



Cyber resilience of enterprises as a component of their crisis management

*Dmutry Levkin,
Yana Kotko,
Artur Levkin,
Volodymyr Syry*

In today's context of digital economic transformation, business operations are increasingly dependent on information systems, digital platforms, cloud services, and automated business processes. On the one hand, this dependence enhances management efficiency and competitiveness; on the other, it creates new risks associated with cyber threats, data breaches, disruptions to operational continuity, and reputational damage. The growing number and complexity of cyberattacks, particularly in the context of military and hybrid threats, underscores the need to rethink approaches to ensuring the economic security of enterprises. Traditional information security systems, which focus primarily on preventing unauthorized access to data, no longer fully address today's challenges. Today, enterprises need to develop a comprehensive cyber resilience system that not only provides protection against cyberattacks but also enables rapid adaptation, minimizes the impact of incidents, ensures business continuity, and enables a swift return to normal operations following a crisis. Thus, cyber resilience is becoming an integral component of a company's crisis management.

The challenge of developing an effective cyber resilience model is closely linked to important scientific and practical tasks, specifically: improving cyber risk management mechanisms, integrating information security systems into the overall strate-

gic and crisis management framework, developing methodologies for assessing an enterprise's level of cyber resilience, and fostering an organizational culture of secure behavior among staff. Addressing these challenges will help increase business resilience to crises, ensure economic security, and strengthen the trust of partners and customers in the digital environment.

The issue of ensuring cybersecurity and cyber resilience for enterprises has attracted significant attention from both the academic community and business management practitioners. In recent years, a number of studies have been published covering various aspects of this phenomenon: cyber risk management models, technical and organizational mechanisms for protecting information assets, risk assessment methods, security standards, and incident response practices. Thus, domestic and foreign researchers are investigating the integration of cybersecurity into the overall corporate governance system. The works [1, 2] are devoted to the challenges of developing IT architecture that takes security requirements into account, emphasizing the importance of building adaptive information systems capable of withstanding external and internal threats. Research in the field of cyber risk management, particularly the works [2, 3], is based on the development of procedures and policies that allow for the identification, assessment, and mini-

mization of the impact of cyber threats on business processes. A separate group of scientific works [3, 4] is related to the assessment of enterprises' cybersecurity levels. Various approaches to developing cyber resilience indicators, threat analysis, and evaluation metrics have been proposed; in particular, the authors of [5, 6] provide a comprehensive analysis of the practical aspects of implementing information cybersecurity management systems, however, these articles partially reveal limitations in the context of ensuring business continuity during crises.

Nowever, despite the significant contribution of these scientific and practical developments, there are still substantial gaps in contemporary publications regarding the consideration of cyber resilience as an integral component of enterprise crisis management: insufficient integration of approaches to cyber resilience with crisis management mechanisms (a significant portion of research focuses on the technical aspects of IT infrastructure protection, but this does not fully address the issue of adapting business processes under crisis conditions); the absence of universal methodologies for assessing cyber resilience specifically in the context of ensuring enterprise stability during crises (existing risk assessments do not always account for the complex interplay between technological, organizational, and strategic risks); limited attention to the organizational and managerial aspects of staff behavior in stressful cyber situations (many studies analyze the human factor from the perspective of error prevention, but do not address the issue of team behavior during crisis incidents); insufficient fundamental analysis of the impact of geopolitical risks on enterprises' cyber resilience (this is particularly relevant for countries facing heightened external threats, where cybersecurity is not merely a business issue but also a component of national security). Thus, current research provides a foundation for understanding the principles of cybersecurity, but requires further devel-

opment toward the creation of comprehensive cyber resilience models that integrate technical, organizational, and strategic mechanisms within the framework of crisis management. This opens up prospects for further research aimed at developing integrated approaches and practical recommendations for strengthening enterprises' resilience to modern digital challenges.

The objective of this study is to provide a theoretical rationale and develop scientific and practical recommendations for establishing a system of cyber resilience for enterprises as a component of crisis management, with the aim of ensuring business continuity, minimizing cyber risks, and enhancing overall economic security. To achieve this goal, the following tasks are to be addressed: to elucidate the economic essence of the concept of «enterprise cyber resilience» and define its place within the crisis management system; to analyze contemporary approaches to cyber risk management and determine their role in ensuring an enterprise's resilience to crises; to investigate the relationship between the level of digitalization of business and the growth of cyber threats; identify the main factors shaping an enterprise's cyber resilience (technical, organizational, managerial, and human resources); develop methodological approaches for assessing an enterprise's level of cyber resilience in crisis situations; and propose practical recommendations for integrating cyber defense mechanisms into the enterprise's crisis management system. The implementation of these tasks will enable the formation of a comprehensive vision of cyber resilience as a strategic element of enterprise management, ensuring its adaptability, competitiveness, and operational stability in the face of digital and crisis challenges.

In today's environment of digital economic transformation, business operations increasingly depend on the use of information and communication technologies, digital platforms, automated management systems, and cloud services. The digitization of business processes contributes to improved

management efficiency, the optimization of production and logistics operations, and expanded opportunities for communication with customers and partners. At the same time, businesses are becoming increasingly dependent on information infrastructure, making them more vulnerable to cyber threats. Under such conditions, cyberattacks, leaks of confidential information, disruptions to information systems, or the blocking of digital services can lead to significant financial losses, reputational risks, and a decline in competitiveness. Increasing instability in the external environment, globalization processes, and the rise in the number of sophisticated and targeted cyberattacks necessitate the development of new approaches to ensuring the security and resilience of businesses in the digital environment.

In this context, the concept of «enterprise cyber resilience» takes on particular relevance; it is viewed as a comprehensive

measure of an organization's ability to function effectively in the face of cyber threats and digital risks. Unlike the traditional approach to information security, which is primarily focused on protecting information resources from unauthorized access, loss, or damage, the concept of cyber resilience has a broader scope. It involves the integration of technological, organizational, and managerial mechanisms aimed not only at preventing incidents but also at ensuring the continuity of business processes, mitigating the negative consequences of cyberattacks, and enabling the system to quickly restore its functionality following crisis situations. An important element of cyber resilience is the establishment of a risk management system that allows for the identification of vulnerabilities in the information infrastructure, the forecasting of possible cyber threat scenarios, and the development of preventive measures to neutralize them (Table 1).

Table 1

Key components of an enterprise's cybersecurity resilience and their characteristics

Components of cybersecurity	Component overview	Practical benefits for the company
Timely detection of potential cyber threats	Involves continuous monitoring of the information infrastructure, the use of intrusion detection systems, cyber risk analysis, and the forecasting of potential cyberattack scenarios. Includes the identification of vulnerabilities in software, network systems, and digital services.	Enables the company to prevent critical cyber incidents, reduce the likelihood of unauthorized access to data, and ensure the stable operation of information systems.
Effective response to cyber incidents	It encompasses a system of procedures and algorithms for rapid response to cyberattacks, including incident containment, threat neutralization, system restoration, and analysis of the causes of incidents. It involves coordination of actions between IT departments, security services, and company management.	Minimizes the negative consequences of cyberattacks, reduces the duration of information system downtime, and helps preserve critical data.
Adaptation of organizational and technological processes	It provides for flexible business processes, the modernization of information infrastructure, the implementation of new security technologies, and the improvement of internal cybersecurity policies. It includes the integration of cybersecurity into the strategic and crisis management system.	It enhances the company's ability to quickly adapt to new digital challenges, maintain business process continuity, and ensure operational stability in an unstable environment.

Minimization of financial, informational, and reputational losses	It involves the implementation of a set of preventive and recovery measures aimed at minimizing financial losses, preventing the leakage of confidential information, and maintaining the company's business reputation. It includes data backup, cyber risk insurance, and a crisis communication policy.	It helps maintain the company's financial stability, builds trust among customers and partners, and ensures the business's long-term competitiveness.
---	--	---

Thus, an enterprise's cyber resilience is characterized by its ability to promptly identify potential threats, effectively respond to cyber incidents, adapt organizational and technological processes to changes in the external environment, and minimize economic, informational, and reputational losses. For a more thorough analysis of an enterprise's

cyber resilience, it is advisable to detail potential cyber threats that could impact the functioning of information infrastructure and business processes. Systematizing such threats allows enterprises to identify risks in a timely manner, assess their potential consequences, and develop effective response measures (Table 2).

Table 2

Major potential cyber threats to business operations

Type of threat	Threat description	Potential consequences for the company
Unauthorized access to information systems	Unauthorized access to a company's information resources by third parties through the exploitation of software vulnerabilities, password cracking, or the theft of login credentials	Leakage of confidential information, data integrity breaches, financial losses, and reputational risks
Malware (viruses, trojans, ransomware)	The use of specially designed programs intended to damage information systems, steal data, or block access to them	Disruption of information systems, data loss, and the need for financial expenditures to restore systems
Phishing attacks	Use of fake emails, websites, or messages to obtain users' confidential data	Theft of login credentials, access to the company's internal systems, compromise of corporate information
Attacks on network infrastructure	Massive attacks on the company's servers or network resources, leading to system overload and the inability of systems to function normally	Temporary or complete unavailability of information services, disruption of online services and business processes
Internal threats (human factor)	Unintentional or intentional actions by company employees that may lead to information leaks or disruptions in the operation of information systems	Data loss or corruption, leakage of commercial information, disruption of internal management processes
Compromise of cloud services	Exploitation of vulnerabilities in cloud platforms or improper configuration of data access	Unauthorized access to corporate data, breach of information confidentiality
Social engineering	Psychological manipulation of company employees to obtain confidential information or access to information systems	Disclosure of confidential data to third parties, compromise of accounts and corporate resources
Cyber espionage	Targeted acquisition of strategic information about the company's operations by competitors or other interested parties	Loss of competitive advantages, disclosure of commercial and technological information

Systematizing potential cyber threats enables organizations to develop more effective cybersecurity strategies and identify priority areas for enhancing cyber resilience. Analysis of these threats is a crucial prerequisite for developing a comprehensive cyber risk management system that includes preventive measures, incident response mechanisms, and tools for restoring the operation of information systems [7, 8].

Modern approaches to cyber risk management are based on integrating information security principles with mechanisms for strategic and crisis management of the enterprise. This approach involves a systematic combination of technical information protection measures, organizational procedures, security policies, and management decisions aimed at ensuring the stability of the enterprise's operations in the face of digital threats. Within the framework of crisis management, cyber resilience serves as a vital tool for ensuring business continuity, as it enables the enterprise to respond promptly to crisis situations involving breaches of information systems and minimize the negative impact on core business processes.

The development of an organization's cyber resilience depends on a range of interrelated factors, including:

- *technological factors* — the level of security of the information infrastructure, the use of modern cyber security measures, and systems for monitoring and responding to incidents;
- *organizational factors* encompass the development of internal information security policies, cyber threat response protocols, and internal control systems;
- *management factors* relate to the integration of cybersecurity into the company's strategic planning, the establishment of a cyber risk management system, and the adoption of effective management decisions in crisis situations;
- *human resources factors* involve improving staff digital literacy, fostering a cybersecurity culture, and training

specialists capable of effectively responding to modern cyber threats.

In today's environment of economic digitalization and the growing number of cyber threats, it is crucial to develop effective methodological approaches for assessing the level of cyber resilience in enterprises. Such an assessment allows for a comprehensive evaluation of an enterprise's ability to withstand cyber threats, respond promptly to cyber incidents, and ensure the continuity of business processes [9, 10]. The scientific rationale for a cyber resilience assessment system involves the use of a set of quantitative and qualitative indicators that characterize the state of the information infrastructure, the effectiveness of cyber risk management, the level of organizational support for cybersecurity, and the enterprise's readiness to resume operations following crisis situations.

Within this approach, the assessment of cyber resilience should be based on a comprehensive analysis of several interrelated components:

- *first*, it is important to consider the level of security of the enterprise's information infrastructure, which includes the availability of modern technical cyber defense tools, network traffic monitoring systems, threat detection software, and data backup mechanisms;
- *second*, it is necessary to assess the effectiveness of the cyber risk management system, which involves identifying potential threats, analyzing vulnerabilities in information systems, and developing preventive measures to neutralize them;
- *third*, an important aspect is the functioning of organizational mechanisms for responding to cyber incidents, covering internal security regulations, protocols for staff actions in the event of threats, and an internal control system;
- *fourth*, it is necessary to consider the enterprise's ability to ensure business continuity, which involves having plans for restoring information systems, backing up critical data, and establishing alternative channels for business processes.

For a more systematic approach to assessing an organization's level of cyber resilience, it is advisable to use a set of relevant indicators that reflect key aspects of the cybersecurity system's operation (Table 3).

Table 3

Key indicators for assessing an organization's level of cyber resilience

Assessment area	Key indicators	Description of indicators
State of the information infrastructure	level of network system security; presence of intrusion detection systems; frequency of software updates	Reflects the level of technical protection of the company's information resources and its ability to counter modern cyber threats
Cyber risk management	availability of a risk identification system; regularity of security audits; vulnerability assessments	Characterizes the effectiveness of processes for analyzing and minimizing cyber risks in the company's operations
Organizational cybersecurity measures	availability of internal security policies; level of staff training; functioning of the information security service	Determines the company's organizational readiness to counter cyber threats
Business continuity planning	availability of incident response plans; data backup; speed of system recovery	Reflects the company's ability to minimize losses and quickly resume operations following cyber incidents

Another key component in developing a cyber resilience assessment system is identifying the key stages of the assessment, which helps structure the analysis process and ensure its systematic nature (Table 4).

Table 4

Stages of a company's cyber resilience assessment

Stage	Stage overview	Expected outcome
Identification of cyber threats	Analysis of potential external and internal cyber threats; identification of vulnerabilities in information systems	Compilation of a list of potential risks
Assessment of security posture	Analysis of technical, organizational, and managerial cyber security mechanisms	Assessment of the company's cybersecurity level
Analysis of response effectiveness	Assessment of the organization's ability to respond to cyber incidents and resume operations	Identification of weaknesses in the response system
Development of management decisions	Development of recommendations for enhancing the organization's cyber resilience	Improvement of the cybersecurity and risk management system

The implementation of a comprehensive system for assessing the cyber resilience of enterprises makes it possible to identify critical vulnerabilities in information infrastructure in a timely manner, evaluate the effectiveness of the cybersecurity system, and make informed management decisions regarding its improvement. This approach contributes to enhancing the enterprise's

economic security, as it ensures more effective management of cyber risks and creates the conditions for the stable operation of business processes.

The practical implementation of the proposed methodological approaches will contribute to the formation of a comprehensive enterprise crisis management system capable of ensuring its resilience to

modern digital challenges. In the long term, this will enhance the competitiveness of enterprises, strengthen the trust of customers and partners, and ensure stable business development amid growing technological risks and global economic instability.

The study found that an enterprise's cyber resilience is a critical component of crisis management systems in the context of economic digitalization and the rise of cyber threats. Modern enterprises are increasingly dependent on information systems, digital platforms, and network technologies, which increases their vulnerability to cyber incidents. In this regard, ensuring an adequate level of cyber resilience has become a prerequisite for the continuity of business processes, the preservation of information resources, and the maintenance of enterprise competitiveness. The essence of the concept of enterprise cyber resilience is substantiated, and its key characteristics are identified, including the ability to detect cyber threats in a timely manner, respond effectively to incidents, restore the operation of information systems, and adapt management and technological processes to changes in the digital environment. It is demonstrated that building cyber resilience requires a comprehensive approach that combines organizational, technological, and managerial measures aimed at reducing cyber risks and minimizing economic, informational, and reputational losses.

Particular attention has been paid to developing methodological approaches for assessing an enterprise's cyber resilience, which involve analyzing cyber threats, evaluating the level of protection of the information infrastructure, determining the effectiveness of responses to cyber incidents, and formulating management decisions to enhance cybersecurity. The proposed approach allows for a systematic assessment of an enterprise's cyber defense status, the identification of vulnerabilities in the functioning of information systems, and the development of effective measures to address them. Thus, the implementation

of a comprehensive cyber resilience management system will contribute to enhancing the economic security of enterprises, strengthening their ability to withstand modern digital challenges, and ensuring stable operation amid growing cyber risks. Prospects for further research include the development of practical tools for monitoring cyber risks, improving methods for assessing cyber resilience, and integrating cybersecurity systems into the overall system of strategic and crisis management of enterprises.

Literature

1. *Zavrazhnyi K., Kulyk A.* Modern business cybersecurity challenges and the role of artificial intelligence in countering threats // *Економічний вісник НТУУ «Київ. політехн. ін.-т»*. 2024. № 30. С. 81–86. DOI: <https://doi.org/10.20535/2307-5651.30.2024.313042>
2. *Мазулевський О.Є., Жолобович Н.В.* Оцінка поточного стану кіберстійкості з урахуванням ситуації у кіберпросторі // *Сучасні інформаційні технології у сфері безпеки та оборони*. 2024. Т. 51. № 3. С. 34–40. DOI: <https://doi.org/10.33099/2311-7249/2024-51-3-34-40>
3. *Сироватченко М.* Правові аспекти забезпечення кібербезпеки в Україні: сучасні виклики та роль національного законодавства. // *Вісник НУ «Львівська політехніка»*. Сер.: Юрид. науки. 2024. № 1(41). С. 314–320. DOI: <http://doi.org/10.23939/law2024.41.314>
4. *Красніков С.А.* Розвиток національної системи кібербезпеки України. // *Інформація і право*. 2025. № 4(55). С. 191–198. DOI: [https://doi.org/10.37750/2616-6798.2025.4\(55\).346414](https://doi.org/10.37750/2616-6798.2025.4(55).346414)
5. *Гайдук О., Зверев В.* Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій // *Кібербезпека: освіта, наука, техніка*. 2024. Т. 3. № 23. С. 225–236. DOI: <https://doi.org/10.28925/2663-4023.2024.23.225236>

6. Летичевський О.О. Сучасні наукові проблеми кібербезпеки // Вісник Нац. акад. наук України. 2023. № 2. С. 12–20. DOI: <https://doi.org/10.15407/visn2023.02.012>

7. Levkin D., Kotko Ya., Levkin A. Software security in times of cyber threats // Матеріали VI Міжнар. наук.-практ. конф. «Механізми забезпечення сталого розвитку економіки: проблеми, перспективи, міжнародний досвід». (Харків, 10 жовт. 2025 р.). Харків : ДБТУ, 2025. С. 445–447.

8. Kavun S., Levkina R., Kotko Y., Levkin D., Levkin A. Information Security in Project Management for the Financial and Budgetary Capacity of the National Economy. // CEUR Workshop Proceedings. 2023. No. 3550. P. 246–254. URL: <https://ceur-ws.org/Vol-3550/short9.pdf>

9. Левкін А.В., Котко Я.М., Левкіна Р.В. Кібербезпека, як фактор підвищення ефективності підприємницької діяльності у АПВ. // Матеріали Міжнар. наук.-практ. конф. «Електроенергетика, електромеханіка та технології в АПК». (Харків, 22.12.2022). Харків : ДБТУ, 2022. С. 182–183.

10. Levkin D.A., Zhernovnykova O.A., Synyavina Yu.V., Levkin A.V. Variability of the choice of the mathematical models in applied security problems // Вчені записки ТНУ ім. В.І. Вернадського. Сер.: Технічні науки. 2023. Т. 34(73). № 5. С. 149–153. DOI: <https://doi.org/10.32782/2663-5941/2023.5/24>

Надійшла до редколегії 17.04.2026

Рекомендовано до друку 21.05.2026

Опубліковано 29.05.2026

Відомості про авторів:

Левкін Дмитро Артурович — кандидат технічних наук, доцент, доцент кафедри фізики та математики; Державний біотехнологічний університет; Харків, Україна; email: dimalevkin23@gmail.com; ORCID: <https://orcid.org/0000-0002-1980-4426>;

Котко Яна Миколаївна — кандидат економічних наук, доцент, старший викладач кафедри економіки та бізнесу; Державний біотехнологічний університет; Харків, Україна; email: kotkoyana@ukr.net; ORCID: <https://orcid.org/0000-0001-6611-8130>

Левкін Артур Володимирович — кандидат технічних наук, доцент, доцент кафедри інформаційних технологій, кібернетики та захисту інформації; Державний біотехнологічний університет; Харків, Україна; email: artur.lav@btu.kharkov.ua; ORCID: <https://orcid.org/0000-0001-5021-5366>;

Сирий Володимир Миколайович — старший викладач кафедри інформаційних технологій, кібернетики та захисту інформації; Державний біотехнологічний університет; Харків, Україна; email: syryvn@gmail.com; ORCID: <http://orcid.org/0000-0002-1060-1710>

Левкін Д., Котко Я., Левкін А., Сирий В. Кіберстійкість підприємств як складова їх антикризового управління.

Досліджено теоретичні та прикладні аспекти формування кіберстійкості підприємств як складової системи антикризового управління. Обґрунтовано актуальність проблеми в умовах активної цифровізації економіки, зростання кількості кіберзагроз, а також посилення нестабільності зовнішнього середовища, що змушує підприємства шукати нові підходи до забезпечення безперервності своєї діяльності. Визначено економічну сутність поняття «кіберстійкість підприємства» та розкрито її відмінність від традиційного трактування інформаційної безпеки. Доведено, що кіберстійкість передбачає не лише захист інформаційних ресурсів і технологічної інфраструктури, але і здатність підприємства своєчасно ідентифікувати потенційні загрози, адаптувати бізнес-процеси до кризових умов, мінімізувати можливі втрати та оперативно відновлювати функціонування після виникнення кіберінцидентів.

Проаналізовано сучасні підходи до управління кіберризиками та інтеграції механізмів кіберзахисту у систему стратегічного і антикризового управління підприємством. Визначено ключові чинники формування кіберстійкості, серед яких: технологічні, організаційні, управлінські та кадрові

складові. Обґрунтовано, що ефективне забезпечення кіберстійкості потребує комплексного підходу, який передбачає поєднання сучасних технічних засобів захисту, ефективних управлінських рішень і розвитку внутрішньої культури кібербезпеки. Запропоновано напрямки удосконалення системи оцінювання рівня кіберстійкості підприємства та окреслено практичні рекомендації щодо підвищення здатності бізнесу протистояти сучасним цифровим викликам. Отримані результати можуть бути використані для вдосконалення механізмів забезпечення економічної безпеки підприємств і підвищення їх конкурентоспроможності в умовах цифрової економіки та слугувати методичною основою для подальших наукових розробок у сфері інформаційної та економічної безпеки підприємств.

Ключові слова: кіберстійкість; антикризове управління; кібербезпека; кіберризики; бізнес.

Levkin D., Kotko Ya., Levkin A., Syry V. Cyber resilience of enterprises as a component of their crisis management.

This article examines the theoretical and practical aspects of building cyber resilience in enterprises as a component of crisis management systems. It substantiates the relevance of this issue in the context of the ongoing digitalization of the economy, the growing number of cyber threats, and increasing instability in the external environment, which compels enterprises to seek new approaches to ensuring business continuity. The economic essence of the concept of «enterprise cyber resilience» is defined, and its distinction from the traditional interpretation of information security is revealed. It is demonstrated that cyber resilience entails not only the protection of information resources and technological infrastructure but also an enterprise's ability to promptly identify potential threats, adapt business processes to crisis conditions, minimize potential losses, and rapidly restore operations following cyber incidents.

The authors analyze modern approaches to cyber risk management and the integration of cyber defense mechanisms into the system of strategic and crisis management of an enterprise. Key factors in the formation of cyber resilience are identified, including technological, organizational, managerial, and human resource components. It has been demonstrated that effectively ensuring cyber resilience requires a comprehensive approach that combines modern technical protection measures, effective management decisions, and the development of an internal cybersecurity culture. Directions for improving the system for assessing an enterprise's level of cyber resilience are proposed, and practical recommendations for enhancing a business's ability to withstand modern digital challenges are outlined. The results obtained can be used to improve mechanisms for ensuring the economic security of enterprises and enhancing their competitiveness in the digital economy, and can serve as a methodological basis for further scientific research in the field of information and economic security of enterprises.

Key words: cyber resilience; crisis management; cybersecurity; cyber risks; business.