UDC 004.056

doi: 10.32620/reks.2025.4.15

Dmytro UZLOV[1], Sergiy YAKOVLEV[1,2], Olena TOLSTOLUZKA[1], Oleksandr KOPYTSIA[1], Sergiy BURCHENKO[1]

[1] *V.N. Karazin Kharkiv National University, Kharkiv, Ukraine*
[2] *Lodz University of Technology, Lodz, Poland*

INTEGRATING CVSS, NATIONAL CRITICALITY LEVELS, AND MCDA FOR MULTI-FACTOR CYBER INCIDENT PRIORITIZATION

This integrated approach aims to prevent suboptimal prioritization, ensure effective resource allocation, and expedite the recovery of information systems. ***Methodology:*** *the proposed methodology establishes a hierarchical, multi-factor prioritization approach. It integrates the quantitative technical severity assessment provided by CVSS with Ukraine's national criticality levels. This dual-layer scoring is further supplemented by a structured tie-breaking mechanism using additional attributes to achieve precise prioritization. A structured dataset was constructed, covering nationwide impact, economic consequences, information-related impacts, functional consequences, recovery capabilities, and system/network specifics. A prioritization methodology was developed, involving five key phases: incident registration, data verification, correlation and aggregation, criticality assessment, and tie-breaking. Dedicated software was implemented to simulate the algorithm within the CERT-UA environment, enabling real-time registration, evaluation, and visualization of prioritized incidents. The simulation tested the algorithm's effectiveness in handling incident inflows and its potential to streamline response efforts.* ***Conclusions:*** *this study presents a robust and novel multi-factor methodology that overcomes the insufficient granularity of existing national criticality levels. Introducing a hierarchical tie-breaking mechanism, the approach provides CERT-UA with a clear, decisive, and efficient tool for incident prioritization. Simulation and pilot implementations confirm the algorithm's practical value and immediate applicability within the existing operational environments, significantly enhancing the ability of national-level response teams to mitigate the negative impacts of cyber threats. The system's simplicity and adaptability ensure its applicability within existing operational environments, while its tie-breaking mechanism minimizes the risk of suboptimal prioritization. Future research directions include integrating artificial intelligence and machine learning to enhance prioritization accuracy and adapting this methodology for diverse organizational contexts. This work lays a strong foundation for advancing cyber incident management, addressing the evolving nature of cybersecurity challenges.*

Keywords: *cyber incident prioritization; criticality levels; cyberattacks; incident handling; CVSS;* MCDA; *simulation tests; emerging technologies; artificial intelligence; machine learning.*

1. Introduction

1.1. Motivation

The number of cyber incidents worldwide continues to grow at an alarming rate. Cybercriminals are becoming more sophisticated, employing increasingly complex methods and tools to carry out their attacks. For example, in the second quarter of 2024, organizations experienced an average of 1,636 cyberattacks per week, representing a 30% increase compared to the previous year [1]. A similar trend is observed in Ukraine, as reported by the governmental Computer Emergency Response Team CERT-UA, part of the State Cyber Protection Center. In 2021, CERT-UA registered and processed 147 cyber incidents; in 2022, the number rose to 415, and by 2023 it reached 1,105 incidents [2].

This explosive growth is attributed to the expansion of connected surveillance systems, improved detection methods, and the escalating activity of state-sponsored cyber units. As a result, the efficiency of cyber incident management has become a critical concern, emphasizing the need for faster response times, minimized damage, and accelerated recovery of information systems. In conditions of limited resources, effective prioritization becomes crucial. Incidents should be processed based on their criticality levels, which are derived from available data on each incident. Prioritization strategies must consider the significance of targeted information systems and the risks associated with their compromise. These challenges have motivated the authors to conduct research in this area.

This paper aims to explore the integrated use of multiple assessment methods for prioritizing cyber incidents. By combining global best practices with national standards and frameworks, we aim to develop a comprehensive methodology that enables organizations to respond more effectively to cyber incidents and allocate resources to the most critical threats.

The structure of the article is organized as follows. The following subsections review various methods for assessing cyber incidents, integrated approaches to decision-making, and practical standards for prioritization, as well as outline the goals and objectives of this study. Section 2 describes the materials and methods used to develop the proposed prioritization methodology. It presents the mechanism for scoring and prioritizing cyber incidents based on severity levels and CVSS metrics. Section 3 introduces the algorithm designed for cyber incident prioritization, while Section 4 illustrates its application using real-world data. Section 5 discusses the obtained results and possible areas for improvement. Finally, Section 6 concludes the paper by summarizing the findings and suggesting directions for future research.

1.2. State of the art

Prioritization of cyber incidents is a cornerstone of modern cybersecurity management. It enables organizations to focus their limited resources on the most significant threats, thereby reducing potential damage.

Cyber incident assessment is a crucial component in the process of determining which incidents should be prioritized. Several methods are employed worldwide to assess the severity and impact of incidents, with the most common being based on specific metrics or scoring systems. One of the most widely used frameworks for vulnerability assessment is the Common Vulnerability Scoring System (CVSS), which provides a numerical score to evaluate the severity of vulnerabilities. This score is frequently leveraged to inform the prioritization of cyber incidents. Additionally, methodologies that incorporate National Institute of Standards and Technology (NIST) frameworks, as well as ISO 27001 standards, are often used to classify incidents based on their criticality and the impact on organizational and national security. These assessments usually rely on factors such as the type of attack, the targeted assets, and the extent of potential damage [4].

By using Multi-Criteria Decision Analysis (MCDA), decision-makers can weigh various factors more effectively and determine the best course of action. The prioritization of cyber incidents has seen a shift towards integrating multiple assessment methods to achieve more accurate and comprehensive decision-making. MCDA is increasingly utilized for this purpose, as it allows for the simultaneous evaluation of various criteria, such as the potential damage, the threat level, and the urgency of response [5]. This approach is vital because single-score metrics often fail to capture the full contextual impact. Recent studies [6] explicitly validate the utility of quantitative prioritization techniques for enhancing security posture, confirming the need to transform complex, qualitative risk assessments into mathematically-derived rankings. Moreover, hybrid risk analysis methods that combine both quantitative and qualitative approaches are becoming more prevalent [7]. These methods integrate risk analysis with decision-making frameworks to evaluate cyber threats more holistically. For example, combining CVSS with national threat intelligence or using scenario-based modeling can help better predict and assess the potential impact of incidents, allowing for more nuanced prioritization.

Practical approaches to prioritizing cyber incidents often draw on both international standards and locally adapted methodologies. National-level CERTs (Computer Emergency Response Teams) such as CERT-UA in Ukraine, or the US-CERT in the United States, have developed tailored approaches to incident prioritization, taking into account the specific context of their respective countries [8]. The development of clear, actionable standards for prioritization has proven essential for managing the increasing volume of cyber incidents. International standards such as ISO/IEC 27035 and NIST SP 800-61 offer guidance for incident handling and prioritization. These standards often recommend that incidents be classified according to predefined criteria such as criticality level, potential business impact, and resources required for mitigation. However, applying these general frameworks to the specific context of an organization or a nation entails adapting them to local needs and available resources.

Beyond technical prioritization, the current state of research highlights the critical importance of quantitatively assessing the multidimensional impact of cyberattacks. A systematic literature review [9] highlights the need to measure consequences not only in technical terms, but also in financial, operational, reputational, and legal categories. While frameworks such as CVSS provide a standardized assessment of technical vulnerability, they often fail to fully capture the contextual damage to business processes or critical infrastructure. This emphasis on comprehensive impact aligns with our methodology, which integrates national criticality levels and additional attributes such as economic and functional consequences that are important in decision-making.

The main approaches can be grouped into the following categories:

- ➢ *Risk and Impact Assessment.* Risk-based prioritization is one of the most common approaches used globally. Standards such as NIST SP 800-61 and ISO/IEC 27035 [10] recommend classifying incidents according to their probability of occurrence, the expected impact on business processes, and potential damages. NIST emphasizes two key factors: criticality (impact severity) and urgency (the need for immediate response) [11]. Risk assessment models help determine the potential consequences of an incident, including financial loss, reputational damage, and data compromise;

➢ *Risk Matrices.* Risk matrices offer a visual tool for decision-making. For example, ENISA recommends multi-dimensional matrices that assess the impact on Confidentiality, Integrity, and Availability (CIA triad), alongside the spread speed and recurrence probability of threats [12]. This approach enables quick identification of critical incidents and more efficient resource allocation;

➢ *AI-Based Prioritization and Automation.* The growing complexity of cyber threats necessitates automation. AI-powered tools, such as SOAR (Security Orchestration, Automation, and Response) platforms [13], leverage machine learning (ML) algorithms to analyze incident data, identify patterns, and assign priorities automatically, thereby reducing response times and minimizing human error [14]. However, the field is rapidly transitioning beyond basic automation toward Hybrid Mathematical Frameworks and Dynamic Prioritization Models to address the inherent limitations of relying solely on static or purely quantitative metrics. These advanced systems combine sophisticated AI/ML techniques with established analytical tools to achieve a more nuanced and context-aware prioritization. A key development in this area is the integration of Fuzzy Q-Learning and Text Analytics [15]. Such models utilize Reinforcement Learning (Q-Learning) and Fuzzy Logic to handle uncertainty and ambiguity in incident reporting, while Text Analytics processes unstructured descriptions to extract critical, time-sensitive contextual attributes;

➢ *Business Impact-Based Prioritization.* Many organizations prioritize incidents based on the criticality of business assets and services [16, 17]. This approach focuses on maintaining operational continuity and protecting revenue streams by assigning higher priority to incidents that jeopardize key functions;

➢ *Compliance-Driven Prioritization.* In highly regulated sectors like finance and healthcare, compliance requirements often dictate response priorities. Laws such as GDPR in Europe and HIPAA in the US require immediate action in the event of personal data breaches, with significant penalties for non-compliance [18];

➢ *Collaborative Approaches and Information Sharing.* National cybersecurity centers and industry-specific CERT/CSIRT teams facilitate the exchange of threat intelligence. Collaborative models enable faster detection and classification of emerging threats, promoting coordinated responses across sectors [19]; Such information sharing enhances situational awareness and resilience;

➢ *Vulnerability-Based Prioritization.* The Common Vulnerability Scoring System (CVSS) provides a standardized method to assess software vulnerabilities [20]. CVSS scores range from 0 to 10, with higher scores indicating more severe risks requiring urgent response. CVSS incorporates base, temporal, and environmental metrics, allowing organizations to adapt assessments to their specific contexts;

➢ *National Practices: The Case of Ukraine.* Ukraine has developed a regulatory framework for cybersecurity that includes the Law on the Basic Principles of Ensuring Cybersecurity of Ukraine [21] and the Cybersecurity Strategy of Ukraine [22]. Crucially for this study, specific guidelines issued by the State Service for Special Communications and Information Protection (SSSCIP/Derszhspetssviazok), particularly Order No. 570 of 2023, establish clear criteria for classifying cyber incidents. These criteria categorize incidents into critical, high, medium, and low levels based on their potential impact on national security and critical infrastructure [23]. While this national framework is essential for establishing macro-level priority based on state-wide consequences, its limited granularity often results in multiple critical incidents sharing the same level, complicating real-time operational prioritization. This gap mandates the integration of a more granular technical scoring system, such as CVSS, to support the operational needs of CERT-UA.

1.3. Objectives and tasks

The primary objective of this study is to develop a comprehensive methodology for prioritizing cyber incidents and attacks, enabling organizations, particularly national-level response teams like CERT-UA, to allocate resources effectively and respond promptly to the most critical threats. To achieve this objective, the study addresses the following specific tasks:

1. *Develop an Integrated Prioritization Methodology* – combine CVSS metrics with national criticality levels to create a multi-factor prioritization approach that accounts for national security, economic impact, and critical infrastructure risks, while addressing the granularity limitations of existing methods.

2. *Design a Prioritization Algorithm* – formulate a structured algorithm that incorporates criticality levels, CVSS scores, and tie-breaking criteria (e.g., national impact, sector importance, economic consequences) to sort and prioritize cyber incidents effectively.

3. *Construct a Comprehensive Dataset* – build a dataset that captures multiple dimensions of cyber incidents, including nationwide impact, economic consequences, information-related impacts, functional

consequences, recovery capabilities, and system/network specifics, using data from CERT-UA's Cyber Incident Report Card and CVSS v3.1 metrics.

4. *Simulate the Algorithm* – implement the proposed algorithm in a software tool to simulate cyber incident prioritization within the CERT-UA environment, designed to illustrate its potential for streamlining operations and optimizing resource utilization.

5. *Identify Areas for Improvement* - assess the scalability, adaptability, and limitations of the proposed methodology, particularly in handling dynamic and emerging threats, and explore the potential integration of artificial intelligence and machine learning to enhance prioritization accuracy.

In summary, while existing research offers powerful tools for incident prioritization, ranging from standardized technical scores (CVSS) to complex dynamic AI models, a significant gap persists in providing a practical and regulatorily compliant methodology for national response teams like CERT-UA. Relying solely on technical scores overlooks critical national impact, while advanced AI models often exceed available operational resources. This study addresses this disparity by proposing a multi-factor prioritization methodology that effectively integrates global best practices (CVSS and MCDA principles) with Ukraine's specific national criticality levels and additional contextual attributes.

2. Materials and Methods

Effective prioritization of cyber incidents requires not only the application of established scoring systems but also the integration of diverse assessment methodologies. Given the increasing complexity of cyber threats and the growing volume of incidents, organizations must adopt a structured, multi-layered approach that considers both international standards and local regulatory requirements. This section presents an integrated methodology for cyber incident prioritization, combining the Common Vulnerability Scoring System (CVSS) with other assessment methods and national regulations. The proposed methodology is designed to enhance decision-making efficiency by aligning incident prioritization with organizational objectives, available resources, and specific risk environments. The methodology includes a detailed algorithm for incident prioritization and practical recommendations for its application in real-world scenarios.

The national regulatory framework governing the classification of cyber incidents in Ukraine is based on a criticality scale with a limited number of levels. Such a scale provides a basic understanding of the severity of a cyber incident at the macro level, in particular, in the context of threats to national cybersecurity. At the same time, this approach lacks sufficient flexibility in cases where multiple incidents share the same criticality level but have different actual processing priorities.

According to the regulatory framework, defined in the Order No. 570 by the State Special Communications Service of Ukraine, the category (or level) of criticality of a cyber incident or cyber attack is determined based on three key criteria that have a detailed scale of values, which allows for a qualitative assessment of the impact of a cyber incident [23]:

A. Threat of disruption to the stable, reliable, and regular operation of systems (system):

A1. No threat;

A2. Immediate threat to the stable, reliable, and normal operation of systems (a specific system of a cybersecurity entity);

A3. Immediate threat to the stable, reliable, and normal operation of several systems of a separate cybersecurity entity;

A4. Immediate threat to the stable, reliable, and normal operation of a significant number of systems of several cybersecurity entities;

A5. Cross-border impact of the threat of disruption to the stable, reliable, and normal operation of systems.

B. Threat of disruption of security (Confidentiality, Integrity, and Availability) of information and data processed in systems (system):

B1. No threat;

B2. Conditions have been created for a breach of security (Confidentiality, Integrity, and Availability) of information and data processed in the systems (system);

B3. Breach of security (Confidentiality, Integrity, and Availability) of information and data processed in the systems (system).

C. Threats to national security and defense, the state of the natural environment, the social sphere, the national economy and its individual sectors, the cessation of functions and/or services provided by critical infrastructure facilities:

C1. No threat;

C2. Prerequisites for the cessation of functions and/or services provided by critical infrastructure facilities;

C3. Potential threats to national security and defense, the state of the natural environment, the social sphere, the national economy and its individual sectors, cessation of functions and/or services provided by critical infrastructure facilities;

C4. Real threats to national security and defense, the state of the natural environment, the social sphere, the national economy and its individual sectors, cessation of functions and/or services provided by critical infrastructure facilities;

C5. An inevitable threat to the full functioning of the state or a threat to the lives of Ukrainian citizens.

Based on the individual assessment of each criterion, the generalized level of criticality of the incident is determined by applying the corresponding summary table (Table 1).

While this categorization offers a structured approach, its granularity is limited. For a more precise prioritization, it is advisable to complement it with numerical methods, such as the Common Vulnerability Scoring System (CVSS).

The CVSS methodology assigns scores on a scale from 0.0 to 10.0, with increments of 0.1, theoretically allowing for up to 100 distinct scores. However, due to predefined coefficient groupings and rounding, the actual number of different outcomes is somewhat lower. CVSS qualitative ratings are mapped to numerical ranges as follows:

- Not critical: 0.0;
- Low: 0.1 – 3.9;
- Medium: 4.0 – 6.9;
- High: 7.0 – 8.9;
- Critical: 9.0 – 9.6;
- Extreme: 9.7 – 10.0.

While this scale increases precision, it still results in multiple incidents sharing identical scores, particularly within high-severity ranges. For example, within the “Extreme” category (9.7–10.0), there are only a few discrete values, meaning incidents may share identical scores.

In environments where only a limited number of incidents are processed concurrently, this level of detail is typically sufficient. However, as the volume of incidents increases, the likelihood of score duplication grows, complicating prioritization efforts.

In the context of CERT-UA, which handles incidents reported by diverse organizations across the nation, it is essential to balance national-level impact considerations with technical assessments. Therefore, it is advisable to use the national Methodological Recommendations for initial categorization and apply CVSS scoring to differentiate between incidents within the same criticality category.

A comprehensive assessment of cyber incident severity requires a dataset that reflects multiple dimensions of each incident. These include the type of incident, source of the threat, attack method, impacts on confidentiality, integrity, and availability, as well as the consequences for business continuity, financial stability, and reputation. Furthermore, recovery capabilities — such as backup availability and response effectiveness— must be considered. It is also crucial to evaluate the attacker’s tactics, potential for persistence, lateral movement within systems, and the phase of incident response.

For national cyber incident response teams, such as CERT-UA, the dataset must capture both the organizational and nationwide impacts of incidents. To achieve this, we combined data from two primary sources:

- ➢ The *Cyber Incident/Cyber Attack Report Card* (Annex 6 of the Order No. 570 by the State Special Communications Service of Ukraine, July 3, 2023);
- ➢ Metrics defined by CVSS version 3.1, developed by the US National Institute of Standards and Technology (NIST).

Crucially, the proposed prioritization methodology assumes that the Criticality Level and the CVSS Score have already been calculated and provided as input attributes for each incident. The focus of this integrated approach is not on calculating primary scores, but on effectively utilizing the combination of resulting values to establish a comprehensive processing queue. This sectional focus serves as the mechanism for combining these values with other data, thereby enhancing decision-making efficiency by aligning incident prioritization with organizational objectives, available resources, and specific risk environments.

The incident classification methodology employs ordinal and logarithmic scales to quantify the complex, post-incident consequences, thereby distinguishing this impact assessment from predictive risk analysis. The design of these scales adheres to international standards, primarily ISO 31000 and ISO/IEC 27005 [24], by establishing customized, structured consequence criteria.

The “National-level risk” scale achieves this alignment by establishing a clear ordinal relationship where the most critical consequences to the state’s sovereignty and public safety are prioritized with the highest values, ranging from National security down to National reputation. Similarly, the “Sector of the attacked entity” scale quantifies national-level severity based on the target, employing a compact ordinal structure developed by grouping economic sectors according to their designation as Critical Infrastructure. This approach ensures that the resulting impact weighting reflects established governmental and economic risk management hierarchies, specifically by concentrating the highest weightings on systemic failure points (e.g., Energy and Financial sectors) that have the potential for systemic national collapse, thereby translating the target of an attack into a precise measure of its national-level impact severity.

The “Impact on services” scale formalizes the operational triage process. This approach is a direct application of international best practices, such as the NIST SP 800-61 Functional Impact metric, ensuring incident response and notification protocols (like those outlined by the SSSCIP in Ukraine) are driven by the direct harm to an entity’s mission-essential services.

Table 1

Determination of Cyber Incident Criticality Level

Criteria for determining the criticality category (level)													Criticality category (level) determined by
A					**B**			**C**					
A1	A2	A3	A4	A5	B1	B2	B3	C1	C2	C3	C4	C5	
●					●			●					0, not critical (white)
	●				●			●					1, low (green)
	●				●				●				1, low (green)
		●			●			●					1, low (green)
		●				●		●					1, low (green)
	●					●		●					2, medium (yellow)
	●					●			●				2, medium (yellow)
		●				●		●					2, medium (yellow)
	●						●	●					3, high (orange)
	●						●		●				3, high (orange)
	●						●			●			3, high (orange)
	●						●				●		4, critical (red)
		●					●				●		4, critical (red)
		●					●					●	5, extraordinary (black)
			●				●					●	5, extraordinary (black)
				●			●				●		5, extraordinary (black)
				●			●					●	5, extraordinary (black)

The “Type of compromised system” scale further refines the consequence by focusing on the functional role of the compromised asset. It prioritizes systems that enable systemic damage, such as Network Control and Segmentation assets (e.g., Firewalls, DNS) at the highest level, recognizing that loss of network command directly affects Integrity and Availability across the entire enterprise. This consequence is weighted higher than the loss of mere Core Data Servers, as loss of control is a prerequisite for total systemic failure. Lower ranks are reserved for systems with contained severity, such as End-User Access Points, where the actual breach impact is typically localized rather than systemic.

The “Impact outcome” scale quantifies the nature of the realized harm by prioritizing consequences according to their severity across the Confidentiality, Integrity, and Availability (CIA) Triad. Unlike traditional models that might prioritize data theft, this scale assigns the highest severity to Integrity Loss / Control Seizure. This weighting is based on the principle that the manipulation of control systems or core data is a more profound threat to national stability than mere exfiltration. Prolonged Critical Service Loss, representing a failure of Availability, is ranked next, reflecting its immediate and high operational cost. Massive Data Exfiltration, representing Confidentiality loss, follows, ensuring the classification mechanism prioritizes functional, operational damage over purely financial or latent costs.

Finally, the continuous impact attributes—including “Financial losses”, “Downtime”, “Number of people affected”, and “Number of compromised systems”—are classified using a logarithmically progressive scale. This non-linear approach is crucial for accurately quantifying severity, as it reflects the heavy-tailed distribution of cyber losses by assigning disproportionately higher scores to extreme events [25, 26]. This ensures the final ranking accurately captures the exponential increase in operational and financial harm associated with high-severity incidents.

A detailed list of selected attributes and their corresponding values is provided below.

➢ *Criticality level (Nationwide impact):*

– Extraordinary – 5;

– Critical – 4;

– High – 3;

– Medium – 2;

– Low – 1;

– Not critical – 0;

➢ *CVSS Score;*

➢ *National-level risk:*

– National security – 6;

- Economic sustainability – 5;
- Government functioning – 4;
- Personal data security – 3;
- National reputation – 2;
- Other – 1;
- No data – 0;

➢ *Sector of the attacked entity:*
- National Security & Core Government – 6;
- Systemic Economy & Essential Services – 5;
- Enabling Critical Infrastructure – 4;
- Health, Safety, & Core Logistics – 3;
- Local Governance & Private Economy – 2;
- Information & Miscellaneous – 1;
- No data – 0;

➢ *Financial losses (UAH thousands):*
- over 2,500,000 – 4;
- 250,001 – 2,500,000 – 4;
- 25,001 – 250,000 – 3;
- 1 – 25,000 – 1;
- No data – 0;

➢ *Downtime (hours):*
- over 168 – 4;
- 48-168 – 3;
- 8-48 – 2;
- 0-8 – 1;
- No data – 0;

➢ *Number of people affected:*
- over 100,000 – 4;
- 10,001–100,000 – 3;
- 1,001–10,000 – 2;
- 1–1,000 – 1;
- No data – 0;

➢ *Impact outcome:*
- Integrity Loss / Control Seizure – 6;
- Prolonged Critical Service Loss – 5;
- Massive Data Exfiltration / Leakage – 4;
- General Service Disruption – 3;
- Limited Data Theft – 2;
- Other – 1;
- No data – 0;

➢ *Impact on services:*
- Loss of critical services – 8;
- Loss of non-critical services – 7;
- Significant impact on critical services – 6;
- Significant impact on non-critical services – 5;
- Minor impact on critical services – 4;
- Minor impact on non-critical services – 3;
- No impact on services – 2;
- No impact at all – 1;
- No data – 0;

➢ *Number of compromised systems:*
- over 100 – 4;
- 50–100 – 3;
- 10–50 – 2;
- 1–10 – 1;
- No data – 0;

➢ *Type of compromised system:*
- Network Control & Segmentation – 6;
- Core Data & Identity Management – 5;
- Application & Business Logic – 4;
- Perimeter/Edge System – 3;
- End-User Access Point – 2;
- Miscellaneous – 1;
- No data – 0;

➢ *Date and time of incident report.*

The order of the values and the corresponding weighting factors reflect their level of importance, but do not provide for a quantitative assessment of the intervals between values.

This structured dataset enables a more nuanced prioritization of incidents, supporting effective decision-making by CERT-UA analysts during incident response.

3. Results

3.1. Developing a Decisive Multi-Criteria Methodology for Incident Prioritization

The proposed methodology for prioritizing cyber incidents is grounded in Multi-Criteria Decision Analysis (MCDA). Existing investigations in multi-factor evaluation and optimization typically distinguish between two main approaches to implement the decision procedure: the synthesis of a single generalized assessment (creating one composite utility function) or ranking based on the implementation of a sequence of single-criterion assessments (successive analysis) [27]. The synthesis approach is challenging in this domain because the primary metrics—the national Criticality Level (a high-level, consequence-driven categorical measure) and the CVSS Score (a granular, technical-severity numerical score)—have fundamentally different methods of derivation and scales, making their direct, weighted aggregation difficult without introducing potential distortion. Therefore, the methodology adopts the ranking based on the implementation of a sequence of single-criterion assessments (successive analysis).

This successive analysis allows for a strictly hierarchical sorting of incidents. First, the Criticality Level provides the essential, consequence-based description, ensuring that all incidents affecting the highest-priority systems are addressed first. For instances where multiple incidents share the same criticality level (e.g., several Level 4 incidents), the CVSS Score is employed to refine the classification, providing a more granular distinction between them. For example, a Level

4 incident with a CVSS score of 9.5 will be prioritized over another Level 4 incident with a CVSS score of 8.0, reducing the likelihood of ties. In the rare cases where several cyber incidents exhibit identical Criticality Levels and CVSS scores, they are treated as equal in severity, and the Time of Receipt is used as the final tie-breaking criterion. Prioritizing the first reported incidents ensures timely action and accounts for the cumulative effect of the incident's duration on the informational system.

This approach provides a straightforward method for prioritizing cyber incidents, using existing, well-established metrics like the criticality scale and CVSS. The prioritization table includes the following key attributes:

- Criticality Level;
- CVSS Score;
- Time of Receipt.

The resulting processing queue is sorted by these attributes, with priority determined first by the Criticality Level (descending severity), then by the CVSS Score (descending severity), and finally by the Time of Receipt (oldest receipt first). Cyber incidents with higher priority values are thus processed earlier.

3.2. General description of the algorithm

The prioritization process is initiated immediately upon the registration of a cyber incident or cyber attack. Once received, the incident is recorded in the List of Cyber Incidents and assessed for inclusion in the Cyber Incident Processing Queue. This decision-making procedure is a multi-step process structured around the following key phases:

➢ *Receiving and registering information about a cyber incident.* This stage involves the receipt of incident reports through designated communication channels, as well as their subsequent recording in the relevant accounting logs or security information systems;

➢ *Verification and clarification of the data received.* The reliability of the primary information about the incident is verified, followed by an analysis of its relevance. Based on the results of this verification, a decision is made on the feasibility of further processing of the incident;

➢ *Correlation and aggregation of cyber incidents.* In cases where several incidents have a common source, occur within the same organization, or manifest themselves within the same attack scenario, it may be decided to combine them into a single generalized incident to simplify processing;

➢ *Criticality assessment and prioritization.* Based on the analysis of the potential impact of cyber incidents on information assets, their processing priority is determined. Parameters such as criticality level, vulnerability level, and potential consequences for the organization are taken into account;

➢ *Hierarchical Multi-Criteria Tie-Breaking.* In situations where several cyber incidents have the same level of criticality, an in-depth comparative analysis of their attributes is performed to make an informed decision on the priority of response.

Cyber incidents that have already been addressed or do not require CERT-level intervention (e.g., incidents resolved by the affected organization or transferred to third-party organizations) are excluded from further prioritization. In cases where reports are unreliable, additional clarification is sought from the organization involved. If clarification cannot be obtained or significant doubts remain, the incident is excluded from consideration.

The incoming set of cyber incidents is hierarchically prioritized. First, incidents are sorted in descending order based on their national criticality level, ranging from the most critical (Level 5) to the least critical (Level 0). Second, incidents that share the same criticality level are further ranked internally by their CVSS scores. Within this structured sorting, the maximum priority is assigned to the incident possessing the highest national criticality level and the highest CVSS score. Once the complete list is sorted, incidents are processed sequentially based on this final priority order.

In scenarios where the system identifies multiple, seemingly distinct incidents that are actually related and represent different components of a single, coordinated cyber event, a consolidated response is often the most effective strategy. It is important to emphasize that the core attributes, while essential for effective incident prioritization, were not designed for determining incident correlation. We presume that the reported cyber incident data allows for the grouping of related events, but the specific relational attributes used to establish this grouping are external to the set of prioritization attributes detailed herein. Future work should focus on enriching the dataset to incorporate these relational data points for improved automated linking.

When related incidents are grouped, the preferred action is for the reporting entity or the analyst team to re-estimate the Criticality Level and CVSS for the consolidated event. This ensures the severity rating reflects the total, accumulated impact of the single large incident, which is typically greater than the sum of its parts.

If, for operational or resource reasons, a full re-estimation of the newly consolidated incident is not immediately feasible, the incident group must still receive a provisional severity level for queuing. In such cases, the Max Severity method serves as a conservative interim measure, aligning with practices in national scoring frameworks such as the US Cybersecurity and

Infrastructure Security Agency's (CISA's) National Cyber Incident Scoring System (NCISS). This principle, also embedded in systems like CVSS, ensures that the most significant potential impacts drive prioritization, directing attention to the most critical threats. Under this approach, the consolidated incident inherits the highest Criticality Level and the maximum CVSS value observed among its constituent incidents. Its rationale is further supported by empirical investigations employing Extreme Value Theory (EVT), which emphasize the importance of accounting for extreme, high-impact outcomes in effective risk management [26]. The corresponding criticality levels and CVSS 3.1 rating scales are presented in Tables 2 and 3.

The consolidated incident record is then added to the processing queue, while the individual, primary incidents are removed from the list. Subsequently, all records in the queue are re-prioritized using the established methodology.

Table 2

Criticality Category (Level)

Criticality level	Numerical value
Not critical	0
Low	1
Medium	2
High	3
Critical	4
Extraordinary	5

Table 3

Rating of levels according to CVSS 3.1

Qualitative assessment	Quantitative assessment
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

3.3. Hierarchical Multi-Criteria Tie-Breaking

In the context of incident prioritization, ties may occur when multiple cyber incidents or attacks retain identical primary scores, specifically their Criticality Level and CVSS metric values, even after all initial refinement procedures have been applied. In-depth analysis of cyber incidents involves a multidimensional assessment of their characteristics, which allows for more accurate prioritization and ensures that response decisions are informed. The main phases of such analysis include:

➢ *Contextualization by industry*. Identification of the sector of the economy in which the organization subject to the incident operates. This allows for taking into account the specifics of industry threats, regulatory restrictions, and the criticality of the information infrastructure;

➢ *Assessment of economic consequences*. Potential and actual economic losses are analyzed, including direct financial losses, recovery costs, and reputational risks that may have a long-term impact on the organization's operations;

➢ *Analysis of information impact*. The degree of information compromise is assessed, including loss of Confidentiality, Integrity, and Availability of data, which may disrupt the organization's key information flows;

➢ *Determination of functional consequences*. The extent to which the incident affected the performance of critical business processes and services is determined. This allows for classifying the incident by the level of operational destabilization;

➢ *Assessment of recovery capabilities*. The organization's potential to respond quickly and restore normal operations, including the availability of backup systems, business continuity plans, and cyber resilience tools, is considered;

➢ *Impact on technological infrastructure*. The degree of damage to information systems, servers, network segments, and other components of the digital infrastructure is analyzed;

➢ *Temporal characteristics of the incident*. Time parameters are studied, including the time of the incident's start, the time of its detection, registration, and elimination, which are important for reconstructing the chain of events and identifying points of delay in response.

To operationalize the findings of the multidimensional assessment above, and to ensure consistent and objective decision-making, the complete set of incidents must be sorted according to the following definitive hierarchical priority list. This hierarchy combines the primary scoring metrics with the secondary, consequence-based indicators, which are derived from the analytical dimensions listed previously:

➢ Criticality Level - The highest-level national threat classification;

➢ CVSS Score - A quantitative technical severity metric;

➢ National Impact - The scale and type of threat posed at the national or governmental level.

➢ Sector of the Targeted Entity - The strategic importance and criticality of the affected industry or sector (e.g., Security, Energy, Financial);

➢ Estimated Losses - Financial consequences, including potential and actual economic losses and recovery costs;

➢ Downtime Duration - The projected or actual duration of operational stagnation for critical services;

- Number of Affected Individuals - The scope of potential or actual harm to people;
- Information Impact - The severity of data compromise (Confidentiality, Integrity, and Availability);
- Functional Consequences - The extent of disruption to core business processes, systems, networks, or services;
- Number of Compromised Systems - The count of affected devices, systems, or network segments;
- Functional Role of Compromised Systems - The operational significance of the systems' function within the broader infrastructure;
- Time of Incident Registration - The time the incident report was received (used as the final, temporal tie-breaker).

This approach implements a successive tie-breaking mechanism based on a predefined hierarchy of attributes. When two or more incidents are indistinguishable by the primary criteria (identical Criticality Level and CVSS score), the system resolves the tie by comparing the National Impact attribute. Should the tie persist, the sorting is determined by the next criterion in the sequence, such as the Sector of the Targeted Entity, and so on, until a decisive order is established.

To maintain efficiency, the secondary indicators may initially be unset and are only fully determined and documented if tie-breaking is necessary for the incident in question. When a new incident is reported, the prioritization cycle must be re-initiated to ensure the ranking reflects the most current and complete assessment of all active cases.

4. Case study

To validate and demonstrate the effectiveness of the proposed prioritization algorithm, dedicated software, named CSIPM (Cyber Security Incident Prioritization Module) [28], was implemented to simulate the processing of cyber incidents within the CERT-UA environment. This tool provides dual functionality for populating and refining the incident queue:

- *Manual Registration & Expert Refinement:* The system allows users to manually add new incidents or modify the data of existing ones. This crucial feature reflects the operational necessity for cybersecurity experts to provide their feedback and adjust incident attributes based on their deep analysis, investigation findings, or updated threat intelligence. The expert-driven changes automatically trigger a recalculation of the priority score;
- *Automated Simulation:* The software can emulate the continuous inflow of cyber incident reports, automatically registering new incidents to enable real-time testing of the prioritization logic.

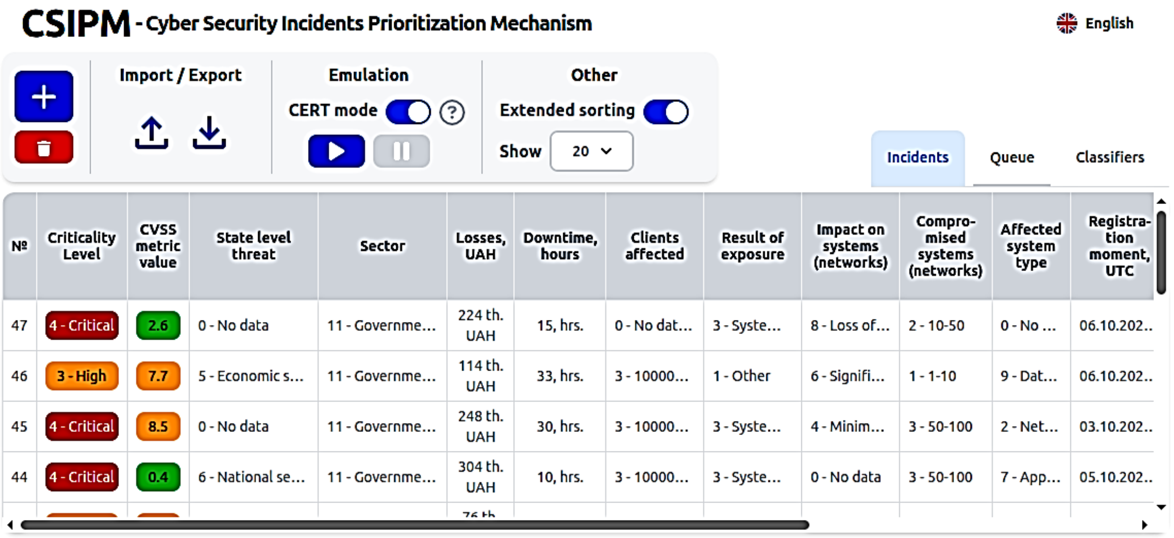
The distribution of key incident attributes (Severity Level, Sector of Attacked Object, Impact) used in the automated simulation accurately corresponds to the official statistical data reported by the State Center for Cyber Defense of the State Service for Special Communications and Information Protection of Ukraine. The emulation specifically relies on the observed incident distribution patterns detailed in the 2023 Work Report [2] to ensure the simulation environment accurately reflects the real-world threat landscape faced by CERT-UA. Auxiliary attributes (such as Cyber Incident Status and Report Reliability) are emulated to demonstrate the system's full range of classification capabilities. For these auxiliary attributes, the distribution is intentionally set to reflect a typical operational load, where the vast majority of incidents are newly registered and reliable, while a minor portion includes already processed or unreliable reports that require further checking before action is taken.

For the purpose of simulating a nuanced economic impact, the "Losses" attribute was modeled to be dependent on the incident's level of criticality and its duration. Furthermore, a specific coefficient depending on the generated downtime was applied to the generated loss value, introducing a realistic functional consequence into the prioritization process. The values of all other auxiliary cyber incident attributes are evenly distributed among all possible values of their corresponding classifiers. All registered cyber incidents are displayed in the Incidents interface (Fig. 1), where their details and status can be reviewed and modified.

Each incident is assessed using the developed prioritization algorithm, which takes into account the criticality level, CVSS score, and additional resolution criteria in case of identical scores. The results of this prioritization process are visualized in the Processing Queue interface (see Figure 2), where incidents are sorted in descending order of priority.

The software also includes a dedicated Classifiers interface (see Figure 3), which provides detailed reference information used in the evaluation process. This includes defined consequence groups, a list of incident attributes, and possible values for each attribute. These classifiers support transparent and reproducible prioritization decisions.

The system allows users to manually add new incidents or edit existing ones, which automatically triggers the recalculation and reordering of the incident queue. This dynamic update feature ensures that prioritization remains accurate as the threat landscape evolves in real time.



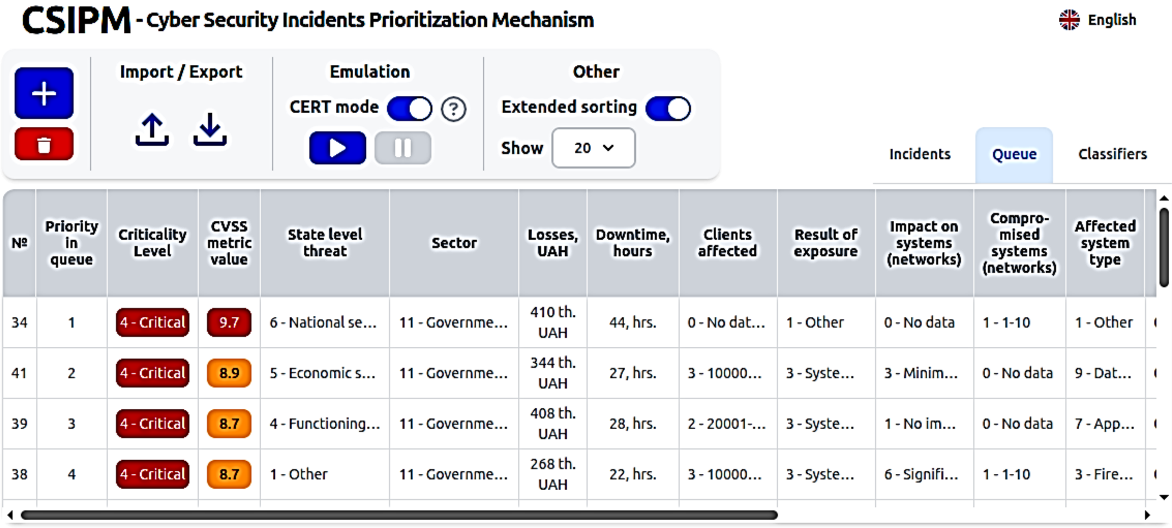
CERT mode ●

Extended sorting ●

Show 20

№	Criticality Level	CVSS metric value	State level threat	Sector	Losses, UAH	Downtime, hours	Clients affected	Result of exposure	Impact on systems (networks)	Compro-mised systems (networks)	Affected system type	Registra-tion moment, UTC
47	4 - Critical	2.6	0 - No data	11 - Governme...	224 th. UAH	15, hrs.	0 - No dat...	3 - Syste...	8 - Loss of...	2 - 10-50	0 - No ...	06.10.202..
46	3 - High	7.7	5 - Economic s...	11 - Governme...	114 th. UAH	33, hrs.	3 - 10000...	1 - Other	6 - Signifi...	1 - 1-10	9 - Dat...	06.10.202..
45	4 - Critical	8.5	0 - No data	11 - Governme...	248 th. UAH	30, hrs.	3 - 10000...	3 - Syste...	4 - Minim...	3 - 50-100	2 - Net...	03.10.202..
44	4 - Critical	0.4	6 - National se...	11 - Governme...	304 th. UAH	10, hrs.	3 - 10000...	3 - Syste...	0 - No data	3 - 50-100	7 - App...	05.10.202..

Fig. 1. User interface showing the list of registered cyber incidents



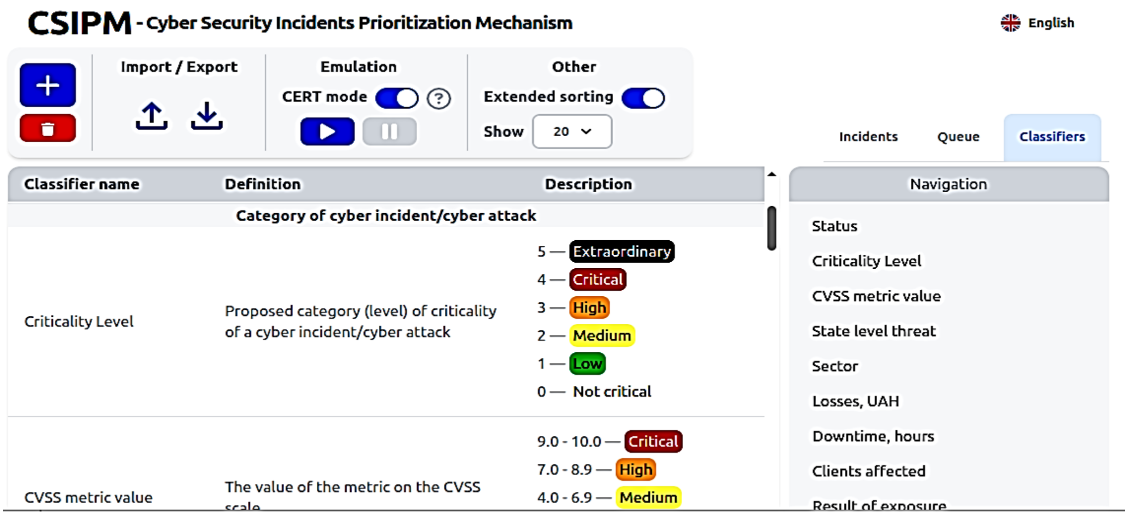
CERT mode ●

Extended sorting ●

Show 20

№	Priority in queue	Criticality Level	CVSS metric value	State level threat	Sector	Losses, UAH	Downtime, hours	Clients affected	Result of exposure	Impact on systems (networks)	Compro-mised systems (networks)	Affected system type
34	1	4 - Critical	9.7	6 - National se...	11 - Governme...	410 th. UAH	44, hrs.	0 - No dat...	1 - Other	0 - No data	1 - 1-10	1 - Other
41	2	4 - Critical	8.9	5 - Economic s...	11 - Governme...	344 th. UAH	27, hrs.	3 - 10000...	3 - Syste...	3 - Minim...	0 - No data	9 - Dat...
39	3	4 - Critical	8.7	4 - Functioning...	11 - Governme...	408 th. UAH	28, hrs.	2 - 20001-...	3 - Syste...	1 - No im...	0 - No data	7 - App...
38	4	4 - Critical	8.7	1 - Other	11 - Governme...	268 th. UAH	22, hrs.	3 - 10000...	3 - Syste...	6 - Signifi...	1 - 1-10	3 - Fire...

Fig. 2. Prioritized processing queue of cyber incidents after evaluation, illustrating hierarchical ordering based on national criticality level, CVSS score, and successive tie-breaking attributes.



CERT mode ●

Extended sorting ●

Show 20

Classifier name	Definition	Description
Category of cyber incident/cyber attack		
Criticality Level	Proposed category (level) of criticality of a cyber incident/cyber attack	5 — Extraordinary 4 — Critical 3 — High 2 — Medium 1 — Low 0 — Not critical
CVSS metric value	The value of the metric on the CVSS scale	9.0 - 10.0 — Critical 7.0 - 8.9 — High 4.0 - 6.9 — Medium

Navigation

Status
Criticality Level
CVSS metric value
State level threat
Sector
Losses, UAH
Downtime, hours
Clients affected
Result of exposure

Fig. 3. Reference section illustrating the structured classifiers, consequence groups, and attribute scales used in the multi-factor prioritization and tie-breaking process

5. Discussion

The prioritization of cyber incidents is a crucial step for ensuring an effective and timely national response. This study successfully developed a novel multi-factor methodology that transcends the limitations of relying solely on technical severity scores. The core achievement is the seamless integration of the standardized Common Vulnerability Scoring System with Ukraine's national criticality levels. This formalization provides a straightforward methodology for determining incident handling priority, enabling national-level response teams, such as CERT-UA, to efficiently optimize resource allocation and expedite response to the most critical threats.

A key strength of the developed methodology is its operational practicality and simplicity. By utilizing proven, existing metrics and adapting them for the national context through weighted criticality levels, the methodology is easily implementable within current operational protocols without the significant computational overhead typical of advanced AI/ML systems. Furthermore, the systematic combination of these metrics, buttressed by the Tie-Breaking Mechanism detailed in Section 3, minimizes the likelihood of suboptimal or ambiguous prioritization across large volumes of data. The implementation of the algorithm in the CSIPM software tool further demonstrated its potential in real-world applications, offering a clear visualization and dynamic recalculation of the prioritization process.

A core element of our scientific contribution lies in the positioning of the proposed methodology relative to established and advanced approaches. When compared to methods relying exclusively on pure CVSS scores, our approach offers significant superiority by mitigating the critical flaw of being context-agnostic. While standardized, CVSS fails to integrate non-technical, yet vital, factors such as national criticality, economic impact, or the sector of the attacked object—factors essential for national-level decision-making. Our methodology directly addresses this by formally integrating national criticality levels and supplementary contextual attributes, transforming a technical severity score into an operationally relevant priority ranking.

Conversely, our methodology also distinguishes itself from highly sophisticated AI-driven and Hybrid Mathematical Frameworks—such as those utilizing Fuzzy Q-Learning or complex dynamic models. While these advanced systems demonstrate exceptional theoretical accuracy, their reliance on massive volumes of data and significant computational infrastructure often renders them impractical for immediate government adoption. Our approach provides a crucial, practical middle ground. It applies the principles of Multi-Criteria Decision Analysis (MCDA) in a transparent, easily auditable, and rapidly deployable manner, as validated by research on quantitative prioritization techniques. Thus, the main scientific contribution is the development of a methodology that is both regulatorily compliant and operationally efficient, filling the existing gap between purely technical assessment and resource-intensive automated models. Although the methodology is demonstrated using the Ukrainian national framework, its conceptual structure is generic and can be adapted to any national or organizational incident classification system that employs categorical severity levels. The proposed hierarchical integration of technical scores and consequence-based attributes is applicable to CERT/CSIRT teams worldwide.

The proposed multi-factor prioritization methodology, while highly effective, faces key limitations that must be acknowledged.

Firstly, a primary scientific limitation is the use of static, expert-defined weighting coefficients for integrating the CVSS score and the national criticality level. These fixed weights may not fully capture or rapidly adapt to the dynamic nature of cyber threats or sudden geopolitical changes, potentially leading to suboptimal prioritization when faced with entirely novel attack techniques. While the methodology provides a systematic method for sorting incidents, the reliance on predefined metrics might not always fully capture this rapid evolution, highlighting the need for ongoing refinement of the prioritization criteria [29].

Furthermore, tie-breaking is an area that may benefit from additional improvements. The current methodology successfully resolves ties based on quantitative and semi-quantitative factors (national impact, financial losses, sector affected), but further studies could examine the role of subjective or long-term elements such as the impact on public trust or long-term security implications [30]. Such factors are more complex to quantify, but are equally important for a comprehensive national security assessment.

Finally, it is essential to assess the scalability and adaptability of the CSIPM system in different organizational contexts, such as private organizations or multinational corporations. By ensuring that the most impactful incidents are addressed first, the proposed prioritization methodology directly contributes to minimizing overall damage and accelerating the recovery of affected information systems.

For future work, we will focus on addressing these limitations by exploring dynamic optimization mechanisms. Specifically, this involves investigating the integration of advanced techniques—such as elements of Fuzzy Logic or adaptive machine learning models—to automatically and dynamically adjust the weighting coefficients based on real-time threat intelligence and current operational goals. Additionally, future research should explore the development of novel classifiers better to incorporate hard-to-quantify subjective impacts into the conflict resolution process.

6. Conclusions

This article presents a comprehensive methodology for prioritizing the processing of cyber incidents and cyber attacks, incorporating a multi-factor assessment of criticality. The structured prioritization process enables faster mitigation of critical incidents, thereby reducing cumulative damage and shortening recovery times for information systems. The proposed methodology is not limited to a single national context and can be adapted for use by governmental and organizational response teams operating under different regulatory frameworks.The approach, which integrates both criticality levels and CVSS metrics, offers a robust and practical methodology for cybersecurity professionals to prioritize incidents effectively. The proposed algorithm has been simulated and tested, showing its ability to streamline incident handling and mitigate the potential negative impacts of cyber threats.

The results of the simulation and pilot implementations provide strong evidence of the approach's effectiveness in real-world applications, proving its potential as a valuable tool for managing cyber incidents. By organizing incidents based on a clear and structured set of criteria, the methodology ensures that the most critical threats are addressed first, enabling faster mitigation and minimizing further damage.

Looking forward, the integration of emerging technologies such as artificial intelligence and machine learning into the incident prioritization process represents an exciting opportunity for improvement [31, 32]. These technologies could enhance the system's ability to detect and respond to previously undetectable threats, further improving the efficiency and accuracy of incident handling.

In conclusion, the proposed approach offers significant improvements over traditional approaches to incident prioritization. It opens up avenues for future research, particularly in refining the methodology, expanding its applicability, and integrating cutting-edge technologies. The findings in this study lay the groundwork for further development in the area of cyber incident management, which will be critical in addressing the growing and evolving nature of cybersecurity threats.

Contributions of authors: conceptualization – **Dmytro Uzlov, Sergiy Yakovlev**; methodology – **Dmytro Uzlov, Olena Tolstoluzka;** formulation of tasks – **Dmytro Uzlov, Sergiy Yakovlev, Olena Tolstoluzka**; analysis **– Sergiy Yakovlev, Olena Tolstoluzka, Oleksandr Kopytsia, Sergiy Burchenko;** development of model **– Dmytro Uzlov, Olena Tolstoluzka, Oleksandr Kopytsia, Sergiy Burchenko;**, software **– Oleksandr Kopytsia, Sergiy Burchenko;**, verification **– Oleksandr Kopytsia, Sergiy Burchenko;** analysis of results **– Dmytro Uzlov, Olena Tolstoluzka;**, visualization **– Oleksandr Kopytsia, Sergiy Burchenko;** writing – original draft preparation – **Dmytro Uzlov, Olena Tolstoluzka, Oleksandr Kopytsia, Sergiy Burchenko;** writing – review and editing **– Sergiy Yakovlev.**

Conflict of Interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship, or otherwise, that could affect the research and its results presented in this paper.

Financing

This study was conducted without financial support.

Data Availability

The work has associated data in the data repository.

Use of Artificial Intelligence

The authors have used artificial intelligence technologies within acceptable limits to provide their own verified data, as described in the research methodology section.

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

References

1. Terranova Security, 2024. *130 Cyber Security Statistics: 2024 Trends and Data*. Available at: https://www.terranovasecurity.com/blog/cyber-security-statistics (accessed 19 June 2025).

2. State Center for Cyber Defense of the State Service for Special Communications and Information Protection of Ukraine, 2023. *Zvit pro robotu 2023* [Work Report 2023]. Available at: https://scpc.gov.ua/api/files/9c21855d-74da-45d1-90f9-5d4f6795996a (accessed 19 June 2025). (In Ukrainian).

3. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. Cyber Risk and Cybersecurity: A Systematic Review of Data Availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, 2022, vol. 47, pp. 698–736. DOI: 10.1057/s41288-022-00266-6.

4. Crotty, J., & Daniel, E. Cyber Threat: Its Origins and Consequence and the Use of Qualitative and Quantitative Methods in Cyber Risk Assessment.

Applied Computing and Informatics, 2022. DOI: 10.1108/ACI-07-2022-0178.

5. Abdiraman, A., Goranin, N., Balevicius, S., Nurusheva, A., & Tumasonienė, I. Application of Multicriteria Methods for Improvement of Information Security Metrics. *Sustainability*, 2023, vol. 15, no. 10, article no. 8114. DOI: 10.3390/su15108114.

6. Jang, J., Jung, S., Ahn, M., Kim, D., Youn, J., & Shin, D. Research on Quantitative Prioritization Techniques for Selecting Optimal Security Measures. *IEEE Access*, 2024, vol. 12, pp. 103855–103867. DOI: 10.1109/ACCESS.2024.3433404.

7. Haji, S., Tan, Q., & Soler Costa, R. A Hybrid Model for Information Security Risk Assessment. *International Journal of Advanced Trends in Computer Science and Engineering*, 2019, vol. 8, no. 1.1, pp. 100–106. DOI: 10.30534/ijatcse/2019/1981.12019.

8. CISA, 2017. *US-CERT Federal Incident Notification Guidelines*. Available at: https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines_2015.pdf (accessed 19 June 2025).

9. Adekoya, O. A., Atlam, H. F., & Lallie, H. S. Quantifying the Multidimensional Impact of Cyber Attacks in Digital Financial Services: A Systematic Literature Review. *Sensors*, 2025, vol. 25, iss. 14, article no. 4345. DOI: 10.3390/s25144345.

10. *ISO/IEC 27035-1:2023. Information Technology — Information Security Incident Management. Part 1: Principles and Process.* Available at: https://www.iso.org/standard/78973.html (accessed 19 June 2025).

11. *NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide*. Available at: https://csrc.nist.gov/pubs/sp/800/61/r2/final (accessed 19 June 2025).

12. ENISA. 2022. *Interoperable EU Risk Management Framework: Methodology for Assessment of Interoperability Among Risk Management Frameworks and Methodologies, Updated Report. December 2022*. Available at: https://www.enisa.europa.eu/sites/default/files/publications/ENISA Report-Interoperable EU Risk Management Framework_Updated.pdf (accessed 19 June 2025).

13. Kinyua, J., & Awuah, L. AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intelligent Automation & Soft Computing*, 2021, vol. 28, no. 2, pp. 527–545. DOI: 10.32604/iasc.2021.016240.

14. Joseph, J. E., Aleke, N., & Onyeanisi, O. P. Intelligent Incident Response Systems Using Machine Learning. *Mikailalsys Journal of Advanced Engineering International*, 2025, vol 2, no. 1, pp. 33-54. DOI: 10.58578/MJAEI.v2i1.4540.

15. Peralta, A., Olivas, J. A., Navarro-Illana, P., & Alvarado, J. A Hybrid Mathematical Framework for Dynamic Incident Prioritization Using Fuzzy Q-Learning and Text Analytics. *Mathematics*, 2025, vol. 13, iss. 12, article no. 1941. DOI: 10.3390/math13121941.

16. Horalek, J. Business Impact Analysis of AMM Data: A Case Study. *Applied System Innovations*, 2023, vol. 6, no. 5, article no. 82. DOI: 10.3390/asi6050082.

17. Mukundhan, H. A Business-Integrated Approach to Incident Response. *ISACA Journal*, 2015, vol. 6, pp. 1–5. Available at: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-6/a-business-integrated-approach-to-incident-response (accessed 19 June 2025).

18. European Parliament and Council, 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504 (accessed 19 June 2025).

19. CISA, 2022. *Traffic Light Protocol 2.0 User Guide (TLP 2.0) for Marking Confidential Information in Cyber Incident Reports*. Available at: https://www.cisa.gov/sites/default/files/2023-02/tlp-2-0-user-guide_508c.pdf (accessed 19 June 2025).

20. FIRST, 2019. *CVSS v3.1 Specification Document - Revision 1*. Available at: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf (accessed 19 June 2025).

21. Verkhovna Rada of Ukraine, 2017. *Law of Ukraine No. 2163-VIII "On the Basic Principles of Ensuring the Cybersecurity of Ukraine"*. Kyiv: Verkhovna Rada of Ukraine. Available at: https://zakon.rada.gov.ua/laws/show/2163-19 (accessed 19 June 2025). (In Ukrainian).

22. National Security and Defense Council of Ukraine, 2022. *Implementation Plan of the Cybersecurity Strategy of Ukraine*. Decision of the National Security and Defense Council of Ukraine dated 30 December 2021, enacted by the Presidential Decree No. 37/2022 of 1 February 2022. Kyiv: National Security and Defense Council of Ukraine. Available at: https://zakon.rada.gov.ua/laws/show/n0087525-21 (accessed 19 June 2025). (In Ukrainian).

23. State Service of Special Communications and Information Protection of Ukraine, 2023. *Order No. 570 dated 3 July 2023 "On Approval of Methodological Recommendations for Cybersecurity Entities' Response to Various Types of Cyber Incidents"*. Available at: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-

zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostori (accessed 19 June 2025). (In Ukrainian).

24.ISO/IEC 27005:2022. *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. Available at: https://www.iso.org/standard/80585.html (accessed 19 June 2025).

25.Shevchenko, P. V., Jang, J., Malavasi, M., Peters, G. W., Sofronov, G., & Trück, S. The nature of losses from cyber-related events: risk categories and business sectors. *Journal of Cybersecurity*, 2023, vol. 9, no. 1. DOI: 10.1093/cybsec/tyac016.

26.von Skarczinski, B., Raschke, M., & Teuteberg, F. Modelling maximum cyber incident losses of German organisations: an empirical study and modified extreme value distribution approach. *Geneva Papers on Risk and Insurance-Issues and Practice*, 2023, vol. 48, iss. 2, pp. 463–501. DOI: 10.1057/s41288-023-00293-x.

27.Ovezgeldiev, A. O., Petrov, E. G., & Petrov, K. E. *Syntez ta identyfikatsiya modeley bahatofaktornoho otsinyuvannya ta optymizatsiyi* [Synthesis and Identification of Models of Multifactor Evaluation and Optimization]. Kyiv, Naukova dumka, 2002. 161 p. (In Ukrainian).

28.Kopytsia, O., & Burchenko, S. *Cyber Security Incidents Prioritization Mechanism*. 2024. Available at: https://csipm.online (accessed 19 June 2025).

29.Zhang, S., Cai, M., Zhang, M., Zhao, L., & de Carnavalet, X. d. C. The Flaw Within: Identifying CVSS Score Discrepancies in the NVD. *2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, Naples, Italy, IEEE, 2023, pp. 185–192. DOI: 10.1109/CloudCom59040.2023.00039.

30.Krisper, M. *Problems with Risk Matrices Using Ordinal Scales*. ArXiv, 2021. DOI: 10.48550/arXiv.2103.05440.

31.Renners, L., Heine, F., Kleiner, C., & Rodosek, G. D. Concept and Practical Evaluation for Adaptive and Intelligible Prioritization for Network Security Incidents. *International Journal on Cyber Situational Awareness*, 2019, vol. 4, no. 1, pp. 99–127. DOI: 10.22619/IJCSA.2019.100127.

32. Vulpe, S.-N., Rughiniș, R., Țurcanu, D., & Rosner, D. AI and Cybersecurity: A Risk Society Perspective. *Frontiers in Computer Science*, 2024, vol. 6, article no. 1462250. DOI: 10.3389/fcomp.2024.1462250.

Received 15.08.2025, Received in revised form 17.10.2025
Accepted date 17.11.2025, Published date 08.12.2025

ІНТЕГРАЦІЯ CVSS, НАЦІОНАЛЬНИХ РІВНІВ КРИТИЧНОСТІ ТА MCDA ДЛЯ БАГАТОФАКТОРНОЇ ПРІОРИТИЗАЦІЇ КІБЕРІНЦИДЕНТІВ

Д. Ю. Узлов, С. В. Яковлев, О. Г. Толстолузька, О. Копиця, С. Бурченко

Метою цього дослідження є розробка багатофакторного підходу до пріоритизації кіберінцидентів, що дозволить організаціям, зокрема командам реагування національного рівня, таким як CERT-UA, ефективно розподіляти свої обмежені ресурси та оперативно реагувати на найкритичніші загрози. Шляхом інтеграції найкращих світових практик, таких як Загальна система оцінки вразливостей (CVSS) та багатокритеріальний аналіз рішень (MCDA), з національними нормативно-правовими стандартами України, дослідження прагне вирішити проблеми недостатньої деталізованості та усунення неоднозначностей в існуючій національній класифікації. Цей інтегрований підхід має на меті запобігти неефективній пріоритизації, забезпечити оптимальний розподіл ресурсів та прискорити відновлення інформаційних систем. **Методологія:** запропонована методологія встановлює ієрархічний, багатофакторний підхід до пріоритизації. Вона інтегрує кількісну оцінку технічної серйозності, надану CVSS, з національними рівнями критичності України. Ця дворівнева система оцінювання додатково доповнюється структурованим механізмом врегулювання суперечностей з використанням додаткових атрибутів для досягнення точної пріоритизації. Було створено структурований набір даних, що охоплює загальнонаціональний вплив, економічні наслідки, інформаційні наслідки, функціональні наслідки, можливості відновлення та особливості системи/мережі. Була розроблена методологія пріоритизації, що включає п’ять ключових фаз: реєстрація інциденту, верифікація даних, кореляція та агрегація, оцінка критичності та врегулювання суперечностей. Було впроваджено спеціалізоване програмне забезпечення для моделювання алгоритму в середовищі CERT-UA, що дозволяє в режимі реального часу реєструвати, оцінювати та візуалізувати пріоритизовані інциденти. Моделювання перевірило ефективність алгоритму в обробці потоку інцидентів та його потенціал для оптимізації заходів реагування. **Висновки:** це дослідження представляє надійну та інноваційну багатофакторну методологію, яка долає недостатню деталізованість існуючих національних рівнів критичності. Запроваджуючи ієрархічний механізм вирішення конфліктів, цей підхід надає CERT-UA чіткий, вирішальний та ефективний інструмент для пріоритизації інцидентів. Моделювання та пілотні впровадження підтверджують практичну цінність алгоритму та його безпосередню застосовність в існуючих операційних середовищах, що значно підвищує здатність команд реагування національного рівня пом’якшувати негативні наслідки кіберзагроз. Простота та адаптивність системи забезпечують її застосовність в існуючих операційних середовищах, а механізм врегулювання суперечностей мінімізує ризик неефективної пріоритизації. Майбутні напрямки досліджень включають інтеграцію штучного інтелекту та машинного навчання для підвищення точності пріоритизації та адаптацію цієї методології до різних організаційних контекстів. Ця робота закладає міцну основу для вдосконалення управління кіберінцидентами, враховуючи мінливий характер викликів у сфері кібербезпеки.

Ключові слова: пріоритизація кіберінцидентів; рівні критичності; кібератаки; обробка інцидентів; CVSS; MCDA; симуляційні тести; новітні технології; штучний інтелект; машинне навчання.

Узлов Дмитро Юрійович – канд. техн. наук, доц., директор навчально-наукового інституту комп’ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна, Харків, Україна.

Яковлев Сергій Всеволодович – член-кореспондент НАН України, д-р фіз.-мат. наук, проф., заступник директора навчально-наукового інституту комп’ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна, Харків, Україна; професор-дослідувач Інституту математики Лодзинського політехнічного університету, Лодзь, Польща.

Толстолузька Олена Геннадіївна – д-р техн. наук, проф., проф. каф. комп’ютерних систем та робототехніки навчально-наукового інституту комп’ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна, Харків, Україна.

Копиця Олександр – асп. навчально-наукового інституту комп’ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна, Харків, Україна.

Бурченко Сергій – асп. навчально-наукового інституту комп’ютерних наук та штучного інтелекту Харківського національного університету імені В. Н. Каразіна, Харків, Україна.

Dmytro Uzlov – Candidate of Technical Sciences, Associate Professor, Director of the Institute of Computer Science and Artificial Intelligence at V. N. Karazin Kharkiv National University, Kharkiv, Ukraine,
e-mail: dmytro.uzlov@karazin.ua, ORCID: 0000-0003-3308-424X, Scopus Author ID: 57201780269.

Sergiy Yakovlev – Corresponding Member of the National Academy of Sciences of Ukraine, Doctor of Physical and Mathematical Sciences, Professor, Deputy Director of the Institute of Computer Science and Artificial Intelligence at V. N. Karazin Kharkiv National University, Kharkiv, Ukraine; Research Professor at the Institute of Mathematics, Lodz University of Technology, Lodz, Poland.
e-mail: s.yakovlev@karazin.ua, ORCID: 0000-0003-1707-843X, Scopus Author ID: 7006718461.

Olena Tolstoluzka – Doctor of Technical Sciences, Senior Researcher, Professor of the Department of Computer Systems and Robotics at the Institute of Computer Sciences and Artificial Intelligence of V.N. Karazin Kharkiv National University, Kharkiv, Ukraine,
e-mail: elena.tolstoluzka@karazin.ua, Scopus Author ID: 57418069200.

Oleksandr Kopytsia – PhD Student, Institute of Computer Science and Artificial Intelligence at V. N. Karazin Kharkiv National University, Kharkiv, Ukraine,
e-mail: oleksandr.kopytsia@student.karazin.ua.

Sergiy Burchenko – PhD Student, Institute of Computer Science and Artificial Intelligence at V. N. Karazin. Kharkiv National University, Kharkiv, Ukraine,
e-mail: serhii.burchenko@karazin.ua.