37, 42]:

- Universal models based on the use of the research process, that is, methods based on finding answers to questions posed by economic and monitoring systems.
- Models that focus on the use of information security vulnerability measures (Diamond, MITRE ATT and CK, PICERL).
- Models that focus on building information security (Defense in Dept, Cyber Kill Chain, Pyramid of Pain, PICERL, CVSS3).

At the same time, it is worth noting that the creation of an enterprise information security system requires significant financial costs, so the principle of cost-effectiveness should be followed, i.e., the costs incurred should be less than the potential consequences of unauthorized information leakage.

Building an effective information security system requires a clear definition of internal and external factors that can lead to information leakage or loss. In addition, the system should provide a backup mechanism by which information can be restored with minimal losses [43, 44].

4. Results and discussions

Let us consider the task of determining the efficiency of an enterprise in the event of an objective possibility of cyber incidents. For this purpose, the main parameter to be monitored is the functionality of the enterprise $f(t)$, which changes during the observation interval [19]. The range of functionality variation is from 0 to 1.

To determine the quantitative content of efficiency, cumulative functionality can be calculated

$$F(t)=\int_{t_1}^{t} f(t)\,dt, \tag{1}$$

or area under the curve (AUC)

$$AUC=\frac{1}{t_2-t_1}\int_{t_1}^{t_2} f(t)\,dt, \tag{2}$$

where t_1 is the moment of the cyber incident, t_2 is the current moment at which the effectiveness is assessed.

An analysis of the literature has shown that various mathematical models can be used to describe the loss of system functionality, among which the linear and exponential models are common. At the same time, in the case of restoring functionality, identical models can be used, but with different numerical values of the relevant parameters.

Let us consider the dependence of enterprise efficiency in terms of cyber resilience on the parameters of the exponential model of loss and restoration of enterprise functionality. In this case, the model of enterprise functionality will have the following form

$$f(t)=\begin{cases} 1 & \text{if } 0<t\leq t_1 \\ \dfrac{a+e^{-\lambda(t-t_1)}}{a+1} & \text{if } t_1<t\leq \tau_1, \\ \dfrac{a+e^{-\lambda(\tau_1-t_1)}}{a+1} & \text{if } \tau_1<t\leq \tau_2,, \\ \dfrac{a+e^{-\lambda(\tau_1-t_1)}}{a+1}+b(e^{\mu(t-\tau_2)}-1) & \text{if } \tau_2<t\leq \tau_3, \\ \dfrac{a+e^{-\lambda(\tau_1-t_1)}}{a+1}+b(e^{\mu(\tau_3-\tau_2)}-1) & \text{if } \tau_3<t\leq t_2, \end{cases} \tag{3}$$

where τ_1 is the moment of the end of the cyber threat, τ_2 is the moment of the beginning of the restoration of functionality, τ_3 is the moment of the end of the restoration of functionality.

Figure 6 shows an example of implementing the functionality dependency for the model parameters $\lambda = 1.1$, $\mu = 0.4$, $t_1 = 20$, $\tau_1 = 25$, $\tau_2 = 27$, $\tau_3 = 30$, $t_2 = 35$.

According to the presented model, the restoration of functionality after a cyber incident may not reach 100 percent. In this case, it is necessary to raise additional funds to perform corrective actions until full functionality is restored.

The graphs of AUC dependence on the parameters of the model of loss and restoration of enterprise functionality are shown in Figure 7 and Figure 8.

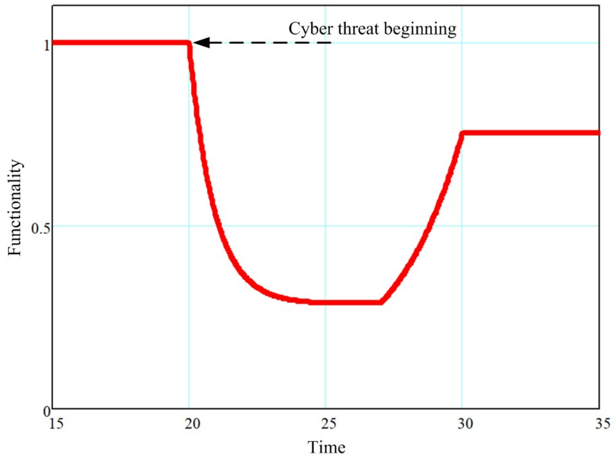


Figure 6: Change in functionality in the event of cyber threats

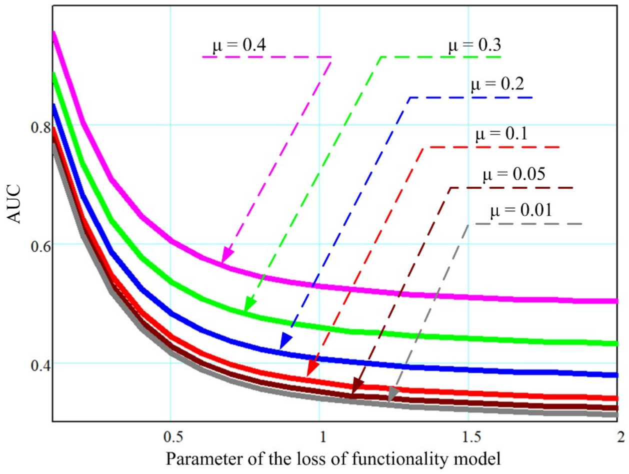


Figure 7: Dependence of AUC on the parameters of the loss of functionality model

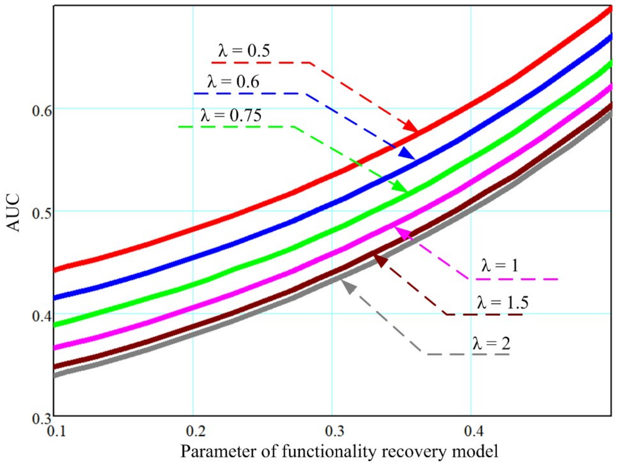


Figure 8: Dependence of AUC on the parameters of the functionality recovery model

Conclusions

Cyber security is an integral part of an enterprise's information security, which is an important part of economic security. The formation of an enterprise's economic security system requires an integrated approach that includes the protection of financial, material, human and information resources. Information security allows an enterprise to ensure business sustainability, protect critical data and prevent financial losses associated with information leaks and cyber attacks.

An effective system of economic security protection against cyber threats should include both preventive and reactive measures. Preventive measures are aimed at preventing potential threats by assessing risks, implementing technological solutions, and monitoring cyber threats. Reactive measures, in turn, involve responding to incidents, eliminating the consequences of attacks and restoring business processes. Building a comprehensive cyber security system minimizes risks and ensures the economic sustainability of the enterprise.

Current trends in cyber threats show an increase in the level of complexity and coordination of attacks, which forces companies to constantly improve their security systems. The main threats are phishing attacks, malware, and exploitation of system vulnerabilities. An important aspect of cyber security is the human factor, as a significant part of information leaks is caused by the actions of employees. Therefore, it is necessary to implement staff awareness programs and a corporate culture of cyber security.

The company's information security system should be built on three levels—strategic, tactical and operational—using modern methods and models of protection. The key functions of such a system include prevention, detection, disabling, and recovery, and investments in cyber security not only help minimize risks but also increase the company's competitiveness, ensuring long-term economic stability in the context of digital transformation.

Prospects for further research in this area lie in the development of innovative cyber security management models that take into account the rapid evolution of threats and the adaptability of criminals in cyberspace. Particular attention should be paid to the integration of artificial intelligence and machine learning to detect, analyze and counteract cyber threats in real time.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] Z. Poberezhna, Comprehensive Assessment of the Airlines' Competitiveness, Economic Annals-XXI 167 (2017) 32–36. doi:10.21003/ea.V167-07

[2] Y. Kostiuk, et al., A System for Assessing the Interdependencies of Information System Agents in Information Security Risk Management using Cognitive Maps, in: 3rd Int. Conf. on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 249–264.

[3] Y. Kostiuk, et al., Models and Algorithms for Analyzing Information Risks during the Security Audit of Personal Data Information System, in: 3rd Int. Conf. on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 155–171.

[4] Y. Kostiuk, et al., Effectiveness of Information Security Control using Audit Logs, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3991, 2025, 524-538.

[5] V. Zaichenko, S. Kovalenko, Economic Security of the Enterprise: Essence and Main Features, Bulliten ofKhNUMH 23 (2013) 410–414.

[6] V. Ivanova, Information Security as a Subsystem in the Economic Security System of an Enterprise, Bulliten of KhNUMH 1 (2013) 67–71.

[7] V. Hnatenko, Information and Economic Security as a Factor of Stable Development of the State, Public Manag. 25(5) (2020) 63–74. doi:10.32689/2617-2224-2020-5(25)-63-74

[8] L. Zhao, X. Wu, J. Li, H. Tong, Economics of cybersecurity Investment and Information Sharing: Firm Decision Making under Policy Constraints, Systems 13 (2025). DOI:10.3390/SYSTEMS13020083

[9] M. Kianpour, S. J. Kowalski, H. Overby, Systematically Understanding Cybersecurity Economics: A Survey, Sustainability 13 (2021). doi:10.3390/su132413677

[10] R. von Solms, J. van Niekerk, From Information Security to Cyber Security, Comput. Secur. 38 (2013) 97–102. doi:10.1016/j.cose.2013.04.004

[11] M. Ezhei, B. T. Ladani, Interdependency Analysis in Security Investment against Strategic Attacks, Inf. Syst. Frontiers 22 (2020) 187–201. doi:10.1007/s10796-018-9845-8

[12] Z. Hu, Y. Khokhlachova, V. Sydorenko, I. Opirskyy, Method for Optimization of Information Security Systems Behavior under Conditions of Influences, Int. J. Intell. Syst. Appl. 9 (2017) 46–58. doi:10.5815/ijisa.2017.12.05

[13] J. Al-Azzeh, et al., Analysis of Selfsimilar Traffic Models in Computer Networks. International Review on Modelling and Simulations, Int. J. Comput. Netw. Inf. Secur. 10 (2017) 328–336. doi:10.15866/iremos.v10i5.12009

[14] S. Obushnyi, et al., Ensuring Data Security in the Peer-to-Peer Economic System of the DAO, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3187 (2021) 284–292.

[15] P. R. J. Trim, Y.-I. Lee, Managing Cybersecurity Threats and Increasing Organizational Resilience, Big Data and Cognitive Computing 7 (2023). doi:10.3390/bdcc7040177

[16] A. Evans, Managing Cyber Risk, Routledge, London, 2019.

[17] G. Tonn, J. P. Kesan, L. Zhang, J. Czajkowski, Cyber Risk and Insurance for Transportation Infrastructure, Transport Policy 79 (2019) 103–114. doi:10.1016/j.tranpol.2019.04.019

[18] D. J. Bodeau, R. D. Graubart, R. M. McQuaid, J. Woodill, Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring. Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods, Bedford, UK, 2018.

[19] M. J. Weisman, A. Kott, J. E. Ellis, B. J. Murphy, T. W. Parker, S. Smith, J. Vandekerckhove, Quantitative Measurement of Cyber Resilience: Modeling and Experimentation (2024). https://arxiv.org/pdf/2303.16307

[20] M. S. d. Araujo, B. A. S. Machado, F. U. Passos, Resilience in the Context of Cyber Security: Areviewof the Fundamental Concepts and Relevance, Appl. Sci. 14 (2024). doi:10.3390/app14052116

[21] G. Dede, A. M. Petsa, S. Kavalaris, E. Serrelis, S. Evangelatos, I. Oikonomidis, T. Kamalakis, Cybersecurity as a Contributor Toward Resilient Internet of Things (Iot) Infrastructure and Sustainable Economic Growth, Information 15 (2024). doi:10.3390/info15120798

[22] B. Gandazyeli, Cyber resilience in digital marketing within the framework of sustainable management, Sustainability 17 (2025). doi:10.3390/su17052080

[23] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, D. A. Alabbad, Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations, Sensors 23 (2023). doi:10.3390/s23156666

[24] S. A. Al-Somali, R. R. Saqr, A. M. Asiri, N. A. Al-Somali, Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture, Sustainability 16 (2024). doi:10.3390/su16051880

[25] I. Ostroumov, N. Kuzmenko, Accuracy Estimation of Alternative Positioning in Navigation, in: 2016 4th Int. Conf. on Methods and Systems of Navigation and Motion Control (MSNMC), 2016, pp. 291–294. doi:10.1109/MSNMC.2016.7783164

[26] G. Bonaccorso, Machine Learning Algorithms, Packt Publishing, Birmingham, 2018.

[27] M. Zaliskyi, O. Solomentsev, O. Kozhokhina, T. Herasymenko, Reliability Parameters Estimation for Radioelectronic Equipment in Case of Change-Point, in: 2017 Signal Processing Symposium (SPSympo), 2017, pp. 1–4. doi:10.1109/SPS.2017.8053676

[28] O. Sushchenko, et al., Algorithm of Determining Errors of Gimballed Inertial Navigation System, in: Computational Science and Its Applications—ICCSA 2024 Workshops. Lecture Notes in Computer Science, 14816, 2024, 206–218. doi:10.1007/978-3-031-65223-3_14

[29] O. Solomentsev, V. Melkumyan, M. Zaliskyi, M. Asanov, UAV Operation System Designing, in: 2015 IEEE International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), 2015, 95–98. doi:10.1109/APUAVD.2015.7346570

[30] M. Zaliskyi, et al., Methodology for Substantiating the Infrastructure of Aviation Radio Equipment Repair Centers, in: Computational Methods in Systems Engineering, 3732, 2024, 136–148.

[31] I. Ostroumov, V. Ivannikova, N. Kuzmenko, M. Zaliskyi, Impact Analysis of Russian-Ukrainian War on Airspace, J. Air Transport Manag. 124 (2025). doi:10.1016/j.jairtraman.2025.102742

[32] E. Calefariu Giol, O. Panazan, C. Gheorghe, Cyber, Geopolitical, and Financial Risks in Rare Earth Markets: Drivers of Market Volatility, Risks 13 (2025). doi:10.3390/risks13030046

[33] M. F. Safitra, M. Lubis, H. Fakhrurroja, Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity, Sustainability 15 (2023). doi:10.3390/su151813369

[34] Verizon, Data Breach Investigations Report 2020; Technical Report, 2021. https://www.verizon.com/business/en-gb/resources/reports/2020-data-breach-investigations-report.pdf

[35] S. Krishna, Paryati, Advancing Cyber Resilience for Autonomous Systems with Novel AI-based Intrusion Prevention Model, Int. J. Data Inform. Intell. Comput. 3 (2024) 1–7. doi:10.59461/ijdiic.v3i3.121

[36] M. Jouini, L. B. A. Rabai, A. B. Aissa, Classification of Security Threats in Information Systems, Procedia Computer Science 32 (2014) 489–496. doi:10.1016/j.procs.2014.05.452

[37] T. Kayworth, D. Whitten, Effective Information Security Requires a Balance of Social and Technology Factors, MIS Quarterly Executive 9 (2010). doi:10.3390/su151813369

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

[39] S. Smerichevskyi, Z. Poberezhna, I. Kryvovyazyuk, L. Ivanenko, D. Malnov, Formation of Principles of a Customer-oriented Approach by Transport Enterprises in Conditions of Sustainable Development, in: E3S Web Conference. Innovations in Construction and Smart

Building Technologies for Comfortable, Energy Efficient and Sustainable Lifestyle (ICSBT 2024), 534, 2024, 01022. doi:10.1051/e3sconf/202453401022

[40] S. Smerichevska, Z. Poberezhna, O. Mykhalchenko, Y. Shtyk, Y. Pokanevych, Modeling and Evaluation of Organizational and Economic Support for Sustainable Development of Transport Enterprises: Innovative and Ecological Aspects, Financial and Credit Activity: Problems of Theory and Practice 4 (2023) 218–229. doi:10.55643/fcaptp.4.51.2023.4121

[41] O. Arefieva, S. Piletska, V. Khaustova, Z. Poberezhna, D. Zyz, Monitoring the Economic Stability of the Company's Business Processes as a Prerequisite for Sustainable Development: Investment and Security Aspects, IOP Conf. Series: Earth and Environmental Science 628 (2021) 012042.

[42] E. Nosova, L. Anisimova, T. Murovana, Y. Sviatiuk, O. Iafinovych, Information Security System in Provision of the Economic Security and Risk Management of the Enterprise, in: Cybersecurity Providing in Information and Telecommunication Systems, 3188, 2022, 21–31.

[43] C. Vishik, F. Sheldon, D. Ott, Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment, Springer Fachmedien Wiesbaden, Wiesbaden, 2013, 133–147. doi:10.1007/978-3-658-03371-2.12

[44] Cybintsolutions, 15 Alarming Cyber Security Facts and Stats, 2020. https://www.cybintsolutions.com/cybersecurity-facts-stats/