Adaptive Approach to Ensuring the Functional Stability of Corporate Educational Platforms under Dynamic Cyber Threats[⋆]

Ihor Hanhalo[1,†], Vadym Chytulian[1,†], Zhebka Viktoriia[1,†], Bohdan Bebeshko[2,†]
and Karyna Khorolska[2,*,†]

[1] *State University of Information and Communication Technologies, 7 Solomiyanska str, 03110 Kyiv, Ukraine*
[2] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., 04053 Kyiv, Ukraine*

Abstract

The functional stability of corporate educational information systems (CEIS) is a key aspect of ensuring the continuity of the educational process and information security. This study proposes a methodology for enhancing the functional stability of CEIS based on mathematical models for risk assessment, financial resource optimization, and cybersecurity measures. The proposed approach includes threat analysis, residual risk calculation, loss prediction depending on response time, and evaluation of security measures' effectiveness. Scenario modeling confirms that the proposed methodology reduces residual risk levels by 40–60% and decreases incident response time to one hour. The results demonstrate that integrating adaptive cybersecurity mechanisms with economic modeling enables an optimal balance between security and costs, enhancing the overall resilience of educational platforms.

Keywords

functional stability, corporate educational information systems, cybersecurity, residual risk, response time, cost optimization, data backup, mathematical modeling, threat prediction, risk management

1. Introduction

The issue of ensuring the functional stability of corporate information systems is particularly relevant in the context of growing cyberthreats and the increasing demand for the continuous operation of information platforms. Despite the availability of numerous studies, many approaches are based on static risk assessment and cost optimization methods that do not account for real-time threat dynamics. This highlights the need for adaptive methodologies that integrate economic models, mathematical forecasting, and automated response mechanisms.

The study in [1] explores mathematical models for risk assessment in information systems based on probabilistic approaches that determine the likelihood of threats occurring in dynamic environments. However, the authors do not address adaptive response mechanisms for adjusting to changes in threat levels.

Cost optimization methodologies for security investments are proposed in [2], where the adaptive allocation of resources between security measures and backup mechanisms is justified depending on the threat level. However, this study does not include real-time threat prediction approaches.

Methods for attack forecasting using machine learning algorithms are discussed in [3], demonstrating the effectiveness of adaptive approaches for detecting anomalous activity. However, the study does not investigate the integration of attack prediction with resource management mechanisms.

[⋆] *CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine*
[*] Corresponding author.
[†] These authors contributed equally.

gangalo.im@gmail.com (I. Hanhalo); chitulyanvadum@gmail.com (V. Chytulian); viktoria_zhebka@ukr.net (V. Zhebka); b.bebeshko@kubg.edu.ua (B. Bebeshko); k.khorolska@kubg.edu.ua (K. Khorolska)
0009-0006-4397-240X (I. Hanhalo); 0009-0001-8846-9094 (V. Chytulian); 0000-0003-4051-1190 (V. Zhebka); 0000-0001-6599-0808 (B. Bebeshko); 0000-0003-3270-4494 (K. Khorolska)

[4] presents approaches to resource backup optimization in corporate systems, taking into account time-dependent recovery characteristics. However, the authors do not consider the interdependence between backup levels and the effectiveness of security measures.

Modern cybersecurity monitoring methods and adaptive models for real-time threat assessment are examined in [5]. However, this study does not consider the integration of monitoring systems with attack prediction mechanisms. The study [6] focuses on functional stability mechanisms in distributed information systems, combining adaptive backup strategies and risk management. However, security cost optimization methods are not considered.

In [7], threat prediction methods using neural networks are explored to minimize losses in the event of incidents. However, the study lacks an analysis of the impact of response time on loss levels.

An approach to automated cybersecurity monitoring and response using blockchain technologies is presented in [8]. However, this methodology does not take into account the optimization of security and backup costs.

The literature analysis indicates that most studies focus on centralized or static risk assessment models, whereas adaptive approaches that consider the temporal dynamics of threats require further research. This confirms the necessity for developing integrative methodologies that combine economic, mathematical, and automated mechanisms to ensure functional stability in corporate educational information systems.

Modern methods for ensuring the functional stability of corporate educational information systems (CEIS) reveal several significant limitations that hinder their effectiveness. One of the main drawbacks is the insufficient consideration of the interdependence between costs, risks, and the dynamics of external and internal factors. In many cases, existing approaches focus on specific aspects, such as enhancing information security or optimizing costs, while ignoring the integrative nature of these processes.

For example, in static models, the costs of implementing and maintaining the system are determined as a one-time expense, whereas risks associated with potential threats may increase over time due to the evolution of cyber threats or the system's insufficient adaptation to environmental changes [9]. These interdependencies are often overlooked due to the limitations of traditional cost assessment approaches, which fail to account for dynamic parameters. The lack of adaptation to changes over time can lead to significant losses, particularly in situations where the system fails to respond promptly to critical events [10].

Another important limitation is the insufficient integration of risk-oriented approaches into economic modeling. In particular, many systems underestimate the role of potential losses associated with downtime, operational failures, or data breaches. The absence of a comprehensive integration of costs and risks significantly complicates effective decision-making. For instance, if security investments do not consider potential losses from realized threats, the allocation of resources may turn out to be irrational [11–14].

Table 1
Disadvantages of existing approaches

Limitation	Cause	Consequence
Static approach to cost assessment	Failure to account for changes in risks over time	Inefficient resource utilization, potential significant losses
Lack of risk integration	Underestimation of the probability of threat realization	Increased costs due to system failures or data breaches
Inefficient backup strategy	Lack of cost optimization for backup systems	Excessive expenditures or insufficient recovery speed
Limited use of forecasting	Absence of tools for real-time adaptation	Reactive decision-making, increased system vulnerability

The shortcomings also extend to the process of system backup and recovery. In many cases, backup systems are implemented without considering the optimal balance between costs and recovery speed. As a result, backup expenses may become economically unjustified, or the available backup resources may fail to ensure a sufficiently fast recovery in critical situations. This issue is particularly crucial for CEIS, where downtime lasting even a few hours can disrupt the educational process and damage the institution's reputation.

Table 2
The impact of redundancy levels on recovery time, costs, and potential losses in corporate educational information systems

Backup Level	Recovery Time	Backup Costs (UAH)	Potential Losses Without Backup (UAH)
Low	High	20,000	150,000
Medium	Medium	50,000	50,000
High	Low	100,000	10,000

Another issue is the limited integration of modern forecasting tools into risk management systems. For example, insufficient use of temporal dynamics models results in many systems failing to adapt to real-time changes, such as fluctuations in server load or the emergence of new types of threats. Without a flexible approach to risk forecasting, management decisions remain predominantly reactive rather than proactive [15–17].

As a result, existing methods fail to achieve a proper balance between economic efficiency and functional stability. This highlights the need for the development of integrative approaches that consider both economic parameters and risk factors in a time-dependent perspective. Future research should focus on adapting existing models to the dynamic operational environment of CEIS.

The objective of this study is to develop a methodology for optimizing expenditures to ensure the functional stability of corporate educational information systems. This methodology integrates risk assessment, cost optimization models, and cybersecurity measures to enhance system resilience while maintaining economic efficiency [18].

2. Theoretical foundations

2.1. Analysis of existing approaches

The functional sustainability of corporate educational information systems (CEIS) is a key factor in their effectiveness in modern conditions. Ensuring this parameter requires taking into account the complex economic dependencies between the costs of implementation, operation, security measures, and risks arising in the process of use. The economic feasibility of measures should be justified by integrating cost and risk assessments into a single model.

The total cost of ownership (TCO) can be used to describe the cost side, which takes into account all the costs of implementing, maintaining, and upgrading the system over its life cycle. Formally, it can be described as:

$$TCO = C_{imp} + \int_{0}^{T} \left(C_{maint}(t) + C_{upgrade}(t) \right) dt, \tag{1}$$

where C_{imp} is the initial cost of implementing the system, $C_{maint}(t)$ is the maintenance cost at time t, and $C_{upgrade}(t)$ is the cost of upgrading technology.

Alongside cost analysis, risk assessment is a crucial component. The risks that arise during the operation of CEIS can be quantified using a loss integration model within a temporal dynamic framework:

$$R_{\text{int}}(t)=\int_{0}^{t}\frac{\sum_{i=1}^{n}P_i(t)\cdot I_i}{1+e^{-\beta(t-)t_0}}dt \tag{2}$$

where $P_i(t)$ represents the probability of occurrence of the i-th threat at time t, I_i is the economic impact of the i-th threat, β s the system's sensitivity coefficient to changes, and t_0 denotes the initial moment of risk assessment. This approach allows for the consideration of not only the probability and impact of risks but also their dynamic nature within a given time frame.

The optimization of security and system resilience costs can be formalized through a multi-criteria model that balances expenditures and risk reduction. The goal of such optimization is to minimize overall costs while ensuring the required level of functional stability. The corresponding model is expressed as:

$$min\,C_{total}=\int_{0}^{T}\left(k_1\cdot R_{loss}(t)+k_2\cdot M_{sec}(t)\right)dt, \tag{3}$$

where R_{loss} represents the losses incurred due to risk realization at time t, $M_{sec}(t)$ denotes the expenditures on security measures, and k_1 and k_2 are weighting coefficients that account for the priorities of reducing losses or costs.

Ensuring the functional stability of CEIS also involves the implementation of backup systems. The costs associated with backup measures include additional servers, data storage, and ensuring system availability in case of failures. The system recovery time can be described using a recovery model:

$$Trec=\frac{\int_{0}^{T}(1-)\cdot f(t)\,dt\,e^{-\mu\cdot t}}{\int_{0}^{T}f(t)\,dt}, \tag{4}$$

where μ is the system recovery rate parameter, and $f(t)$represents the distribution of resources allocated for recovery.

The complexity of economic analysis in CEIS lies in the need to account for interdependencies between different system components. For instance, increasing monitoring expenditures may reduce the probability of risks but lead to higher operational costs. Therefore, decision-making must rely on integrative approaches based on advanced mathematical models.

The conclusions drawn from this analysis confirm the necessity of combining quantitative risk assessment methods with economic models that consider the temporal dynamics of costs. This approach enables well-founded managerial decisions regarding resource allocation in educational systems.

2.2. Scientific Contribution of the Study

The scientific contribution of this study lies in the development of an approach to ensuring the functional stability of corporate educational information systems (CEIS), considering the complex interdependencies between costs, risks, and response speed to incidents. The foundation of this approach is based on mathematical models that allow not only for the assessment of the system's current state but also for predicting its stability over time.

One of the key elements of the proposed methodology is the balancing of expenditures between security measures and backup strategies. This issue is addressed through a model that establishes the relationship between the key budget components allocated for ensuring system resilience:

$$M_{sec} + M_{backup} = C_{safe}, \tag{5}$$

where M_{sec} represents the expenditures on security measures, M_{backup}denotes the expenditures on backup and recovery, and C_{safe} is the total budget. This model serves as a universal framework for assessing the efficiency of resource allocation, as each of these components significantly impacts the overall system resilience.

For instance, insufficient funding for backup mechanisms may result in prolonged downtimes in case of failures, whereas excessive spending on this area might be economically unjustified. Thus, the proposed approach enables budget optimization based on priorities and actual threats.

Another critical aspect is considering the temporal dynamics of losses incurred during system failures. It has been established that the level of losses can decrease exponentially with a reduction in response time. This justifies the economic feasibility of investing in system responsiveness. To model this, the following equation is proposed:

$$R_{loss}(t) = R_{init} \cdot e^{-k T_{rec}}, \tag{6}$$

where R_{init} is the initial level of losses, k is the coefficient determining the rate of loss reduction depending on the recovery time, and T_{rec} represents the time required for full system recovery.

This model confirms that even a slight reduction in response time can significantly impact overall economic outcomes. Specifically, analysis shows that the less time is spent on recovery, the lower the risks of incurring major losses, which is crucial for educational platforms where failures can severely disrupt the learning process.

Particular attention is given to evaluating the impact of expenditures on the functional resilience of the system. To model the relationship between security investments and system stability, a nonlinear model is used, which accounts for the threshold effect of security measures' efficiency:

$$S_{sys} = \frac{1}{1 + e^{-\alpha (M_{sec} - M_{crit})}}, \tag{7}$$

where S_{sys} represents the system's stability level, M_{sec} denotes the expenditures on security measures, M_{crit} is the critical level of expenditures required to achieve a minimum level of stability, and $\alpha$is the sensitivity parameter that determines how system stability responds to changes in security spending.

This model demonstrates that expenditures below a certain critical threshold have little impact on system stability while exceeding this threshold leads to a sharp increase in effectiveness. This highlights the importance of rational budget management, as excessive investments may become inefficient if the system has already reached the required level of protection.

Thus, the developed models provide a comprehensive approach to assessing and improving the functional stability of CEIS. They enable the integration of economic, temporal, and technical parameters into a unified system, facilitating optimal managerial decisions. This approach not only reduces losses and enhances efficiency but also ensures the economic feasibility of educational platform usage in the long-term perspective.

3. Methodology for Ensuring the Functional Stability of Corporate Educational Information Systems Considering Cybersecurity

3.1. General Principles and Methods for Assessing CEIS Functional Stability

The functional stability of corporate educational information systems (CEIS) is a critical factor in ensuring the continuity of the learning process, data protection, and effective resource management within an educational institution. In the modern landscape of increasing cybersecurity threats, ensuring system stability becomes a complex challenge requiring the integration of risk analysis mathematical methods, economic modeling, and adaptive cybersecurity mechanisms.

The proposed methodology for assessing and enhancing functional stability consists of the following key stages:

1. Threat identification and risk analysis—Evaluating potential security threats and their probability of occurrence.
2. Optimization of security measures and resource allocation—Balancing investments between security measures and backup strategies.
3. Cybersecurity monitoring and evaluation of security measures' effectiveness—Continuous assessment of the system's ability to mitigate risks.
4. Attack forecasting and incident management—Implementing proactive mechanisms to detect and respond to emerging threats.

To ensure an adaptive approach to functional stability assessment, the following mathematical models are applied:

1. Cyber risk assessment model, which is based on the probability of threat realization and its potential impact on the system.
2. Cost optimization model for balancing security measures and backup systems, enabling an optimal trade-off between protection efficiency and economic feasibility.
3. A stochastic model for incident response time prediction, which assesses the effectiveness of security measures depending on response time.

The proposed approach provides a comprehensive assessment of system resilience and enables effective resource management to minimize potential attack-induced losses. By integrating predictive risk modeling, economic evaluation, and adaptive cybersecurity strategies, this methodology enhances the overall reliability and efficiency of corporate educational systems.

3.2. Detailing the Methodology for Assessing and Enhancing CEIS Functional Stability

Stage 1. Threat and Risk Assessment

The first stage of the methodology involves identifying, classifying, and assessing potential cybersecurity threats that may impact the functional stability of CEIS. Risk analysis considers the probability of a threat occurring, denoted as $P_{threat}(t)$, which is determined based on statistical data and attack history. The system's vulnerability level, represented as $P_{vuln}(t)$, depends on the implemented security measures and system architecture. Additionally, the level of threat control denoted as $P_{control}(t)$, reflects the effectiveness of security measures in mitigating potential risks.

$$P_{success}(t) = \frac{P_{threat}(t) \cdot P_{vuln}(t)}{P_{control}(t)}, \tag{8}$$

where $P_{success}$ represents the probability that a threat will be successfully executed.

Based on the obtained values, the potential loss level in the event of a successful attack is evaluated as

$$R_{attack}(t) = \sum_{i=1}^{N_{threats}} P_{success,i}(t) \cdot I_{loss,i} \cdot e^{-\lambda T_{rec}}, \tag{9}$$

where $I_{loss,i}$ represents the potential financial losses resulting from the execution of the i-th threat, and T_{rec} denotes the incident response time.

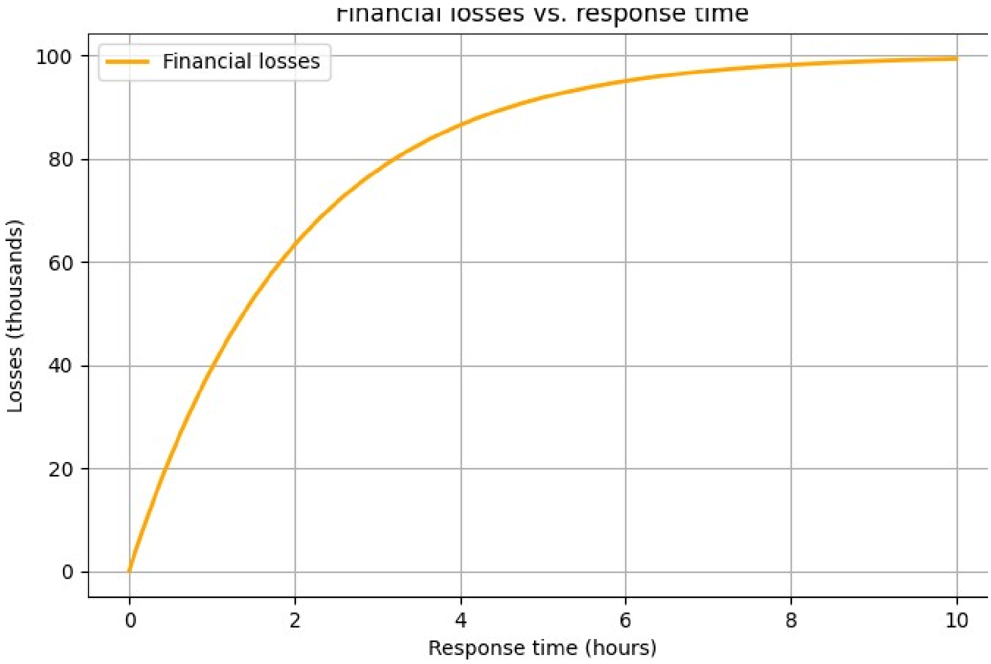

Figure 1: Dependency of Financial Losses on Incident Response Time

The graph illustrates how losses $R_{attack}(t)$ decrease as the incident response time T_{rec} shortens. This confirms that rapid response significantly reduces financial losses.

Stage 2. Threat and Risk Assessment

The second stage involves determining the optimal allocation of financial resources between security measures and backup mechanisms. To achieve this, an economic model, described in Equation 6, is utilized. By integrating this model with a risk-based approach, it becomes possible to evaluate how financial investments influence the overall security posture of the system. The determination of the optimal expenditure level is carried out by constructing a dependency function between security levels and financial investments, as described in Equation 7.

Stage 3. Cybersecurity Monitoring and Attack Prediction

The third stage involves dynamic tracking of system security levels and predicting potential attacks. This process is implemented through attack trend analysis and the identification of changes in threat levels. By continuously monitoring system activity and analyzing historical attack patterns, it becomes possible to detect emerging threats and adjust security measures proactively. This approach enhances threat intelligence capabilities and allows for the early identification of vulnerabilities, improving the overall resilience of the corporate educational information system.

1. Anomalous activity monitoring in the system is carried out using machine learning algorithms, enabling the detection of new types of threats.

2. Attack prediction is based on the analysis of previous incidents and the identification of behavioral patterns of attacking entities.

This stage enables a proactive adaptation of security measures to current threats, minimizing the likelihood of attacks being executed.

The flowchart (Fig. 2) illustrates the cybersecurity decision-making process within CEIS. It begins with threat analysis and attack probability assessment, based on historical data and predictive models. Next, resource allocation is performed, distributing funds and infrastructure between security measures, backup mechanisms, and incident response strategies.

Following the implementation of security measures, effectiveness monitoring is conducted to identify weaknesses and adjust the strategy accordingly. In the event of an incident, a response mechanism is activated, minimizing losses and recovery time. A key component of this process is feedback integration, which allows the system to continuously adapt to emerging threats and improve its resilience.

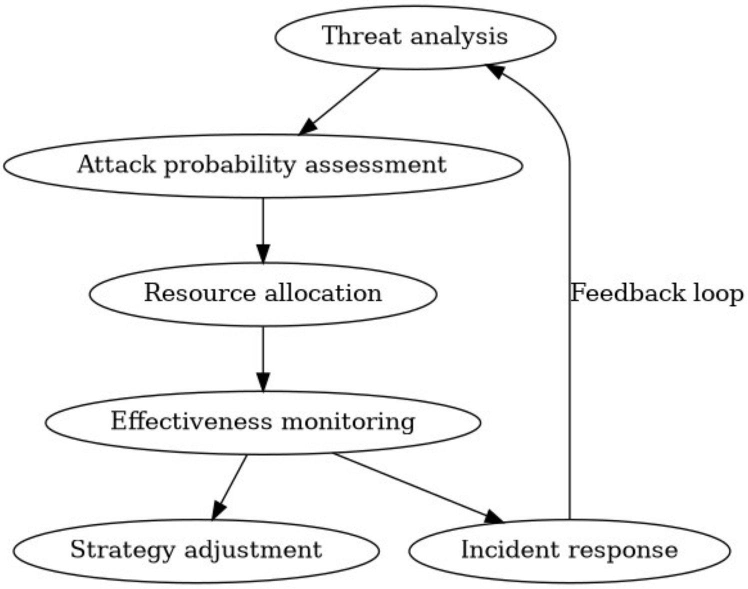

Figure 2: Cybersecurity Decision-Making Process

4. Evaluation of the effectiveness of the methodology for ensuring the functional resilience of CEIS

The assessment of the effectiveness of the proposed methodology for ensuring the functional resilience of corporate educational information systems (CEIS) is conducted based on a quantitative and qualitative analysis of risk levels, cost optimization, and the response system’s time characteristics. The main efficiency criteria include reducing the level of residual risk, minimizing incident response time, optimizing security costs, and ensuring the economic feasibility of the implemented mechanisms. The analysis of indicators is carried out through the modeling of CEIS operation scenarios under different threat levels and security funding conditions.

Determining the level of residual risk is one of the key parameters for assessing the effectiveness of the methodology. Its dynamics are reflected in a formula that takes into account the impact of security measures on the level of threats that remain relevant after the implementation of protection policies:

$$R_{res} = R_{init} \cdot e^{-\eta M_{sec}}, \qquad (10)$$

where R_{init} is the initial risk level, η is the efficiency coefficient of security measures, and M_{sec} is expenditures on cybersecurity measures. This equation demonstrates that as security expenditures increase, the level of residual risk decreases exponentially. However, after reaching a certain critical expenditure level, further increases in security funding do not yield a significant effect. This confirms the necessity of determining the optimal security budget that ensures maximum risk reduction with minimal costs.

Incident response time has a significant impact on overall system losses, as prolonged downtime can lead to substantial economic damage and the loss of critical data. The system recovery time is evaluated using a stochastic model, which considers response speed and the scale of the threat, as described in Equation 9.

The implementation of automated cybersecurity mechanisms and early warning systems significantly reduces response time and, accordingly, the level of financial losses.

To confirm the effectiveness of the methodology, system operation was modeled in three main scenarios. In the first scenario, the system operates without active cybersecurity, leading to a high residual risk level of 85%, while the average recovery time after attacks exceeds 12 hours. In the second scenario, only backup and recovery mechanisms are implemented, reducing the residual risk level to 60% and shortening the average recovery time to 4 hours. In the third scenario, a comprehensive approach is implemented with the introduction of active cybersecurity mechanisms, allowing the residual risk level to be reduced to 25% and the incident response time to be shortened to 1 hour. The obtained results demonstrate that a comprehensive approach, which includes adaptive access control mechanisms, attack prediction, and automated backup, significantly enhances system resilience.

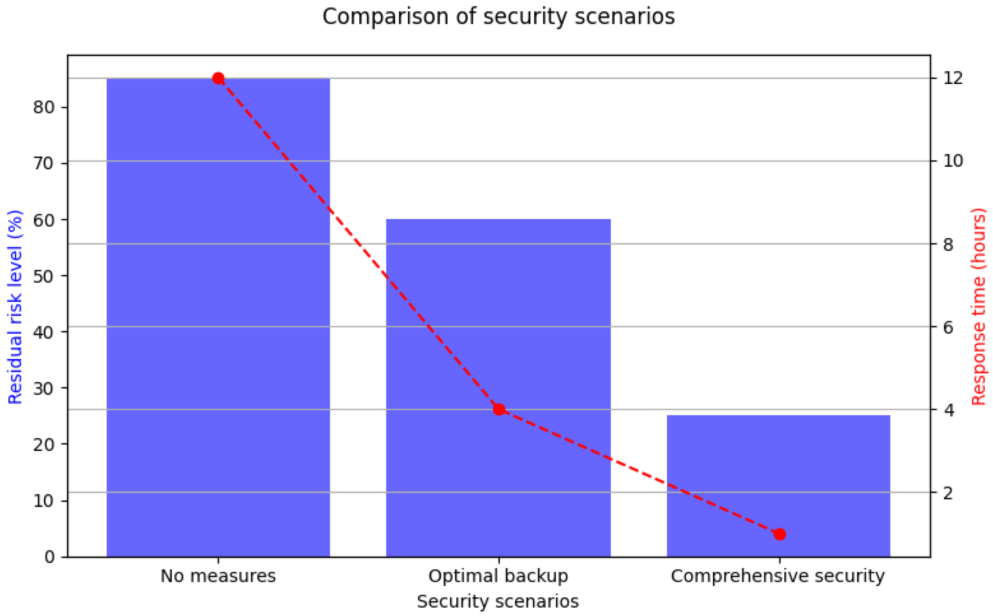

Figure 3: Comparison of Security Scenarios

A detailed analysis of the dependence of the residual risk level on the level of security funding shows that the optimal budget for achieving maximum efficiency should be at the level of M_{crit}, after which further increases in funding do not provide a proportional increase in security effectiveness. The dynamics of this dependence are described by Equation 7. This model confirms the necessity of finding a balance between the level of cybersecurity expenditures and the overall resilience of the system.

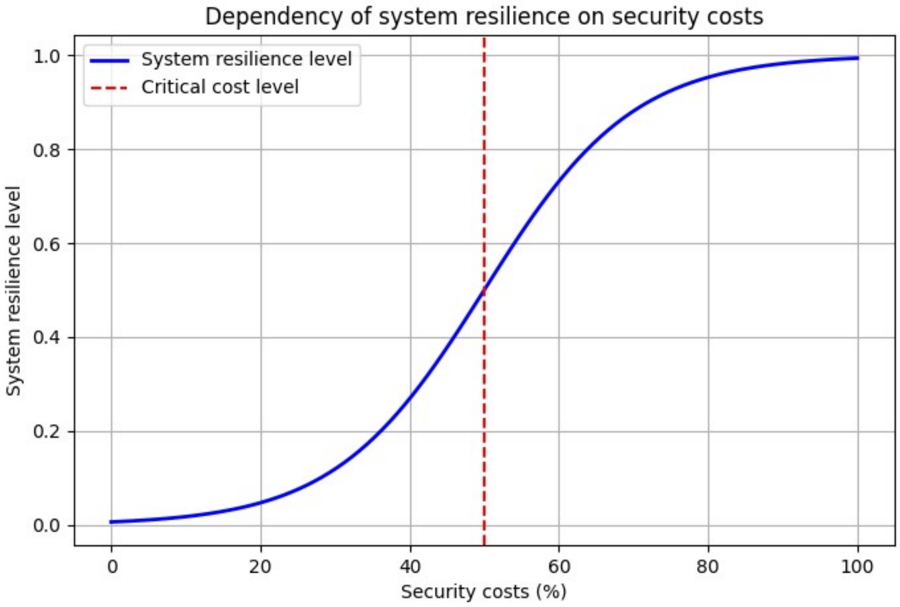

Figure 4: Dependency of System Resilience on Security Costs

Graphical visualization of the obtained results shows that in systems without security measures, the number of attacks remains consistently high, and the recovery costs exceed economically feasible values. The proposed approach helps to avoid such issues and ensures an efficient allocation of resources between security measures, backup, and rapid response mechanisms.

Thus, the conducted evaluation of the methodology's effectiveness confirms that the proposed approach significantly reduces risk levels, optimizes financial expenditures, and improves the overall resilience of corporate educational systems. The integration of mathematical risk assessment models, economic cost analysis, and automated response mechanisms allows for achieving maximum efficiency at an optimal funding level. The proposed methodology is adaptive and can be used to enhance cybersecurity in various information systems utilized in the education sector.

Conclusions

As a result of the conducted research, a comprehensive methodology for ensuring the functional stability of corporate educational information systems (CEIS) has been proposed, taking into account economic, temporal, and technical parameters. The methodology is based on the integration of mathematical models for risk assessment, cost optimization, and adaptive cybersecurity mechanisms. The developed approach enhances system protection, minimizes economic losses, and ensures uninterrupted operation in a dynamic threat environment.

The proposed mathematical models allow for optimized financial resource allocation between security measures and backup systems while also evaluating the effectiveness of security measures based on incident response time. A comprehensive approach to residual risk assessment and attack prediction improves cybersecurity system efficiency and its adaptability to emerging threats.

Future research directions include the integration of artificial intelligence and machine learning technologies to automate risk assessment, attack forecasting, and decision-making processes. Further advancements in adaptive resource backup models and anomaly detection monitoring will improve system responsiveness and optimize expenditures. A relevant research area is the development of real-time security measure effectiveness evaluation methodologies, which will facilitate the operational adaptation of CEIS to environmental changes.

The proposed approach can be applied to enhance the functional stability of information systems across various industries, including the education, financial, and corporate sectors.

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] V. T. Busel, Large explanatory dictionary of the modern Ukrainian language: 250000, Kyiv, Irpin, Perun, VIII, 2005.

[2] E. Ukkonen, Approximate string-matching with q-grams and maximal matches, Theor. Comput. Sci. 92(1) (1992) 191–211. doi:10.1016/0304-3975(92)90143-4

[3] S. Kumar, T. Utsab, A. Raychoudhury, Image compression using approximate matching and run length, Int. J. Adv. Comput. Sci. Appl. 2(6) (2011). doi:10.14569/ijacsa.2011.020617

[4] A. Gupta, A. Bansal, V. Khanduja, Modern lossless compression techniques: Review, comparison and analysis, in: 2nd Int. Conf. on Electrical, Computer and Communication Technologies, ICECCT, 2017, 1–8. doi:10.1109/icecct.2017.8117850

[5] P. Venkatram, A new lossless data compression algorithm exploiting positional redundancy, arXiv, 2021. doi:10.48550/arXiv.2107.13801

[6] S. Yamagiwa, Stream-based lossless data compression, in: Sublinear Computation Paradigm, 2021, 391–410. doi:10.1007/978-981-16-4095-7_16

[7] A. Serkov, et al., Noise-like signals in wireless information transmission systems, Adv. Inf. Syst. 1(2) (2017) 33–38. doi:10.20998/2522-9052.2017.2.06

[8] A. Pieshkin, et al., The comparative assessment of corrective parameters for antinoise convolutional and block codes, in: Int. Conf. on Inf. and Telecom. Technologies and Radio Electronics, UkrMiCo, 2018, 1–4. doi:10.1109/ukrmico43733.2018.9047530

[9] Y. Kostiuk, et al., Models and algorithms for analyzing information risks during the security audit of personal data information system, in: 3rd International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 155–171.

[10] 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 Manag. in Global Inf. Networks (CH&CMiGIN), vol. 3925, 2025, 249–264.

[11] B. Zhurakovskyi, et al., Enhancing information transmission security with stochastic codes, in: Classic, Quantum, and Post-Quantum Cryptography, CQPC, vol. 3829, 2024, 62–69.

[12] M. Pratsiovytyi, Two-symbol image systems (coding) of real numbers, in: Students' Physical and Mathematical Sketches, vol. 9, 2010, 6–26.

[13] M. Pratsiovytyi, Geometry of real numbers in their encodings by means of an infinite alphabet as the basis of topological, metric, fractal and probabilistic theories, Sci. J. Natl. Pedag. Dragomanov Univ. 1(14) (2013) 189–216.

[14] M. Pratsiovytyi, et al., G-representation of real numbers and some of its applications, Nonlinear Oscil. 25(4) (2022) 377–387.

[15] I. Lysenko, Y. Maslova, M. Pratsiovytyi, The binary number system with different bases and special functions associated with it, in: Proceedings of the Institute of Mathematics of the NAS of Ukraine, vol. 16(2), 2019, 50–62.

[16] M. Pratsiovytyi, I. Lysenko, Y. Maslova, Geometry of number series: a series as a model of a real number in a new two-symbol number coding system, in: Proceedings of the Institute of Mathematics of the NAS of Ukraine, vol. 15(1), 2018, 132–146.

[17] M. Pratsiovytyi, Two-symbol encoding systems of real numbers and their application, 2022.

[18] V. Zhebka, et al., Optimization of machine learning method to improve the management efficiency of heterogeneous telecommunication network, in: Cybersecurity Providing in Information and Telecommunication System, vol. 3288, 2022, 149–155.