UDC 004.056:004.774:378 DOI: 10.31673/2409-7292.2026.026315

Elizaveta Zavhorodnya
PhD (international economic relations), the Head of Library Department
State University of Trade end Economics, Kyiv, Ukraine
ORCID: 0000-0003-0549-7020
E-mail: y.zavhorodnya@knute.edu.ua

Yaroslav Shestak
PhD (computer sciences), Senior Lecturer at the Department of Software Engineering and Cybersecurity
State University of Trade and Economics, Kyiv, Ukraine
ORCID: 0000-0002-5102-9642
E-mail: shestack@knute.edu.ua

Olena Kryvoruchko
Doctor of Technical Science, Professor at the Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0002-7661-9227
E-mail: ev_kryvoruchko@ukr.net

Oleh Kulinich
Candidate of Technical Sciences, Associate Professor at the Department of Computer Systems, Networks and Cybersecurity
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0002-0643-6898
E-mail: o.kulinich@nubip.edu.ua

MODELING AN EVALUATION SYSTEM FOR DDoS ATTACK DETECTION TOOLS IN HEI'S WEB RESOURCES

This study addressed the need for a comprehensive approach to the assessment and selection of cybersecurity tools for protecting web resources in higher education institutions (HEIs) against modern cyber threats, particularly distributed denial-of-service (DDoS) attacks. This study examined contemporary threats to the information security of web resources and justified the need for their timely identification, analysis and neutralisation in order to ensure the continuity of information systems, particularly in HEIs. The academic literature review showed that traditional approaches to monitoring and protecting information systems are inefficient in spite of modern multi-vector attacks, requiring a shift towards integrated, adaptive and intelligent cybersecurity systems. Short-term but intense cyberattacks (e.g. DDoS incidents), can significantly disrupt service availability in the absence of proper protection measures. Additionally, we found that effective protection of web resources requires a thorough approach that ensures the confidentiality, integrity, and availability of information, along with the ability to adapt to the changing conditions in cyber environment. A multi-layered cybersecurity architecture and a hybrid DDoS detection framework were proposed. The proposed framework combined signature-based, behavioural, and statistical methods to facilitate effective and modifiable threat detection system. In order to support objective decision-making, a multi-criteria hierarchical evaluation model was designed. The proposed evaluation model included nine criteria groups that were aimed at assessing technical performance, scalability, adaptability, integration capability, automation, and cost-effectiveness. The proposed method enables an organised and transparent comparison of DDoS detection tools on specific conditions of higher research institutions.

Keywords: cyber threats, SIEM systems, higher education institution web resources, DDoS attacks, cyber resilience, attack detection, provision of educational services.

Introduction

The accelerated advancement of information and communication technologies (ICTs) is associated with a constant increase in the number of web resources, the emergence of new economic entities, and, consequently, the evolution of cyber threats scope. In such circumstances, the cyberspace becomes a high-risk environment, where the probability of attacks, malicious interference, or large-scale technical failures is an integral element of how information systems operate. In terms of cybersecurity, the web environment is constantly under pressure, driven both by the increasing number of possible attack vectors and by the advanced complexity of their methods. At present, users and organisations should consider the risks of unauthorised access, data leaks,

breaches of information integrity, and denial-of-service incidents. In this regard, the implementation of cybersecurity systems that include prevention, detection, and response procedures is crucially important.

All economic entities (from small businesses to large companies and public institutions) necessitate a systematic method to ensure information security, which integrates monitoring technologies, incident management systems, risk assessment techniques, and the development of resilient ICT infrastructures that can effectively counteract modern cyber threats. Moreover, it is essential to focus on maintaining operational continuity and protecting critical digital assets.

Higher education institutions (HEIs), including their web resources and educational process management systems, are exposed to cyber threats. Due to the open nature of educational environment and considerable volume of processed data, information systems become attractive targets for cybercriminals. Therefore, the issue of developing approaches aimed to ensure cyber resilience, reliability and security of HEIs' information infrastructure is a fundamental requirement for fostering user confidence and securing the educational service provision continuity.

Accordingly, there is an imperative to implement efficient security procedures for existing and recently designed HEIs' information resources, including advanced cybersecurity technologies utilisation, the regular security audits performance, user awareness and cyber hygiene skills strengthening, as well as overarching cyber resilience strategy development. Hence, these measures will enhance HEI's secured digital environment.

Literature review

In [1-3], HEIs are viewed as complex and intricate socio-technical systems composed of educational, administrative, and resource information systems (IS), which are greatly dependent on information infrastructure (II) reliability. In particular, [3] proposes a systemic approach to modelling the HEI cybersecurity, encompassing the analysis of infrastructure components interrelationships and the assessment of their influence on HEIs' overall cyber resilience. Simultaneously, [1] highlights the constraints of conventional monitoring systems, which fail to perform a detailed examination of the HEIs' II state and are incapable to respond proactively to cybersecurity incidents. Further development in this area is presented in [2], where the authors substantiated adaptive and intelligent cybersecurity systems (e.g. SIEM) implementation practicability, since they are capable to consolidate heterogeneous data sources and perform unified cybersecurity management. However, even advanced SIEM systems possess substantial limitations, notably low effectiveness in detecting DDoS attacks unless additional network traffic analysis tools or machine learning (ML) algorithms are used [4].

The study [5] highlights the increasing complexity and multidimensional nature of DDoS attacks, as well as the necessity to utilise several detection methodologies (e.g. signature analysis, anomaly detection and network monitoring tools). Additionally, the study [6] proves decision trees high effectiveness (with accuracy exceeding 99%) if the selection of features and training parameters was appropriate. However, the accuracy and applicability of decision trees depend on datasets quality and experimental conditions.

Another direction of development involves the inclusion of AI in network architectures (SDN, NFV), enabling adaptive resource management and proactive threat detection [7]. In the study [8] authors generalised approaches to cyberattack classification and distinguished the main quality characteristics of cybersecurity systems (i.e., performance, efficiency, compatibility, security and stability), stressing the importance of their formalisation and application in standardised models. At the same time, the utilisation of AL in monitoring systems increases threat detection accuracy and reduces the number of false positives [9]. Notably, multi-layered security strategy is essential due to insufficient efficiency of conventional security tools and methods (e.g., firewalls) against modern DDoS attacks [10].

Thorough examination of security systems is also important; however different scanning and auditing tools may produce varying and inconsistent assessments of the security level, thus complicating unbiased comparison of their effectiveness [11]. Furthermore, recent study indicates the

© Zavhorodnya E.O., Shestak Y.I., Kryvoruchko O.V., Kulinich O.M. Modeling an evaluation system for DDoS attack detection tools in HEI's web resources. Сучасний захист інформації, 2(66), 178–190. https://doi.org/10.31673/2409-7292.2026.026315

emergence of new types of attacks, in particular slow DDoS attacks, which are difficult to detect using traditional methods. In [12], an approach to their detection is proposed based on correlation analysis of user behaviour trajectories and traffic parameter prediction.

Thus, the literature review demonstrates that existing approaches to detecting DDoS attacks are diverse but fragmented: they are either focused on individual tools or on individual methods, without taking into account a comprehensive assessment of their effectiveness under the real HEI operating conditions.

The aim is to develop a model for evaluating and comparing DDoS attack detection tools.

Results

The foundation of this study is the substantiated need for a comprehensive assessment and selection of optimal approaches to protecting web resources from contemporary cyber threats. The implementation of this objective requires a comprehensive analysis of the information infrastructure, including the identification of data flows, the determination of information sources, the examination of transmission channels, and the assessment of vulnerabilities inherent in web resources as objects of information interaction. This approach enables the formation of a holistic understanding of potential risks and the identification of critical points of influence within the system.

Considering the evolution of information technologies and cyber threats, traditional security methods, such as data archiving, backup, and physical monitoring of infrastructure, are losing their value and adequacy as means of protection. Under contemporary conditions, they should be regarded solely as components of an integrated cybersecurity system. Particular attention should be devoted to the analysis of distributed denial-of-service (DDoS) attacks, which may be external, internal or hybrid in nature. Each of these types of attack is characterised by specific mechanisms of execution and requires the application of differentiated approaches to their detection and neutralisation.

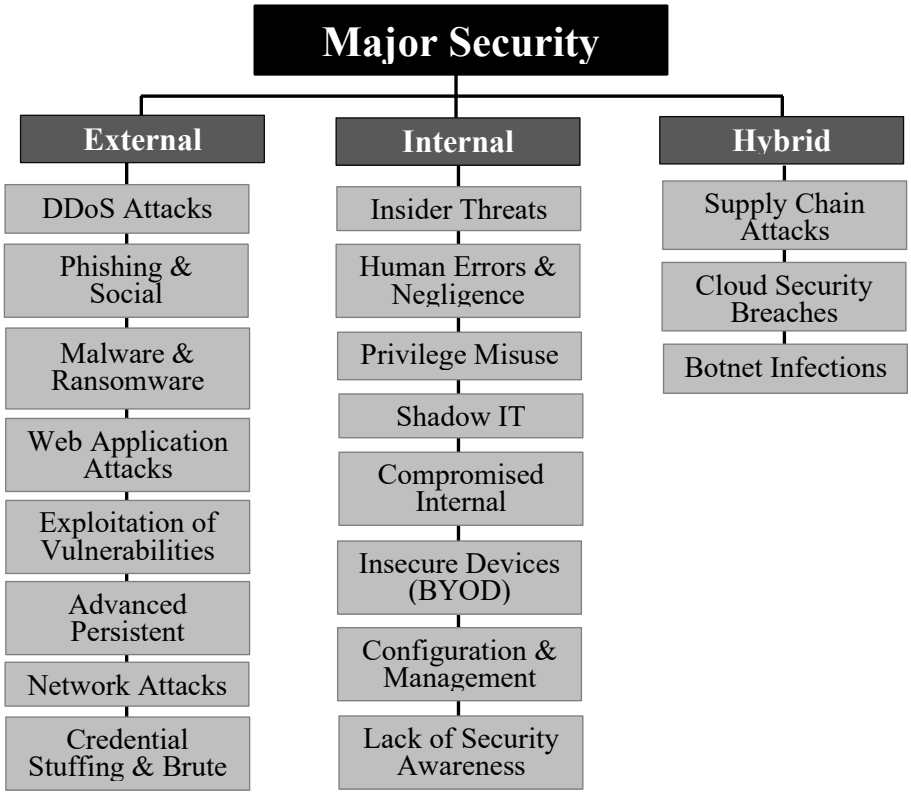

Fig. 1. Major Cyber Threats to HEI's Information Infrastructure

HEIs' web resources play a significant role in facilitating information exchange with both internal and external systems, including state and municipal platforms such as Smart City, USEDE,

‘Prozorro’ and other information services. This increases the requirements for their reliability, availability and compliance with established information security standards. Such responsibility may involve both administrative and criminal liability, particularly within the context of integration into the international educational environment and cooperation with foreign partners. At the same time, a lack of awareness of this liability among management staff creates additional risks to the information security of institutions.

The threat landscape of HEIs’ II includes high-impact attacks and internal weaknesses in operations and ISs protection mechanisms, as well as hybrid threats (Fig. 1). In order to mitigate negative impact of DDoS attacks, this combination requires development of a holistic system of cybersecurity measures, along with formalisation model to assess detection and protection tools effectiveness.

The aforementioned threats form a complex, multi-layered system of risks that require timely identification, classification and prompt notification of the relevant cybersecurity specialists in order to support managerial decision-making aimed at their neutralization or impact minimisation. A distinctive feature of modern cyber threats is their high degree of dynamism: a considerable proportion of attacks are executed instantly, are short-term in nature, yet remain capable of causing significant disruptions to the functioning of information systems. Without appropriate technical and organisational methods to detect and countermeasure cyber risks, even known threats may lead to serious consequences (e.g. compromise of resources, data loss or the complete downtime of web services), thus affecting HEIs’ ability to maintain educational process and deliver online services.

A key aspect in the development of an effective protection system is the substantiated selection of tools capable of not only counteracting current threats but also of adapting to changes in the cyber environment. Such tools must satisfy the requirements of scalability, flexibility and compatibility, thereby enabling their future modernisation, updating, restructuring or integration with other information systems. An important feature of modern cybersecurity solutions is their capability to automate the processes of incident detection, threat analysis and response.

Despite the availability of a wide range of both commercial and free cybersecurity solutions, their effectiveness depends to a large extent on the proper allocation of administrative functions, as well as on the clear segmentation of web resources and associated services. Consequently, the lack of proper distribution lowers security levels and complicates the incident management. From this perspective, it is imperative to regularly update the software for information systems that support web resources, since consistent updates help to maintain system stability, eliminate exposures and ensure uninterrupted user access to information.

The selection of appropriate security measures necessitates a comprehensive knowledge of the object being protected, including analysis of its architecture, functionalities, types of information it processes, and possible channels of attack. Based on this analysis, existing cybersecurity solutions are monitored and an integrated web resource protection system is developed. Such a system comprises a set of interrelated software, hardware tools and organisational measures aimed at preventing unauthorised access, information theft, data integrity breaches and the disruption of web resources. The fundamental components of a web resource security system include specialised tools for analysing and filtering traffic. In particular, a Web Application Firewall (WAF) performs deep inspection of HTTP/HTTPS requests and blocks attacks at the application protocol level, including SQL injection and cross-site scripting (XSS). An important element is intrusion detection and prevention systems (IDS/IPS), which continuously monitor network traffic, detect anomalies and respond in accordance with defined security policies. Integrating such systems with SIEM platforms enables centralised management of security events, their correlation, and automated incident responses. Protection against DDoS attacks is achieved through the specialised load balancing and traffic filtering services in order to distribute request flows, detect anomalous activity, and block of malicious traffic, ensuring users can access HEI’s web resources even under intense load. Network threats can be both long-term and short-term, which means tools for constant analysis and forecasting possible outcomes become integral part of HEIs’ cybersecurity management system.

© Zavhorodnya E.O., Shestak Y.I., Kryvoruchko O.V., Kulinich O.M. Modeling an evaluation system for DDoS attack detection tools in HEI’s web resources. Сучасний захист інформації, 2(66), 178–190. https://doi.org/10.31673/2409-7292.2026.026315

Vulnerability scanners play a significant role in ensuring cybersecurity, since they automate auditing of ISs, find weaknesses in software code, configurations and network infrastructure. Consistent utilisation of vulnerability scanners helps to promptly address potential external, internal and hybrid threats. Furthermore, SSL/TLS cryptographic protocols provide additional security layer, keeping data private during transmission between client and server components.

Contemporary cyber security trends include using artificial intelligence (AI) and machine learning (ML) technologies to automate threat detection based on user and system behaviour analysis. Automated software update measures are equally crucial, since a significant proportion of vulnerabilities arises from outdated system components. Comprehensive security platforms merge various protection measures into a cohesive environment, which improves the management of cyber threat. The development of a resilient web resource protection system is based on a combination of several security layers, including infrastructure protection (servers and file systems), data protection (encryption and backup procedures) and continuous activity monitoring (analysis of event logs and network traffic). This approach ensures the implementation of the key principles of information security – confidentiality, integrity and availability of information. The proposed model of a resilient web resource protection system for a HEI (Fig. 2) integrates infrastructure protection, data security procedures and permanent surveillance of processes within a unified security management framework. The model (Fig. 2) features a user interaction layer at the top, serving as the primary entry point to institutional web resources and defines the need for controlled and secure access mechanisms.

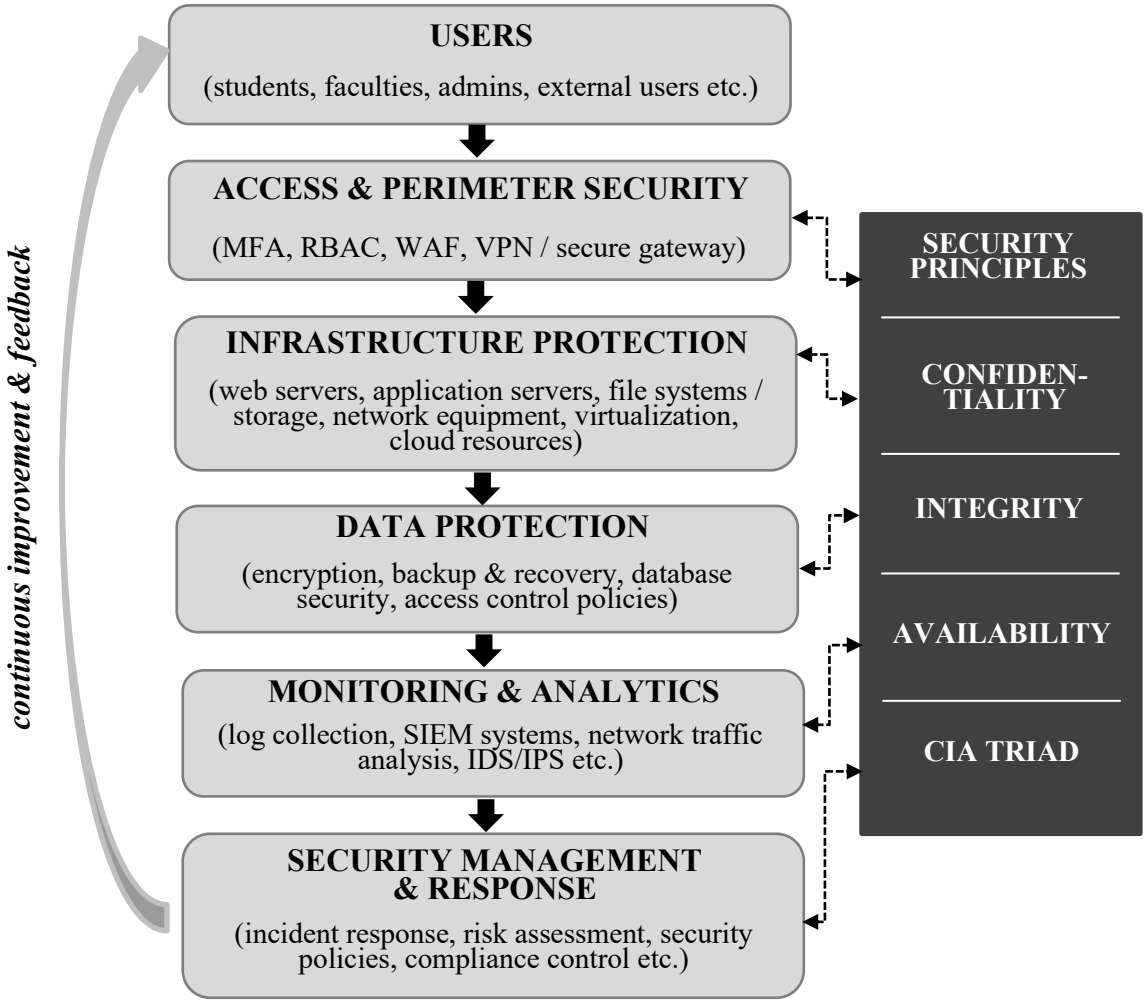

Fig. 2. HEI's resilient web resource protection system

© Zavhorodnya E.O., Shestak Y.I., Kryvoruchko O.V., Kulinich O.M. Modeling an evaluation system for DDoS attack detection tools in HEI's web resources. Сучасний захист інформації, 2(66), 178–190. https://doi.org/10.31673/2409-7292.2026.026315

The second layer, access and perimeter security, performs the critical function of regulating user access to system resources. It implements authentication mechanisms, as well as authorisation models. Additionally, this layer integrates perimeter defence technologies, which protect against unauthorised access and external cyber threats.

The infrastructure protection layer is responsible for HEI's II security and resilience, as it supports ISs operational stability and protects against disruptions resulting from hardware attacks or vulnerabilities at the system level.

The data protection layer aims to secure sensitive information processed and stored within the system. This layer is essential for maintaining data integrity and preventing unauthorised access or accidental loss of information.

The monitoring and analytics layer aggregates event logs, analyses network traffic and utilises IDS/IPS and SIEM approaches to unusual activities in HEIs' II, detect possible security risks, and support proactive security measures.

The security management and response layer ensures the overall efficiency of protection system operations of protection system to manage security events, help to appropriately respond to emerging threats through continuous modification and improvement.

An important aspect of the model is a feedback loop, connecting the security management layer to higher levels of the architecture. The proposed mechanism allows for adjustments in security policies and controls based on identified threats and changes in system performance.

The primary objectives of the proposed approach are to:

- ensure thorough protection of web resources within a HEI;
- provide a structured and scalable approach to cybersecurity measures implementation;
- enable continuous monitoring and rapid detection of security incidents;
- meet security standards and regulatory requirements;
- support the reliable and uninterrupted operation of HEI's services.

The model performs key functions including user access control and verification management (to prevent unauthorised system entry), protection of infrastructure components against cyberattacks and system failures, data security management (using encryption and regular backups), real-time monitoring and threat detection via log and traffic analysis, incident response and risk mitigation (to minimise the impact of security breaches), and continuous improvement through feedback-driven adaptation of security policies.

The implementation of the proposed model provides several advantages for HEIs, including an enhanced security posture achieved through a layered, defence-in-depth strategy that minimises system vulnerabilities and protects against various of cyber threats (e.g. DDoS attacks, unauthorised access, and data breaches); effective protection of sensitive academic and administrative data (by ensuring the confidentiality and integrity of student records, research outputs, and institutional information); increased system availability and reliability (with continuous monitoring and rapid response mechanisms that minimise downtime and ensure the continuity of educational services); scalability and adaptability common for a modular architecture (in accordance with changing technological and organisational needs); regulatory compliance and governance through the enforcement of security policies and adherence to cybersecurity standards and legal requirements; and proactive threat management supported by continuous monitoring and analytics (with early anomaly detection and timely response to potential security incidents before they become critical threats).

The detection and response to DDoS attacks on web resources involve several methods, each with its own strengths and limitations. The signature-based approach depends on predefined attack patterns and is accurate for known threats; however, it struggles with new or modified attacks. The behavioural approach identifies deviations from normal system activity, thereby allowing for the detection of previously unknown threats. Nevertheless, this approach can generate false positives and requires constant refinement. Statistical methods analyse quantitative traffic trends, e.g. request

© Zavhorodnya E.O., Shestak Y.I., Kryvoruchko O.V., Kulinich O.M. Modeling an evaluation system for DDoS attack detection tools in HEI's web resources. Сучасний захист інформації, 2(66), 178–190. https://doi.org/10.31673/2409-7292.2026.026315

intensity or packet timing, and are effective for detecting large-scale attacks, but require setting threshold values and regularly adjusting operational parameters.

Thus, effectively detecting and responding to modern cyber threats demands a thorough integration of various approaches and technologies, which help the protection system to adapt to the dynamic cyber environment and enhance HEIs' web resources cyber resilience. The presented flowchart (Fig. 3) illustrates a universal approach for detecting and mitigating DDoS attacks targeting HEIs' web resources. The approach incorporates a hybrid detection strategy that combines signature-based, behavioural, and statistical methods within a unified cybersecurity framework. This integration enables the system to identify both known and new attack patterns while continuously adjusting to evolving cyber threats.

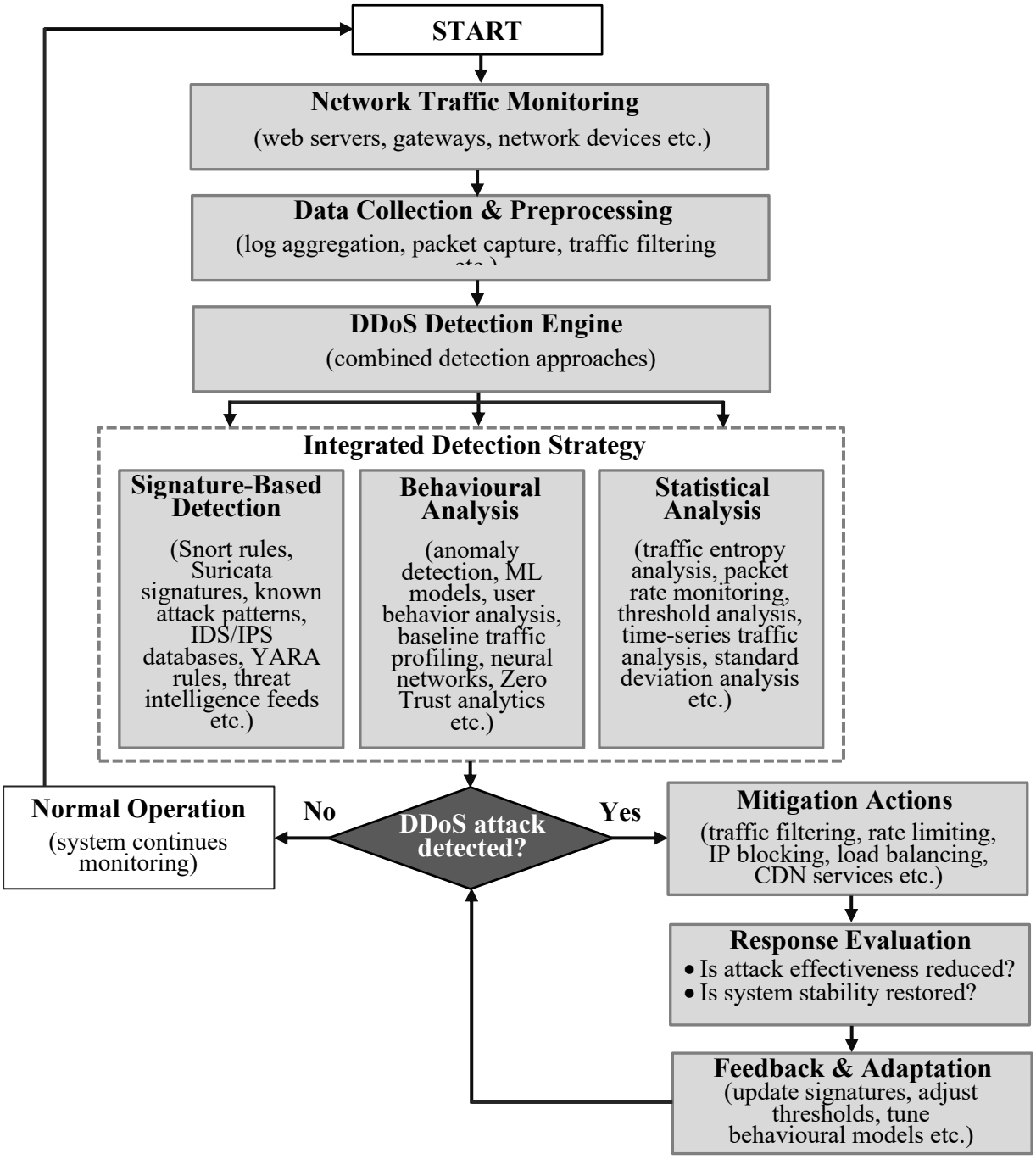

Fig. 3. Flowchart of DDoS attack detection and mitigation in HEIs

© Zavhorodnya E.O., Shestak Y.I., Kryvoruchko O.V., Kulinich O.M. Modeling an evaluation system for DDoS attack detection tools in HEI's web resources. Сучасний захист інформації, 2(66), 178–190. https://doi.org/10.31673/2409-7292.2026.026315

The process begins with monitoring network traffic from web servers, gateways and network devices in real-time. This stage gives insight into the operational state of HEI's network infrastructure and serves as the main source of security data. The gathered information is then transferred to the data collection and pre-processing stage, where irrelevant or duplicate data is removed, and traffic features are normalised for further analysis. This pre-processing step makes the detection processes more efficient and accurate.

The core component of the approach is the hybrid DDoS detection engine, which combines three complementary detection methodologies:

- signature-based detection identifies known attack patterns using set rules, signatures and intrusion detection system databases to ensure high accuracy for recognised threats and to enable rapid recognition of common attack types;
- behavioral analysis aims to capture anomalies and deviations from baseline traffic behaviour to detect unknown or modified attacks;
- statistical analysis evaluates quantitative traffic characteristics to identify large-scale volumetric DDoS attacks through the examination of abnormal traffic fluctuations.

The analytical modules provide outputs that are used within the decision-making stage. At this stage the system assesses whether the observed activity is a DDoS attack. If no malicious activity is detected, the system continues to operate normally while monitoring remains active. However, if an attack is detected, the model activates the mitigation layer, applying defensive measures. After mitigation, the system proceeds to the response evaluation stage to assess how effective the countermeasures were. The system checks whether the attack intensity has decreased and whether the stability and availability of institutional web services have been restored. An important feature of the proposed approach is feedback and adjustment mechanism, which supports continuous improvement of the protection system. This feedback loop boosts the resilience of the system and ensures its capability to respond to changes in the cyber threats.

Implementing the proposed hybrid DDoS detection and mitigation approach offers the following advantages for HEIs:

1) the combination of multiple detection methods significantly improves threat identification by merging signature-based, behavioural, and statistical analysis, thereby reducing false positives and false negatives while enabling the detection of both known and unknown attacks;

2) the model enhances the availability and continuity of educational services by enabling rapid response and mitigation of cyberattacks, thereby ensuring uninterrupted access to institutional online resources (e-learning platforms, digital libraries, research repositories etc.);

3) the model strengthens the cyber resilience of HEIs by introducing adaptable security mechanisms, whereby the continuous updates of detection parameters and analytical models keep the system effective against evolving attack techniques and changing network conditions;

4) the modular design of the model allows HEIs to add security technologies, analytical tools, or mitigation services according to their infrastructure size and cybersecurity requirements;

5) the use of automated monitoring and analytical processes reduces the workload on cybersecurity personnel and improves the efficiency of incident response efforts;

6) the proposed approach contributes to improved information security governance and regulatory compliance by supporting systematic monitoring, incident documentation, and policy enforcement.

To evaluate the effectiveness of DDoS detection tools, we suggest a multi-criteria hierarchical model. The overall assessment is the weighted sum of normalised metrics across nine groups of criteria, covering detection accuracy, timing, scalability, resource consumption, costs, as well as integration and automation capabilities (1).

$$S_j = \sum_{k=1}^{9} W_k \times G_{kj} \,, \tag{1}$$

where W_k is the weight of the criterion group, and G_{kj} is the score of the k^{th} group for tool j.

© Zavhorodnya E.O., Shestak Y.I., Kryvoruchko O.V., Kulinich O.M. Modeling an evaluation system for DDoS attack detection tools in HEI's web resources. Сучасний захист інформації, 2(66), 178–190. https://doi.org/10.31673/2409-7292.2026.026315

Table 1 presents a proposed weight distribution for a balanced consideration of the technical, operational and economic aspects of evaluating DDoS attack detection tools, which can be further adapted depending on the specific operating conditions of the HEI's information infrastructure. The weighting coefficients of the criteria groups were determined taking into account the specific nature of the operation of the HEI's information infrastructure, which is characterised by an openness of the network environment, high traffic dynamism and limited cybersecurity resources.

Table 1

System of criteria for evaluating DDoS attack detection tools

Criteria Group	Criteria	Weight W_k	Comment
Detection Performance	True Positive Rate (TPR, Recall), False Positive Rate (FPR), Precision, F1-score, ROC-AUC, False Negative Rate (FNR)	0.25	in HEI environment, a high FPR may disrupt or paralyse the operation of institutional services
Detection latency	time from attack initiation to detection, time to mitigation (TTM), real-time capability, throughput under attack	0.15	DDoS-attacks produce rapid effects; therefore, if the system responds with delay, even accurate detection loses practical value
Scalability	ability to operate under increasing numbers of users, network nodes, and traffic volumes	0.10	workloads across different elements of the HEI information infrastructure are uneven and frequently peak-oriented
Performance Overhead	CPU/RAM utilization, impact on network throughput, traffic processing latency	0.10	limited HEI budgets require the implementation of economically justified security solutions
Total Cost of Ownership (TCO)	licensing, deployment, maintenance, updates	0.10	
Adaptability and Learning Capability	ability to detect zero-day attacks, updating of models/signatures, operation under dynamic traffic conditions	0.10	HEI traffic is unstable; therefore, static rules are often ineffective
Supported Attack Types	types of DDoS-attacks detected by the system/tool, including volumetric (UPD flood), protocol-based (SYN flood), application layer (HTTP flood) attacks	0.08	HEI actively utilize web services; consequently, the detection of multiple attack types is essential
Integration Capability	compatibility with SIEM systems, IDS/IPS, network equipment, API	0.07	the ability of the tool to be easily integrated into the HEI cybersecurity infrastructure is important
Automation Capability	ability of the system to automatically block traffic, modify firewall rules, and initiate response scenarios	0.05	limited cybersecurity staffing in HEIs necessitates the minimization of manual intervention

The 'Detection Performance' (G_1) criteria group characterises the system's ability to correctly identify DDoS attacks, taking into account sensitivity and precision metrics, thereby enabling the assessment of the balance between attack detection and the number of false positives (2).

$$G_1 = 0.25\begin{pmatrix}0.25TPR + 0.20Precision + 0.15F1 + 0.15ROC + \\ 0.15(1 - FPR) + 0.10(1 - FNR)\end{pmatrix}. \quad (2)$$

The FPR and FNR metrics are represented as *(1 – FPR)* and *(1 – FNR)*, as reducing them is desirable. The 'Detection Latency' (G_2) criteria group assesses how quickly the system responds to an attack (3). The detection time *L* and time-to-mitigation *TTM* metrics are used in an inverse manner (-1), meaning that lower values are considered more preferable.

$$G_2 = 0.15(0.35L^{-1} + 0.25TTM^{-1}) + 0.20RTC + 0{,}20T_{attack} . \quad (3)$$

The ‘Scalability’ criteria group (G_3) reflects how well the tool can work properly when the load increases (4). The greatest weight is assigned to user load, which is typical for a HEI environment with a large number of simultaneous connections.

$$G_3 = 0.10(0.4Users + 0.3Nodes + 0.3Traffic) . \quad (4)$$

The ‘Performance Overhead’ (G_4) criteria group assesses the impact of the tool on system resources (5). Using inverse indicator values ensures correct interpretation: lower resource consumption corresponds to a higher value for the criterion.

$$G_4 = 0.10(0.4CPU^{-1} + 0.3RAM^{-1} + 0.3Latency^{-1}) . \quad (5)$$

The ‘Total Cost of Ownership’ (G_5) criteria group addresses the economic viability of using the tool (6). All cost components (licensing, implementation, support, updates) are treated as cost indicators and are therefore presented in inverted form. The licence cost carries the greatest weight, as it constitutes the principal share of expenditures.

$$G_5 = 0.10(0.4License^{-1} + 0.2Deploy^{-1} + 0.2Support^{-1} + 0.2Update^{-1}) . \quad (6)$$

The ‘Adaptability’ criteria group (G_6) characterises the system’s ability to adapt to new threats (7). The greatest weight is given to the ability to detect unknown (zero-day) attacks, which is critical under contemporary conditions.

$$G_6 = 0.10(0.4ZeroDay + 0.3Update + 0.3DynamicTraffic) . \quad (7)$$

The ‘Supported Attack Types’ criteria group (G_7) assesses the comprehensiveness of coverage for various types of DDoS attacks (8). The greatest weight is assigned to volumetric and application-level attacks, as they are the most common and critical for web-oriented services of HEIs.

$$G_7 = 0.08(0.35Vol + 0.30Prot + 0.35App) . \quad (8)$$

The ‘Integration Capability’ (G_8) criteria group determines the tool’s ability to integrate into existing infrastructure (9). The greatest weight is given to integrations with SIEM and IDS/IPS systems, which provide centralised security management.

$$G_8 = 0.07(0.3SIEM + 0.3IDS + 0.2Network + 0.2API) . \quad (9)$$

The ‘Automation Capability’ criteria group (G_9) measures how automated the response to attacks is (10). The ability to automatically block traffic is given the highest weighting, as it directly affects response speed.

$$G_9 = 0.05(0.4AutoBlock + 0.3Firewall + 0.3Scenarios) . \quad (10)$$

The indicators are normalised for positive (11) and cost-related/negative criteria (12).

$$x' = \frac{x}{max(x)} , \quad (11)$$

$$x' = \frac{min(x)}{x} . \quad (12)$$

One of the principal advantages of the proposed approach is its ability to thoroughly assess cybersecurity tools, as it combines nine criteria groups to evaluate these tools not only from the perspective of technical efficiency but also regarding operational sustainability and financial practicality. A significant advantage of the model is its adaptability to the specific characteristics of higher education environments (including dynamic traffic, open network architectures, numerous simultaneous users and limited cybersecurity resources) thereby ensuring realistic and context-oriented evaluation results. The inclusion of the adaptability and learning capability criterion represents another important advantage of the proposed approach, as it enables the assessment of tools’ ability to update detection models, learn behavioural patterns and maintain long-term

© Zavhorodnya E.O., Shestak Y.I., Kryvoruchko O.V., Kulinich O.M. Modeling an evaluation system for DDoS attack detection tools in HEI’s web resources. Сучасний захист інформації, 2(66), 178–190. https://doi.org/10.31673/2409-7292.2026.026315

effectiveness against evolving DDoS attacks in dynamic cyber environments. Furthermore, the model strengthens operational resilience and service continuity within HEIs by prioritising criteria related to detection latency, automation capability and mitigation efficiency, allowing for rapid attack response and minimising service disruption across critical digital platforms. Another advantage is the focus on economic efficiency and resource optimisation, allowing HEIs to find a balance between protection efficacy, infrastructure effects and long-term maintenance expenses, thus facilitating financially justified cybersecurity strategies. The proposed hierarchical framework also boosts interoperability within HEI cybersecurity systems by evaluating the degree of compatibility with SIEM, IDS/IPS systems, firewalls, cloud services and APIs, thereby ensuring efficient operation within existing security architectures and enabling centralised security management. Another important advantage of the approach is the emphasis on automation and reduction of manual intervention. Methodologically, the proposed approach provides significant flexibility and scalability, as its weighting coefficients and evaluation parameters can be modified based on institutional priorities, infrastructure scale, threat environment or available resources. The proposed approach enhances cybersecurity governance and strategic decision-making within HEIs by providing a clear and reproducible mechanism for comparing DDoS detection tools.

Despite its advantages, the model has limitations that need consideration when interpreting the evaluation results and using the framework within HEI contexts. A primary limitation is its dependence on expert-defined weighting factors, as institutions may prioritise criteria differently, thus impacting the final evaluation and tool rankings. Another limitation relates to the constantly changing nature of cyber threats and attack techniques, where new DDoS methods may require regular updates to the evaluation framework to keep its relevance. The model also depends on the availability and quality of empirical performance data for the tools assessed, which can be inconsistent due to incomplete vendor information and varying testing conditions. Additionally, while normalising metrics allows for a unified assessment, it may oversimplify the relationships between performance characteristics, resulting in disproportionate influence from extreme values on the final evaluation result. The model may struggle to address context-specific operational factors specific to individual HEIs. Furthermore, it mainly focuses on technical and operational factors, giving limited attention to human and organisational elements (e.g. training, incident response maturity, administrative procedures, cybersecurity culture and policy enforcement). A further constraint concerns ML-based detection system, as the frameworks generally assesses adaptability but does not consider factors such as bias, overfitting, concept drift or adversarial manipulation. Implementing the model may additionally require considerable computational and analytical resources. Finally, the framework evaluates tools primarily at the level of individual system characteristics and does not fully account for interdependencies between security components within broader cybersecurity systems.

Conclusions

The modern information environment is characterised by the rapid development of web resources and a simultaneous increase in the number and complexity of cyber threats, which necessitates the constant monitoring, analysis and control of the status of information systems, regardless of the form of ownership of the organisations concerned.

The web infrastructure of HEIs is critical to the educational process and operates as a complex socio-technical system. Breaches of cyber resilience can directly impact educational services and user trust. Therefore, guaranteeing the cyber resilience of HEIs' web resources can only be achieved by implementing thorough, unified and adaptive security systems that can operate efficiently against constantly changing cyber threats, supported by cyber security specialists. The study proposes a layered framework for a resilient web resource protection system, which combines infrastructure security, data protection, continuous monitoring, and automated incident response. This framework boosts cybersecurity governance, improves service continuity, and strengthens the overall cyber resilience of HEIs. A significant aspect of the work is the development of a multi-criteria hierarchical

© Zavhorodnya E.O., Shestak Y.I., Kryvoruchko O.V., Kulinich O.M. Modeling an evaluation system for DDoS attack detection tools in HEI's web resources. Сучасний захист інформації, 2(66), 178–190. https://doi.org/10.31673/2409-7292.2026.026315

model for DDoS detection tools comparative evaluation. The proposed approach provides HEIs with a comprehensive, adaptive and practically oriented framework for evaluating DDoS attack detection tools. Its integration of technical, operational and economic factors enables HEIs to improve cyber resilience, optimise security investments and ensure the stable and secure operation of critical digital services. Therefore, while the proposed multi-criteria hierarchical approach provides a comprehensive and structured mechanism for evaluating DDoS attack detection tools, its results should be interpreted within the context of institutional requirements, available data quality and the dynamic nature of cybersecurity threats. Future research may focus on reducing subjectivity in weighting procedures, incorporating real-time adaptive evaluation mechanisms, and extending the framework to include organisational, behavioural and ecosystem-level cybersecurity factors.

Declaration of Generative AI

The free versions of DeepL, Grammarly and ChatGPT 5.3 Mini were used to prepare the English translation of the study and to carry out the initial editing of the manuscript. After reviewing the results, the authors made corrections and edited the manuscript to improve the quality of the final translation of the study. The authors accept full responsibility for the quality of the content of this publication.

References

1. Kryvoruchko, O., Shestak, Y., Kulinich, O., & Zavhorodnya, E. (2026). Intellectualization of information flow management as a means of ensuring the cyber resilience of a higher education institution's infrastructure. Management of Development of Complex Systems, (65), 194–203. https://doi.org/10.32347/2412-9933.2026.65.194-203.

2. Kryvoruchko, O., Kulinich, O., Shestak, Y., & Zavhorodnya, E. (2026). Conceptual approaches to creating a sustainable information infrastructure for higher education institutions. In Science, Technology and Global Challenges (p. 166–173). CPN Publishing Group. https://sci-conf.com.ua/wp-content/uploads/2026/01/SCIENCE-TECHNOLOGY-AND-GLOBAL-CHALLENGES-11-13.01.26.pdf.

3. Kryvoruchko, O., Shestak, Y., Zavhorodnya, E., & Fesenko, A. (2025). Higher education cyber resilience: Intelligent protection of educational, administrative and resource systems. Cyber Security and Data Protection 2025 (p. 117–131). https://ceur-ws.org/Vol-4042/paper9.pdf.

4. Sevastieiev, Y., Dovgan, M., & Limar, I. (2026). Analysis of the effectiveness of detecting attacks using Wazuh SIEM. Informatics and Mathematical Methods in Simulation, 16(1), 85–95. https://doi.org/10.15276/imms.v16.no1.85.

5. Dudkin, V. (2024). Analiz zasobiv vyiavlennia ta poperedzhennia DDoS atak u kiberprostori [Analysis of methods for detecting and preventing DDoS attacks in cyberspace]. In Free and Open-Source Software (c. 17–18). Simon Kuznets Kharkiv National University of Economics. https://foss.kn-it.info/uploads/foss-2024-theses.pdf.

6. Kavetskyi, M., Sievierinov, O., Gvozdov, R., & Smirnov, A. (2024). Using machine learning to classify DOS/DDoS attacks. Radiotekhnika, (217), 55–63. https://doi.org/10.30837/rt.2024.2.217.04.

7. Ryzhakov, M., & Ponochovnyi, P. (2025). Model of network function transformation with elements of DDoS protection. Scientific Journal «Applied Problems of Computer Science, Security and Mathematics», (4), 14–32. https://apcssm.vnu.edu.ua/index.php/Journalone/article/view/128.

8. Cherniashchuk, N., & Dudko, A. (2025). Phishing, DDoS attacks and other cyberattacks – how to protect yourself. International Scientific-Practical Conference "Problems of Computer Sciences, Software Modeling and Security of Digital Systems", 145–147. Retrieved from https://apcssm.vnu.edu.ua/index.php/conf/article/view/229.

9. Havrylov, M. (2024). Zakhyst informatsiinykh system pidpryiemstva vid kiberzahroz: pidkhody ta instrumenty v umovakh tsyfrovoi transformatsii biznesu [Protection of enterprise information systems against cyber threats: approaches and tools in the context of business digital transformation]. Transformatsiia biznesu dlia staloho maibutnoho: doslidzhennia, tsyfrovizatsiia ta innovatsii: monograph, 287-305. PE Palianytsia V.A. [in Ukrainian]. https://elartu.tntu.edu.ua/bitstream/lib/46653/2/ColMon_2024_Havrylov_M-Protection_of_enterprise_287-305.pdf.

10. Shcherbyna, Y. V., Kazakova, N. F., Lohinova, N. I., & Bazarov, D. A. (2024). Modern approaches to protection against distributed denial-of-service attacks. Modern Information Security, 58(2), 77–83. https://doi.org/10.31673/2409-7292.2024.020009.

11. Derkach, M. V., Khomyshyn, V. G., & Hudzenko, V. O. (2023). Testing the security of a web resource using tools for scanning and identifying vulnerabilities. Scientific news of Dahl university. https://doi.org/10.33216/2222-3428-2023-25-1.

12. Savchenko, V., Haidur, H., & Lehominova, S. (2025). Prohnozuvannia povilnykh DDoS atak na osnovi koreliatsiinoho analizu indyvidualnykh traiektorii trafiku [Predicting slow DDoS attacks based on correlation analysis of individual traffic trajectories]. In Security of Modern Information & Communication Systems (SMI&CS-2025). Ivan Franko National University of Lviv. https://smics.lnu.edu.ua/uk/prognozuvannya-povilnyh-ddos-atak-na-osnovi-korelyaczijnogo-analizu-indyvidualnyh-trayektorij-trafiku/.

Завгородня Єлизавета Олександрівна
доктор філософії (міжнародні економічні відносини), завідувач відділу бібліотеки
Державний торговельно-економічний університет, Київ, Україна
ORCID: 0000-0003-0549-7020
E-mail: y.zavhorodnya@knute.edu.ua

Шестак Ярослав Іванович
доктор філософії (комп'ютерні науки), старший викладач кафедри програмної інженерії та кібербезпеки
Державний торговельно-економічний університет, Київ, Україна
ORCID: 0000-0002-5102-9642
E-mail: shestack@knute.edu.ua

Криворучко Олена Володимирівна
доктор технічних наук, професор кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0000-0002-7661-9227
E-mail: ev_kryvoruchko@ukr.net

Кулініч Олег Миколайович
Кандидат технічних наук, доцент кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID: 0000-0002-0643-6898
E-mail: o.kulinich@nubip.edu.ua

МОДЕЛЮВАННЯ СИСТЕМИ ОЦІНКИ ІНСТРУМЕНТІВ ВИЯВЛЕННЯ DDoS-АТАК У ВЕБ-РЕСУРСАХ ВНЗ

Це дослідження розглядає необхідність комплексного підходу до оцінки та вибору інструментів кібербезпеки для захисту веб-ресурсів у вищих навчальних закладах (ВНЗ) від сучасних кіберзагроз, зокрема розподілених атак типу «відмова в обслуговуванні» (DDoS). У цьому дослідженні розглянуто сучасні загрози інформаційній безпеці веб-ресурсів та обґрунтовано необхідність їх своєчасного виявлення, аналізу та нейтралізації для забезпечення безперервності інформаційних систем, зокрема у ВНЗ. Огляд академічної літератури показав, що традиційні підходи до моніторингу та захисту інформаційних систем є неефективними, незважаючи на сучасні багатовекторні атаки, що вимагає переходу до інтегрованих, адаптивних та інтелектуальних систем кібербезпеки. Короткострокові, але інтенсивні кібератаки (наприклад, інциденти DDoS) можуть суттєво порушити доступність послуг за відсутності належних заходів захисту. Крім того, ми виявили, що ефективний захист веб-ресурсів вимагає ретельного підходу, який забезпечує конфіденційність, цілісність та доступність інформації, а також здатність адаптуватися до змінних умов у кіберсередовищі. Було запропоновано багаторівневу архітектуру кібербезпеки та гібридну систему виявлення DDoS. Запропонована система поєднує методи на основі сигнатур, поведінкові та статистичні методи для сприяння створенню ефективної та модифікованої системи виявлення загроз. Для підтримки об'єктивного прийняття рішень було розроблено багатокритеріальну ієрархічну модель оцінювання. Запропонована модель оцінювання включала дев'ять груп критеріїв, спрямованих на оцінку технічної продуктивності, масштабованості, адаптивності, можливостей інтеграції, автоматизації та економічної ефективності. Запропонований метод дозволяє організовано та прозоро порівнювати засоби виявлення DDoS-атак у конкретних умовах вищих наукових установ.

Ключові слова: кіберзагрози, SIEM-системи, веб-ресурси вищих навчальних закладів, DDoS-атаки, кіберстійкість, виявлення атак, надання освітніх послуг.

Надійшла до редакції (Received): 10.05.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

© Zavhorodnya E.O., Shestak Y.I., Kryvoruchko O.V., Kulinich O.M. Modeling an evaluation system for DDoS attack detection tools in HEI's web resources. Сучасний захист інформації, 2(66), 178–190.
https://doi.org/10.31673/2409-7292.2026.026315