https://doi.org/10.31891/csit-2025-2-14
UDC 004.49

RAMSKYI Ihor, DROZD Andriy, LYHUN Oleksii
Khmelnytskyi National University
PONOCHOVNA Olena
Poltava State Agrarian University

SYSTEM FOR CYBERSECURITY EVALUATION OF CORPORATE NETWORKS

In the context of rapidly increasing cyber threats and the growing complexity of corporate IT infrastructure, ensuring a reliable and proactive approach to cybersecurity is becoming critically important for organizations of all sizes. Traditional cybersecurity assessment methods often fail to keep up with the dynamic nature of emerging threats – necessitating the development of more adaptive and intelligent evaluation systems. This article presents a comprehensive modular system for assessing the cybersecurity level of corporate networks – offering a holistic view of the security landscape by integrating both technical and organizational indicators.

The proposed system utilizes self-organizing analytical methods to dynamically process large volumes of data related to vulnerabilities, configuration states, and network behavior patterns. Through intelligent algorithms and adaptive learning, the system is capable of autonomously detecting anomalies, evaluating potential attack vectors, and correlating threats with the network's weak points. Additionally, the inclusion of organizational factors – such as policy compliance, user behavior, and access structures – enables a more contextual and in-depth risk assessment.

A key advantage of the system is its ability to perform real-time monitoring and dynamic risk evaluation – empowering decision-makers to take informed actions in response to incidents. The system's architecture supports scalability and compatibility with existing security tools and network management platforms.

To validate its effectiveness, the system was implemented and tested in a simulated corporate environment reflecting modern structural and operational challenges. The experimental results confirmed its capability to identify vulnerabilities, prioritize responses, and enhance overall cyber resilience.

This research contributes to the advancement of next-generation cybersecurity assessment tools – ensuring the continuous improvement of corporate defense mechanisms in an ever-changing cyber landscape.

Keywords: Corporate networks, distributed systems, cybersecurity

РАМСЬКИЙ Ігор, ДРОЗД Андрій, ЛИГУН Олексій
Хмельницький національний університет
ПОНОЧОВНА Олена
Полтавський державний аграрний університет

СИСТЕМА ОЦІНЮВАННЯ КІБЕРБЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

У контексті стрімкого зростання кіберзагроз та зростаючої складності корпоративної IT-інфраструктури забезпечення надійного та проактивного підходу до кібербезпеки стає критично важливим для організацій будь-якого масштабу. Традиційні методи оцінювання кібербезпеки часто не встигають за динамікою змін у загрозах, що зумовлює необхідність розробки більш адаптивних та інтелектуальних систем оцінки. У цій статті представлено комплексну модульну систему для оцінки рівня кібербезпеки корпоративних мереж, яка забезпечує цілісне бачення безпекової ситуації шляхом інтеграції як технічних, так і організаційних показників.

Запропонована система використовує самоорганізуючі аналітичні методи для динамічної обробки великих обсягів даних про вразливості, конфігураційні стани та поведінкові особливості мережі. Завдяки інтелектуальним алгоритмам та адаптивному навчанню система здатна автономно виявляти аномалії, оцінювати потенційні вектори атак і співвідносити загрози з вразливими місцями системи. Додатково, врахування організаційних факторів – таких як відповідність політикам, поведінка користувачів та структура доступу – забезпечує більш контекстуальну та глибоку оцінку ризиків.

Однією з ключових переваг системи є можливість здійснення моніторингу в реальному часі та динамічної оцінки ризиків, що дозволяє керівникам приймати обґрунтовані рішення для своєчасного реагування на інциденти. Архітектура системи передбачає масштабованість і сумісність з існуючими засобами захисту та платформами управління мережею.

Для підтвердження ефективності система була реалізована та протестована у моделюваному корпоративному середовищі, що відображає сучасні структурні та операційні виклики. Результати експерименту підтвердили її здатність виявляти вразливості, визначати пріоритети реагування та зміцнювати загальну кіберстійкість.

Це дослідження робить внесок у розвиток інструментів оцінювання кібербезпеки нового забезпечуючи постійне вдосконалення корпоративних механізмів захисту в умовах мінливого кіберсередовища.

Ключові слова: корпоративні мережі, розподілені системи, кібербезпека.

Introduction

In today's digitally interconnected world, corporate networks have become critical infrastructures that support core business operations, data exchange, and communication processes. As organizations increasingly rely on complex information systems, the potential attack surface expands, exposing networks to a broad range of cyber threats. These threats – ranging from malware and ransomware to advanced persistent threats and insider attacks – continue to grow in sophistication, frequency, and impact. Consequently, ensuring the cybersecurity of corporate networks has evolved from a technical challenge into a strategic necessity for maintaining operational continuity, protecting sensitive data, and preserving stakeholder trust.

Traditional cybersecurity assessment methods often rely on periodic audits, rule-based monitoring, or reactive measures that are insufficient in addressing modern, dynamic threat landscapes. Static approaches fail to capture real-time changes in network topology, user behavior, or system configurations, limiting their effectiveness in identifying and mitigating emerging threats. Furthermore, many existing solutions focus primarily on technical vulnerabilities while neglecting the organizational and procedural factors that also influence the overall security posture.

To address these limitations, there is a growing need for adaptive, comprehensive systems capable of continuously evaluating the cybersecurity state of corporate networks. Such systems should integrate both technical and organizational indicators, provide real-time insights, and support proactive risk management strategies.

This article presents a novel system for cybersecurity evaluation designed specifically for corporate networks. The system incorporates self-organizing analytical methods to interpret vulnerability data, configuration states, and behavioral patterns across the network. It enables real-time monitoring, dynamic risk assessment, and prioritization of mitigation efforts based on contextual analysis. The architecture is modular and scalable, allowing for seamless integration into diverse IT environments.

The following sections describe the system's design and implementation, followed by an evaluation of its performance within a simulated enterprise environment. The results demonstrate the system's ability to enhance situational awareness, support decision-making, and improve the overall cybersecurity resilience of corporate networks.

Related works

Assessing cybersecurity in corporate networks requires sophisticated methods for detecting and responding to various threats. Modern corporate networks function as distributed systems with partial centralization, where decision-making on malware detection is structured as a decentralized subsystem. The use of characteristic indicators and analytical models allows the system to evaluate the constituent states and determine the corresponding reactions. Among the existing approaches, there is one that combines several methods for detecting malware, treating system components as integral sensors [1][2].

Ensuring resilience to cyberattacks, particularly botnets, is a critical aspect of cybersecurity assessment. The reviewed literature provides an example of a self-adaptive system for reconfiguring corporate networks based on security scenarios obtained as a result of cluster analysis of network traffic features. Using a semi-supervised fuzzy c-means clustering approach, the system detects cyber threats and selects security strategies to mitigate botnet attacks, increasing network resilience [3]. Another three-tier botnet detection system model provides the ability to identify both known and unknown botnets by combining host-level Bayes classification with network-level extensions. This approach allows for efficient exchange of information in a distributed system and has demonstrated promising results in the accuracy of botnet detection [4].

Distributed denial-of-service (DDoS) attacks are another major cybersecurity issue, especially in software-defined networks (SDNs). To detect and mitigate these attacks, a machine learning-based framework has been developed that uses the Support Vector Classifier and the Gradient Boost Classifier (SVC-GBC). With 99.4% accuracy, this hybrid approach significantly improves SDN security by refining detection granularity and strengthening defense mechanisms [5]. In addition to intrusion detection, anomaly detection in distributed systems remains a challenge due to complex dependencies between system logs. A deep learning-based Time Logical Attention Network (TLAN) has been introduced to model both time series patterns and logical dependencies, improving anomaly detection performance while reducing false signals [6].

The reliability of cybersecurity assessments in distributed systems is further enhanced by failure detection mechanisms. These mechanisms monitor the activity of nodes to identify faults and increase the fault tolerance of the system. Systematic analysis of fault detectors in distributed environments highlights their role in ensuring the reliability of services by solving matching and failure problems [7]. Log-based anomaly detection (LAD) also plays an important role in cybersecurity assessment, using system logs to identify potential threats and service anomalies. The overall structure of LAD for distributed systems includes logging grouping and feature mining to improve detection efficiency, demonstrating its applicability in real-world distributed environments [8].

In addition, privacy issues in distributed computing require robust security systems. The study of privacy in distributed systems focuses on the risks associated with data evaluation and information tracking, emphasizing the relevance of zero-trust security models for the secure implementation of systems in cloud architectures [9]. As the complexity of distributed systems continues to grow, effective system audit mechanisms that combine advanced analytics and artificial intelligence are becoming important for vulnerability monitoring and improving security [10].

These advances together contribute to the creation of a comprehensive cybersecurity assessment system that ensures the resilience of corporate networks to evolving threats. Cybersecurity assessments in corporate networks should address issues related to reliability, anomaly detection, and compliance with security policies. The zero-trust security model emphasizes the need to validate on-premises servers on corporate intranets, however, existing certification methods remain unavailable to small organizations due to cost and complexity. This gap leads to dependence on self-signed certificates, increasing vulnerability to impersonation and unauthorized access, which ultimately violates the principles of zero trust [11]. To improve the detection of security threats in large-scale

distributed systems, a federated approach based on learning has been proposed, integrating multimodal large language models. This system handles a variety of data sources, achieving 96.4% accuracy while maintaining data confidentiality and computational efficiency, demonstrating significant improvements over traditional detection methods [12].

Anomalies in distributed systems pose significant risks due to time delays and deterioration in data quality. A deep learning-based real-time data quality assessment system has been implemented, which uses adaptive neural networks and parallel processing to provide scalable, low-latency anomaly detection. Evaluations on large-scale datasets confirm the system's effectiveness in maintaining high detection accuracy when processing more than 1.2 million events per second [13]. In cloud computing environments, optimizing resource allocation is critical to maintaining efficiency. Machine learning-based approaches, combining deep learning and genetic algorithms, have been developed to improve resource planning, addressing issues such as load imbalances and low utilization [14].

Further advances in distributed computing focus on accountability, leadership selection, and safe randomness generation. The framework for accountable and reconfigured distributed systems enables seamless adaptation in response to failures using lattice agreement abstraction. In addition, innovative cryptographic protocols improve leadership elections on partially synchronous blockchains, improving consensus mechanisms and system resilience [15]. As distributed systems increasingly rely on log-based monitoring to assess security, the reliability of deep learning models against malicious attacks is a growing concern. A new attack method, LAM, manipulates streaming logs to avoid detecting anomalies, highlighting the need for enhanced security measures against adversarial manipulation [16].

Security policies in distributed systems also need to be flexible and validated in different implementations. A language-independent policy review system ensures compliance with security policies by analyzing I/O behavior instead of relying on programming language restrictions. Evaluations demonstrate its applicability in real-world protocols, which reinforces the need for adaptive security policies [17]. Blockchain technology also contributes to cybersecurity by increasing the transparency and security of data in distributed governance systems. However, issues such as scalability and interoperability must be addressed in order to fully exploit the potential of blockchain to protect sensitive data [18]. Finally, advances in deep learning to detect anomalies in distributed system logs introduce models that integrate global spatiotemporal features, greatly improving the accuracy of detecting security threats in complex environments [19]. These changes combine to contribute to the reliability and effectiveness of cybersecurity assessments in corporate networks.

Cybersecurity assessments in corporate networks must constantly adapt to changing threats and technological advancements. Distributed systems and computational approaches, including blockchain technology and distributed ledgers, offer significant potential to improve financial crime prevention and cybersecurity by increasing transparency and reducing fraud risks. However, issues such as regulatory compliance, interoperability, and integration with existing infrastructures must be addressed to maximize these benefits [20]. A proactive approach to security is essential in distributed environments, and the integration of DevOps methodologies enhances security by embedding threat detection into the development lifecycle, automating monitoring, and using behavioral analytics to detect anomalies in real-time. This strategy contributes to the formation of a culture of shared responsibility for safety and compliance with legal standards [21].

The diversity of systems is another key factor in improving the reliability and security of distributed communication networks. Analytical models based on tension-force analysis quantify these improvements, providing valuable information about the stability of the system [22]. In the context of intelligent distributed systems (SDS), ensuring data security and interoperability is critical for the seamless exchange of information between industries such as healthcare, utilities, and supply chains. Setting global security standards can provide a framework for authentication, collaboration, and protection against cyber threats in SDS environments [23]. The growing integration of IoT with cloud computing introduces new vulnerabilities, requiring a comprehensive security framework that increases resilience to cyber threats while maintaining scalability and adaptability in distributed environments [24].

Data privacy remains a major concern, especially in areas such as education and healthcare. Distributed computing offers improvements in security and response times, however, centralized platforms often outperform distributed systems with privacy-preserving techniques such as k-anonymity, t-proximity, and β-probability. Comparative analysis of these approaches reveals trade-offs in runtime, memory requirements, and suppression levels [25]. In healthcare, foggy computing is a promising solution for real-time patient monitoring, but security and privacy concerns must be addressed through encryption, access control, and data analysis techniques that preserve privacy [26]. Risk assessment in distributed information systems requires a dynamic, multi-layered approach that integrates quantitative, qualitative, and hybrid methodologies, using security metrics for accurate and reliable cybersecurity assessments [27].

Cybersecurity threats in smart networks highlight the importance of advanced threat detection mechanisms. Traditional supervised learning methods for detecting cyberattacks require a variety of training datasets that may not always be available. Unsupervised data mining approaches, especially for detecting false data attacks (FDIA), offer a more efficient alternative, relying solely on conventional event data to train detection models. Comparative studies demonstrate that unsupervised algorithms are superior to supervised and deep learning methods in detecting

unknown attack patterns, increasing cybersecurity in smart grid infrastructures [28].

These advances combine to strengthen cybersecurity assessment systems in corporate networks, ensuring resilience to sophisticated cyber threats. Cybersecurity assessments in corporate networks should include advanced cryptographic techniques to reduce the risks of data breaches in distributed environments. Cloud cryptography plays a crucial role in protecting data storage and transmission through the use of encryption mechanisms, intrusion detection systems, and firewalls. These technologies strengthen data protection in cloud-based distributed systems, preventing unauthorized access and infiltration of malware [29]. With the expansion of cloud and edge computing, AI-powered forensic tools have become effective solutions for detecting and mitigating the effects of cyber incidents in real-time. Machine learning and deep learning techniques improve forensic analysis by improving scalability, accuracy, and response time when detecting cyber threats in distributed systems [30].

The function for evaluation fo cybersecurity of computer stations

Let's set two functions to assess the level of network security, where the first will reflect the likelihood of significant interference of an attacker in any critical component of the network.

First, let's define the vulnerability of a component as the probability of its compromise regardless of the rest present in the network. Corresponding formula is:

$$V = \omega_S S + \omega_P(1 - P) + \omega_U U, \tag{1}$$

where S is the software vulnerability level in range [0,1], P is the effectiveness of cybersecurity policies in range [0, 1], 1 standing for maximal security, U – probability of compromise due to a human error, $\omega_S, \omega_P, \omega_U$ are the weight coefficients.

Let's reveal the components of the formula further. P should be defined by cybersecurity professionals independently on a case-by-case basis, as different organizations have different approaches to setting up appropriate processes. In the context of this work, we will determine U according to the frequency of phishing attacks and other situations of compromise of network users in its history. S will be determined by the formula

$$S = \sum_{k=1}^{N_e} \omega_k * \frac{CVSS_k}{10}, \tag{2}$$

where N_e is the total number of vulnerabilities on the node, $CVSS_k$ is the assessment of the criticality of the k-th vulnerability on the CVSS scale (from 0 to 10), ω_k is the weighting coefficient, which determines the impact of each vulnerability.

Vulnerability search for S calculation can be organized using vulnerability scanners. Thus, the formula for the vulnerability of one component independently of the rest of the network:

$$V = \omega_S \sum_{k=1}^{N_e} \omega_k * \frac{CVSS_k}{10} + \omega_P(1 - P) + \omega_U U, \tag{3}$$

It should also be borne in mind that the compromise of one host in the network also endangers other components of the network. To do this, we will specify a formula to determine the probability of compromise of host j if host i was compromised:

$$G_{ij} = \omega_T T_{ij} + \omega_F(1 - F_{ij}) + \omega_L(1 - L_{ij}), \tag{4}$$

where T_{ij} is the the level of connection openness normalized in the range [0,1], where 1 means a fully open channel and 0 is a fully isolated connection, F_{ij} is the effectiveness of firewalls and traffic filtering (from 0 to 1, where 1 means maximum protection), L_{ij} is the encryption level (0 to 1, where 1 means full encryption and 0 means fully open traffic).

Let's put these two formulas together to determine the probability of its compromise for each host and, accordingly, calculate the chance of compromise of any of the important hosts.

$$CS = \prod_{i=1}^{M} \left(\left(1 - V_{a_i}\right) * \prod_{j=1}^{N} \left(1 - V_j P_{a_i}\right) \right), \tag{5}$$

where CS is the overall level of cybersecurity in the corporate network, M is the number of important network components, a is the list of important network components.

These formulas are based on comprehensive mathematical modeling that adequately accounts for both the internal characteristics of each host and the interdependencies between them. The vulnerability level of each node V is determined by three key parameters: software vulnerabilities S, the effectiveness of security policies P, and the probability of compromise due to human factors U. This structure aligns with modern cybersecurity threat analysis practices, where most incidents stem not only from technical flaws but also from social engineering and imperfect

security administration. The use of weighting coefficients enables the model to reflect the relative importance of each factor in a given context, making the evaluation adaptable to the specific conditions of the network.

Further modeling of the probability of attack propagation across the network through the function $G(i,j)$ captures the probabilistic nature of inter-node interaction, where the risk of transmission depends on parameters such as connection openness, firewall effectiveness, encryption levels, and anomaly detection capabilities. This formula is crucial, as it accounts for not only the vulnerability of individual components but also their potential influence on other nodes—an essential distinction from traditional approaches that treat hosts in isolation.

The final stage involves the calculation of the overall cybersecurity level of the network CS, which is derived by combining all obtained V and G values. The formula for CS implements a multiplicative scheme that accurately reflects the cumulative nature of risks: even if a single host is highly vulnerable and located in a poorly protected segment, it can impact the security of the entire system. This approach allows for the estimation of the probability of a successful attack not only on isolated components but on critical infrastructure as a whole.

Taken together, the proposed formulas are not only mathematically sound but also effective in addressing the task of constructing a comprehensive cybersecurity evaluation model for corporate networks. They provide a high degree of accuracy, adaptability to changes in system configuration, and the ability to tailor to specific threats and architectures, making the proposed methodology universally applicable across a wide range of practical implementations.

Practical implementation of the system

The method for synthesizing self-organizing systems for cybersecurity assessment of computer stations is based on constructing a system capable of real-time monitoring of the corporate network and individual computer stations. It continuously collects relevant metrics and computes a cybersecurity evaluation function. The central element of this system is a function that reflects the current level of protection of the information infrastructure, taking into account numerous interdependent factors. This function should be formed based on aggregated indicators of system process activity, configuration integrity, network connection status, and the degree of vulnerability derived from known technical software characteristics and the enforcement level of access control policies.

To deploy the evaluation system, an initial configuration of coefficients and values is required—parameters that cannot be accurately assessed using purely technical methods. Let us now consider Formula 3, which calculates the vulnerability of each individual computer in the network:

$$V = \omega_S \sum_{k=1}^{N_e} \omega_k * CVSS_k + \omega_P(1-P) + \omega_U U$$

In this formula, the weighting coefficients $\omega_S, \omega_P, \omega_U$, as well as the values of P and U under ideal circumstances, should be determined by cybersecurity experts for each specific case of a corporate network. This approach assumes individual customization of the evaluation system, taking into account the architecture's specifics, the types of information assets, the organizational structure of the enterprise, as well as the potential attack vectors characteristic of a particular industry or region. Alternatively, the following values for the weighting coefficients are proposed:

Network Scenario	ω_S	ω_P	ω_U
Techno-centric organization	0.7	0.2	0.1
Institution with a bureaucratic structure	0.2	0.5	0.3
Company under active phishing conditions	0.3	0.2	0.5

Similarly, the values P and U should also be determined by cybersecurity experts (ideally) based on an audit that demonstrates the network's security policies comply with the latest standards and that personnel are knowledgeable and proficient in computer usage. Alternatively, the value of P can be roughly estimated based on components such as the existence of documented security policies, the currency of the policies, access control, password management, and incident response. Likewise, the value of U can be approximated based on other factors and historical data: the frequency of phishing incidents over the past year, the level of personnel awareness (tests/surveys), the availability of regular training, incidents of password/access loss, and the results of social engineering simulations.

To determine the remaining values in the formula $(\omega_k, N_e, CVSS_k)$ specialized software and additional resources are required. To obtain $CVSS_k$, it is recommended to use the OpenVAS vulnerability scanner. This is a free and open-source software – which ensures there is no misuse of network access by the developers – provided that changes to the open code are regularly reviewed. For the cybersecurity evaluation system to function properly, it is necessary to regularly run vulnerability scans on the computer. As a result of these scans, the program generates a report, and the CVSS values extracted from it will be used for further calculations.

To determine ω_k, N_e , it is proposed to use daily updated data from the Exploit Prediction Scoring System (EPSS) model. This is a system that estimates the probability that a specific vulnerability will be exploited in the real world within the next 30 days. Data can be obtained via API or by downloading reports in CSV format. Each row in the file is a triplet: CVE (vulnerability identifier), EPSS (probability of exploitation), Percentile (probability percentile for the given vulnerability). N_e will be taken as the number of vulnerabilities in the EPSS report, and ω_k – $EPSS_k$, normalized in such a way that the sum of all values equals one. In this way, the weight of a vulnerability will be proportional to the probability of encountering it.

Let us consider formula 4:

$$G_{ij} = \omega_T T_{ij} + \omega_F(1 - F_{ij}) + \omega_L(1 - L_{ij}) + \omega_D(1 - D_{ij}),$$

where T_{ij} is the level of openness within the range [0, 1], F_{ij} is the effectiveness of firewalls and traffic filtering within the range [0, 1], L_{ij} is the level of encryption within the range [0, 1], D_{ij} is the level of anomaly detection within the range [0, 1], $\omega_T, \omega_F, \omega_L, \omega_D$ – the weighting coefficients.

The weighting coefficients $\omega_T, \omega_F, \omega_L, \omega_D$ should be defined by the CISO (Chief Information Security Officer) or a security analyst. For example, in a cloud environment with many open ports but strong encryption – more weight should be assigned to ω_T, and less to ω_L, whereas in an environment without IDS/IPS (Intrusion Detection/Prevention Systems) – ω_D should be increased.

This can be implemented in the form of a risk profile table:

Scenario	ω_T	ω_F	ω_L	ω_D
Cloud infrastructure	0.1	0.5	0.2	0.2
Corporate local network	0.1	0.4	0.3	0.2
Minimal access control	0.1	0.2	0.1	0.4

It is also necessary to define $T_{ij}, F_{ij}, L_{ij}, D_{ij}$. Let us calculate T_{ij}:

$$T_{ij} = \frac{N_o}{N_a}, \tag{4.1}$$

where N_o is the number of open ports excluding standard encrypted ones (e.g., HTTPS), and N_a is the maximum allowable number of open ports, typically set to 10.

Let us calculate F_{ij}. This is done through periodic active testing – by generating requests that simulate malicious traffic. It is recommended to use the open-source tool hping to generate such traffic. The formula is:

$$F_{ij} = \frac{N_{failed}}{N_{tests}}, \tag{4.2}$$

where N_{failed} is the number of malicious test requests that were not blocked during testing, and N_{tests} – is the total number of tests conducted.

Let us calculate L_{ij}. It is proposed to use the tool SSLyze to scan network connections and assess the strength of encryption. Based on the scan results, a numerical value can be estimated for use in formula (4). Since TLS 1.3 is currently considered the most secure transport layer encryption protocol, it is rated as $L_{ij} = 1$. SSL, being outdated and known to contain vulnerabilities, is rated as $L_{ij} = 0$. . For intermediate values, we assign $L_{ij} = 0.7$ for TLS 1.2 and $L_{ij} = 0.3$ for TLS 1.1.

Results of the experiment

To evaluate the effectiveness of the proposed model, an experiment was conducted that simulates the operation of the implemented cybersecurity assessment system under conditions close to a real-world environment. The testing involved simulating the activity of network nodes over the course of one week with an hourly time step. During the experiment, dynamic updates of input parameters were implemented – these parameters influence the vulnerability level of individual computers and the probability of their compromise as a result of interaction with other nodes in the network.

The model components responsible for forming the vulnerability and compromise probability functions were manually configured based on assumptions about the typical characteristics of an organizational IT environment. In particular, the weight coefficients for the technical, policy-related, and human vulnerability components were set according to conditionally prioritized security concerns. Similarly, the weights for traffic, filtering, encryption, and network remoteness parameters were chosen to reflect the characteristic risks of network intrusion through interactions between individual computers. The values of the manually configured parameters are as follows: $\omega_S = 0.7, \omega_P = 0.2, \omega_U = 0.1, \omega_T = 0.1, \omega_F = 0.4, \omega_L = 0.3, \omega_D = 0.2, P = 0.9, U = 0.1$.

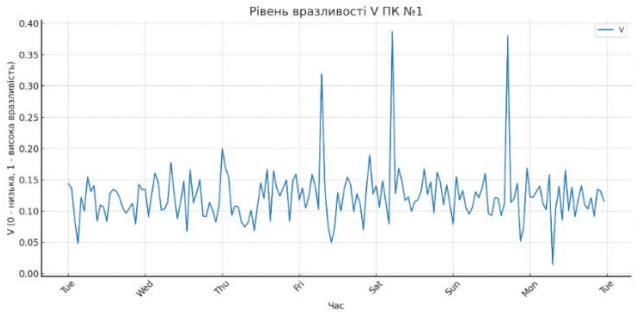

Fig. 1

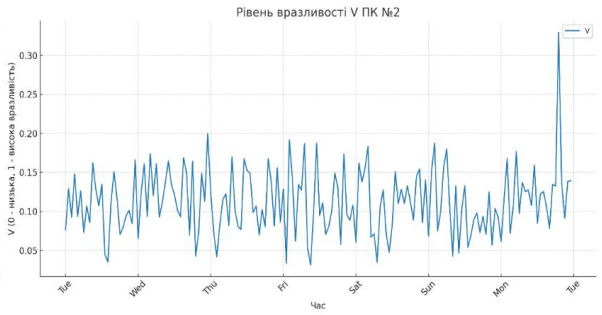

Fig. 2

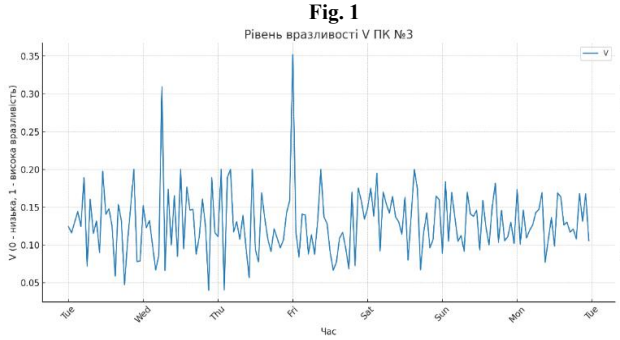

Fig. 3

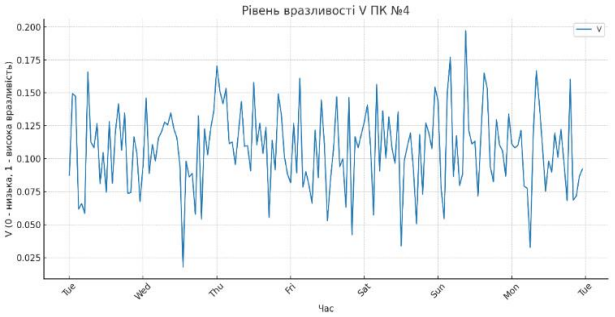

Fig. 4

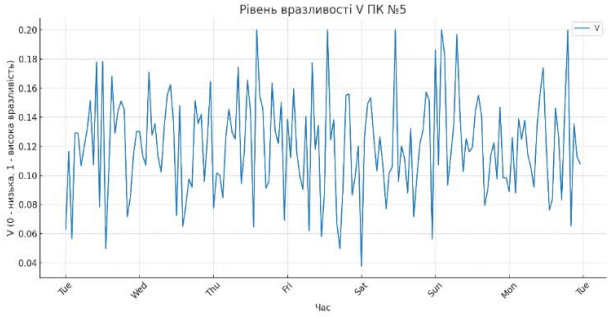

Fig. 5

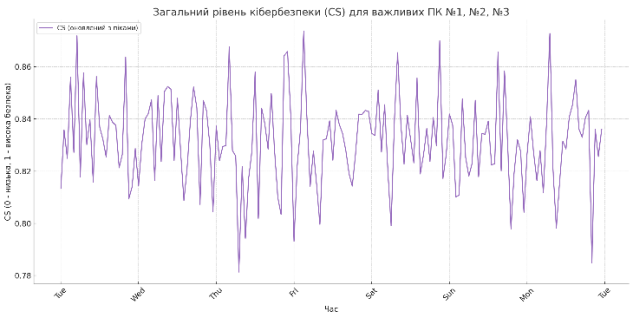

Fig. 6

As part of the experiment, isolated peak deviations were manually introduced for critical nodes – computers No. 1-3, – simulating episodic increases in risk level. These peaks were implemented by artificially adding a noticeable number of high-rated technical vulnerabilities, equivalent to a situation where a new set of critical vulnerabilities is discovered on a specific host, for example, due to a missed update or newly identified software flaws. As a result, there were short-term but sharp increases in the V indicator, which are clearly visible in Fig. 1–3. Fig. 4-5 show vulnerability chart with no serious peaks.

The chart of the overall cybersecurity level CS (Fig. 6) serves as a key analytical tool that enables a comprehensive assessment of the security situation within the network, taking into account both the local characteristics of individual nodes and the impact of inter-node interactions. The construction of this indicator is based on integrating the vulnerability assessments of critical computers with the probabilities of their compromise by other elements of the system. This approach provides a multidimensional view of risks, allowing not only for isolated evaluations of individual hosts but also for tracking systemic dependencies and potential attack chains.

This chart holds particular value from the perspective of real-time monitoring – it makes it possible to identify critical time intervals during which a sharp decline in the security level is observed, and to correlate these changes with specific hosts exhibiting increased vulnerability or an escalating threat of compromise. In combination with the V_i graphs, which provide detailed insight into the sources of these changes, the CS graph enables the operator to instantly assess the overall network situation, localize problem areas, and take timely measures to eliminate vulnerabilities or reduce the risk of attack propagation.

Thus, CS visualization serves as an effective real-time decision-making mechanism, which is especially important in the context of a rapidly changing threat landscape. Its integration into the security management system significantly enhances the response speed and the rationality of actions taken by the administrator or automated defense systems.

Conclusions

The proposed system for cybersecurity evaluation of corporate networks effectively integrates technical, organizational, and human factors into a comprehensive framework. By employing adaptive mathematical modeling

and real-time data analysis, it provides an accurate, dynamic assessment of a network's security posture. The approach's strength lies in its flexibility—allowing parameter customization based on the specifics of an organization—and its capability to evaluate not only isolated vulnerabilities but also interdependencies between network nodes. Experimental implementation demonstrated the model's practical applicability and its usefulness for identifying weak points, prioritizing response measures, and enhancing decision-making in security management. This system represents a significant step forward in proactive cybersecurity assessment, offering organizations a scalable and intelligent tool to fortify their digital infrastructure against evolving threats.

References

1. Savenko B., Kashtalian A., Lysenko S., Savenko O. Malware Detection By Distributed Systems with Partial Centralization. *2023 IEEE 12th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Dortmund, Germany.* 2023. 265–270. https://doi.org/10.1109/IDAACS58523.2023.10348773
2. Kashtalian A., Lysenko S., Savenko O., Nicheporuk A., Sochor T., Avsiyevych V. Multi-computer malware detection systems with metamorphic functionality. *Radioelectronic and Computer Systems.* 2024. No. 1, 152–175. https://doi.org/10.32620/reks.2024.1.13
3. Lysenko S., Savenko O., Bobrovnikova K., Kryshchuk A. Self-adaptive System for the Corporate Area Network Resilience in the Presence of Botnet Cyberattacks. *Computer Networks. CN 2018. Communications in Computer and Information Science,* Vol. 860. 2018. https://doi.org/10.1007/978-3-319-92459-5_31
4. Savenko O., Sachenko A., Lysenko S., Markowsky G., Vasylkiv N. Botnet Detection Approach Based on the Distributed Systems. *International Journal of Computing.* 2020. Vol. 19(2), 190–198. https://doi.org/10.47839/ijc.19.2.1761
5. Yadav A., Kaur M., Sharma C., Prashar D. Next-gen distributed denial-of-service detection and mitigation in software-defined networking using hybrid machine learning approach. *Soft Computing in Smart Manufacturing and Materials.* 2025. 97–133. https://doi.org/10.1016/B978-0-443-29927-8.00005-9
6. Liu Y., Ren S., Wang X., Zhou M. Temporal Logical Attention Network for Log-Based Anomaly Detection in Distributed Systems. *Sensors.* 2024. Vol. 24. https://doi.org/10.3390/s24247949
7. Chaurasia B., Verma A., Verma P. An in-depth and insightful exploration of failure detection in distributed systems. *Computer Networks.* 2024. Vol. 247. https://doi.org/10.1016/j.comnet.2024.110432
8. Wei X., Wang J., Sun C., Towey D., Zhang S., Zuo W., Yu Y., Ruan R., Song G. Log-based anomaly detection for distributed systems: State of the art, industry experience, and open issues. *Journal of Software: Evolution and Process.* 2024. Vol. 36(8). https://doi.org/10.1002/smr.2650
9. Vankayalapati R.K. Zero-Trust Security Models for Cloud Data Analytics: Enhancing Privacy in Distributed Systems. *SSRN.* 2025. https://doi.org/10.2139/ssrn.5121185
10. Di Pilla P., Pareschi R., Salzano F., Zappone F. Listening to what the system tells us: Innovative auditing for distributed systems. *Frontiers in Computer Science.* 2022. Vol. 4. https://doi.org/10.3389/fcomp.2022.1020946
11. Botha-Badenhorst D., McDonald A.M., Barbour G.D., Buckinjohn E., Gertenbach W. On The Zero-Trust Intranet Certification Problem. *Proceedings of The 19th International Conference on Cyber Warfare and Security.* 2024. Vol. 19(1). https://doi.org/10.34190/iccws.19.1.2054
12. Wang Y., Yang X. Design and implementation of a distributed security threat detection system integrating federated learning and multimodal LLM. *arXiv.* 2025. https://doi.org/10.48550/arXiv.2502.17763
13. Zhang H., Jia X., Chen C. Deep Learning-Based Real-Time Data Quality Assessment and Anomaly Detection for Large-Scale Distributed Data Streams. *International Journal of Medical and All Body Health Research.* 2025. Vol. 6(1). https://doi.org/10.54660/IJMBHR.2025.6.1.01-11
14. Wang B., He Y., Shui Z., Xin Q., Lei H. Predictive optimization of DDoS attack mitigation in distributed systems using machine learning. *Applied and Computational Engineering.* 2024. Vol. 64(1), 89–94. https://doi.org/10.54254/2755-2721/64/20241350
15. Freitas de Souza L. Achieving accountability, reconfiguration, randomness, and secret leadership in byzantine fault tolerant distributed systems. *Distributed, Parallel, and Cluster Computing [cs.DC], Institut Polytechnique de Paris.* 2024. URL: https://hal.science/tel-04984550 (access date: 21.01.2025)
16. Herath J.D., Yang P., Yan G. Real-Time Evasion Attacks against Deep Learning-Based Anomaly Detection from Distributed System Logs. *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy (CODASPY '21).* 2021. 29–40. https://doi.org/10.1145/3422337.3447833
17. Wolf F.A., Müller P. Verifiable Security Policies for Distributed Systems. *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24).* 2024. 4–18. https://doi.org/10.1145/3658644.3690303
18. Chandan R.R., Torres-Cruz F., Figueroa E.N.T., Mendoza-Mollocondo C.I., Sisodia D.R., Alam T., Tiwari M. Revolutionizing Data Management and Security with the Power of Blockchain and Distributed System. *Meta Heuristic Algorithms for Advanced Distributed Systems.* 2024. Chapter 11. https://doi.org/10.1002/9781394188093.ch11
19. Han P., Li H., Xue G., Zhang C. Distributed system anomaly detection using deep learning-based log analysis. *Computational Intelligence.* 2023. Vol. 39(3), 433–455. https://doi.org/10.1111/coin.12573
20. Singh V.B.P., Singh P., Guha S.K., Shah A.I., Samdani A., Nomani M.Z.M., Tiwari M. The Future of Financial Crime Prevention and Cybersecurity with Distributed Systems and Computing Approaches. *Meta Heuristic Algorithms for Advanced Distributed Systems.* 2024. Chapter 19. https://doi.org/10.1002/9781394188093.ch19
21. Allam A.R. Enhancing Cybersecurity in Distributed Systems: DevOps Approaches for Proactive Threat Detection. *Silicon Valley Tech Review.* 2023. Vol. 2(1), 54–66. URL: https://www.researchgate.net/publication/385886881_Enhancing_Cybersecurity_in_Distributed_Systems_DevOps_Approaches_for_Proactive_Threat_Detection (access date: 21.01.2025)
22. Popov G., Popova A. Application of System Diversity for Increasing Security and Reliability of Distributed Systems. *2022 XXXI International Scientific Conference Electronics (ET), Sozopol, Bulgaria.* 2022. 1–4. https://doi.org/10.1109/ET55967.2022.9920304
23. Maher D.P., Ahatlan H.E., Poonegar A.D. A Standardized Trust Model for Enabling Data Security and Interoperability within Smart Distributed Systems. *2023 IEEE International Smart Cities Conference (ISC2), Bucharest, Romania.* 2023. 1–4. https://doi.org/10.1109/ISC257844.2023.10293630
24. Raja M. Comprehensive Framework for Secure Cloud Computing and Distributed Systems with Integrated Cybersecurity and Information Assurance in the Era of Internet of Things. *International Journal of Information Technology Research and Development (IJITRD).* 2025. Vol. 6(2), 7–16. URL: https://ijitrd.com/index.php/home/article/view/IJITRD_6_2_2 (access date: 21.01.2025)
25. Lamaazi H., Alneyadi A.M.M., Serhani M.A. Academic Data Privacy-Preserving using Centralized and Distributed Systems: A Comparative Study. *Proceedings of the 2024 6th International Conference on Big-data Service and Intelligent Computation (BDSIC '24).* 2024. 8–16. https://doi.org/10.1145/3686540.3686542

26. Arora D., Sharma O. Fog Computing in Healthcare: Enhancing Security and Privacy in Distributed Systems. *Artificial Intelligence and Cybersecurity in Healthcare.* 2025. Chapter 3. https://doi.org/10.1002/9781394229826.ch3
27. Palko D., Babenko T., Bigdan A., Kiktev N., Hutsol T., Kuboń M., Hnatiienko H., Tabor S., Gorbovy O., Borusiewicz A. Cyber Security Risk Modeling in Distributed Information Systems. *Applied Sciences.* 2023. Vol. 13(4), 2393. https://doi.org/10.3390/app13042393
28. Pinto S.J., Siano P., Parente M. Review of Cybersecurity Analysis in Smart Distribution Systems and Future Directions for Using Unsupervised Learning Methods for Cyber Detection. *Energies.* 2023. Vol. 16(4), 1651. https://doi.org/10.3390/en16041651
29. Dubey H., Kumar S., Chhabra A. Cyber Security Model to Secure Data Transmission using Cloud Cryptography. *Cyber Security Insights Magazine.* 2022. Vol. 2. URL: https://insights2techinfo.com/wp-content/uploads/2022/11/Cyber-Security-Model-to-Secure-Data-Transmission-using-Cloud-Cryptography_final_2.pdf (access date: 21.01.2025)
30. Kyle J., Alexander D. AI-Driven Forensic Tools for Cloud and Edge Computing. *International Journal of Computational Intelligence in Digital Systems.* 2022. Vol. 11(1), 29–45. URL: https://www.researchgate.net/publication/388494481_AI-Driven_Forensic_Tools_for_Cloud_and_Edge_Computing (access date: 21.01.2025)

Ihor Ramskyi **Ігор Рамський**	Master's degree student, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: ramskyihor@gmail.com https://orcid.org/0009-0007-6175-1923	Магістрант, Хмельницький національний університет
Andriy Drozd **Андрій Дрозд**	PhD student, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: andriydrozdit@gmail.com https://orcid.org/0009-0008-1049-1911	Аспірант, Хмельницький національний університет
Oleksii Lyhun **Олексій Лигун**	PhD student, Khmelnytskyi National University, Khmelnytskyi, Ukraine e-mail: oleksii.lyhun@gmail.com https://orcid.org/0009-0004-5727-5096	Аспірант, Хмельницький національний університет
Olena Ponochovna **Олена Поночовна**	Assistant at the Department of Economics and International Economic Relations, Poltava State Agrarian University, Poltava, Ukraine, e-mail: olena.ponochovna@pdau.edu.ua https://orcid.org/0000-0002-4377-0633	Асистент кафедри економіки та міжнародних економічних відносин, Полтавський державний аграрний університет, м. Полтава, Україна,