I. J. Computer Network and Information Security, 2026, 5, 17-29
Published Online on October 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2026.05.02

Model for calculating the level of Cybersecurity of Critical Infrastructure Facilities

Sergiy Gnatyuk*
Faculty of Computer Science and Technology, State University "Kyiv Aviation Institute", Kyiv, Ukraine
State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine
E-mail: s.gnatyuk@kai.edu.ua
ORCID iD: https://orcid.org/0000-0003-4992-0564
*Corresponding author

Diana Yudina
Faculty of Computer Science and Technology, State University "Kyiv Aviation Institute", Kyiv, Ukraine
E-mail: diana.yudina22@gmail.com
ORCID iD: https://orcid.org/0000-0002-1277-8771

Received: March 3, 2026; Revised: April 2, 2026; Accepted: July 9, 2026; Published: October 8, 2026

Abstract: The article examines the problem of ensuring the cyber resilience of critical information infrastructure in the context of the global transformation of cyberattack methods and the growing role of foreign state actors in destabilizing critical systems. Given the unprecedented increase in the number of incidents and the emergence of new threat vectors associated with the use of artificial intelligence, traditional approaches to security assessment are becoming insufficient. This creates a critical need to develop tools for quantitatively calculating the level of critical information infrastructure cybersecurity in order to respond quickly to challenges and objectively predict risks. Based on a systematic analysis of international standards and frameworks, such as the National Institute of Standards and Technology Cybersecurity Framework, the article justifies the need for a formalized mathematical apparatus for the transition from a qualitative description of security measures to their quantitative measurement. The authors propose a hierarchical Multi-Criteria Decision Making model for calculating an integral indicator of the level of cybersecurity. This model is based on a synthesis of the theoretical-multiple approach, the Analytic Hierarchy Process, and non-compensatory gating thresholds. The mathematical apparatus allows for the inequality of different groups of cybersecurity measures to be taken into account by applying a system of weighting coefficients calculated on the basis of expert assessments using the Saaty scale. The development process includes eight distinct stages, from determining criteria sets to integrating non-compensatory gating mechanisms to prevent technical deficiencies from being masked by administrative achievements. Experimental testing of the model was conducted using a representative critical infrastructure facility grounded in anonymized real-world audit data from the energy sector. The results confirmed the model's effectiveness, yielding an integral indicator of 0.56, while specifically identifying the detection domain as a vulnerable segment with a score of 0.36. This confirms the practical significance of the model for supporting management decisions on priority resource allocation.

Index Terms: Cybersecurity, Cybersecurity Level, Critical Information Infrastructure Facility, Model, Criteria System.

1. Introduction

The current architecture of global cybersecurity is characterized by an unprecedented intensification of threats and a fundamental transformation of attack methods. Analysis of current data from the European Union Agency for Cybersecurity (ENISA) shows not only a quantitative increase in incidents, but also a significant qualitative change in their nature. Traditional attack vectors are gradually being replaced by complex campaigns based on automation and artificial intelligence tools to scale the destructive impact on critical infrastructure. The cyber resilience of critical infrastructure is becoming a central element of national security, as the energy and transport sectors are among the top three in terms of the number of attacks [1].

The Microsoft Digital Defense Report 2025 highlights the growing role of foreign state-sponsored actors in destabilizing energy and government systems. Researchers note the implementation of cognitive artificial intelligence technologies to automate offensive operations, enabling attackers to carry out attacks with a high degree of adaptability

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

and unprecedented reach [2].

At the same time, the systemic problem of technological vulnerability of CII is detailed in the IBM X-Force Threat Intelligence Index 2025. According to the monitoring results, more than 25% of successful compromises are the result of exploiting outdated systems and slow patch management cycles for critical software [3]. The destructive potential of such incidents is confirmed in the Verizon Data Breach Investigations Report (DBIR) 2025 [4], which notes a record increase in ransomware activity in strategic sectors of the economy. This trend indicates the evolution of cybercrime from the theft of confidential information to full-fledged cyberterrorism aimed at blocking vital services.

The problem is particularly acute in Ukraine, where there has been an intense quantitative and qualitative increase in cyber threats. According to official statistics from the National Computer Emergency Response Team of Ukraine (CERT-UA), 3018 cyber incidents were processed during the first half of 2025, which is 74% more than in the same period of the previous year (1739 incidents) [5-6]. The priority threats recorded by the CERT-UA remain the spread of malware, phishing campaigns, and the compromise of accounts and systems [5].

The convergence of conclusions from leading international analytical institutions and national regulators confirms the urgent need for a conceptual review of CII cybersecurity strategies. In today's cyberspace, where countermeasure resources are typically limited, the ability to objectively identify the most vulnerable segments of infrastructure is critical. This necessitates an accurate assessment of the current state of CII cybersecurity, which is a prerequisite for determining priority areas of protection and the effective allocation of resources.

An urgent scientific and practical task is to develop a mathematical model for calculating the level of cybersecurity of CII. Existing approaches are often limited to a qualitative description or a simple list of protection measures, which does not allow for an accurate quantitative indicator of cybersecurity of CII. The key problem lies in the absence of a formalized mathematical apparatus that would allow for the hierarchical ordering of heterogeneous cybersecurity criteria and take into account their inequality through a system of weighting coefficients. This necessitates a model that synthesizes the results of assessing technical and organizational measures with expert analysis methods to form an objective integral indicator of the level of cybersecurity.

2. Background

An analysis of scientific and methodological research shows that there are a significant number of approaches to assessing the level of cybersecurity. To solve security monitoring and auditing tasks, the international community uses standards, frameworks, and maturity models, in particular ISO/IEC 27001:2022, which defines the requirements for information security management systems (ISMS) and their continuous optimization [7], NIST Cybersecurity Framework 2.0 (NIST CSF 2.0), which structures cybersecurity as a set of functional domains from identification to strategic risk management [8-9], Capability Maturity Model Integration (CMMI) as a generalized approach to assessing process maturity [10], Cybersecurity Capability Maturity Model (C2M2) as a model of cybersecurity capability maturity for electrical networks [11], Smart Grid Maturity Model (SGMM) as a strategic planning and management tool that helps assess the current state of cybersecurity for the creation of “smart grids” [12], and CISA Cybersecurity Performance Goals (CPGs) as goal-oriented indicators developed by the Cybersecurity and Infrastructure Security Agency (CISA) [13].

Although these studies offer substantive content, the question of their adaptability to the conditions of CII functioning in Ukraine remains relevant.

The authors propose to classify existing approaches according to their focus on cybersecurity management. Researchers Blessing Reuben-Owoh and Ella Haig emphasize in their review that different categories of standards and frameworks have significantly different properties and areas of application [14].

The first group consists of process-oriented standards, led by ISO/IEC 27001. These standards focus on creating a formal information security management system (ISMS), which is fundamental to the stability of an organization and its ability to continuously improve [7]. However, researchers Shevchenko S. M., Zhdanova Yu. D., and Kiy O. S. emphasize that such standards often suffer from excessive formalism and a focus on compliance: compliance with standards can be achieved without a significant increase in technical resistance to targeted attacks (APT threats) [15].

The second group consists of maturity assessment models (e.g., CMMI, C2M2, SGMM). As noted by Alenka Baggia and Alenka Brezavšček, models of this type are effective for strategic planning of cybersecurity development over long periods of time and allow for the gradual build-up of an organization's capabilities [16]. However, as Büyüközkan Gülçin and Güler Merve note, the complexity of implementing such models (in particular CMMI) often becomes a barrier for medium and even large enterprises operating in conditions of limited resources and a shortage of qualified personnel [17].

The third group consists of functional-outcome frameworks and objectives, such as NIST CSF and CISA CPGs, which, according to the authors [9], are focused on achieving specific cybersecurity outcomes. These approaches focus not only on processes but also on specific functional outcomes, making them more flexible than formal standards. In particular, the latest version of NIST CSF 2.0, released in 2024, includes a governance function (Govern) that strengthens the management component of organizational security and makes the framework more adaptable to new types of threats [18].

To objectify the choice of the modeling basis, a comparative analysis of key approaches was conducted using a system of defined criteria, in particular: Descriptiveness (DS) is the descriptive nature without establishing specific requirements or standards; Flexibility (FX) is the ability to adapt or change rules, requirements, or recommendations in accordance with specific conditions, situations, or needs; Integration (IN) is the possibility of integration with other standards and guidelines; Ease of Implementation (EI) is the ease of implementation in terms of the time and resources required to meet specific requirements; Jurisdictional Relevance (JR) is the degree of compliance of the document with the current legislation of Ukraine (in particular, the requirements of the Resolution of the Cabinet of Ministers of Ukraine No. 1426 of 29.12.2021), national terminology, the structure of management bodies, and the context of CII; and Contextual Relevance (CR) is the degree to which the document complies with the context of the CII's activities, reflecting how well the document fits into the real conditions, operational needs, and specific risks of a particular CII [19].

Table 1. Comparative analysis of approaches to cybersecurity assessment.

Approach / Criterion	DS	FX	IN	EI	JR	CR
ISO/IEC 27001:2022	Low	Medium	High	Low	Medium	Medium
NIST CSF 2.0	High	High	High	Medium	Medium	High
CMMI / C2M2	High	Low	Medium	Low	Low	Medium
CISA CPGs	Low	Medium	Low	High	Low	Medium
SGMM	High	Low	Low	Low	Low	High

The comparison results show that NIST CSF 2.0 is the most balanced option for building a model for assessing the level of cybersecurity of CII. Its descriptiveness allows it to cover a wide range of measures without imposing strict restrictions, and its high flexibility makes it possible to tailor it to the needs of a specific organization. Of particular importance is the ability to integrate NIST CSF 2.0 with other guidelines, allowing specific industry requirements, including domestic regulations, to be layered on top of it [15].

However, the choice of NIST CSF 2.0 comes with certain challenges. First, the framework has limited jurisdictional relevance to Ukrainian legislation in its basic form, as it does not use legally established domestic terms and norms and does not take into account the structure of the national cybersecurity system. Second, contextual relevance requires additional refinement: the framework is general and does not contain specific parameters for industrial control systems (ICS/SCADA) characteristic of certain critical infrastructure sectors (e.g., the fuel and energy sector).

The most significant drawback of NIST CSF 2.0 in the context of calculating the level of cybersecurity is the lack of a mathematically sound mechanism for aggregating indicators. The standard provides a qualitative description of the results but does not contain equations for determining the final coefficient, which may lead to subjectivity in the assessment of information security by different auditors. It is this methodological gap that necessitates the development of an author's model that would preserve the advantages of NIST CSF 2.0 and supplement them with a rigorous mathematical apparatus.

Thus, the analysis of publications and current standards confirms the feasibility of using the NIST CSF 2.0 structure as a hierarchical basis. However, in order to obtain an objective result, this basis needs to be supplemented with a mathematical component — in particular, a theoretical set description and an Analytic Hierarchy Process (AHP) — to take into account the inequality of cybersecurity measures and their specificity.

The purpose of the article is to develop and experimentally confirm a mathematical model for calculating the integral indicator of the level of cybersecurity of CII, which takes into account the inequality of security measures through a system of weighting coefficients.

3. Development of a Model for Calculating the Level of Cybersecurity of CII

The proposed methodological approach is designed as a hierarchical multi-criteria decision-making (MCDM) framework. Unlike traditional audit tools, this model formalizes the transition from qualitative expert judgments to a quantitative metric space. The mathematical core of the model is a structured synthesis of heterogeneous indicators that accounts for both local functional significance (v_{ij}) and global strategic priorities (w_i), thereby mitigating the subjectivity and "false precision" inherent in critical infrastructure assessments. The development of the model includes several stages:

Stage 1. Determining the set of criteria (SC)

A theoretical set approach was used to formalize the process of building a model for calculating the level of cybersecurity of CII. A set of criteria (*SC*) was introduced, covering groups of cybersecurity measures:

$$SC = \{\cup_{i=1}^{n} SC_i\} = \{SC_1, SC_2, \dots, SC_n\}, \quad (1)$$

where $SC_i \subseteq SC(i = \overline{1,n})$ is the identifier of the corresponding criteria subsystem.

Stage 2. Determination of a subset of parameters for each group of cybersecurity measures (SC_i)

Each system of criteria is characterized by a subset of detailed parameters:

$$SC_i = \left\{\bigcup_{j=1}^{k_i} S\,C_{ij}\right\} = \{SC_{i1}, SC_{i2}, \dots, SC_{ik_i}\}, \quad (2)$$

where $SC_i \subseteq SC_{ij}(j = \overline{1,k_j})$ is a subset of parameters of the *i*-th class of cybersecurity measures. The number of parameters k_i varies depending on the specific system.

Stage 3. Developing detailed cybersecurity measures in the form of performance indicators

At this stage, the parameters are transformed into specific verification indicators (criteria) that correspond to cybersecurity measures. The complete set of indicators for the criteria system is presented as follows:

$$SC = \left\{\bigcup_{i=1}^{n} \bigcup_{j=1}^{k_i} SC_{ij}\right\}, \quad (3)$$

where each element SC_{ij} corresponds to a specific question (for example, SC_{21} – "Has an official responsible for cybersecurity been appointed?").

Stage 4. Introduction of quantitative characteristics to formalize the result.

To ensure the granularity of the assessment and capture the nuances of security measure implementation, the model utilizes a five-level maturity-based scoring scale for each cybersecurity measure SC_{ij}:

"Full implementation" (the measure is fully implemented and operational) – 1.0;
"Partial implementation" (the measure is in the testing phase or has minor non-critical deviations) – 0.5;
"Planned/In progress" (implementation is officially documented, scheduled, and budgeted) – 0.2;
"Negative/Insufficient evidence" (the measure is missing, ineffective, or lacks documentary proof) – 0;
"Not applicable" (the measure is not required due to specific technical architecture) – 0.

Stage 5. Determination of the primary level of cybersecurity of CII in the form of a quantitative indicator.

To determine the initial level of cybersecurity of the CII facility, primary indicators are calculated for each functional group of measures. The primary integrated level is derived through a hierarchical aggregation framework, which ensures the necessary analytical depth by integrating diverse security controls into a mathematically consistent indicator. By introducing local significance coefficients, the model moves beyond simple weighted averages, allowing for a weighted representation of the security posture:

$$SA_{SC} = \frac{\sum_{i=1}^{n} SA_{SC_i}}{n}. \quad (4)$$

To account for the functional inequality of individual cybersecurity measures within a single subsystem, a weighted aggregation rule is applied. This ensures that foundational technical measures have a proportionately greater impact on the final result than supplementary or administrative procedures. The score for each class of cybersecurity measures is calculated as follows:

$$SA(SC_i) = \sum_{j=1}^{k_i} v_{ij} \times SC_{ij}, \quad (5)$$

where SC_{ij} is the local significance coefficient of the *j*-th measure within the *i*-th subsystem, satisfying the normalization condition $\sum_{j=1}^{k_i} v_{ij} = 1$;

SC_{ij} is the quantitative score of the measure (0; 0.2; 0.5; 1.0) assigned according to the maturity scale defined in Stage 4;

k_i is the total number of parameters in the *i*-th subsystem.

Taking into account the local weighting introduced in (5), the expanded equation for the primary level calculation (6) is represented as:

$$SA_{SC} = \frac{\sum_{i=1}^{n} \sum_{j=1}^{k_i} v_{ij} \times SC_{ij}}{n}, \quad (6)$$

where $SA(SC_i)$ is the weighted mean indicator of the criteria system SC_i.

The resulting indicator SA_{SC} represents the baseline cybersecurity state of the CII facility before applying the global priority weights (which are addressed in Stage 6). Due to the normalization of both maturity scores and significance coefficients, the final primary indicator remains within the range from 0 to 1, where 1 represents the ideal implementation of all prioritized measures.

Stage 6. Input of weighting coefficients for the criteria system

Since different groups of measures have different impacts on the overall sustainability of an object, the Analytic Hierarchy Process (AHP) is used to calculate weighting coefficients (w_i). This method allows for the decomposition of a complex decision problem into a multi-level hierarchical structure, ensuring mathematical rigor in prioritizing heterogeneous security controls [20]. To ensure the objectivity and analytical reliability of the weights, the model involves an expert panel. The selection criteria for experts include a minimum of 10 years of professional experience in cybersecurity or critical infrastructure protection and relevant academic (Ph.D.) or industry certifications (e.g., CISA, CISSP). The expert group conducts pairwise comparisons of criteria systems using the standardized fundamental Saaty scale, which ranges from 1 to 9. Since the assessment is carried out by a group of independent experts, the key stage is the mathematical aggregation of individual judgments to reach a consensus. Each expert forms their own matrix of pairwise comparisons A_k. To obtain a single aggregated matrix A_{agr} the principle of combining individual judgments is applied using the geometric mean, which preserves the property of matrix reciprocity.

The assessments are consolidated by calculating the geometric mean for each element among all experts:

$$\overline{a}_{ij} = \frac{\prod_{k=1}^{N} a_{ij,k}}{N}, \tag{7}$$

where N is the total number of experts;

$a_{ij,k}$ is a judgment of the k-th expert regarding the comparison of criteria i and j.

Based on the obtained aggregated matrix A_{agr} a mathematical calculation of the priority vector (w_i) is performed by normalizing the matrix and averaging the rows:

$$w_i = \frac{1}{n}\sum_{j=1}^{n} \frac{a_{ij}}{\sum_{l=1}^{n} a_{lj}}, \tag{8}$$

where n is the total number of criteria being compared.

To verify the reliability and auditability of expert judgments, the Consistency Ratio (CR) is calculated. First, the Consistency Index (CI) is determined:

$$CI = \frac{\lambda_{max} - n}{n-1}, \tag{9}$$

where λ_{max} is the maximum eigenvalue of the matrix.

The final Consistency Ratio is:

$$CR = \frac{CI}{RI} \tag{10}$$

where RI is the Random Index for a matrix of order n.

This vector, after verification of its consistency (where $CR \leq 0.1$), is used as a normalized weight coefficient for the corresponding system of criteria in the equation for calculating the integral indicator.

Stage 7. Determination of the integral indicator of the level of cybersecurity of CII

The final result of the model is an integral quantitative indicator (SA_{SC}^{w}), which synthesizes the initial assessments of subsystems and their weight coefficients:

$$SA_{SC}^{w} = \sum_{i=1}^{n} w_i \times SA_{SC_i}, \tag{11}$$

where SA_{SC}^{w} is the integral indicator of the level of cybersecurity of CII;

w_i is the weight coefficient for the i-th system of criteria (SC_i).

The synthesis of local priorities into a global integral indicator follows the additive composition principle fundamental to the AHP framework [20].

The general structure of the developed model is presented in Fig. 1.

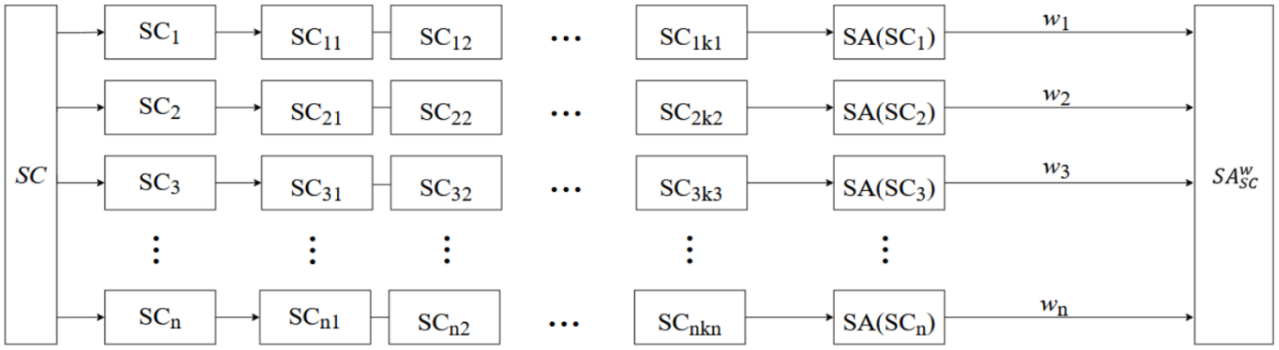


Fig. 1. Model for calculating the level of cybersecurity of CII.

Figure 1 shows the hierarchical structure of the model, which allows calculating the integral indicator of the level of cybersecurity of CII (SA_{SC}^{w}) by aggregating data from individual subsystems of criteria. The diagram shows the process of transforming primary maturity-based indicators (SC_{ij}) into local average estimates (SA_{SC_i}), which are weighted using expert coefficients (w_i) to obtain an objective final result.

The thresholds for the five-level interpretation scale (Table 2) were defined through a structured calibration process combining expert elicitation and alignment with established maturity models, including Capability Maturity Model Integration (CMMI) and Cybersecurity Capability Maturity Model [10,11]. A panel of domain experts (n = 5) applied a modified Delphi method to identify consensus-based cutoff points corresponding to meaningful transitions in cybersecurity capability, a widely used approach for structuring expert judgment in the absence of complete empirical data [21,22].

The selected thresholds represent key maturity shifts: 0.46 indicates the transition to consistently defined controls across domains, 0.71 reflects the introduction of monitoring and measurable performance indicators, and 0.90 corresponds to continuous optimization and adaptive security practices. Sensitivity analysis demonstrated that moderate variations in thresholds (±0.05) do not significantly affect classification outcomes, supporting robustness of the scale (cf. Sensitivity Analysis).

While the scale was qualitatively cross-validated against audit assessments and simulated risk scenarios, it should be interpreted as partially heuristic. This is consistent with prior work on cybersecurity metrics and maturity assessment, where expert-based calibration is commonly applied in the absence of longitudinal incident data (e.g., National Institute of Standards and Technology frameworks). Further empirical validation using incident and breach data is recommended to strengthen generalizability.

Table 2. Scale for interpreting the integrated indicator of the level of cybersecurity of CII.

Scale levels	Range of the obtained indicator
Initial/unacceptable (critical)	0 – 0.2
In the process of development/low level	0.21 – 0.45
Defined/average level	0.46 – 0.7
Controlled/high level	0.71 – 0.89
Optimized/excellent level	0.9 – 1

Stage 8. Integration of non-compensatory gating thresholds.

To ensure the model's suitability for safety-critical environments, a non-compensatory gating mechanism is integrated into the assessment framework, based on the fundamental principles of the outranking approach developed by B. Roy [23]. This prevents the "compensability effect," where high scores in administrative domains might offset critical technical deficiencies. In addition to the weighted aggregate score (SA_{SC}^{w}), minimum safety thresholds are applied to core functional domains:

Critical Threshold (0.20): Corresponds to the "Initial" maturity level. Any core subsystem score below this value triggers an automatic downgrade of the entire facility to "Critical," regardless of the aggregate index.

Warning Threshold (0.40): Flags high-risk conditions that require immediate remediation but do not yet trigger a full classification override.

The interpreted integrated indicator of the level of cybersecurity of CII will allow for an objective assessment of the state of CII and identify deviations from the “optimized” level. This information is the basis for the development and implementation of effective strategies and measures aimed at improving the level of cybersecurity.

4. Experimental Study of a Model for Calculating the Level of Cybersecurity of CII

To confirm the effectiveness of the developed model, an experimental study was conducted based on a

representative model of a critical information infrastructure facility in the fuel and energy sector. While security constraints and non-disclosure agreements regarding CII protection prevent the publication of the specific organization's identity, the study utilizes anonymized data derived from real-world cybersecurity audits. The parameters used for the assessment reflect the actual operational environment of the Ukrainian energy grid. This approach ensures that the validation is not merely illustrative but demonstrates the model's practical reliability in processing heterogeneous data from functioning industrial control systems (ICS).

The study was implemented in three stages: determining weight coefficients using an expert method, conducting an internal audit, and calculating the integral indicator.

Before starting the experimental study of the model for calculating the level of cybersecurity of CII, a system of criteria (SC), subsystems of criteria (SC_i) and detailed parameters (SC_{ik_i}) were defined.

The system of criteria (SC), subsystem of criteria (SC_i) and detailed parameters (SC_{ik_i}) are based on six functions with 22 corresponding categories and 106 measures recommended for use in the NIST Cybersecurity Framework 2.0.

Thus, the following data were obtained:

Table 3. Description of the criteria system.

System of criteria	Name of the criteria system	Meaning k_i	Criteria indicators	Criteria
SC_2	GV = "Govern"	$k_2 = 31$	$SC_{2.1}, SC_{2.2}, \dots, SC_{2.31}$	GV.OC-01, GV.OC-02, GV.OC-03, GV.OC-04, GV.OC-05, GV.RM-01, GV.RM-02, GV.RM-03, GV.RM-04, GV.RM-05, GV.RM-06, GV.RM-07, GV.RR-01, GV.RR-02, GV.RR-03, GV.RR-04, GV.PO-01, GV.PO-02, GV.OV-01, GV.OV-02, GV.OV-03, GV.SC-01, GV.SC-02, GV.SC-03, GV.SC-04, GV.SC-05, GV.SC-06, GV.SC-07, GV.SC-08, GV.SC-09, GV.SC-10
SC_3	ID = "Identify"	$k_3 = 21$	$SC_{3.1}, SC_{3.2}, \dots, SC_{3.21}$	ID.AM-01, ID.AM-02, ID.AM-03, ID.AM-04, ID.AM-05, ID.AM-07, ID.AM-08, ID.RA-01, ID.RA-02, ID.RA-03, ID.RA-04, ID.RA-05, ID.RA-06, ID.RA-07, ID.RA-08, ID.RA-09, ID.RA-10, ID.IM-01, ID.IM-02, ID.IM-03, ID.IM-04
SC_4	PR = "Protect"	$k_4 = 22$	$SC_{4.1}, SC_{4.2}, \dots, SC_{4.22}$	PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AA-06, PR.AT-01, PR.AT-02, PR.DS-01, PR.DS-02, PR.DS-10, PR.DS-11, PR.PS-01, PR.PS-02, PR.PS-03, PR.PS-04, PR.PS-05, PR.PS-06, PR.IR-01, PR.IR-02, PR.IR-03, PR.IR-04
SC_5	DE = "Detect"	$k_5 = 11$	$SC_{5.1}, SC_{5.2}, \dots, SC_{5.11}$	DE.CM-01, DE.CM-02, DE.CM-03, DE.CM-06, DE.CM-09, DE.AE-02, DE.AE-03, DE.AE-04, DE.AE-06, DE.AE-07, DE.AE-08
SC_6	RS = "Respond"	$k_6 = 13$	$SC_{6.1}, SC_{6.2}, \dots, SC_{6.13}$	RS.MA-01, RS.MA-02, RS.MA-03, RS.MA-04, RS.MA-05, RS.AN-03, RS.AN-06, RS.AN-07, RS.AN-08, RS.CO-02, RS.CO-03, RS.MI-01, RS.MI-02
SC_7	RC = "Recover"	$k_7 = 8$	$SC_{7.1}, SC_{7.2}, \dots, SC_{7.8}$	RC.RP-01, RC.RP-02, RC.RP-03, RC.RP-04, RC.RP-05, RC.RP-06, RC.CO-03, RC.CO-04

At the same time, in order to take into account the specific industry requirements for cybersecurity of the fuel and energy sector, it is proposed to add one system of criteria:

$$SC_1 = SE_{FE} = "Sectoral\ component\ of\ the\ fuel\ and\ energy\ sector".$$

The sectoral subsystem consists of five indicators that reflect the unique operational and legal environment of the Ukrainian energy sector. The justification for these indicators is based on a three-tier approach:

1. Regulatory Compliance (FE_1, FE_2): these criteria are strictly derived from Order No. 338 and Order No. 285 of the Ministry of Energy of Ukraine, which mandate periodic cybersecurity reviews and specific protection measures for electrical networks.

2. National Strategic Cooperation (FE_3): this indicator aligns with the Law of Ukraine "On the Basic Principles of Ensuring the Cybersecurity of Ukraine", which requires CII facilities to establish information-sharing mechanisms with national authorities (CERT-UA) and sectoral partners.

3. Operational Technology (OT) Resilience (FE_4, FE_5): these criteria address the technical specificity of the energy sector, focusing on the ability to restore heavy industrial systems after a blackout and the necessity of specialized training for personnel working with SCADA/ICS environments, which is often underrepresented in general IT frameworks.

Table 4. Representation of the criteria system "Sectoral component of the fuel and energy sector".

Name of the criteria system	Meaning k_i	Criteria
SE_{FE} = "Sectoral component of the fuel and energy sector"	$k_1 = 5$	FE_1 – "Has a comprehensive assessment of your CII been carried out in accordance with Order No. 338 of the Ministry of Energy of Ukraine dated September 10, 2024, "On Approval of the Procedure for Reviewing the Cybersecurity Status of the Fuel and Energy Sector of Critical Infrastructure"?"; FE_2 – "Has an assessment of the cybersecurity status of electrical networks been carried out in accordance with Order No. 285 of the Ministry of Energy of Ukraine dated August 5, 2024, "On Approval of the Methodology for Assessing the Cybersecurity Status of Electrical Networks and Cybersecurity Practices for Electrical Networks"?"; FE_3 – "Are there mechanisms for sharing information about cyber threats with other entities in the energy sector?"; FE_4 – "Can your CII effectively restore normal operation of energy systems after a large-scale cyberattack aimed at disabling critical infrastructure?"; FE_5 – "Does operational personnel working with OT systems receive specialized cybersecurity training that takes into account the characteristics and risks of industrial systems?".

As a result, a list of criteria (*SC*), subsystem of criteria (SC_i) and detailed parameters (SC_{ik_i}) was obtained.

Step 1. Calculation of weight coefficients (w_i).

For this study, a panel of seven independent experts meeting the criteria defined in Stage 6 was formed. They conducted pairwise comparisons of seven criteria systems using the Saaty scale. The individual judgments were aggregated using the geometric mean (7) to form the consensus matrix shown in Table 5. The consistency of the judgments was verified: the calculated Consistency Ratio is *CR*=0.068 (where λ_{max}=7.542; *CI*=0.090; *RI*=1.32), which confirms the high reliability of the obtained weights.

Table 5. Aggregated pairwise comparison matrix and weights for criteria systems.

Criteria	SC_1	SC_2	SC_3	SC_4	SC_5	SC_6	SC_7	Weight (w_i)
SC_1	1	1.84	1.22	0.34	0.98	1.12	1.76	0.134
SC_2	0.54	1	0.82	0.24	0.64	0.72	1.44	0.082
SC_3	0.82	1.22	1	0.28	0.88	0.94	1.28	0.104
SC_4	2.94	4.17	3.57	1	2.82	3.14	4.84	0.312
SC_5	1.02	1.56	1.14	0.35	1	1.18	1.68	0.141
SC_6	0.89	1.39	1.06	0.32	0.85	1	1.72	0.132
SC_7	0.57	0.69	0.78	0.21	0.60	0.58	1	0.095

Step 2. Collection and processing of primary data.

A checklist of indicators (SC_{ij}) was completed by means of a questionnaire and verification of the facility's documentation. The results of the calculation of estimates (SA_{SC_i}), according to (5), are presented in the table below:

Table 6. Results of calculating initial cybersecurity indicators for each subsystem.

Subsystem	Number of criteria (k_i)	Measures implemented	Indicator (SA_{SC_i})
$SC_1(SE)$	5	3	0.60
$SC_2(GV)$	31	18	0.58
$SC_3(ID)$	21	15	0.71
$SC_4(PR)$	22	12	0.54
$SC_5(DE)$	11	4	0.36
$SC_6(RS)$	13	7	0.53
$SC_7(RC)$	8	6	0.75

Step 3. Determination and interpretation of the integral indicator

Using (11), the final integral indicator of the level of cybersecurity was calculated:

$$SA_{SC}^{w} = (0.15 \times 0.60) + (0.10 \times 0.58) + (0.12 \times 0.71) + (0.25 \times 0.54) + (0.15 \times 0.36) + (0.15 \times 0.53) + (0.08 \times 0.75) = 0.56$$

Analysis of results.

The resulting score of 0.56 according to the developed five-level scale (Table 2) corresponds to the "Defined/Average Level" (range 0.46–0.7). The analysis revealed that the most critical area of the CII is "Detect" (SC_5 with a score of 0.36), despite high recovery readiness scores (SC_7). The experiment proved that the model allows not only to obtain an overall assessment, but also to accurately identify priority areas for strengthening the cybersecurity of

CII.

Step 4. Robustness and Sensitivity Analysis

To verify the stability of the developed model and minimize potential expert bias, a sensitivity analysis was conducted. The procedure involved perturbing the weighting coefficients within a range of their original values.

The analysis demonstrated that despite the variations in weights, the hierarchical ranking of the criteria systems remained unchanged. Specifically, the "Protect" (SC_4) and "Detect" (SC_5) domains consistently maintained their status as the most critical subsystems. Furthermore, a 10% shift in the highest weight (w_4) resulted in only a 3.4% change in the final integrated indicator. This confirms that the model is robust against minor fluctuations in expert judgments and provides reliable results for cybersecurity assessment in the energy sector.

5. Discussion and Comparative Validation

To evaluate the effectiveness of the proposed hierarchical MCDM model, a benchmark comparison with a traditional arithmetic mean approach, commonly used in checklist-based assessments, was conducted. While the baseline method produced a similar aggregate score (0.58), it failed to reflect the critical imbalance across functional domains. In contrast, the proposed model yielded a lower score (0.56) by explicitly weighting domain importance and penalizing deficiencies in the 'Detect' subsystem, thereby providing greater diagnostic sensitivity rather than merely aggregate equivalence.

The reliability of expert judgments was assessed within the Analytic Hierarchy Process framework using the Consistency Ratio (CR=0.068), which satisfies the accepted threshold (CR<0.1). This indicates a high level of internal consistency in pairwise comparisons. In addition, the stability of results was supported by low variance in expert-provided weights ($\sigma^2 < 0.02$), suggesting convergence of independent evaluations.

Although direct longitudinal incident data were not available, the model's output demonstrates construct and face validity. In particular, the identification of the 'Detect' function as the weakest component (0.36) is consistent with established cybersecurity findings, where insufficient detection capability is associated with prolonged attacker dwell time and increased incident impact. This alignment with widely observed industry patterns supports the plausibility of the model's risk representation.

The application of the non-compensatory gating mechanism allows the model to avoid the "compensability effect", following the logic of veto thresholds and outranking relations [23]. In the evaluated case, the 'Detect' score (0.36) does not breach the critical failure threshold (0.20) but falls within the warning range (< 0.40). Therefore, while the aggregate score (0.56) supports a "Defined" classification, it is interpreted with explicit constraints. The system is marked as conditionally acceptable, highlighting that the overall security posture is heavily dependent on urgent improvements in detection capabilities to prevent an automatic classification override.

Compared to a simple checklist approach, which obscures critical weaknesses through averaging, the proposed indicator enhances interpretability and prioritization of risk. Nevertheless, the absence of direct empirical validation using incident datasets remains a limitation. Future work will focus on validating the model against historical incident records and benchmarking its predictive capability against alternative assessment methods.

The results of the experimental study confirm the hypothesis that the use of an integral indicator weighted by expert assessments provides a more accurate view of the level of cybersecurity of CII than a simple quantitative summation of the measures implemented.

To clearly show the strengths and weaknesses of the CII cybersecurity system, it's a good choice to use a radial chart. It lets you compare the actual assessment values with the ideal state for each cybersecurity subsystem.

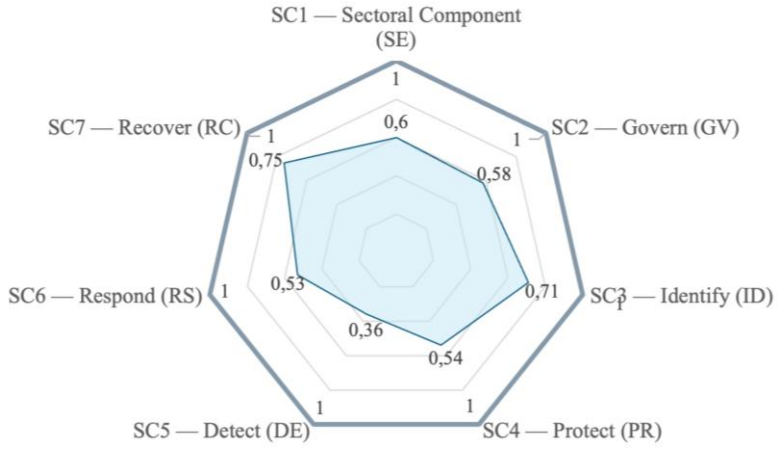


Fig. 2. Results of calculating the integral level of cybersecurity for each subsystem.

Fig. 2 demonstrates asymmetry in the security system. High scores in the "Recovery" (0.75) and "Identify" (0.71) subsystems indicate that an asset inventory database has been established and that backup procedures are in place. However, a critical gap in the "Detect" subsystem (0.36) indicates the absence of security information and event management (SIEM) systems or insufficient staff qualifications in anomaly analysis. This creates a situation where the CII is ready to recover after an attack but is unable to detect it in time, which increases the time the attacker spends on the network.

An important feature of the proposed model is the implementation of AHP. When using the simple arithmetic mean method, the cybersecurity level indicator is 0.58. However, the calculation according to the developed model shows a lower indicator, which is 0.56. This difference is due to the logic of the model: the final indicator is not a simple sum of indicators but depends on their priority. The algorithm provides for a priority-based weighted adjustment, which lowers the overall indicator if significant deficiencies are found in key subsystems. Thus, low scores in critically important domains have a greater negative impact on the overall level. In particular, low scores in the categories of "Protect" (weighting coefficient 0.312) and "Detect" (0.141) significantly offset high achievements in less important subsystems, ensuring high representativeness and relevance of the obtained integrated indicator to the actual state of cybersecurity.

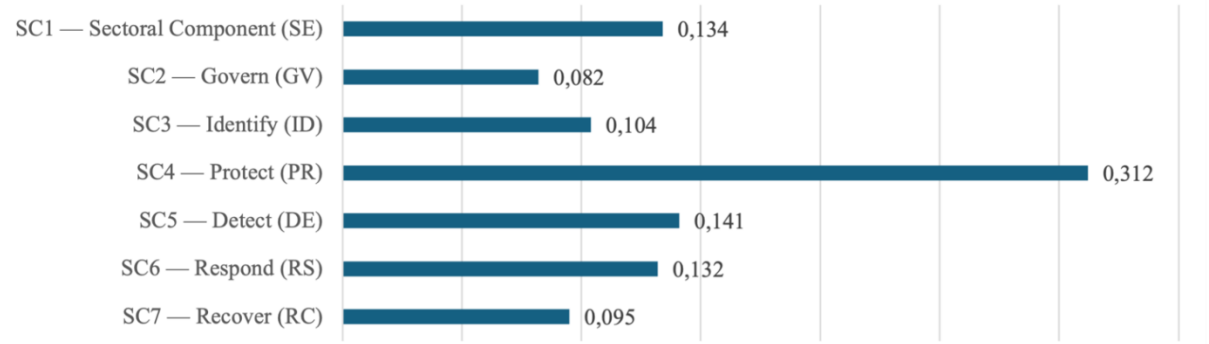


Fig. 3. Distribution of subsystem influence on the integral indicator (weight coefficients).

Analysis of the obtained weight coefficients (Fig. 3) indicates the hierarchy of priorities determined by the expert community for the object under study. It is important to note that the use of AHP allows the model to flexibly adapt to the specifics of different objects: a change in expert judgments will lead to a redistribution of weight coefficients, which will change the level of influence of each subsystem.

Visualization of the calculated integral indicator on a five-level scale (Fig. 4) allows one to move from an abstract quantitative value to a qualitative assessment of the state of cybersecurity of the CII. The resulting indicator (0.56) localizes the state of the CII within the "Defined/Medium Level" (range 0.46–0.7), which graphically corresponds to the yellow segment of the scale.

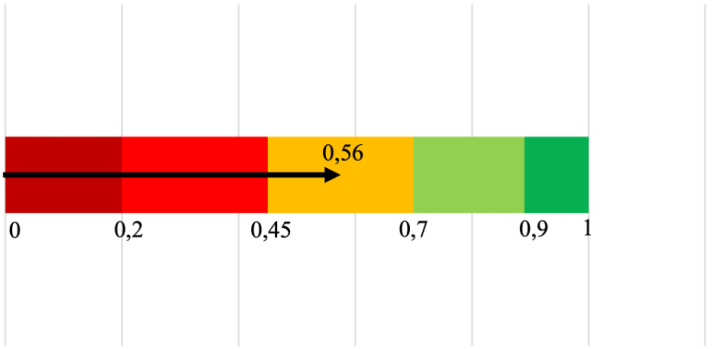


Fig. 4. Visualization of the integral indicator on a five-level scale.

Thus, graphical interpretation of the results serves as a tool to support management decision-making by visualizing the gap between the current state (0.56) and the target state of cybersecurity (1). This confirms the practical significance of the developed model as a basis for optimizing the distribution of CII resources aimed at achieving cybersecurity targets within the "optimized" (green) sector.

6. Conclusion

As a result of the study, a mathematical model for assessing the cybersecurity level of critical infrastructure was

developed, based on a synthesis of the Multi-Criteria Decision Making (MCDM) approach and the Analytic Hierarchy Process. The proposed framework provides a structured and transparent mechanism for translating qualitative security assessments into a quantitative metric.

Through the application of expert-based weighting coefficients and verification of the Consistency Ratio (CR = 0.068), the model reduces the influence of individual evaluator bias compared to non-weighted checklist approaches. The experimental application demonstrated its ability to identify critical technical imbalances, such as the detection gap (0.36) observed in the case study.

The introduction of non-compensatory gating thresholds further provides safeguards against the masking of critical technical weaknesses by higher scores in other domains, supporting a safety-oriented interpretation of results. The model should therefore be considered a decision-support tool for prioritizing cybersecurity improvements and resource allocation in critical infrastructure contexts, rather than a predictive instrument.

Future research will focus on empirical validation using longitudinal incident data and benchmarking against alternative assessment methods to further evaluate the model's reliability and practical effectiveness.

All the Declarations and Statements

Author Contributions Statement

Sergiy Gnatyuk – Conceptualization, Methodology, Supervision, and Writing – Review & Editing: Proposed the research framework, defined the methodological approach for calculating the cybersecurity level, provided strategic guidance throughout the study, and performed a critical review of the manuscript.
Diana Yudina – Investigation, Software Implementation, Formal Analysis, Data Curation, Validation, Visualization, Writing – Original Draft, and Writing – Review & Editing: Conducted the primary research and literature survey, implemented the mathematical MCDM model, performed the experimental audit at the representative facility, carried out statistical and sensitivity analyses, developed all visual representations of results, and authored the initial manuscript.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data Availability Statement

The study is grounded in anonymized data derived from real-world cybersecurity audits of critical information infrastructure facilities. Due to security constraints and non-disclosure agreements, the specific raw data cannot be made publicly available.

Ethical Declarations

The authors declare that this study does not involve human subjects or animals and complies with all ethical standards for scientific research.

Acknowledgments

We sincerely thank the experts for their professional evaluation and valuable recommendations, which have contributed to improving the quality of the experiment and the reliability of its results.

Declaration of Generative AI in Scholarly Writing

During the preparation of this work, the authors used Gemini (Google) to improve the language and formatting of the manuscript. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the published article.

Abbreviations

The following abbreviations are used in this manuscript:

AHP - Analytic Hierarchy Process
APT - Advanced Persistent Threat
C2M2 - Cybersecurity Capability Maturity Model

CERT-UA - National Computer Emergency Response Team of Ukraine
CI - Consistency Index
CII - Critical Information Infrastructure
CISA - Cybersecurity and Infrastructure Security Agency
CMMI - Capability Maturity Model Integration
CPGs - Cybersecurity Performance Goals
CR - Consistency Ratio
ENISA - European Union Agency for Cybersecurity
ICS - Industrial Control Systems
ISMS - Information Security Management System
ISO/IEC - International Organization for Standardization / International Electrotechnical Commission
MCDM - Multi-Criteria Decision Making
NIST CSF - National Institute of Standards and Technology Cybersecurity Framework
OT - Operational Technology
SCADA - Supervisory Control and Data Acquisition
SGMM - Smart Grid Maturity Model
SIEM - Security Information and Event Management

Appendix

None.

References

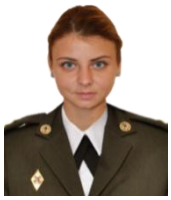
[1] European Union Agency for Cybersecurity, "ENISA Threat Landscape 2025," ENISA, Oct. 2025. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025
[2] Microsoft Corporation, "Microsoft Digital Defense Report 2025," Microsoft Digital Security & Threat Intelligence, 2025. [Online]. Available: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=1
[3] IBM Corporation, "IBM X-Force 2025 Threat Intelligence Index," IBM Institute for Business Value, 2025. [Online]. Available: https://www.ibm.com/thought-leadership/institute-business-value/report/2025-threat-intelligence-index
[4] Verizon Business, "2025 Data Breach Investigations Report (DBIR)," Verizon Business Resources, 2025. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/
[5] State Service of Special Communications and Information Protection of Ukraine, "Russian Cyber Operations: H1 ’2025," 2025. [Online]. Available: https://cip.gov.ua/services/cm/api/attachment/download?id=71278
[6] State Service of Special Communications and Information Protection of Ukraine, "Russian Cyber Operations: H2 ’2024," 2024. [Online]. Available: https://cip.gov.ua/services/cm/api/attachment/download?id=68769
[7] Information technology — Security techniques — Information security management systems — Requirements, ISO/IEC 27001:2022, International Organization for Standardization, 2022.
[8] National Institute of Standards and Technology (NIST), "NIST Cybersecurity Framework Version 2.0," U.S. Department of Commerce, 2024. [Online]. Available: https://www.nist.gov/cyberframework
[9] T. A. Ivanochko and S. A. Semenyuk, "Cybersecurity risk management using NIST CSF 2.0," Modern Information Protection, vol. 63, no. 3, pp. 75–82, 2025, doi: 10.31673/2409-7292.2025.030936.
[10] CMMI Institute, "Capability Maturity Model Integration (CMMI) for Development, Version 3.0," 2023. [Online]. Available: https://cmmiinstitute.com/cmmi
[11] U.S. Department of Energy, "Cybersecurity Capability Maturity Model (C2M2), Version 2.1," Jun. 2022. [Online]. Available: https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf
[12] Carnegie Mellon University Software Engineering Institute (SEI), "Smart Grid Maturity Model, Version 1.2," SEI Technical Report, 2012. [Online]. Available: https://www.sei.cmu.edu/library/smart-grid-maturity-model-assets-collection-version-12/
[13] Cybersecurity and Infrastructure Security Agency (CISA), "CISA Cybersecurity Performance Goals (CPGs)," 2023. [Online]. Available: https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf
[14] G. Kotzamani et al., "A Systematic Review of Voluntary Cybersecurity Standards and Frameworks," Springer Nature, 2025, doi: 10.1007/s10207-025-01121-0.
[15] S. M. Shevchenko, Y. D. Zhdanova, and O. S. Kiy, "Semi-automated tool for multi-standard assessment of an organization's cyber maturity based on NIST CSF 2.0, ISO/IEC 27001:2022, COBIT 2019, and CIS Controls V8," Cybersecurity: Education, Science, Technology, vol. 31, no. 3, pp. 43–60, 2025.
[16] O. Mikhailova, A. Petrov, and J. Smith, "Recent Trends in Information and Cyber Security Maturity Assessment: A Systematic Review," Systems, vol. 13, no. 1, p. 52, 2025, doi: 10.3390/systems13010052.
[17] G. Büyüközkan and M. Güler, "Cybersecurity maturity model: Systematic literature review and a proposed model," Technological Forecasting and Social Change, vol. 213, 2025.
[18] Y. Zakharova and A. Partika, "Evolyutsiya upravlinnya kiber-ryzykamy kriz prismu NIST Cybersecurity Framework," Cybersecurity: Education, Science, Technology, vol. 30, no. 2, pp. 333–347, 2025, doi: 10.28925/2663-4023.2025.30.980.

[19] D. Yudina, "Modification of the Model for Calculating the Level of Cyber Security of Critical Infrastructure Facilities," Cybersecurity: Education, Science, Technology, vol. 29, no. 1, pp. 818–836, 2025, doi: 10.28925/2663-4023.2025.29.943.
[20] L. G. Vargas and T. L. Saaty, *Models, Methods, Concepts & Applications of the Analytic Hierarchy Process*. Kluwer Academic Publishers, 2001. doi: 10.1007/978-1-4615-1665-1.
[21] Norman Dalkey and Olaf Helmer, "An Experimental Application of the Delphi Method to the Use of Experts," *Management Science*, vol. 9, no. 3, pp. 458–467, 1963, doi: 10.1287/mnsc.9.3.458.
[22] C. Hsu and B. A. Sandford, "The Delphi Technique: Making Sense of Consensus," *Practical Assessment, Research, and Evaluation*, vol. 12, no. 1, art. 10, 2007, doi: 10.7275/pdz9-th90
[23] Roy, B. The outranking approach and the foundations of electre methods. *Theor Decis* 31, 49–73 (1991). https://doi.org/10.1007/BF00134132

Authors' Profiles



Sergiy Gnatyuk, Professor and Vice-rector for research and technology transfer at State University "Kyiv Aviation Institute" (Kyiv, Ukraine). He is the Chief researcher at the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection. He received M.Sc. degree in Information Security as well as Ph.D. / D.Sc. in Engineering (Cybersecurity). Full Professor in Computer Science. Major research interests: Cryptography, Quantum Key Distribution, Network and Internet Security, Incident Response, UAV, Critical Information Infrastructure Protection, AI/ML-based Security Systems.



Diana Yudina received a master's degree in computer science in 2021. The topic of her master's thesis is devoted to researching methods for assessing cybersecurity risks to critical information infrastructure. She is currently pursuing a PhD at the State University "Kyiv Aviation Institute". Her research topics include calculating the level of cyber protection for critical information infrastructure objects, assessing the state of cyber protection for critical infrastructure, and researching the hierarchy of cybersecurity maturity models.

How to cite this paper:

Sergiy Gnatyuk, Diana Yudina, "Model for calculating the level of Cybersecurity of Critical Infrastructure Facilities", International Journal of Computer Network and Information Security(IJCNIS), Vol.18, No.5, pp. 17-29, 2026. DOI:10.5815/ijcnis.2026.05.02