

Experimental validation of the method for enhancing the security of critical information systems

Viktoriia Sydorenko^{1,*†}, Artem Polozhentsev^{1†}, Kamila Kluczewska-Chmielarz^{2†}, Serhii Sydorenko^{1†} and Oksana Zhyharevych^{3,†}

¹National University "Kyiv Aviation Institute", Liubomyra Huzara Ave., 1, Kyiv, 03058, Ukraine

²University of the National Education Commission, Podchorazych Str., 2, Krakow, 30-084, Poland

³Lesya Ukrainka Volyn National University, Voli Ave., 13, Lutsk, 43025, Ukraine

Abstract

An increasing number of cyber threats and the growing complexity of critical infrastructure systems require effective methods of assessing and improving the level of protection of critical information systems. Current approaches frequently concentrate on individual technical or organizational elements, failing to consider the interplay between risk, reliability, resilience, and resource limitations. This paper presents a method for enhancing the security level of critical information systems, which is based on the formalization of key security parameters and the use of an integral security level indicator. This method enables the current state of security to be assessed, vulnerable components to be identified, and rational organizational and technical measures to be selected to improve protection with limited resources. The method was experimentally validated using critical information systems in the transport sector, including air traffic management, railway traffic safety and road traffic control systems. The results demonstrate an increase in the integral protection-level indicator, confirming the method's effectiveness and applicability in supporting cybersecurity risk management decisions at critical infrastructure facilities.

Keywords

critical information systems, critical information infrastructure, cybersecurity, cyber resilience, security measures, experimental validation, critical infrastructure protection

1. Introduction

Ensuring the security and resilience of critical information systems (CIS) is one of the key challenges of modern cybersecurity, especially in the context of increasing cyber threats, technological complexity, and hybrid destabilizing influences. Critical information systems support essential state functions and provide operational continuity for sectors such as transport, energy, healthcare, telecommunications, and public administration.

The resilience of such systems is determined by their ability to withstand, adapt to, and recover from internal and external destabilizing factors while maintaining an acceptable level of operational functionality. In recent years, the issue of critical infrastructure resilience has become particularly relevant due to the growing number of cyberattacks targeting state information resources and the increasing dependence of societal processes on digital services.

According to the Law of Ukraine "On Critical Infrastructure" [1], ensuring the protection and resilience of critical infrastructure facilities is a strategic priority for national security. Additional regulatory requirements are defined by the Cabinet of Ministers of Ukraine in the relevant resolutions concerning security and resilience assurance for critical infrastructure facilities [2, 3, 4].

WCH'26: Fifth International Workshop on Cyber Hygiene, June 25–26, 2026, Krakow, Poland

*Corresponding author.

†These authors contributed equally.

✉ viktoriia.sydorenko@npp.kai.edu.ua (V. Sydorenko); artem.polozhentsev@kai.edu.ua (A. Polozhentsev); kamila.kluczewska-chmielarz@uken.krakow.pl (K. Kluczewska-Chmielarz); serh.sydorenko@gmail.com (S. Sydorenko); zhyharevych.oksana@vnu.edu.ua (O. Zhyharevych)

ORCID 0000-0002-5910-0837 (V. Sydorenko); 0000-0003-0139-0752 (A. Polozhentsev); 0000-0003-4301-7438 (K. Kluczewska-Chmielarz); 0000-0002-7170-123X (S. Sydorenko); 0000-0002-7154-9733 (O. Zhyharevych)



© 2026 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

Existing approaches to assessing the security state of critical information systems primarily focus on isolated technical or organizational indicators. Such approaches do not fully account for the interdependencies between risk exposure, reliability characteristics, and resilience indicators. This creates the need for integrated assessment methods capable of formalizing these relationships and supporting decision-making regarding security enhancement measures.

Recent studies have proposed mathematical and probabilistic approaches to resilience assessment for critical systems. In particular, the resilience-oriented model introduced in [5] establishes formal relationships between destabilizing factors and system response characteristics. Other works consider quantitative resilience assessment under risk and uncertainty conditions [6, 7, 8, 9].

The purpose of this study is to develop and experimentally validate a method for enhancing the security level of critical information systems through an integrated assessment of risk, reliability, and resilience parameters. The proposed method enables quantitative estimation of the current security level, prediction of security degradation under destabilizing impacts, and selection of optimal improvement strategies under resource constraints.

2. Literature review

The problem of ensuring the resilience and security of critical information systems has attracted significant attention in recent years due to the growing complexity of cyber threats and the increasing digitalization of critical infrastructure sectors.

Modern approaches to resilience assessment are primarily focused on probabilistic, reliability-oriented, and risk-based models. In particular, Mahmood et al. [6] proposed an integrated framework for evaluating infrastructure sustainability from the perspectives of risk, reliability, and resilience. Their approach demonstrates the importance of considering interdependencies between these parameters when assessing infrastructure stability.

Reliability estimation methods remain an essential component of resilience analysis. Mohd Safari et al. [10] presented robust statistical approaches for reliability estimation under uncertain operational conditions. Such methods provide a mathematical foundation for evaluating system performance degradation and recovery capabilities.

Optimization-based approaches have also been widely applied to resilience enhancement. Kong et al. [7] developed a methodology for optimizing resilience improvement measures for interdependent infrastructures exposed to regional hazards. Their results confirm the effectiveness of combined mitigation strategies under constrained resource conditions.

A significant contribution to resilience methodology was made by Rehak et al. [8], who extended the CIERA method by introducing resistance as an additional resilience component. This extension improved the ability to assess the capacity of critical systems to withstand disruptive impacts.

A holistic multi-scenario approach to resilience assessment was proposed by Irankunda et al. [11]. Their framework emphasizes the need for integrated consideration of operational, technical, and environmental destabilizing factors when evaluating infrastructure resilience.

In the context of Ukraine, several studies address resilience and security assessment of critical infrastructure under conditions of elevated cyber and hybrid threats. Murasov and Melnyk [12] investigated cybersecurity assessment approaches for critical infrastructure facilities. Sukhodolia [13] analyzed resilience challenges for critical energy infrastructure. Shevchenko and Plakhotniuk [14] proposed methodological approaches for resilience assessment under special economic conditions, while Kyrylenko and Tyshchenko [15] focused on risk assessment under armed conflict conditions.

Recent studies by Sydorenko et al. [5, 16] introduced mathematical models for ensuring resilience and enhancing the security level of critical information systems. These works provide an important basis for further development of integrated security assessment methods.

Despite the considerable number of existing studies, current approaches typically focus on individual aspects of resilience, reliability, or risk assessment [17, 18, 19]. Limited attention is paid to formalized

integration of these parameters into a unified security-level indicator that would support decision-making for selecting optimal protection enhancement strategies.

Therefore, there remains a need for comprehensive methods that combine resilience modeling, probabilistic reliability analysis, and risk-oriented assessment within a single formalized framework for critical information systems.

3. Methodological framework

The mathematical formulation of the proposed method for improving the security level of critical information systems (CIS) is implemented through the following stages, taking into account the approaches presented in [20, 6, 7, 8, 11, 16].

3.1. Stage 1. Identification of potential CIS threats

To determine the overall set of potential threats to a CIS, the set H is introduced as

$$H = \left\{ \bigcup_{k=1}^n H_k \right\} = \{H_1, H_2, \dots, H_n\} \quad (1)$$

where $H_k \subseteq H$ denotes the types of potential threats to the CIS, and n is the total number of identified threats.

3.2. Stage 2. Identification of threat scenarios

To define the set of scenarios characterizing a specific threat H_k , the set Ω_k is introduced as

$$\Omega_k = \left\{ \bigcup_{p=1}^{m_k} \Omega_{kp} \right\} = \{\Omega_{k1}, \Omega_{k2}, \dots, \Omega_{km_k}\} \quad (2)$$

where Ω_{kp} represents scenarios describing the realization of threat H_k .

A threat realization scenario is represented as

$$\omega_{kp} = \langle h_k, cond_{kp}, t_{kp} \rangle \quad (3)$$

where:

- h_k denotes the threat type;
- $cond_{kp}$ represents environmental conditions;
- t_{kp} is the realization time interval.

3.3. Stage 3. Risk assessment of a CIS element

The expected level of losses resulting from threat realization is determined as

$$RISK_i = \sum_{k=1}^n \sum_{p=1}^{m_k} \sum_{d=1}^D w_d \cdot P_{ikp} \cdot V_{ikp} \cdot C_{kd}^{(p)} \quad (4)$$

where w_d is the weighting coefficient for consequence category d , P_{ikp} is the probability of realization, V_{ikp} is the vulnerability level, and $C_{kd}^{(p)}$ denotes expected consequences.

Table 1
Scale for Evaluating the Integral Indicator of CIS Security Level

Interval of $PSI_i^{(0)}$	Security level	State characteristics
$0.85 < PSI_i^{(0)} \leq 1.00$	Ensures	The system provides the required level of security and operates stably. No critical vulnerabilities are identified.
$0.65 < PSI_i^{(0)} \leq 0.85$	Limited assurance	Security partially satisfies requirements. Certain components require optimization or improvement.
$PSI_i^{(0)} \leq 0.65$	Does not ensure	The security level is insufficient and requires implementation of additional resilience-enhancing measures.

3.4. Stage 4. Reliability assessment

The reliability of a CIS element is defined as

$$R_i(t) = e^{-\lambda_i t} \quad (5)$$

where λ_i is the failure rate.

The failure rate is calculated as

$$\lambda_i = \frac{N_{fail,i}}{T_{obs,i}} \quad (6)$$

The extended reliability is determined as

$$R_i^* = R_i + (1 - R_i) \cdot B_s \cdot R_{island} \quad (7)$$

3.5. Stage 5. Resilience assessment

The resilience index is defined as

$$RI_i = \frac{1}{T} \int_0^T \frac{P(t)}{P_{nom}} dt \quad (8)$$

The integral resilience indicator is

$$RI_{sys} = \sum_l \beta_l RI^{(l)}, \quad \sum_l \beta_l = 1 \quad (9)$$

3.6. Stage 6. Integral security assessment

The integral security-level indicator is calculated as

$$PSI_i^{(0)} = \alpha \overline{RISK}_i + \beta \overline{R}_i + \gamma \overline{RI}_i \quad (10)$$

subject to

$$\alpha + \beta + \gamma = 1 \quad (11)$$

To interpret the obtained values of the integral indicator $PSI_i^{(0)}$, the security-level scale defined in the methodology for assessing the protection state of critical infrastructure facilities is applied.

Thus, the obtained values enable classification of the CIS state into three assurance categories.

3.7. Stage 7. Optimization of security strategies

To determine the optimal set of security enhancement strategies, the following optimization problem is formulated:

$$\max_{\{s_k\}} \sum_i w_i \cdot PSI_i^{(0)}(s_k) \quad (12)$$

subject to

$$\sum_k C_k s_k \leq B \quad (13)$$

$$R_i^* \geq R_{min} \quad (14)$$

$$RI_{sys} \geq RI_{min} \quad (15)$$

where:

- s_k denotes a security enhancement strategy;
- C_k is the implementation cost;
- B is the available resource budget;
- R_{min} is the minimum acceptable reliability threshold;
- RI_{min} is the minimum acceptable resilience threshold;
- w_i is the importance coefficient of CIS element i .

This optimization procedure enables the selection of the most effective protection strategy under resource constraints.

3.8. Stage 8. Assessment of security improvement effect

The effectiveness of implemented improvement strategies is evaluated as

$$E_i = \frac{PSI_i^{(1)} - PSI_i^{(0)}}{PSI_i^{(0)}} \cdot 100\% \quad (16)$$

where:

- $PSI_i^{(0)}$ is the initial security level;
- $PSI_i^{(1)}$ is the security level after strategy implementation.

The obtained value E_i quantitatively reflects the effectiveness of the selected improvement strategy. Therefore, the proposed method enables:

- quantitative assessment of the current CIS security state;
- forecasting the impact of destabilizing factors;
- optimization of protection strategies;
- evaluation of the effectiveness of implemented security measures.

This provides a formalized basis for adaptive decision-making regarding the enhancement of critical information system resilience under limited resources and operational constraints.

4. Experimental study of the method

The experimental study of the proposed method uses the stages presented in [16]. These stages include identifying threats, forming threat realization scenarios, and assessing the risk, reliability, and resilience of critical information systems (CIS). This is followed by determining the integral security-level indicator. This approach enables an objective evaluation of the method's effectiveness and facilitates a comparison of the system state before and after the implementation of security-enhancing measures.

For the study, the CIS of the transport sector was selected: the Automated Air Traffic Control System (ATCS), which provides navigation and air traffic control services within Ukrainian airspace. This system was chosen due to its strategic importance for national security and the high criticality of potential consequences associated with system failures or cyber interference. Studying the resilience and security of the ATCS is particularly relevant under martial law conditions. Since 2022, Ukraine's civil airspace has largely been closed to commercial flights, and the ATCS operates in limited mode, performing functions related to state, humanitarian, evacuation, and military aviation operations. This situation is accompanied by changes in the threat profile, increased relevance of cyberattacks and electronic warfare impacts, and the need to maintain operational capability during hostilities, infrastructure damage, and energy system instability.

4.1. Stage 1. Identification of the set of potential CIS threats

In accordance with the proposed method, an example of forming the overall set of potential threats to the ATCS is considered based on an analysis of regulatory documents issued by ICAO, EASA, EUROCONTROL, and NOTAM. Taking into account the general threat identification model and setting $n = 5$, the set of potential threat types to the ATCS is defined as follows:

$$H = \left\{ \bigcup_{k=1}^5 H_k \right\} = \{H_1, H_2, H_3, H_4, H_5\}. \quad (17)$$

Here, H_1 denotes cyberattacks targeting servers, navigation complexes, and radar systems; H_2 denotes failure or disruption of ATC-pilot or ATC-ATC communication channels; H_3 denotes technical malfunction, accident, or degradation of ATC centers, radar, or server equipment; H_4 denotes the human factor, including controller errors, stress conditions, and workload overload; and H_5 denotes external impacts, including infrastructure damage, power supply interruptions, electronic warfare (EW), and hostilities.

4.2. Stage 2. Identification of scenarios characterizing potential CIS threats

For the list of potential threats H_k defined at the previous stage, with $n = 5$, and taking into account the scenario identification model, the set of scenarios is represented as follows:

$$\Omega = \left\{ \bigcup_{p=1}^5 \Omega_p \right\} = \{\Omega_1, \Omega_2, \Omega_3, \Omega_4, \Omega_5\}. \quad (18)$$

Here, Ω_1 is the set of cyber-impact scenarios affecting the ATCS; Ω_2 is the set of scenarios related to degradation or disruption of ATC communication channels; Ω_3 is the set of scenarios involving technical failures of radar, server, or ATC center equipment; Ω_4 is the set of scenarios associated with the human factor; and Ω_5 is the set of scenarios related to external impacts, including energy-related, electronic warfare, and combat-related impacts.

To represent a specific scenario Ω_{kp} that characterizes the realization of a given threat H_k , a tuple ω_{kp} is introduced. This tuple reflects the combination of the threat type, environmental conditions, and the time of its realization.

For cyber-impact scenarios, the set Ω_1 is defined as follows:

$$\Omega_1 = \{\omega_{11}, \omega_{12}\}, \quad \omega_{11} = \langle H_1, \text{cond}_{11}, t_{11} \rangle, \quad \omega_{12} = \langle H_1, \text{cond}_{12}, t_{12} \rangle. \quad (19)$$

In this case, cond_{11} denotes the absence of network segmentation and the presence of server vulnerabilities, while t_{11} corresponds to peak load periods or system update windows. Similarly, cond_{12} represents the presence of open ports and insufficient IDS/IPS control, while t_{12} refers to the moment of an external information attack, such as a DDoS attack.

For communication channel degradation scenarios, the set Ω_2 is represented as follows:

$$\Omega_2 = \{\omega_{21}, \omega_{22}\}, \quad \omega_{21} = \langle H_2, \text{cond}_{21}, t_{21} \rangle, \quad \omega_{22} = \langle H_2, \text{cond}_{22}, t_{22} \rangle. \quad (20)$$

Here, cond_{21} denotes damage to ground communication channels or loss of VHF communication, while t_{21} corresponds to periods of adverse weather conditions. In turn, cond_{22} represents degradation of SATCOM/ADS-B signals, while t_{22} refers to periods of military interference or electronic warfare.

For technical failure scenarios, the set Ω_3 is defined as follows:

$$\Omega_3 = \{\omega_{31}, \omega_{32}\}, \quad \omega_{31} = \langle H_3, \text{cond}_{31}, t_{31} \rangle, \quad \omega_{32} = \langle H_3, \text{cond}_{32}, t_{32} \rangle. \quad (21)$$

In this case, cond_{31} denotes equipment wear or lack of redundancy, while t_{31} corresponds to peak operating hours or software update periods. The condition cond_{32} represents a database failure or server crash, while t_{32} refers to the transition to a backup segment.

For human-factor scenarios, the set Ω_4 is represented as follows:

$$\Omega_4 = \{\omega_{41}, \omega_{42}\}, \quad \omega_{41} = \langle H_4, \text{cond}_{41}, t_{41} \rangle, \quad \omega_{42} = \langle H_4, \text{cond}_{42}, t_{42} \rangle. \quad (22)$$

Here, cond_{41} denotes personnel fatigue or information overload, while t_{41} corresponds to high traffic density or emergency situations. The condition cond_{42} represents errors in command transmission, while t_{42} refers to critical situations or periods of increased stress.

For external impact scenarios, the set Ω_5 is defined as follows:

$$\Omega_5 = \{\omega_{51}, \omega_{52}\}, \quad \omega_{51} = \langle H_5, \text{cond}_{51}, t_{51} \rangle, \quad \omega_{52} = \langle H_5, \text{cond}_{52}, t_{52} \rangle. \quad (23)$$

In this case, cond_{51} denotes power supply interruptions or the absence of backup generators, while t_{51} corresponds to shelling or large-scale attacks. The condition cond_{52} represents the impact of electronic warfare or GNSS jamming, while t_{52} refers to critical periods of flight operations.

4.3. Stage 3. Risk assessment of a CIS element

Taking into account the defined sets Ω_k and tuples ω_{kp} , experimental data are formed to calculate the risk. For the ATCS case study, two consequence categories are considered: $d = 1$, which corresponds to safety-related consequences with weight $w_1 = 0.7$, and $d = 2$, which corresponds to economic consequences with weight $w_2 = 0.3$. For each scenario, the parameters of the ATCS risk scenarios are specified in Table 2.

Next, the results of the risk calculation for each identified threat are presented.

For threat H_1 , which corresponds to cyberattacks, the risk value is calculated as follows:

$$\begin{aligned} R_1 = & (0.7 \cdot 0.10 \cdot 0.8 \cdot 0.95 + 0.3 \cdot 0.10 \cdot 0.8 \cdot 0.85) \\ & + (0.7 \cdot 0.12 \cdot 0.75 \cdot 0.9 + 0.3 \cdot 0.12 \cdot 0.75 \cdot 0.80) = 0.1072. \end{aligned} \quad (24)$$

For threat H_2 , which corresponds to communication channel disruption, the risk value is calculated as follows:

$$\begin{aligned} R_2 = & (0.7 \cdot 0.06 \cdot 0.7 \cdot 0.85 + 0.3 \cdot 0.06 \cdot 0.70 \cdot 0.60) \\ & + (0.7 \cdot 0.05 \cdot 0.65 \cdot 0.80 + 0.3 \cdot 0.05 \cdot 0.65 \cdot 0.55) = 0.0558. \end{aligned} \quad (25)$$

Table 2

Parameters of Risk Scenarios for the ATCS

Threat H_k	Scenario ω_{kp}	P_{ikp}	V_{ikp}	$C^{(1)}$	$C^{(2)}$
H_1	ω_{11}	0.10	0.80	0.95	0.85
	ω_{12}	0.12	0.75	0.90	0.80
H_2	ω_{21}	0.06	0.70	0.85	0.60
	ω_{22}	0.05	0.65	0.80	0.55
H_3	ω_{31}	0.04	0.85	0.95	0.70
	ω_{32}	0.07	0.60	0.75	0.50
H_4	ω_{41}	0.10	0.50	0.70	0.45
	ω_{42}	0.08	0.55	0.65	0.40
H_5	ω_{51}	0.05	0.60	0.80	0.65
	ω_{52}	0.07	0.70	0.85	0.55

For threat H_3 , which corresponds to technical equipment failure, the risk value is calculated as follows:

$$R_3 = (0.7 \cdot 0.04 \cdot 0.85 \cdot 0.95 + 0.3 \cdot 0.04 \cdot 0.85 \cdot 0.70) + (0.7 \cdot 0.07 \cdot 0.60 \cdot 0.75 + 0.3 \cdot 0.07 \cdot 0.60 \cdot 0.50) = 0.0638. \quad (26)$$

For threat H_4 , which corresponds to the human factor, the risk value is calculated as follows:

$$R_4 = (0.7 \cdot 0.10 \cdot 0.50 \cdot 0.70 + 0.3 \cdot 0.10 \cdot 0.50 \cdot 0.45) + (0.7 \cdot 0.08 \cdot 0.55 \cdot 0.65 + 0.3 \cdot 0.08 \cdot 0.55 \cdot 0.40) = 0.0439. \quad (27)$$

For threat H_5 , which corresponds to external impacts, including energy supply disruptions, electronic warfare, and hostilities, the risk value is calculated as follows:

$$R_5 = (0.7 \cdot 0.05 \cdot 0.60 \cdot 0.80 + 0.3 \cdot 0.05 \cdot 0.60 \cdot 0.65) + (0.7 \cdot 0.07 \cdot 0.70 \cdot 0.85 + 0.3 \cdot 0.07 \cdot 0.70 \cdot 0.55) = 0.0577. \quad (28)$$

In accordance with the risk assessment formula, the overall risk of the ATCS element is determined as follows:

$$RISK_i = R_1 + R_2 + R_3 + R_4 + R_5 = 0.1072 + 0.0558 + 0.0638 + 0.0439 + 0.0577 = 0.3284. \quad (29)$$

4.4. Stage 4. Reliability assessment of a CIS element

Within the experimental study, the operational parameters of a critical ATCS element, such as a server node or a radar subsystem, are assumed as follows: over an observation period of three years, $N_{fail,i} = 3$ failures were recorded, and the total operating time during this period was

$$T_{obs,i} = 3 \cdot 8760 = 26280. \quad (30)$$

The failure rate is calculated as follows:

$$\lambda_i = \frac{N_{fail,i}}{T_{obs,i}} = \frac{3}{26280} \approx 1.14 \cdot 10^{-4}. \quad (31)$$

To calculate the probability of failure-free operation, an annual time interval of $t = 8760$ hours is considered. According to the reliability function, the following value is obtained:

$$R_i(t) = e^{-\lambda_i t} = e^{-1.14 \cdot 10^{-4} \cdot 8760} \approx e^{-0.999} \approx 0.368. \quad (32)$$

Thus, the probability that the ATCS element operates without failure over one year is equal to 0.368.

Some ATCS elements may support autonomous restart or isolated operation modes, such as backup radars or redundant servers. The extended reliability is calculated assuming $B_s = 0.85$, which denotes the probability of successful automatic recovery, and $R_{island} = 0.90$, which denotes the reliability of the isolated operating mode:

$$R_i^* = R_i + (1 - R_i) \cdot B_s \cdot R_{island} = 0.368 + (1 - 0.368) \cdot 0.85 \cdot 0.90 = 0.851. \quad (33)$$

4.5. Stage 5. Resilience assessment of a CIS element

For the experimental study, a typical operational cycle of the ATCS over a 12-hour period after a destabilizing impact, such as loss of a communication channel or a technical failure, is considered. Three characteristic stages of system operation are identified:

- disruption stage, from 0 to 2 hours: the system operates with reduced efficiency, and the performance level is $P(t)/P_{nom} = 0.40$ of the nominal value;
- partial recovery stage, from 2 to 6 hours: after corrective measures are applied, the system performance increases to $P(t)/P_{nom} = 0.70$;
- stabilization stage, from 6 to 12 hours: the system returns to near-normal operation, demonstrating a performance level of $P(t)/P_{nom} = 0.95$.

The resilience index is calculated as follows:

$$\begin{aligned} RI_i &= \frac{1}{T} \int_0^T \frac{P(t)}{P_{nom}} dt \\ &= \frac{1}{12} \left(\int_0^2 0.40 dt + \int_2^6 0.70 dt + \int_6^{12} 0.95 dt \right) \\ &= \frac{1}{12} (0.8 + 2.8 + 5.7) = 0.775. \end{aligned} \quad (34)$$

For complex ATCS systems, resilience is formed at several levels:

- technological level, including servers and network equipment, where $RI^{(1)} = 0.78$ and $\beta_1 = 0.5$;
- information level, including data integrity and availability, where $RI^{(2)} = 0.80$ and $\beta_2 = 0.3$;
- organizational level, including procedures and the human factor, where $RI^{(3)} = 0.72$ and $\beta_3 = 0.2$.

Thus, the integral resilience index is determined as a weighted sum of partial indices:

$$RI_{sys} = \sum_l \beta_l \cdot RI^{(l)} = 0.5 \cdot 0.78 + 0.3 \cdot 0.80 + 0.2 \cdot 0.72 = 0.774. \quad (35)$$

4.6. Stage 6. Integral assessment of the CIS security level

At this stage, the results of the three components of the method, namely $RISK_i$, R_i , and RI_{sys} , are combined using weighting coefficients $\alpha = 0.4$, $\beta = 0.35$, and $\gamma = 0.25$ into a single integrated indicator of the CIS security level.

It should be noted that the results of risk, reliability, and resilience assessments of the CIS element are converted into a comparable form by transforming the risk indicator into a benefit-oriented scale:

$$\overline{RISK}_i = 1 - RISK_i = 1 - 0.3284 = 0.6716. \quad (36)$$

The normalized reliability and resilience indicators are defined as follows:

$$\overline{R}_i = R_i = 0.851, \quad \overline{RI}_i = RI_{sys} = 0.774. \quad (37)$$

The baseline value of the integral security-level indicator is calculated as follows:

$$\begin{aligned} PSI_i^{(0)} &= \alpha \cdot \overline{RISK}_i + \beta \cdot \overline{R}_i + \gamma \cdot \overline{RI}_i \\ &= 0.4 \cdot 0.6716 + 0.35 \cdot 0.851 + 0.25 \cdot 0.774 = 0.7599. \end{aligned} \quad (38)$$

According to the security-level scale presented in Table 1, the obtained value $PSI_i^{(0)} = 0.7599$ corresponds to the “Limited assurance” level.

4.7. Stage 7. Optimization of CIS security strategies

To determine the optimal set of strategies, it is necessary to ensure that the CIS element complies with regulatory reliability and resilience criteria. In accordance with ICAO and EUROCONTROL requirements for critical ATCS systems, the minimum acceptable probability of failure-free operation is assumed as $R_{min} = 0.90$, while the minimum acceptable resilience level is assumed as $RI_{min} = 0.80$. The values obtained in the previous stages for the ATCS element [21], in particular $RI_{sys} = 0.774 < 0.80$, indicate non-compliance with the required resilience threshold and confirm the necessity of implementing corrective strategies.

The available budget for implementing security measures is $B = 250$ thousand UAH. Within the experimental study, five potential strategies for improving the ATCS security level were formulated. Each strategy has a specific impact on risk, reliability, or resilience indicators, as shown in Table 3.

Table 3
ATCS Security Enhancement Strategies

Strategy s_k	Measure description	Expected impact	Cost, thousand UAH
s_1	Modernization of ATCS servers	Increases reliability	120
s_2	Redundancy of ATC communication channels	Reduces communication risks	90
s_3	Implementation of automated response procedures	Increases resilience	70
s_4	Protection of network infrastructure against cyberattacks	Reduces cyber risks	110
s_5	Personnel qualification improvement, including controllers and IT staff	Reduces human factor impact	45

Impact on reliability. Strategy s_1 ensures a change in the reliability indicator. Server modernization reduces the failure rate and increases reliability by $\Delta R_i = +0.07$ after its implementation:

$$R_i^*(s_1) = 0.851 + 0.07 = 0.921 \geq R_{min}. \quad (39)$$

Impact on resilience. Strategy s_3 affects the system recovery speed after incidents. The resilience increment is $\Delta RI_{sys} = +0.05$ after its implementation:

$$RI_{sys}(s_3) = 0.774 + 0.05 = 0.824 \geq RI_{min}. \quad (40)$$

Thus, the minimum required set of strategies consists of strategies s_1 and s_3 .

The budget feasibility check shows that

$$C_{s_1} + C_{s_3} = 120 + 70 = 190 \leq B. \quad (41)$$

Therefore, the selected combination fits within the available budget. Strategies s_2 , s_4 , and s_5 are not critical in the context of meeting the defined constraints and do not provide a significant additional increase in the integrated security indicator under the selected resource limitation.

Next, the results of the three components of the method, namely $RISK_i$, R_i , and RI_{sys} , are combined again using the weighting coefficients $\alpha = 0.4$, $\beta = 0.35$, and $\gamma = 0.25$ into a single integrated CIS security indicator.

After implementing the selected strategies, two indicators change. For strategy s_1 , the reliability increment is $\Delta R_i = +0.07$, which gives

$$\widehat{R}_i^{new} = 0.851 + 0.07 = 0.921. \quad (42)$$

For strategy s_3 , the resilience increment is $\Delta RI_{sys} = +0.05$, which gives

$$\widehat{RI}_i^{new} = 0.774 + 0.05 = 0.824. \quad (43)$$

It should be noted that, for this combination of strategies, the risk level remains unchanged:

$$\widehat{RISK}_i^{new} = 0.6716. \quad (44)$$

The value of the integral security-level indicator after implementing the selected strategies is calculated as follows:

$$\begin{aligned} PSI_i^{(1)} &= \alpha \cdot \widehat{RISK}_i + \beta \cdot \widehat{R}_i + \gamma \cdot \widehat{RI}_i \\ &= 0.4 \cdot 0.6716 + 0.35 \cdot 0.921 + 0.25 \cdot 0.824 = 0.7969. \end{aligned} \quad (45)$$

4.8. Stage 8. Assessment of the effect of improving the CIS security level

At this stage, the effect of improving the CIS security level as a result of implementing the optimal strategies is determined. The improvement effect is calculated as follows:

$$\begin{aligned} E_i &= \frac{PSI_i^{(1)} - PSI_i^{(0)}}{PSI_i^{(0)}} \cdot 100\% \\ &= \frac{0.7969 - 0.7599}{0.7599} \cdot 100\% = 4.9\%. \end{aligned} \quad (46)$$

The experimental study confirmed the effectiveness of the proposed method for improving CIS security. Based on an integrated assessment of risk, reliability, and resilience, the current state of the system was identified and corrective measures were justified. Strategy optimization made it possible to select a combination that ensures compliance with regulatory thresholds and the rational use of resources. The increase in the integrated indicator after implementing the selected strategies confirms the effectiveness of the proposed approach. The developed method enables quantitative assessment of the security state, forecasting of the impact of threats, and selection of optimal resilience-enhancement measures under limited resources.

4.9. Verification across transport-sector critical information systems

To confirm the applicability of the proposed method beyond a single case study, the verification results were generalized for three experimental scenarios involving critical information systems of the transport sector. These scenarios include the automated air traffic control (ATC) system, the railway traffic safety system, and the road traffic control system.

The comparison of the integral security-level indicator before and after the implementation of the selected strategies makes it possible to evaluate the effectiveness of the method and the practical relevance of the proposed security enhancement measures. The generalized verification results are presented in Table 4.

Table 4

Verification Results of the Method for Enhancing the CIS Security Level

Indicator	Verification 1	Verification 2	Verification 3
Transport-sector CIS	Automated ATC	Railway traffic safety	Road traffic control
Initial value of the integral security-level indicator	0.759	0.704	0.727
Initial security level	Limited assurance	Limited assurance	Limited assurance
Final value of the integral security-level indicator	0.796	0.888	0.855
Final security level	Ensures	Ensures	Ensures
Improvement effect	4.9%	26.1%	17.5%

The results of the three verification scenarios confirm the applicability and effectiveness of the proposed method for different types of transport-sector critical information systems. In all scenarios, the implementation of the selected strategies led to an increase in the integral security-level indicator. In the first verification scenario, the ATC system remained within the “Limited assurance” level, but the indicator improved from 0.7599 to 0.7969. In the second and third verification scenarios, the selected strategies ensured a transition from the “Limited assurance” level to the “Ensures” level. The improvement effect ranged from 4.9% to 26.1%, which confirms the effectiveness of the proposed strategies and the validity of the resource allocation decisions.

The conducted experimental verification also confirms the universality of the proposed approach for CIS with different interconnection topologies, threat characteristics, and operating conditions. This demonstrates the possibility of using the method to support decision-making in tasks related to improving the security level of critical infrastructure facilities.

4.10. Practical recommendations for selecting organizational and technical security measures

Based on the experimental validation, practical recommendations were formulated for selecting a rational set of organizational and technical measures for protecting critical information infrastructure facilities. These recommendations are aimed at supporting operators of critical infrastructure in choosing appropriate security enhancement strategies under conditions of military and hybrid threats. Figure 1 summarizes the key practical recommendations derived from the conducted study.

The proposed recommendations include:

- phased implementation of security measures, taking into account the criticality of functions and the level of risk;
- prioritization of investments in measures that provide the maximum reduction of integral risk with minimum resource costs;
- combination of technical measures, such as redundancy, infrastructure modernization, and strengthened cybersecurity, with organizational measures, such as formalization of response procedures and personnel training;

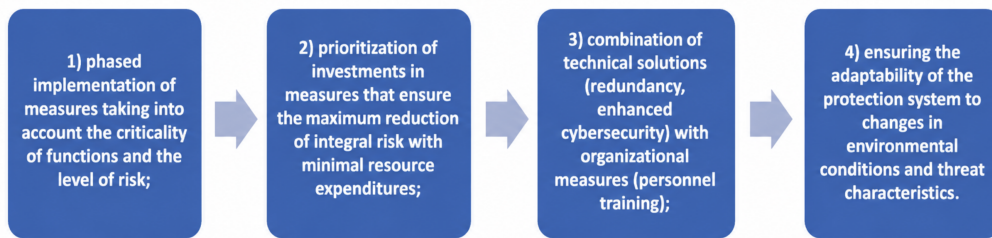


Figure 1: Practical recommendations for selecting a rational set of organizational and technical measures for protecting critical infrastructure facilities.

- ensuring the adaptability of the protection system to changes in environmental conditions and threat characteristics.

The formulated recommendations can be used by critical information infrastructure operators to make justified management decisions regarding the selection of rational strategies for enhancing the security level under conditions of military and hybrid threats.

5. Conclusions

This study proposed a method for enhancing the security level of critical information systems (CIS) through a comprehensive assessment of their security state based on the formalization of interrelationships among risk, reliability, and resilience. The proposed approach uses an integral security-level indicator that enables quantitative assessment of the current protection state, evaluation of the potential impact of threats, and justification of security enhancement strategies under resource constraints.

Unlike approaches that consider risk, reliability, or resilience as separate assessment dimensions, the proposed method integrates these parameters into a unified methodological framework. This makes it possible to assess the CIS security level more comprehensively and to support decision-making regarding the selection of rational organizational and technical protection measures.

The experimental study was conducted using the Automated Air Traffic Control System (ATCS) as a case study. This system was selected due to its high criticality, complex structure, and strict requirements for security, reliability, resilience, and operational continuity. Under martial law conditions, ATCS operations in Ukraine are limited; however, the aviation sector remains a strategically important element of the state's critical infrastructure, taking into account the prospects of restoring civil aviation, supporting defense and humanitarian needs, and ensuring further integration into the international aviation domain.

The obtained results confirmed the applicability of the proposed method for quantitative assessment of the CIS security level under real and potential threats. Based on the integrated assessment of risk, reliability, and resilience, the initial security state of the system was determined, corrective strategies were selected, and the improvement effect was calculated. The implementation of the selected strategies increased the integral security-level indicator and confirmed the effectiveness of the proposed approach.

In addition, the generalized verification across three transport-sector CIS demonstrated the broader applicability of the method. The method was verified for the automated air traffic control system, the railway traffic safety system, and the road traffic control system. In all three cases, the implementation of the selected strategies led to an increase in the integral security-level indicator. In the first case, the ATC system remained within the "Limited assurance" level, while the second and third cases demonstrated a transition from the "Limited assurance" level to the "Ensures" level. The improvement effect ranged from 4.9% to 26.1%, which confirms the effectiveness of the proposed strategies and the validity of resource allocation decisions.

Based on the experimental validation, practical recommendations were formulated for selecting a rational set of organizational and technical security measures. These recommendations include phased

implementation of measures according to the criticality of functions and risk level, prioritization of investments in measures that provide maximum reduction of integral risk with minimum resource costs, combination of technical and organizational measures, and ensuring adaptability of the protection system to changes in environmental conditions and threat characteristics.

Further research will focus on extending the validation of the proposed method to critical information systems in other sectors, including energy, finance, information and communication technologies, life-support services, healthcare, public administration, and security. This will make it possible to evaluate the universality of the method, adapt it to the specific characteristics of different sectors, and improve comprehensive security assurance for the state's critical infrastructure.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

- [1] Verkhovna Rada of Ukraine, Law of Ukraine “on critical infrastructure” no. 1882-ix, 2021. URL: <https://zakon.rada.gov.ua/laws/show/1882-20>.
- [2] Cabinet of Ministers of Ukraine, Resolution no. 1109 “certain issues of ensuring the security and resilience of critical infrastructure”, 2021. URL: <https://zakon.rada.gov.ua/laws/show/1109-2021-%D0%BF>.
- [3] Cabinet of Ministers of Ukraine, Resolution no. 518 “on approval of criteria for classifying objects into criticality categories”, 2022. URL: <https://zakon.rada.gov.ua/laws/show/518-2022-%D0%BF>.
- [4] Administration of the State Service of Special Communications and Information Protection of Ukraine, Methodology for assessing the security level of critical infrastructure facilities, 2025. URL: <https://zakon.rada.gov.ua/laws/show/z0375-25>.
- [5] V. Sydorenko, A. Maksymets, A model for ensuring the resilience of critical information systems under internal and external destabilizing factors, *Cybersecurity: Education, Science, Technology* 27 (2025) 560–571. doi:10.28925/2663-4023.2025.27.779.
- [6] Y. Mahmood, T. Afrin, Y. Huang, N. Yodo, Sustainable development for oil and gas infrastructure from risk, reliability, and resilience perspectives, *Sustainability* 15 (2023) 4953. doi:10.3390/su15064953.
- [7] J. Kong, C. Zhang, S. Simonovic, Optimizing the resilience of interdependent infrastructures to regional natural hazards with combined improvement measures, *Reliability Engineering & System Safety* 210 (2021) 107538. doi:10.1016/j.res.s.2021.107538.
- [8] D. Rehak, L. Flynnova, M. Hromada, C. Fuggini, The importance of resistance in the context of critical infrastructure resilience: An extension of the ciera method, *Systems* 11 (2023) 506. doi:10.3390/systems11100506.
- [9] Z. Hu, S. Gnatyuk, T. Okhrimenko, S. Tynymbayev, M. Iavich, High-speed and secure PRNG for cryptographic applications, *International Journal of Computer Network and Information Security* 12 (2020) 1–10. doi:10.5815/ijcnis.2020.03.01.
- [10] M. Mohd Safari, N. Masseran, M. Abdul Majid, Robust and efficient reliability estimation for exponential distribution, *Computers, Materials & Continua* 69 (2021) 2807–2824. doi:10.32604/cmc.2021.018815.
- [11] G. Irankunda, W. Zhang, M. Fernand, J. Zhang, Assessing the resilience of critical infrastructure facilities toward a holistic and theoretical approach: A multi-scenario evidence and case study, *Sustainability* 16 (2024) 8735. doi:10.3390/su16208735.
- [12] R. Murasov, Y. Melnyk, Assessment of cyberspace security of Ukraine's critical infrastructure facilities, *Modern Information Technologies* (2023) 98–112. URL: <https://sit.nuou.org.ua/article/view/280288>.

- [13] O. Sukhodolia, Resilience of Critical Energy Infrastructure and Community Vital Activity, Technical Report, National Institute for Strategic Studies, 2022.
- [14] N. Shevchenko, R. Plakhotniuk, Methodological approaches to assessing the resilience of critical infrastructure facilities under special economic conditions in ukraine, *Economic Reforms and Innovative Development Strategies* 14 (2024) 112–126.
- [15] S. Kyrylenko, V. Tyshchenko, Risk assessment models for critical infrastructure under armed conflict conditions, *Life Safety* 9 (2023) 74–88.
- [16] V. Sydorenko, S. Sydorenko, Method for enhancing the security level of the state's critical information systems, *Cybersecurity: Education, Science, Technique* 30 (2025) 500–510. doi:10.28925/2663-4023.2025.30.988.
- [17] J. S. Al-Azzeh, M. Al Hadidi, R. S. Odarchenko, S. Gnatyuk, Z. Shevchuk, Z. Hu, Analysis of self-similar traffic models in computer networks, *International Review on Modelling and Simulations* 10 (2017).
- [18] M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Y. Petrova, A. Chaplits, Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, in: *CEUR Workshop Proceedings*, volume 2255, 2018, pp. 193–204.
- [19] S. Smerichevska, L. Ivanenko, Z. Poberezhna, S. Smerichevskyi, T. Konrad, D. Dudko, Matrix-vector approach to assessing the competitiveness of logistics enterprises in the context of economic security and information risks, in: *CEUR Workshop Proceedings*, volume 4024, 2025, pp. 440–451.
- [20] O. Tretiakov, B. Khalmuradov, N. Kichata, A. Remska, An approach to quantitative assessment of the resilience of critical infrastructure facilities, *Control, Navigation and Communication Systems* 79 (2025) 178–183. doi:10.26906/SUNZ.2025.1.178-183.
- [21] International Federation of Air Traffic Controllers' Associations, Report on the ICAO Air Navigation Commission, Working Paper WP No. 05, 63rd IFATCA Annual Conference, Singapore, 2024. URL: https://ifatca.org/wp-content/uploads/WP5-_AMD.pdf.