https://doi.org/10.31891/2307-5732-2026-365-102
УДК 004.056:004.94

LESYNSKY VALENTYN
Yuriy Fedkovych Chernivtsi National University
https://orcid.org/0000-0002-1259-1974
e-mail: lesynsky@chnu.edu.ua
LASTIVKA HALYNA
Yuriy Fedkovych Chernivtsi National University
https://orcid.org/0000-0003-3639-3507
e-mail: g.lastivka@chnu.edu.ua
HRES OLEKSANDR
Yuriy Fedkovych Chernivtsi National University
https://orcid.org/0000-0002-8465-193X
e-mail: o.hres@chnu.edu.ua
LASTIVKA OLEKSANDR
Yuriy Fedkovych Chernivtsi National University
https://orcid.org/0009-0002-6232-3270
e-mail: Sokol4612@gmail.com

RESEARCH OF MONITORING TOOLS AND AUDIT METHODS FOR ENSURING THE CYBERSECURITY OF EDUCATIONAL PLATFORMS

The article presents a comprehensive analysis of open-source security monitoring tools, the architecture of a university information and communication system (ICS), and methods for auditing and assessing its security. The study emphasizes the role of open-source solutions, including Nagios, Zabbix, Prometheus+Grafana, OSSEC, Snort/Suricata, and Wazuh, in providing scalable and cost-effective monitoring of educational infrastructures.

The architecture of the information and communication system of the Center for Digital Transformation is represented as a three-tier Core–Distribution–Access model based on the principles of network segmentation, fault tolerance, redundancy, and multi-layered protection, ensuring the continuity of educational processes and compliance with international standards.

Special attention is devoted to the analysis of modern information security auditing tools, which are classified into three main categories: technical, organizational, and procedural. In addition, a comparative analysis of the effectiveness of modern security audit and monitoring platforms was conducted. The study demonstrates that the integrated use of open-source monitoring systems in combination with regular security audits minimizes the impact of cyber incidents and forms a comprehensive cybersecurity model for the educational environment aimed at ensuring the confidentiality, integrity, and availability of information.

The research results indicate that the implementation of open-source monitoring tools, modern architectural approaches, and systematic audit procedures enhances the security level of educational platforms, ensures compliance with international standards, and contributes to the development of a resilient and adaptive cybersecurity system for higher education institutions.

Keywords: cybersecurity, educational infrastructure, open-source monitoring tools, audit methods, SIEM, defense-in-depth, ISO/IEC 27001, OWASP, NIST.

ЛЕСІНСЬКИЙ ВАЛЕНТИН, ЛАСТІВКА ГАЛИНА, ГРЕСЬ ОЛЕКСАНДР, ЛАСТІВКА ОЛЕКСАНДР
Чернівецький національний університету імені Юрія Федьковича

ДОСЛІДЖЕННЯ ІНСТРУМЕНТІВ МОНІТОРИНГУ ТА МЕТОДІВ АУДИТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОСВІТНІХ ПЛАТФОРМ

У статті представлено комплексний аналіз інструментів моніторингу безпеки з відкритим кодом, архітектури інформаційно-комунікаційної системи (ІКС) університету а також методів аудиту та оцінки її безпеки. У дослідженні підкреслено роль рішень з відкритим кодом, таких як Nagios, Zabbix, Prometheus+Grafana, OSSEC, Snort/Suricata та Wazuh, у забезпеченні масштабованого та економічно ефективного моніторингу освітніх інфраструктур.

Архітектуру інформаційно-комунікаційної системи Центру цифрової трансформації представлено у вигляді трирівневої моделі Core–Distribution–Access, яка базується на принципах сегментації мережі, відмовостійкості, резервування та багаторівневого захисту, що забезпечує безперервність освітніх процесів та відповідність міжнародним стандартам.

Окрему увагу приділено аналізу сучасних засобів аудиту інформаційної безпеки, які систематизовано за трьома основними категоріями: технічні, організаційні та процедурні. Також здійснено порівняльний аналіз ефективності сучасних платформ аудиту та моніторингу безпеки та визначено, що комплексне використання відкритих систем моніторингу у поєднанні з регулярним аудитом безпеки дозволяє мінімізувати наслідки кіберінцидентів та створює цілісну модель кіберзахисту освітнього середовища, орієнтовану на забезпечення конфіденційності, цілісності та доступності інформації.

Результати дослідження показують, що впровадження відкритих інструментів моніторингу, сучасних архітектурних рішень та систематичних процедур аудиту дозволяє підвищити рівень захищеності освітніх платформ, забезпечити відповідність міжнародним стандартам, а також сформувати стійку та адаптивну систему кібербезпеки для закладів вищої освіти.

Ключові слова: *кібербезпека, освітня інфраструктура, інструменти моніторингу з відкритим кодом, методи аудиту, SIEM, глибинний захист, ISO/IEC 27001, OWASP, NIST.*

Стаття надійшла до редакції / Received 17.03.2026
Прийнята до друку / Accepted 14.04.2026
Опубліковано / Published 28.05.2026

Problem Statement

In the context of the active digital transformation of society, ensuring information security has become critically important for the stable operation of educational, scientific, and administrative institutions. The intensive implementation of information and communication technologies in higher education institutions is accompanied by a continuous increase in data volumes, the use of cloud platforms, distance learning services, and remote access mechanisms. Consequently, this leads to a growing number of potential cyber threats and complicates the process of maintaining an appropriate level of protection for information and communication systems (ICS) [1].

Modern educational infrastructure includes a significant number of interconnected components, such as web portals, electronic document management systems, electronic journals, repositories of educational materials, database servers, local and wireless networks, as well as distance learning platforms. These systems ensure the continuity of the educational process; however, at the same time, they represent potential targets for cyberattacks aimed at violating the confidentiality, integrity, and availability of information [2]. This issue becomes especially relevant due to the increasing number of ransomware, phishing, and DDoS attacks, as well as attempts of unauthorized access to the personal data of students and educational institution staff [3, 4].

An important direction for improving the security level of ICS is the use of open-source monitoring and security auditing tools, which provide continuous control of network infrastructure status, anomaly detection, event log analysis, and timely incident response. The advantages of open-source solutions include scalability, flexibility of configuration, community support, and the absence of significant financial costs, making them particularly relevant for educational institutions.

According to studies conducted by the European Union Agency for Cybersecurity (ENISA) [4], a considerable proportion of incidents in the educational sector are associated with the human factor, misconfigurations of access systems, and the use of outdated software. Furthermore, modern analytical reports on threats in the education sector demonstrate a continuous increase in the number of sophisticated multi-vector attacks targeting the information resources of universities and research institutions. In this regard, there is a need to implement comprehensive systems for monitoring, auditing, and assessing the security level of information infrastructure.

Overview of open-source security monitoring tools and audit methods for educational institution infrastructure

The digitalization of the educational environment has significantly increased the role of information systems in supporting the educational process, organizing scientific activities, and managing educational institutions. Electronic journals, distance learning systems, cloud services, data storage servers, and internal networks have become critically important elements of educational infrastructure. At the same time, the concentration of large volumes of personal data and the use of open network services increase the risk of cyber incidents, which necessitates the implementation of a comprehensive approach to security monitoring and auditing [4].

Therefore, the use of open-source tools in this context is an optimal solution, as it allows ensuring a high level of protection without significant financial costs and also contributes to the development of practical skills among students of technical specialties.

The first monitoring systems appeared in the late 1990s, when the rapid spread of the Internet and server technologies required tools for controlling resource availability. Nagios (1999) became one of the pioneers in this field, laying the foundation for the further development of open-source solutions, while its architecture focused on simplicity and modularity defined the direction for subsequent generations of systems [5].

In the 2000s, the increasing complexity of networks and the emergence of virtualization contributed to the development of more scalable platforms such as Zabbix (2001), which integrated real-time metric collection and advanced visualization capabilities. Alongside this, intrusion detection systems evolved, among which Snort (1998) became the de facto standard for network traffic analysis.

Since the mid-2010s, the focus has shifted toward analytics and interactive dashboards. Prometheus (2012) and Grafana (2014) reflected a new monitoring paradigm oriented toward flexibility, scalability, and integration with cloud services. During the same period, next-generation solutions such as Wazuh (2015) emerged, combining monitoring, security, and compliance management functions.

The prospects of modern monitoring and security systems for information and communication systems (ICS) in educational institutions can be considered in several directions:

- Integration with cloud platforms – as universities increasingly use cloud services such as Microsoft Azure, AWS, and Google Cloud, tools like Prometheus + Grafana and Wazuh provide adaptive monitoring in hybrid environments.
- Protection of student data cybersecurity – tools such as OSSEC, Snort, and Suricata remain relevant for protecting student databases, electronic journals, and internal networks from attacks.
- Scalability for large campuses – Zabbix and Wazuh enable centralized control of thousands of nodes, which is especially important for universities with extensive infrastructures.
- Analytics and forecasting – the use of Prometheus + Grafana opens opportunities for analyzing the workload of distance learning servers and forecasting peak periods, contributing to resource optimization.
- Compliance with international standards – Wazuh integrates with SIEM systems and supports compliance auditing according to ISO/IEC 27001 standards, which is important for universities participating in international educational programs such as Erasmus+.

Based on the conducted analysis of the development of monitoring and security tools, it is possible to note the transition from basic availability control to comprehensive platforms capable of providing multi-level protection and

analytics (Table 1). For educational institutions, their implementation is not only a technical solution but also a strategic factor determining the quality and security of the educational process in the context of digital transformation.

Modern information security audit systems for educational platforms can be classified into three main categories: technical, organizational, and procedural methods.

Technical audit methods include vulnerability scanning, penetration testing, network traffic analysis, server configuration auditing, the use of IDS/IPS systems, and event log monitoring. The use of automated scanners makes it possible to promptly identify critical vulnerabilities in web applications, network services, and server software.

Organizational audit methods cover the analysis of security policies, access management mechanisms, authentication procedures, and risk assessment. An important element is compliance monitoring with international standards, particularly ISO/IEC 27001, as well as the recommendations of the OWASP Foundation regarding the protection of web resources and information systems.

Procedural methods involve the creation of incident response plans, implementation of backup mechanisms, ensuring service continuity, and the use of SIEM systems for centralized analysis of security events. The integration of procedural auditing with monitoring systems enables rapid anomaly detection, forecasting of potential risks, and minimization of the consequences of cyberattacks.

A special role in modern cybersecurity systems is played by comprehensive security auditing and monitoring platforms, particularly Wazuh and OSSEC. These solutions combine monitoring functions, event log analysis, file integrity control, anomaly detection, and compliance verification with international information security standards. Integration of Wazuh with SIEM platforms allows centralized processing of security events, automation of incident response, and compliance auditing according to the requirements of the International Organization for Standardization and the recommendations of the National Institute of Standards and Technology [6, 7].

Based on the conducted analysis of the development of monitoring and security tools, it can be concluded that there has been a transition from basic availability monitoring to comprehensive platforms capable of ensuring multi-level protection and advanced analytics (Table 1). For educational institutions, their application is not only a technical solution but also a strategic factor determining the quality and security of the educational process under conditions of digital transformation.

Table 1.

Comparative Table of Prospects for the Application of Monitoring and Security Tools in Universities

Tool	Main Functions	Prospects for Application in Universities
Nagios	Monitoring of Server and Service Availability	Used for basic monitoring of educational platforms and electronic libraries; suitable for small educational institutions with simple infrastructure.
Zabbix	Real-time metric collection, triggers, and visualization	Centralized monitoring of local networks and campus Wi-Fi; a scalable solution for large universities with extensive infrastructure.
Prometheus+Grafana	Metric collection and interactive visualization	Load analytics for distance learning servers; forecasting of peak periods; integration with cloud platforms
OSSEC	HIDS: log analysis and file integrity monitoring	Protection of electronic journal servers and student databases; suitable for medium-sized institutions where host-level control is important.
Snort/Suricata	IDS/IPS: traffic analysis and attack detection	Protection of internal networks from external attacks (DoS, SQL Injection, XSS); relevant for universities with open access to resources.
Wazuh	Centralized monitoring, SIEM integration, compliance auditing	A comprehensive solution for controlling the entire IT infrastructure; ensuring compliance with international standards (ISO/IEC 27001); supporting participation in international programs (Erasmus+).

It should be noted that the choice of monitoring and security auditing tools largely depends on the scale of the educational institution's information infrastructure, the number of users, network traffic volume, and cybersecurity requirements. For example, small institutions may adopt Nagios or OSSEC as simple and easy-to-implement solutions; medium-sized universities may use Zabbix and Snort/Suricata to achieve a balance between monitoring and security. In contrast, large universities and international educational centers require comprehensive solutions based on Wazuh and Prometheus + Grafana, which provide scalability, analytics, and compliance with standards.

In addition, open-source monitoring and auditing tools form the basis for building a comprehensive cybersecurity system for educational institutions, aimed at ensuring the confidentiality, integrity, and availability of information resources. The integration of such solutions into the educational environment not only enhances the security level of information and communication systems but also enables their use in the educational process as practical tools for training future specialists in cybersecurity, system administration, and network technologies.

Design of the information and communication system (ics) infrastructure of an educational institution

Typically, the information and communication system of the Digital Transformation Center is a key component of the university's digital infrastructure, ensuring the operation of educational, scientific, and administrative services. The architecture is designed based on the principles of scalability, reliability, and security, which guarantee the continuity of educational processes and integration with national and international digital platforms.

The Center performs functions related to ICS infrastructure management, administration of information resources, cybersecurity assurance, and implementation of advanced digital technologies in the educational process. The main areas of activity include supporting corporate network services, administering local networks of faculties and departments, managing electronic document systems, distance learning platforms, and communication between university units. The infrastructure includes network architecture, server infrastructure, software and services, and the security component.

The network infrastructure of the Center is implemented using the three-tier model of the Cisco Enterprise Network Design Guide [7] (Fig. 1), which includes:

- Core Layer: high-performance switches Cisco Catalyst 9500 and Arista 7050X, combined into a StackWise Virtual cluster. They form a unified fiber-optic backbone with throughput up to 25 Gbps and ensure fault tolerance and load balancing.
- Distribution Layer: Cisco Catalyst 9300 and MikroTik CRS326 switches that implement VLAN segmentation, inter-subnet routing, and access control lists (ACLs).
- Access Layer: Cisco Catalyst 9200 and HPE Aruba 2930F switches with PoE+ support, powering Wi-Fi access points, IP phones, and video surveillance systems.

The network topology has a hybrid structure ("star + ring"), which ensures high throughput (up to 6 Tbps) and channel redundancy using the Rapid PVST+ protocol. VLAN segmentation isolates traffic between administrative, educational, and research networks, improving the effectiveness of security policies.

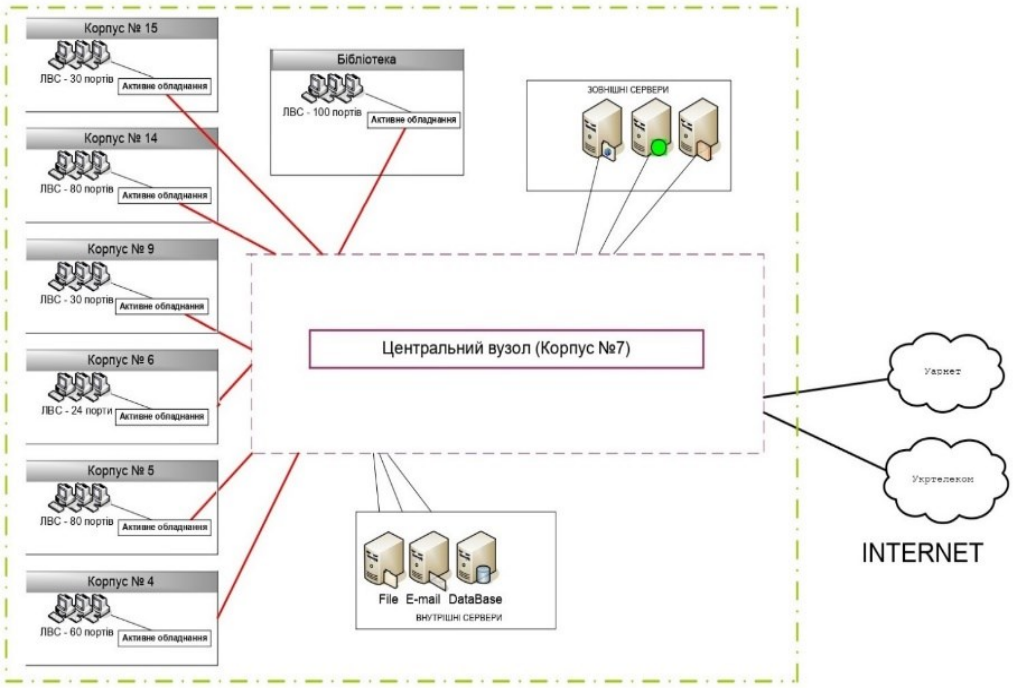

Fig. 1. Network topology of the Center

The server infrastructure is based on Dell PowerEdge R740 and HP ProLiant DL380 Gen10 physical servers, which support virtualization platforms such as VMware ESXi and Hyper-V. The servers are organized into a clustered system with redundancy and load balancing mechanisms.

Critical services are deployed on this infrastructure, including corporate email (Microsoft Exchange 2019), file storage systems (Windows Server DFS), database systems (PostgreSQL, MySQL), and university web portals (Nginx, Apache).

For data management, a SAN storage system with multi-level redundancy is used. Backup is performed using Veeam Backup and Acronis according to the "3-2-1" principle.

Network connectivity is provided through two independent Internet service providers — "UarNet" (Ukrainian NREN) and "Ukrtelecom" — ensuring BGP routing and fault-tolerant Internet access. At the perimeter, NGFW firewalls FortiGate and Cisco ASA are deployed in an Active-Active cluster, providing DPI, SSL inspection, IDS/IPS functionality, and request filtering.

The ICS of the Center uses a combination of commercial and open-source software solutions, including operating systems Windows Server 2019, Ubuntu 22.04 LTS, and Kali Linux, as well as platforms such as Moodle, Nextcloud, Microsoft 365 Education, Google Workspace for Education, PostgreSQL, and MS SQL. For monitoring and logging, Splunk Enterprise, Zabbix, and SIEM modules are used, integrated with antivirus solutions ESET Protect and CrowdStrike Falcon.

From a cybersecurity perspective, the ICS is implemented according to the Defense-in-Depth principle, which includes physical protection of server rooms, traffic and user authentication control, event logging, and system redundancy.

Modern cryptographic mechanisms are applied: TLS 1.3 for data in transit and AES-256 for data at rest. Two-factor authentication (2FA) is implemented using YubiKey tokens and mobile applications, along with a centralized strong password policy.

The organizational cybersecurity model is based on the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine" (2017), the National Cybersecurity Strategy (2023–2027), as well as internal university regulations (risk management policy, access control, incident response, backup procedures, and business continuity planning) [8].

Authentication and identity management systems. The Digital Transformation Center has implemented a centralized Single Sign-On (SSO) system [9], which integrates Google Workspace, Moodle, Nextcloud, and local services based on LDAP. For administrative users, multi-factor authentication (2FA) is mandatory. Access control is implemented using the Role-Based Access Control (RBAC) model, which ensures that users are granted only the minimum necessary privileges according to their role. All access rights changes are recorded in SIEM logs.

Thus, the infrastructure of the educational institution, built on modern principles of scalability, fault tolerance, and multi-layered security, includes a three-tier network architecture, a clustered server system, integration of commercial and open-source software solutions, implementation of the Defense-in-Depth approach, and a centralized authentication system.

Consequently, the ICS of the Digital Transformation Center ensures the continuity of educational processes, protection of information assets, and compliance with international and national cybersecurity standards.

Methods of auditing and security assessment of educational infrastructure

Security auditing of educational infrastructure is a complex process that combines technical, organizational, and procedural methods. Its purpose is to systematically identify vulnerabilities, assess the effectiveness of implemented security controls, and develop recommendations for their improvement. A specific feature of educational institutions is the need to balance open access to resources for students and teachers with the protection of critical data, which requires the use of international standards (ISO/IEC 27001, NIST Cybersecurity Framework, OWASP Testing Guide) and their adaptation to Ukrainian conditions [10–13].

Security audit methods include technical methods, organizational methods, and monitoring and response mechanisms.

Technical methods are aimed at practical assessment of the state of information systems and networks; they provide an objective view of the technical security level and help identify the most critical vulnerabilities. The main tools include:

- Vulnerability scanning (OpenVAS, Nessus, Nikto) – automated detection of known configuration and web application issues;
- Penetration testing (Burp Suite, Metasploit) – simulation of real attacks to evaluate system resilience;
- Log analysis (Splunk, ELK Stack) – detection of anomalies in user behavior and system processes;
- Intrusion Detection/Prevention Systems (IDS/IPS) (Snort, Suricata) – monitoring network traffic and blocking attacks in real time.

Organizational methods cover the management of security policies and processes, ensuring the consistency and stability of cybersecurity practices. The main aspects include:

- Access policy assessment – verification of RBAC model compliance and the principle of least privilege;
- Risk management – identification, classification, and mitigation of risks in accordance with ISO/IEC 27005;
- Regulatory compliance – auditing compliance with the Law of Ukraine "On the Basic Principles of Cybersecurity of Ukraine," GDPR, and internal university regulations;
- Staff training – regular cybersecurity awareness training, including detection of social engineering and phishing attacks.

Monitoring and response are key elements of continuous security auditing, enabling not only threat detection but also timely response and minimization of impact on the educational process. These include:

- SIEM systems (Wazuh, Splunk Enterprise) – centralized collection and analysis of security events;
- Incident Response Procedures (IRP) – structured procedures for handling cybersecurity incidents;
- Business Continuity Planning (BCP) – ensuring the operation of critical services even during attacks or failures;
- Backup and recovery – implementation of the "3-2-1" principle for data protection.

The comprehensive combination of open-source monitoring tools, modern infrastructure, and systematic auditing forms the foundation of cybersecurity in educational institutions. This approach enables the continuity of educational processes, protection of critical information assets, compliance with international security standards (ISO/IEC 27001, NIST, OWASP), and integration of practical tools into the learning process for training future specialists.

Thus, the digital infrastructure of a university becomes not only a technical platform for education and research but also an example of implementing modern cybersecurity practices aligned with global trends and national priorities.

Experimental study of the developed information and communication system of the educational institution

The experimental study of the developed information and communication system (ICS) of the educational institution is carried out in several stages:

- Testing of the network infrastructure: evaluation of the throughput of the fiber-optic backbone (DWDM, 10–25 Gbps); assessment of network recovery time during topology changes (Rapid PVST+).
- Server performance testing: load simulation on the Dell PowerEdge R740 and HP ProLiant DL380 Gen10 cluster; testing of backup systems (Veeam Backup, Acronis).

- Security assessment: configuration audit of NGFW firewalls FortiGate and Cisco ASA; testing of user authentication mechanisms (SSO, 2FA, RBAC); vulnerability scanning using OpenVAS and Burp Suite.
- Monitoring and logging: use of Splunk Enterprise and Zabbix for event collection and analysis; integration of SIEM modules with antivirus solutions ESET Protect and CrowdStrike Falcon.

In addition, to eliminate vulnerabilities in the ICS, a multi-layered security approach based on the Defense-in-Depth model has been implemented, where each system layer has its own monitoring and response tools (Fig. 2).

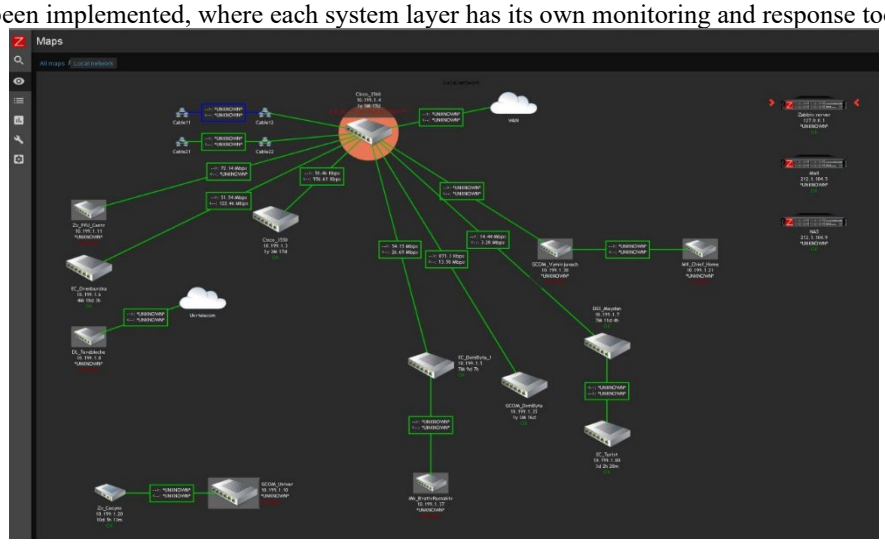

Fig. 2. Infrastructure map of the ICS

At the network perimeter, a FortiGate 200E NGFW is deployed, providing SSL inspection, IDS/IPS functionality, web request filtering, and VPN access. Within the internal network, a Suricata IDS system operates, interacting with Splunk SIEM for centralized log and event analysis.

Node status and load monitoring are performed using Zabbix. Authentication is managed through Active Directory combined with RADIUS, while Network Access Control (NAC) is implemented using Cisco ISE, which verifies each device before it is granted access to the network (Fig. 3).

.

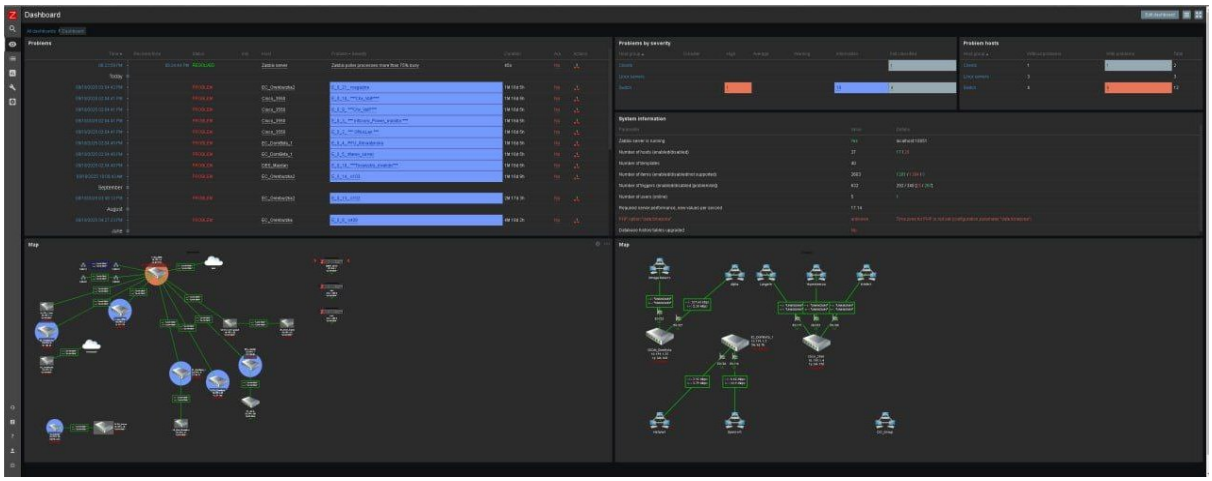

Fig. 3. Monitoring of the current state of the ICS infrastructure

Based on the data collected by the Zabbix monitoring system, a unified set of indicators is formed for analyzing the state of information security. These data are used as an information source for further automated processing. The integration between Zabbix and the aggregator is implemented via a JSON-RPC API or webhook, which enables real-time incident notifications and ensures dynamic updates of the asset database and vulnerability status. This approach provides a continuous vulnerability management cycle and enhances the level of operational response to information security events.

The audit of the Digital Transformation Center ICS after the implementation of the above security measures was carried out in two stages: first, an automated scanning of servers, software, and network services was performed using Nessus [14], and then the Wazuh platform [15] was used to monitor security events, analyze agent activity, correlate incidents, and assess threats. The scanning results are shown in Fig. 4 and Fig. 5.

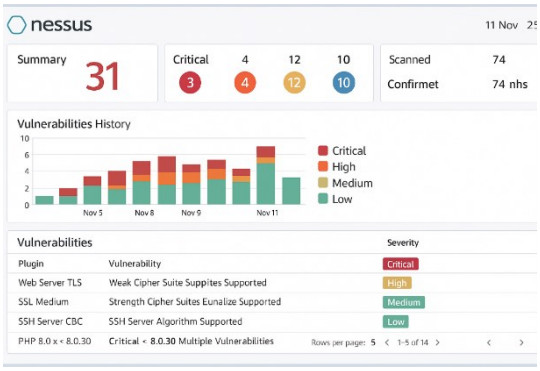

Fig. 4. Nessus Summary Dashboard

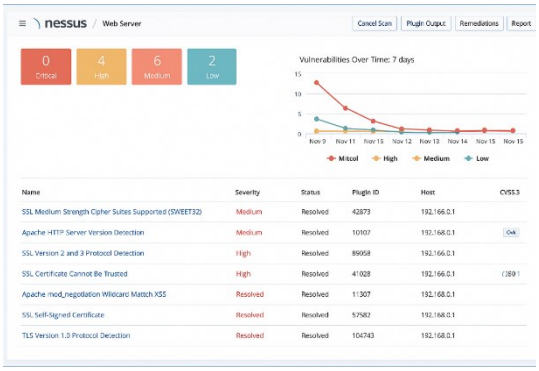

Fig. 5. Nessus Web Server Scan

The consolidated Nessus dashboard after the rescan demonstrates the overall vulnerability status with a distribution by severity level. The visual interface structure, presented in the form of cards and a historical trend graph, enables a rapid assessment of positive dynamics, namely a reduction in the number of critical and high-severity threats. The obtained results confirm the elimination of outdated algorithms and the strengthening of secure protocol parameters, which indicates the effectiveness of the implemented security improvements. For a more detailed analysis of the web server, a Nessus Web Server Scan was performed (Fig. 5).

The web server scan covers key network services and components of the web platform, while the upper part of the interface presents criticality indicators (Fig. 5), which demonstrate the absence of critical vulnerabilities and a significant reduction in high and medium-level threats. The 7-day trend graph shows a decrease in the number of identified issues after optimization of TLS/SSL configurations and updates of server software.

The tabular section lists specific CVEs and their status, where most are marked as “Resolved”, confirming their successful remediation. The identified vulnerabilities are related to weak cryptographic suites found in older versions of Apache HTTP Server, as well as SSL mechanisms that were updated in accordance with modern security standards. Some vulnerabilities are associated with XSS and other web-based attacks, which are now mitigated by properly configured security headers. The scan results indicate that the server has migrated to modern cryptographic libraries and uses TLS 1.2/1.3.

Overall, it can be concluded that the performed procedures resulted in a significant improvement of the web server configuration and an increased level of security.

Next, a Nessus scan of the mail server was performed (Fig. 6). The rescan of the mail server confirmed the absence of critical vulnerabilities and a reduction in issues related to SMTP configuration parameters and weak TLS modes. In the “Vulnerabilities by Plugin Family” section, the main threats (SMTP, SSL/TLS, service detection) are marked as “Resolved”. There is confirmation of the elimination of insecure plaintext authentication, weak cipher suites, and outdated STARTTLS mechanisms.

The new Postfix configurations and secure mail protocol settings have been aligned with CIS Benchmarks, which mitigated the risks of unauthorized access. The audit confirmed an increased resilience of the system against authentication-based attacks.

The next stage involved the analysis of the database server (Fig. 7). The Nessus assessment of the database server revealed only medium-level vulnerabilities, while critical and high-severity issues were absent. The identified issues related to weak cryptographic algorithms, self-signed certificates, RC4 usage, and improper authorization were eliminated after database management system updates and the implementation of CIS recommendations. The host received all security patches, ensuring compliance with modern security requirements. The scan results are presented in Fig. 6 and Fig. 7.

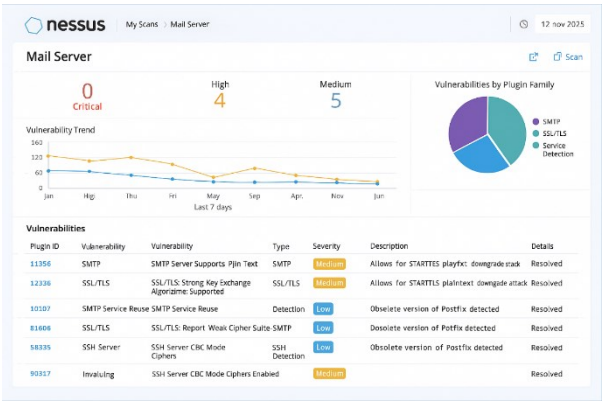

Fig. 6. Nessus Mail Server Scan

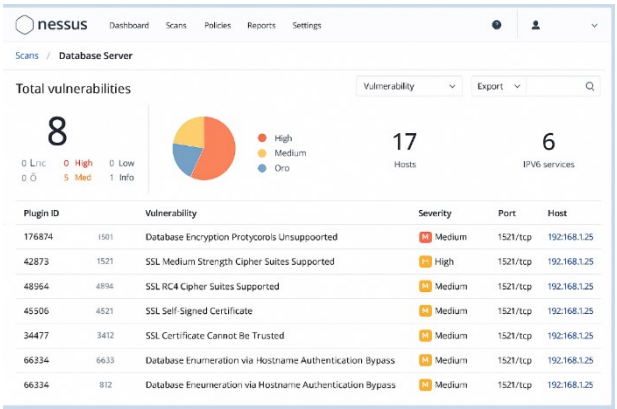

Fig. 7. Nessus Database Server Scan

Next, an analysis of the ICS was conducted using Wazuh (Fig. 8). The telemetry data showed the number of events, level 12+ incidents, and authentication attempts. The “Alerts evolution” dashboard illustrated agent activity across different operating systems.

The MITRE ATT&CK diagram (Fig. 9) indicated prevalent tactics such as Credential Access, Initial Access, and Execution. Most critical incidents were related to Windows processes and login attempts using non-existent accounts.

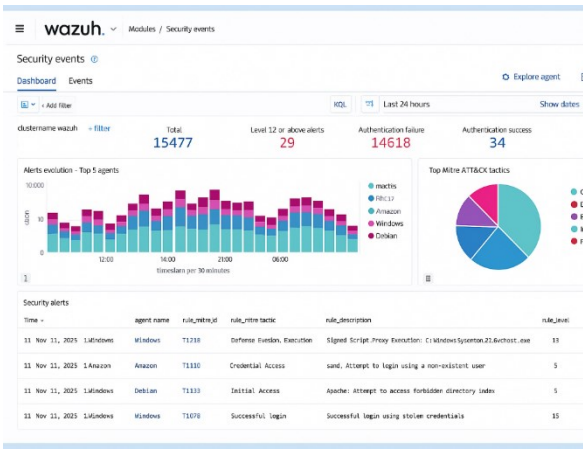

Fig. 8. Security Events Dashboard

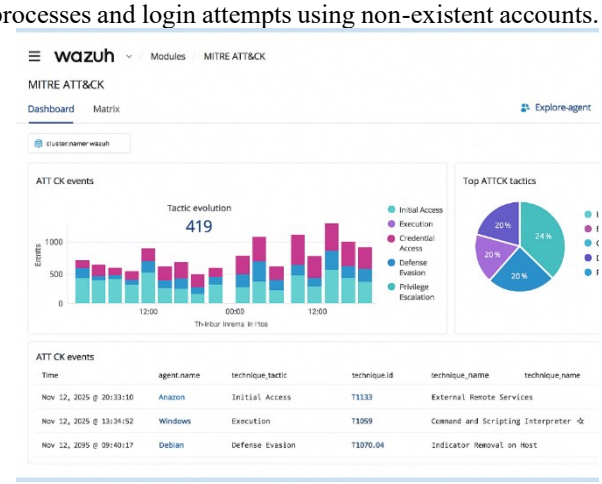

Fig. 9. Wazuh MITRE ATT&CK Mapping

The MITRE ATT&CK module provided incident classification and a tactic evolution chart, which showed a decrease in events in the Initial Access, Execution, and Credential Access categories. The sector diagram (Fig. 10) demonstrates an even distribution of attacks, while the table includes incidents mapped to MITRE techniques (External Remote Services, Command & Scripting Interpreter, Indicator Removal on Host).

The reduction of complex attacks confirms the effectiveness of monitoring policies and the resilience of the system. The next stage involved the analysis of the agent Activity Timeline (Fig. 10).

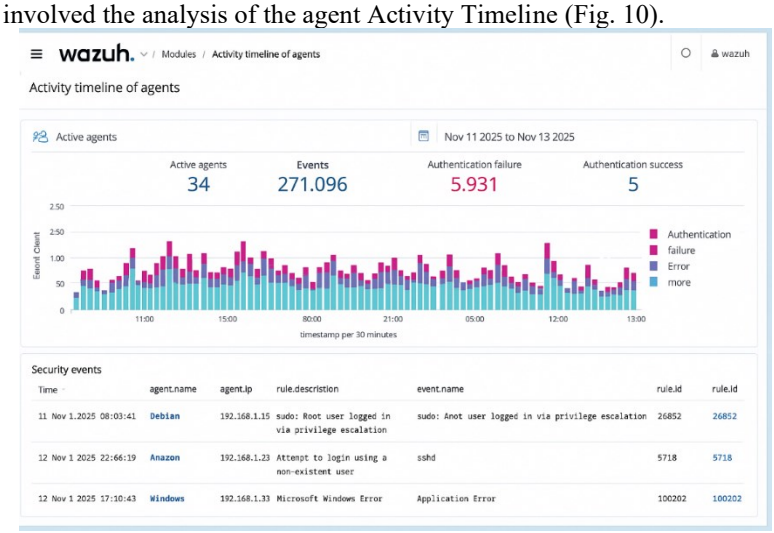

Fig.10. Wazuh Agent Timeline

The agent Activity Timeline illustrated daily system behavior and anomalies. Metrics displayed the number of agents, events, and authentication attempts; peak loads decreased after the implementation of security measures. Color coding allowed for assessing the ratio of successful and failed logins. The table included examples of suspicious activity, such as root logins, attempts using non-existent accounts, and Windows system errors. The reduction in critical events confirmed the effectiveness of the implemented protection mechanisms, while a stable baseline indicated the "healthy" functioning of the system.

Thus, the results of the conducted research on the network infrastructure confirmed that the backbone throughput reached up to 25 Gbps, and the connection recovery time was less than 1 second. VLAN segmentation ensured effective traffic isolation.

The clustered server environment demonstrated stable performance under peak loads, and the backup system complied with the "3-2-1" principle.

Security mechanisms implemented on NGFW firewalls successfully blocked DDoS and SQL injection attacks, while the deployed SSO system with 2FA provided a high level of authentication security. The RBAC model minimized the risk of excessive privileges.

Monitoring using Nessus and Zabbix enabled timely detection of anomalies, and integration of SIEM with antivirus solutions ensured centralized event control.

Conclusions

The conducted audit of the information and communication system of the Digital Transformation Center confirmed the effectiveness of the implemented technical and organizational security measures. The results of the Nessus scans demonstrated the absence of critical vulnerabilities in the web, mail, and database servers, as well as the elimination of outdated cryptographic algorithms and insecure configurations. Monitoring in Wazuh and incident classification using MITRE ATT&CK showed a reduction in the number of complex attacks, stabilization of the agent activity timeline, and an

increased resilience of the system against brute-force and unauthorized access attempts. Thus, the implemented measures ensured compliance with modern security standards and significantly improved the cybersecurity level of the ICS.

The conducted experimental study confirmed that the developed ICS meets the requirements of scalability, fault tolerance, and multi-layered protection. The use of open-source tools combined with commercial solutions provides a balance between cost efficiency and a high level of security. The study also indicates that special attention should be given to further integration of artificial intelligence systems for proactive threat detection and automated incident response, which represents the next stage in the development of the ICS.

The research results demonstrate that the implementation of open-source monitoring tools, modern architectural solutions, and systematic audit procedures enhances the security level of educational platforms, ensures compliance with international standards, and enables the formation of a resilient and adaptive cybersecurity system for higher education institutions.

Література

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems. Geneva : International Organization for Standardization, 2022.

2. National Institute of Standards and Technology. NIST SP 800-53 Rev. 5: Security and privacy controls for information systems and organizations. Gaithersburg : NIST, 2023.

3. OWASP Top Ten 2024: The ten most critical web application security risks. OWASP Foundation, 2024.

4. CERT-UA. Звіти про кіберінциденти в Україні : вебсайт. URL: https://cert.gov.ua (дата звернення: 28.05.2026).

5. IBM Security X-Force. Cybersecurity education sector threat landscape 2024. IBM, 2024.

6. ISO/IEC 27005:2023 Information security, cybersecurity and privacy protection – Information security risk management. Geneva : International Organization for Standardization, 2023.

7. Cisco Systems. Campus network design guide: Three-tier architecture and security segmentation. Cisco, 2023.

8. Національна стратегія кібербезпеки України на 2023-2027 роки / Кабінет Міністрів України. Київ, 2023.

9. Dell Technologies. Veeam backup best practices for enterprise infrastructure. Dell Technologies, 2022.

10. Arista Networks. High availability in campus networks. Arista Networks, 2024.

12. ISO/IEC 22301:2019 Security and resilience – Business continuity management systems. Geneva : International Organization for Standardization, 2019.

13. ISO/IEC 27018:2023 Code of practice for protection of personally identifiable information (PII) in public clouds. Geneva : International Organization for Standardization, 2023.

14. Tenable Inc. (2024). Nessus vulnerability assessment report 2024. Tenable

15. Wazuh Inc. (2024). Open source security monitoring platform documentation. Wazuh.

References

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems. Geneva : International Organization for Standardization, 2022.

2. National Institute of Standards and Technology. NIST SP 800-53 Rev. 5: Security and privacy controls for information systems and organizations. Gaithersburg : NIST, 2023.

3. OWASP Top Ten 2024: The ten most critical web application security risks. OWASP Foundation, 2024.

4. CERT-UA. Zvity pro kiberintsydenty v Ukraini : vebsait. URL: https://cert.gov.ua (data zvernennia: 28.05.2026).

5. IBM Security X-Force. Cybersecurity education sector threat landscape 2024. IBM, 2024.

6. ISO/IEC 27005:2023 Information security, cybersecurity and privacy protection – Information security risk management. Geneva : International Organization for Standardization, 2023.

7. Cisco Systems. Campus network design guide: Three-tier architecture and security segmentation. Cisco, 2023.

8. Natsionalna stratehiia kiberbezpeky Ukrainy na 2023–2027 roky / Kabinet Ministriv Ukrainy. Kyiv, 2023.

9. Dell Technologies. Veeam backup best practices for enterprise infrastructure. Dell Technologies, 2022.

10. Arista Networks. High availability in campus networks. Arista Networks, 2024.

12. ISO/IEC 22301:2019 Security and resilience – Business continuity management systems. Geneva : International Organization for Standardization, 2019.

13. ISO/IEC 27018:2023 Code of practice for protection of personally identifiable information (PII) in public clouds. Geneva : International Organization for Standardization, 2023.

14. Tenable Inc. (2024). Nessus vulnerability assessment report 2024. Tenable

15. Wazuh Inc. (2024). Open source security monitoring platform documentation. Wazuh.