Higher education cyber resilience: Intelligent protection of educational, administrative and resource systems*

Olena Kryvoruchko[1,†], Yaroslav Shestak[2,†], Elizaveta Zavhorodnya[2,†] and Andriy Fesenko[3,4,*,†]

[1] National University of Life and Environmental Sciences of Ukraine, 15 Heroiv Oborony str., 03041 Kyiv, Ukraine
[2] State University of Trade and Economics, 19 Kyoto str., 02156 Kyiv, Ukraine
[3] State university "Kyiv Aviation Institute", 1 Lubomyra Guzara ave., 03058 Kyiv, Ukraine
[4] State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, 3/6 Maksym Zalizniak str., 03142 Kyiv, Ukraine

Abstract

This paper focuses on the cybersecurity system of a higher education institution (HEI) as a key element of ensuring the reliability and sustainability of its information infrastructure. The imperative to develop an effective cybersecurity system necessitates a comprehensive analysis of the information infrastructure of a higher education institution, including its: objects, interconnections, data transmission channels, communication tools, regulatory documentation and mechanisms for interaction with external infrastructures. In addition, the components of the information infrastructure of higher education institutions are considered and arranged into three main groups: educational, administrative and resource systems. Particular attention is given to an overview of the main cybersecurity risks and the consequences higher education institutions face in the event of successful cyberattacks by malicious actors. Furthermore, the study formulates the principles and proposes the main criteria that a comprehensive cybersecurity system in a higher education institution should meet. The main stages of implementing a comprehensive cybersecurity system architecture of higher education institutions have been outlined and characterised, as well as the main constraints to the implementation of each of these stages. For a deeper understanding of this infrastructure, the study also proposes its modelling as a means of assessing the current state, forecasting development trajectories, and analysing the impact of implementing modern computing tools and applications.

Keywords

cybersecurity, information infrastructure, information technologies, modelling, model, cybersecurity system architecture, cyber defence systems, cyber resilience of infrastructure, neural network technologies, communication networks

1. Introduction

At the current stage of development of higher education institutions (HEIs), ensuring the effective functioning of a cybersecurity system has become critically important, as it is a prerequisite for the stable and uninterrupted operation of the HEI's information infrastructure. Such a system encompasses all actors within both the internal and external information environment (including clients) and is aimed at protecting against cyber threats, attacks and unauthorised interference in information processes. The cybersecurity system constitutes a set of organisational and technical measures designed to detect external and internal threats, identify potential vulnerabilities and implement protection mechanisms. Its functioning is based on the provisions of the Decree of the President of Ukraine No. 447/2021 dated August 26, 2021, 'On the Cybersecurity Strategy of Ukraine'. The information infrastructure of a higher education institution should be regarded as a functional system that depends on the interaction of its structural elements and their functional capacities.

*CSDP'2025: Cyber Security and Data Protection, July 31, 2025, Lviv, Ukraine
* Corresponding author.
† These authors contributed equally.
ev_kryvoruchko@ukr.net (K. Kryvoruchko); shestack@knute.edu.ua (Y. Shestak); y.zavhorodnya@knute.edu.ua (E. Zavhorodnya); aafesenko88@gmail.com (A. Fesenko)
0000-0002-7661-9227 (K. Kryvoruchko); 0000-0002-5102-9642 (Y. Shestak); 0000-0003-0549-7020 (E. Zavhorodnya); 0000-0001-5154-5324 (A. Fesenko)

2. Related works

Scholars have approached the study of the systems in question from various perspectives. In particular, the implementation and use of protection technologies and systems in HEIs have been explored by A. Androshchuk, V. Afanasiev, V. Hryha, S. Ivanova, O. Dubach, O. Kosenko, M. Shyshkina, Y. Nosenko, L. Zabrodska, V. Kremen, B. Odiagailo, P. Orlov, L. Fishman, S. Londar, O. Bryniuk, S. Dvoretska, O. Shpak, V. Luzhetskyi, O. Bilyk, etc.

In the process of developing an effective cybersecurity system of HEIs' information infrastructure, the use of modelling methods is of paramount importance. These methods make it possible to represent complex information processes, analyse potential threats, and anticipate the consequences of introducing advanced technologies. In this context, particular attention should be paid to the approach proposed by Prus A. [1, p. 58–59], who describes mathematical modelling as a 'lens of the real world' and identifies four groups of competencies that are critically important for successful implementation of modelling process.

In particular, the first group of competencies emphasises a deep understanding of the problem, the formulation of realistic assumptions and the ability to distinguish between relevant and irrelevant information, which is essential for analysing cyber threats. The second group involves construction of a mathematical model based on real-world conditions, simplification, and use of appropriate visualisation methods, enabling an accurate representation of the architecture of the information infrastructure and its vulnerabilities. The third group focuses on interpreting mathematical results within HEI's actual operational environment, while the fourth concerns the critical evaluation of the model's adequacy, its flexibility, and readiness for adaptation in response to changes in cyber environment.

Thus, the application of modelling to the HEIs' information infrastructure within cybersecurity system should be viewed not merely as a technical process, but as a comprehensive competence-based activity that encompasses analysis, formalisation, interpretation, and critical reflection on the results obtained.

The information infrastructure of a higher education institution comprises a set of information systems, communication tools, users, databases, servers, gateways, access control systems, etc. To ensure the stability of the information infrastructure, encryption protocols such as AES-256, SSL\TLS can be employed, which enhance the resilience of information systems against cyberattacks. Given the inherent risks of the internet environment, it is not recommended to use information resources without adhering to established security protocols. Therefore, building a robust cyber security system and conducting continuous monitoring of all information systems is of critical importance, which includes vulnerability assessments, updates and implementation of security protocols, password policy enforcement (e.g., generation and regular renewal of strong passwords), users and administrators notifications regarding system breaches or intrusion attempts, blocking of potentially malicious users, and thorough analysis of incidents and their consequences. To identify and effectively deploy all the aforementioned security tools, protection systems, and mechanisms, artificial intelligence procedures should be applied to enable in-depth analysis, the modelling of cyberattack prototypes, and the forecasting of potential consequences through the use of neural networks.

3. Organisational approaches to protecting the information infrastructure of a higher education institution

In order to provide high-quality educational services, conduct cutting-edge sectoral research, ensure effective institutional governance, and maintain a competitive position in the educational services market, higher education institutions must be capable of offering educators, researchers, staff, and students reliable and uninterrupted access to their digital environment, represented by information infrastructure, including digital platforms, communication networks, data transmission systems, and cybersecurity systems. At the same time, preserving institutional

integrity and the trust of all stakeholders depends on the HEI's ability to guarantee cybersecurity, data privacy and resilience to cyber threats.

The concept of cyber resilience has become an important strategic goal for HEIs in light of rapid digital transformation. In order to support the continuity, quality and security of academic and operational procedures, HEIs are increasingly dependent on complex information infrastructures that encompass various administrative, educational and resource systems. However, as reliance on technology increases, so does vulnerability to a wide range of cyber threats. Therefore, it is crucial to first identify and classify core elements of HEIs' digital environment in order to design smart and adaptive cybersecurity measures. Table 1 below presents the main components of an HEI's information infrastructure, grouped into three functional categories: resource systems, administrative systems, and educational systems.

Table 1
Higher education institution information infrastructure components

Category	System type	Key data and information
Educational systems	Learning Management Systems (LMS)	Course materials, assignments, grades, student-teacher communication logs
	E-learning Platforms	Video lectures, tutorials, quizzes, participation data
	Student Information System (SIS)	Transcripts, enrolment data, exam schedules, attendance logs
	Virtual Labs	Lab reports, input-output datasets, simulation parameters
	Academic Advising Systems	Individual study plans, advising notes, academic history
	Plagiarism Detection Systems	Student submissions, plagiarism reports
	Assessment & Exam Management Systems	Question banks, exam results, timing records
	Internship & Career Services Platforms	Students CVs, job applications, employer data
Administrative systems	Financial Management Systems	Payrolls, invoices, grants, tuition payments
	HR Management Systems	Staff personal data, performance reviews, salary information
	Document Management Systems	Contracts, regulations, meeting minutes
	Admissions & Enrollment Systems	Personal applicant data, test scores, admission decisions
	Scheduling & Timetabling Systems	Class schedules, room use logs, lecturer assignments
	Campus Security & Incident Reporting	Incident logs, security video metadata, reports
	Communications & Notification Systems	Bulk emails, official notices, student and staff contacts
Resource systems	ICT Infrastructure Monitoring & Control Systems	Logs, IP traffic, server load data
	Library Information Systems	Book records, research access logs, borrower data
	Research Information	Research proposals, grants, institutional affiliations

Systems	
Access Control & Identity Management Systems	User roles, biometric scans, access logs
Asset & Inventory Management Systems	Serial numbers, condition reports, usage records
Energy & Facility Management Systems	Energy usage data, sensor data, schedules
Cloud Storage & Backup Systems	Course files, administrative backups, personal folders
Software Licensing & Deployment Systems	License keys, installation tracking, usage analytics

In particular, studies [2–4] indicate that in 2024 alone, higher education institutions were one of the most targeted sectors of the economy: 66% of respondents reported experiencing cyberattacks, and 79% faced at least one security incident. Although data theft was the least frequently reported type of breach, only 18% of HEIs officially disclosed such incidents. Nevertheless, the overall impact of cyberattacks was significant and often severe. The most dangerous threat remains ransomware, as the majority of affected HEIs ended up paying up to 122% of the initial ransom demand, with an average pay-out of USD 5.85 million—ranking the third highest among all sectors. Additionally, half of the affected HEIs reported direct damage to their ICT infrastructure, while over 60% experienced substantial operational and financial disruptions. Moreover, in 77% of cases, the data was encrypted, and in 95% of cases, attackers attempted to access backups, thus significantly complicating recovery efforts [2–4].

In light of these challenges, it is essential to clearly define the principles that a comprehensive cybersecurity system for higher education institutions must uphold in order to provide all-encompassing protection for institutional systems and resources. These principles include [5, p. 140–142]: the principle of confidentiality, the principle of integrity, the principle of availability of information and resources at the right time for authorised users, the principle of monitoring and evaluating security systems, the principle of legal compliance, the principle of accountability for actions within the HEI's information infrastructure, the principle of digital risk management, the principle of security awareness among all users of the HEI's information infrastructure, the principle of adaptive security architecture, the principle of zero trust, the principle of resilience of HEI's information systems, the principle of HEI's data sovereignty, and the principle of integrated threat analysis from both internal and external sources within the security architecture, to enable proactive threat prediction and response [6–9].

It is noteworthy that the cybersecurity system architecture of a higher education institution constitutes an organised set of policies, tools, procedures, and control mechanisms that interact to protect the institution's data infrastructure from cyberattacks. This architecture defines the design, implementation mechanisms, interrelationships, and governance of security components to ensure the availability, confidentiality, integrity, and resilience of administrative, resource, and educational systems. Moreover, a comprehensive and integrated cybersecurity architecture in an HEI must meet several key criteria, specifically it should:

- Align with the academic mission, strategic goals and HEI's digital transformation priorities.
- Be based on a risk-oriented strategy that includes frequent risk assessments and threat modelling tailored to the higher education context.
- Ensure the protection of the HEI's network, endpoints, applications, data and user layer through a multi-layered security system.
- Include protective mechanisms that guarantee the availability, confidentiality, and integrity of data across all administrative, resource, and educational systems.
- Comply with national regulations and international standards.

- Be adaptive and scalable to accommodate future growth, the integration of emerging technologies, and evolving cyber threats.
- Be capable of employing SIEM and advanced analytical tools for automated incident response, real-time threat detection, and continuous monitoring.
- Support backup procedures, failover strategies, and disaster recovery planning.
- Enforce strict verification of all users and devices.
- Integrate both internal and external threat intelligence sources.
- Incorporate mechanisms for regular auditing, compliance verification, and evaluation for security system's effectiveness.
- Be governed by clearly defined roles, responsibilities, and protocols for resource allocation, decision-making, and incident escalation.
- Preserve sovereignty over private and confidential data while ensuring secure data sharing, collaboration, and research activities.

In particular, the development of such a comprehensive cybersecurity system for a HEI involves several stages, each with its own objectives and tasks:

1. Preliminary assessment and strategic planning (conducted to establish a foundational understanding of the current state of cybersecurity within the HEI and to define strategic goals for the security architecture), including identification and classification of HEI's information infrastructure critical components (educational, administrative, and resource systems), evaluation of existing cybersecurity policies, technologies, and practices; analysis of applicable regulatory requirements; as well as defining cybersecurity goals in alignment with the HEI's mission and digital transformation strategy.

The implementation of this stage can be hindered by several factors, including: lack of commitment from senior leadership regarding cybersecurity; absence of a comprehensive and up-to-date inventory of digital assets, leading to "blind spots" in planning; fragmented governance structures and unclear cybersecurity management responsibilities; insufficient awareness of the applicable cybersecurity regulations within HEIs; limited financial and human resources; misalignment between IT planning and academic planning; absence of a formal cybersecurity governance framework.

2. Risk assessment and threat modelling (conducted to identify, analyse and prioritise potential cyber threats, vulnerabilities and risks specific to the HEI environment), which entails performing a comprehensive risk assessment across all HEI's systems, developing a model of internal and external threats to its information security, evaluating the likelihood and impact of various cyber incidents, identifying high-risk zones for prioritised protection, and creating a formal risk register.

The successful completion of this stage may be hampered by several factors, including the lack of standardised methodologies for identifying and analysing cyber risks; insufficient documentation of past cyber incidents; limited awareness of cyber risks specific to the education sector (which affects modelling accuracy); underestimation of internal threats, as well as mismatch between identified risks and mitigation measures; over-reliance on outdated cyber threat models; and limited access to real-time cyber threat intelligence.

3. Architectural design and development of the "framework" (aimed at creating a structured, multi-layered security system that defines the functional and technical components of the cybersecurity system), that involves developing a multi-layered defence model (covering network, software, data, identities, and endpoint security), defining security domains and access control mechanisms, integrating core security technologies into the design,

implementing key security principles, and ensuring that the architecture complies with international standards and best practices.

Barriers to developing a reliable cybersecurity architecture for HEIs may include a lack of technical expertise in secure architectural design; limited stakeholder involvement; ambiguity in defining access rights and responsibilities; excessive dependence on a single vendor for hardware/software/technology solutions; lack of documentation of architectural solutions; and failure to consider future scalability, interoperability, and modularity.

4. Implementation and integration (focused on deploying cybersecurity tools, controls and policies in accordance with the developed architecture and institutional requirements), which includes the procurement, configuration and integration of cybersecurity technologies and platforms, implementation of identity and access management systems, application of encryption/authentication/monitoring mechanisms and endpoint protection mechanisms, establishment of incident response protocols and backup solutions, as well as coordination of deployment across HEI's departments.

Challenges during this stage may arise from operational disruptions in academic and administrative processes during system deployment; inadequate communication and coordination between IT staff and academic or administrative units; compatibility issues between new and legacy systems; incomplete configuration of cybersecurity tools; delays in approval and procurement processes; inadequate testing prior to full deployment; and the absence of a comprehensive system change management strategy.

5. Testing, verification and optimisation (conducted to assess the functionality, effectiveness and reliability of the implemented cybersecurity architecture), which includes penetration testing/vulnerability assessment/system audits, etc., verification of compliance with internal security policies and external regulatory standards, analysis of incident logs and monitoring of system behaviour under stress conditions, identification of weak points and performance issues, as well as optimisation of configuration and workflows based on test results.

The successful implementation of this stage may be complicated by the HEI's limited capacity to conduct thorough security testing; reluctance to schedule cybersecurity system downtime for testing (especially during academic semesters); lack of documented performance metrics for cybersecurity system operations; inadequate tools for detecting and monitoring cyber threats; resistance to implementing changes based on test results; and refusal to engage independent auditors.

6. User training and awareness raising (aimed at fostering institutional cyber hygiene by educating users and administrators about security protocols, risks and responsibilities), which involves designing and delivering regular cybersecurity training for staff, students and administrators, as well as disseminating instructions and policies in accessible formats, encouraging reporting of suspicious activity within HEI's information systems, etc.

The effectiveness of this stage may be limited by the perception among staff, faculty and students that cybersecurity training is optional; one-off or outdated approaches to cybersecurity training; insufficient integration of cybersecurity knowledge and practices into the institutional culture of the HEI; inconsistent enforcement of cybersecurity policies; and lack of feedback mechanisms to evaluate training outcomes.

7. Continuous monitoring and lifecycle management of the cybersecurity system (conducted to ensure the ongoing effectiveness, adaptability and resilience of the cybersecurity architecture), which includes the implementation of continuous monitoring tools, regular

updates to threat intelligence channels and security policies, review and update of the architecture in response to new risks/incidents/institutional changes, as well as periodic performance audits and compliance reviews, etc.

The implementation and effectiveness at this stage may be hindered by limited real-time visibility of network activity; insufficient integration with cyber threat intelligence systems; budget constraints and resource shortages for updating and maintaining cybersecurity infrastructure; lack of automation, excessive reliance on manual monitoring and delays in cyber incident response procedures; fragmented monitoring systems across HEI's information infrastructure; and the absence of regular security audits and system reviews.

4. Modelling the information infrastructure of a higher education institution

One of the key challenges in building an effective cyber defence system within HEI's information infrastructure is the absence of unified standards for structuring information: each HEI operates under its own specific institutional characteristics, internal policies and regulated procedures, which necessitates the use of additional protocols, interfaces, queries and communication tools to facilitate interaction between subsystems and controlled access to resources. It is important to note that modern communication tools that are capable of adaptive information transfer in compliance with established security protocols are already used.

In the context of cyber defence system modelling, it is essential to recognise that the resilience of information systems to cyber-attacks, unauthorised access or destruction attempts is one of the key criteria for its reliability. The construction of such a system requires, first and foremost, rigorous definition of organisational security measures, the design of secure communication channels and strict adherence to established procedures. All system users must undergo authentication and, in some cases, multi-factor identification is required (e.g. via SMS, mobile applications, digital keys, electronic digital signatures (EDS), qualified electronic signatures (QES), UES, cloud-based QES, biometric data).

A way to strengthen the cyber resilience of the HEI infrastructure is to implement modern cryptographic protocols, such as AES-256, SSL/TLS, which significantly reduce the risk of intrusion. However, even the most advanced technical solutions are ineffective without continuous system monitoring, detection of vulnerabilities, timely updating of security mechanisms and thorough incident analysis. Models should incorporate recommendations for regular password changes, blocking suspicious activities, alerting responsible personnel, and clearly defined threat response mechanisms.

In this process, it is important to use artificial intelligence tools, especially for simulating prototypes of potential cyber-attacks, predicting their consequences and constructing adaptive response systems. The application of neural network technologies significantly expands the scope of classical modelling, aligning with the conceptual approach to modelling as a method for understanding the real-world functioning of complex systems, as substantiated by Prus A. [1].

It is also important to emphasise that the use of a knowledge base in combination with artificial intelligence (AI) tools opens new opportunities for managing the information infrastructure of higher education institutions. Such systems enable not only the analysis of available data, but also to filtering, generation, selection and recommendation of effective development strategies for information systems. This approach ensures both the integrity and flexibility of the infrastructure operations, supports predictive modelling of its evolution, as well as facilitates timely responses to deviations from the expected outcomes. System performance monitoring becomes a continuous and automated process, significantly increasing the reliability and resilience of the educational environment against external threats and internal disruptions.

In this context, the use of neural networks in managing educational processes holds strategic importance. Neural networks can adapt HEI's infrastructure to new educational challenges, foster

digital transformation, expand the range of educational services, attract more students, and individualise the provision of system resources according to the needs of each user.

The development of an intelligent system based on a robust knowledge base and neural network algorithms creates a powerful decision-support environment. Such a system performs not only user authentication functions, but also autonomously adapts content, routes data to external infrastructures such as a Smart City ecosystem, e-Government platforms, international research networks, etc., thus expanding its applicability from the local level (within a HEI or city) to the national and global educational and scientific cyberspace [10–19].

As a result, HEI's information systems can interact with each other, adhering to international standards, supporting data exchange and ensuring secure operation within an open digital environment. This lays the groundwork for the deploying isolated subsystems, in particular, for scientific experiments, cyber threats modelling, testing security protocols, etc. (see Figure 1). All these factors directly affect the development of HEI's information infrastructure and its capacity for adaptation, resilience and innovation.

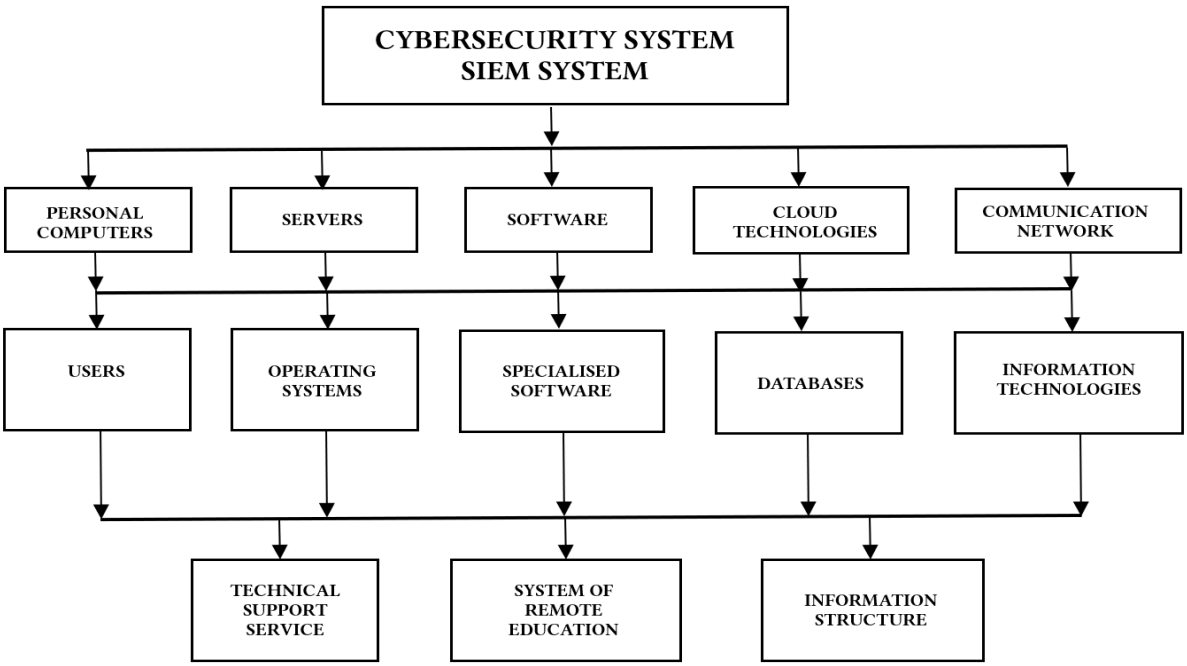

Figure 1: Hierarchical structure of HEI's cybersecurity system

In addition to the resources distributed by the HEI among its stakeholders, there exists a managed environment for secure connectivity and control of information flows, which incorporates gateways and firewalls that distributes resource load across the HEI's information infrastructure.

Figure 2 presents a model of all HEI's resources and their optimal communication pathways. Despite the extensive deployment of computers, communication systems, databases, and access to external information resources, all users within HEI's information infrastructure operate under certain limitations related to resource access. The lack of system-wide unification means that administrators manage each system and provide access rights separately. Consequently, any structural changes (such as modifications in personnel roles or responsibilities) can cause complications in updating user permissions and allocating new access rights across various HEI's systems. This approach illustrates a significant drawback of the uncoordinated information and automated systems in use within the same HEI's infrastructure. The model reveals that the electronic network is excessively large and administratively complex, as well as it covers the entire HEI's campus, and enables all infrastructure users to participate in the system management based on their access level. The viability of the HEI's entire network is regulated by national legal

frameworks and HEI's policy documents. The design of information security systems should consider the peculiarities and specifics of the HEI. Thus, the components of the information infrastructure include a physical communication network, switching devices, wireless access points, computers, servers, FireWall, and the Internet connectivity. To protect specific segments of the infrastructure, multi-layered managed switches (upon which firewalls are built) are deployed to secure HEI's information resources.

Particular attention is given to ensuring secure access to Internet. Therefore, all infrastructure elements are connected via hybrid wired and wireless switching network, allowing predefined resources to be accessible regardless of whether personnel are physically present at their workstations. Also, all HEI's resource servers are hosted internally within HEI's network and are operated and maintained by system administrators. Secure access to HEI's information resources is ensured through VPN configurations, which provide encrypted and authenticated connectivity to internal systems.

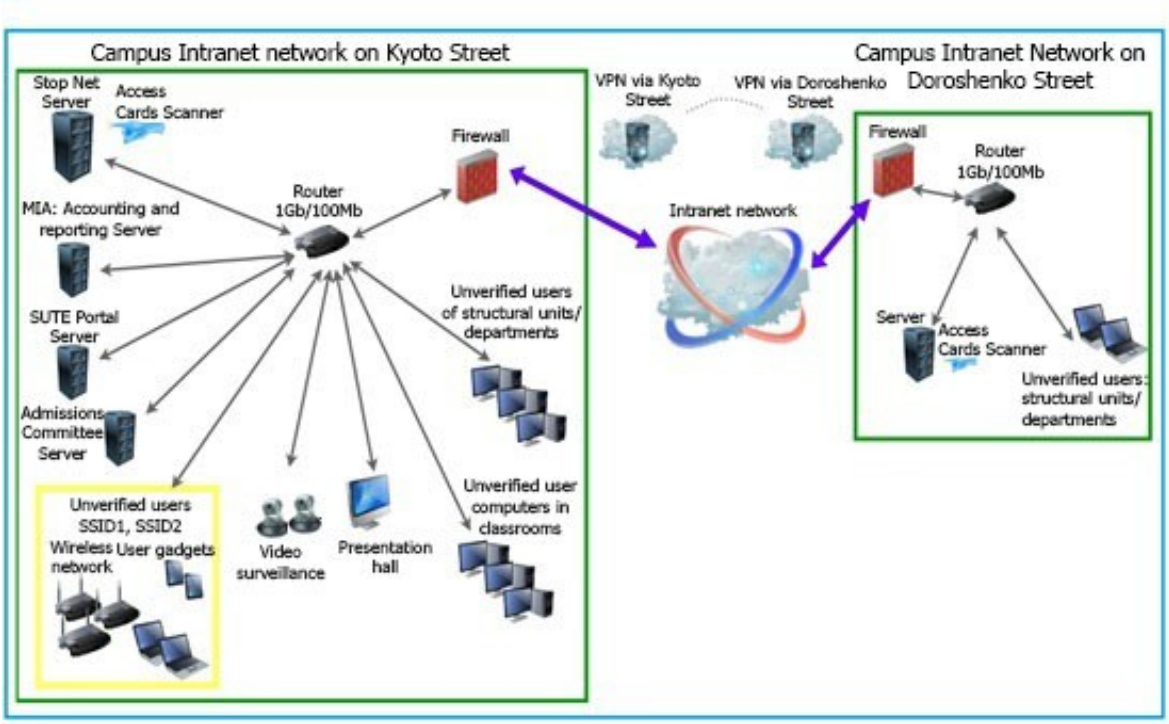

Figure 2: Model of HEI's information infrastructure (communication tools and resources), via Yaroslav Shestak [20]

It should be noted that the model in Figure 2 lacks clearly defined and structured mechanisms for managing the components of HEI's information infrastructure. In addition, Figure 2 illustrates a model of the resource protection system of HEI's information infrastructure.

Thus, the HEI employs a software-based protection model with resource load auditing for the HEI's information infrastructure. Its main and arguably only advantage is the ability to manage automated educational systems independently, manually, and with direct access. However, this advantage can also be considered the most significant disadvantage: the approach relies heavily on human resources with the expertise to administer different automated systems, who must coordinate efforts across various internal or external information automated systems. As a result, this infrastructure becomes costly and highly dependent on qualified IT specialists to maintain and manage all the HEI's automated systems. Thus, the management of the HEI's via information systems remains poorly automated and requires significant technical coordination. Moreover, building an effective cybersecurity system is challenging due to varying configurations and inconsistent access rights across different automated systems.

One of the main shortcomings of this approach is the fragmentation of information systems and database management mechanisms, which fail to provide comprehensive capabilities for data analysis or for adjusting resource access based on whenever a participant (e.g. (teacher or student) is on-site or accessing remotely. The administration of the HEI and its information resources is primarily conducted manually, with limited oversight due to weak feedback mechanisms. A large number of IT specialists with diverse competencies are required to ensure the administration of all components of HEI's information infrastructure. Access can be affected due to changes in the operation of managed switches and power outages, both of which can impact the performance of the entire HEI's information infrastructure. All devices (e.g. gadgets, laptops, and other wireless equipment and resources) are connected through switching mechanisms that provide constant network control and monitoring. For a comprehensive system map, all resource elements of the database infrastructure used by the information system must be analysed, revealing the vulnerability of HEI user databases. Effective coordination of information flows requires system interventions to support decision-making and resolve basic queries through interactive interfaces. Another significant issue is the lack of reliable data about individual users of HEI's systems [20–26].

5. Model of higher education institution information infrastructure: intelligent access, needs analytics and cybersecurity

All of the aforementioned shortcomings can be addressed by implementing an intelligent control centre for HEI's information infrastructure built on the basis of a central control hub that utilises neural network algorithms. The system of HEI's information infrastructure proposed herein incorporates an intelligent centre, which leverages neural networks to enable comprehensive and rapid analysis of the entire information infrastructure and offer optimised solutions to operational issues.

Figure 3 shows a model of the HEI's information infrastructure, illustrating the proposed use of an Intelligent Management Centre, based on the State University of Trade and Economics.

The proposed model for the operation of the HEI's information infrastructure envisions the implementation of controlled processes of information flow management and intelligent resource allocation in accordance with the current needs of users. Within this model, analytical assessments of resource demand are conducted, followed by their verification and conditional access provisioning. Resources in the wireless environment are divided into zones with controlled and guest access.

At the stage of user identification, a customised resource pool is generated via the access control system, tailored to the user's role and functional needs. If the user requires access to additional information systems, such access is provided without disrupting connection to the main environment.

Interaction between information systems is carried out by generating electronic requests processed by the Intelligent Management Centre that structures the relevant information for integration into other systems depending on current requests. The information infrastructure resources are allocated dynamically according to the level of workload and user demands, enabling flexible database management, the forecasting of peak loads and the implementation of optimisation techniques, such as data redistribution or compression.

The system also supports user authentication and subsequent provision of access to both local networks with assigned privilege levels and virtual networks or environments. In case of remote work, electronic digital keys can be used for secure connections. This approach ensures maximum efficiency in the utilisation of information resources under conditions of variable load on individual segments of the HEI's infrastructure.

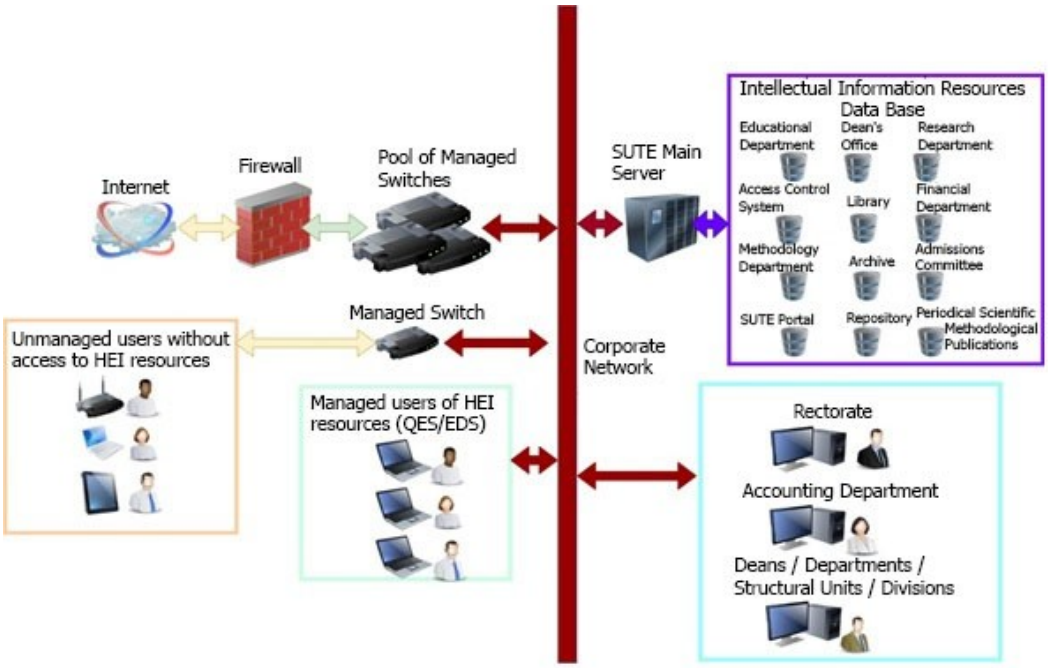

Figure 3: Model of HEI's information infrastructure (physical connections and changes in the switching architecture)

Figure 3 illustrates the communications, physical connections and architectural changes in the switching infrastructure resulting from the implementation of the Intelligent Management Centre that assumes full control over resource distribution, increases the efficiency of their utilisation, performs analytical data processing and generates recommendations for decision-making within HEI's information infrastructure.

A comparative analysis of the model in Figure 3 reveals significant qualitative improvements in the management of information flows, allocation of resources among different user categories and the functioning of the authentication system.

The Intelligent Management Centre performs a wide range of functions, including: predicting the outcomes of user authorisation, managing access to computing resources, databases, automated systems, optimising the load on the HEI's Internet resources, notifying of system failures, and detecting unauthorised access attempts. This approach enables rapid analysis of incidents and implementation of corrective measures by HEI's information infrastructure administrators.

The integration of the intelligent system into the structure of the HEI's information infrastructure ensures seamless interoperability with all automated subsystems and the cybersecurity mechanisms. Among its core functions is the management of user administrative rights, which allows assigning and regulating access types within various automated information systems based on a predefined user profile, with the possibility of future adjustments.

Moreover, an important component is the recording of the user's the physical presence. Scanning an access card through the access control system registers the individual's presence in the general system, which can be further confirmed by video surveillance by matching the user's face with a stored photo.

The system also provides for the possibility of using alternative biometric identification methods, such as voice recognition or fingerprint scanning. However, the implementation of such approaches requires significant financial resources and modernisation of the university's access control points, which is currently a limiting factor.

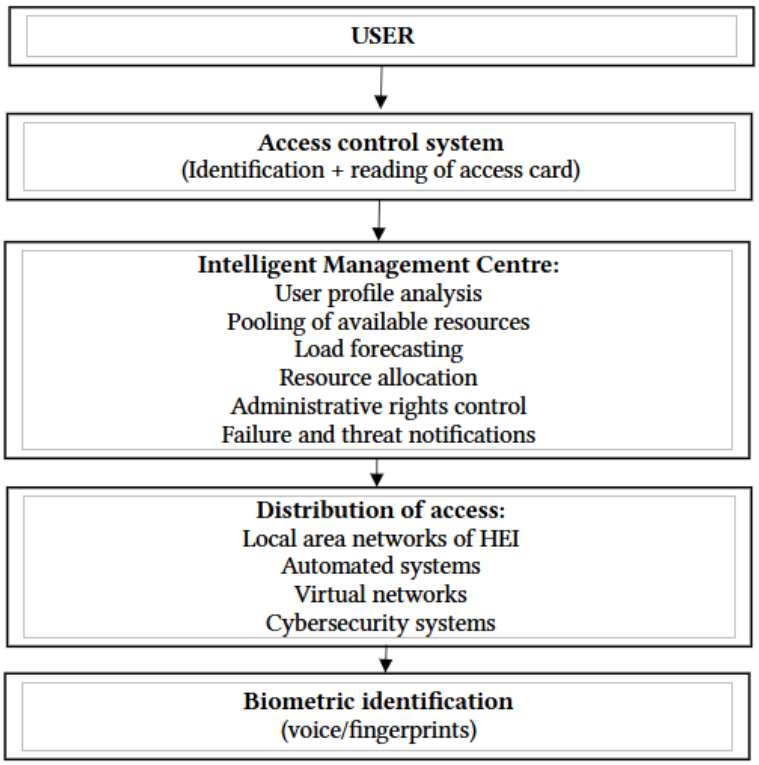

Figure 4: The scheme of interaction of an intelligent system in HEI's information infrastructure

After confirming the user's physical presence on campus, the intelligent system automatically provides them with access to all available resources based on the user's role and permission level. At the same time, the system is able to adapt to individual habits and needs: it can notify about new library acquisitions related to their research topics, changes in class schedules, workloads, and announcements of scientific events and meetings, as well as consider dietary preferences to optimise food preparation.

The proposed intelligent system can also automatically record the actual presence of employees at their workplace, transmitting this data to the financial and economic management systems. Users may receive reminders about upcoming changes in access rights, professional development training and other internal updates.

To ensure comprehensive cybersecurity, we recommend configure, adapt and implement SIEM systems that continuously collect, process and analyse security events, detect threats in real time, perform security analysis and management, and conduct incident investigations. Such systems are particularly valuable because they can be configured and adapted for the entire information infrastructure of HEI. In cases where cybersecurity experts are lacking, we recommend using a system that can also be operated by IT specialists who have undergone specific targeted training. These systems support automatic updates, utilize automated auditing of the HEI's information infrastructure, and enable event filtering, security breach detection, alerts, and real-time threat analysis and management. They also support receiving alerts in response to detected threats or predicted cyberattacks on institutional information resources.

Once the intelligent system completes user authentication, it ensures seamless access to required platforms and services without any additional actions on the part of the user. If necessary, administrators can modify the level of access individually or collectively, with mandatory confirmation of changes.

The cyber defence system performs the function of continuous security monitoring mechanism, promptly notifying the responsible personnel of any detected threats, attempts of unauthorised intrusions or attacks, and administrator actions taken to neutralise them, while also forecasting potential consequences. After the threats are neutralised, the system assesses the time required to

restore the stable operation of the HEI's information infrastructure, thereby ensuring the continuity of the educational process.

Upon verifying the user's physical presence on campus through authentication systems (e.g. biometric scanners, RFID tags or mobile applications), the intelligent system automatically activates a personalised access profile. This mechanism allows immediate use of the HEI's information resources—educational platforms, databases, administrative services, laboratories, libraries or canteens—according to the user's role (student, teacher, researcher, technician) and pre-assigned level of access rights.

The system performs contextual analysis of the user's previous actions, service interaction history, attendance at events, requests to the library or canteen menu, thereby allowing to predict needs and personalise the environment for each individual. For instance, the nutrition module can analyse user habits and optimise portion sizes, reducing food waste and costs. The educational module sends notifications about new library acquisitions according to the user's academic profile, and also notifies about changes in the schedule, cancelled sessions, available slots for consultations, upcoming scientific events, guest lectures, and scholarship opportunities.

The administrative module of the system provides automatic recording of employees' working hours in terms of physical presence, synchronizing this data with accounting and HR modules. Additionally, the system is capable of informing in advance about planned changes in access rights to resources, mandatory certifications, trainings or professional development events.

Automated access rights management provides a transparent and flexible governance model: when a user's status changes (for example, a student transfers to another mode of study or an employee is promoted), the administrator can promptly update the access profile at both the individual and group levels with instant confirmation of the changes.

A central component in the operation of the entire system is a cyber security suite, that performs round-the-clock monitoring of all nodes within the digital infrastructure. It is capable of detecting anomalies, blocking potential intrusions, logging suspicious activities, including administrator interference, and promptly inform the responsible personnel. The system automatically generates forecasts of the damage caused by attacks, provides recommendations for threat mitigation, estimates the timeframe for restoring the stable functioning of the HEI's information infrastructure (i.e., the information infrastructure of the State University of Trade and Economics) and ensures the uninterrupted continuity of the educational process even in emergency situations.

Conclusions

The integration of intelligent systems into the internal infrastructure of a higher education institution demonstrates significant potential for a qualitative transformation of all processes related to resource management, education, and user service. Through multi-level authentication, personalised access to services and systematic data collection, a dynamic digital environment is created that continuously adapts to the needs of each stakeholder in the educational process, whether a student, teacher or administrative employee.

The functionality of the system extends far beyond simple access to informational resources. It also performs predictive and analytical functions, including the study of user behavioural patterns to optimise resource utilisation (e.g., campus facilities or library services), automates routine administrative tasks (attendance tracking, payroll calculation), and improves institutional efficiency through centralised management of access rights.

A pivotal component of this infrastructure is the cybersecurity system, which not only ensures the confidentiality and integrity of data, but also provides the conditions for an uninterrupted educational process even in the face of cyber threats. Its ability to proactively respond, block intrusions and predict the consequences of attacks significantly improves the HEI's digital resilience. In addition, SIEM systems are adaptive and particularly useful for building effective cybersecurity framework within higher education institutions.

Overall, the deployment of such an intelligent system within the university environment not only meets the requirements of the digital transformation of education, but also lays the foundation for a secure, flexible and efficient educational space of the future, capable of responding to contemporary challenges with the maximum level of adaptability.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] Prus, Mathematical Modeling as a Lens of the Real World, Physical and Mathematical Education 38(4) (2023) 56–61. doi:10.31110/2413-1571-2023-038-4-008

[2] SOPHOS, The State of Ransomware 2025, 2025. https://www.sophos.com/en-us/content/state-of-ransomware

[3] BlueVoyant, Cybersecurity in Higher Education, 2025. https://www.bluevoyant.com/resources/cybersecurity-in-higher-education

[4] E. Zavhorodnya, Y. Shestak, O. Kryvoruchko, Digital Risk Management in Higher Education, in: Modern Achievements and Prospects of Socio-Economic Development, Proceedings of the 2nd Int. Sci. and Practical Conf., Eastern European Center for Scientific Research, 2025, 138–143.

[5] Y. Shestak, E. Zavhorodnya, Protection Principles of HEIs Information Infrastructure, in: Innovations and Their Impact on the Economy and Society, Proceedings of the Int. Sci. and Practical Conf., Eastern European Center for Scientific Research, Sumy, Ukraine, 2024, 138–143.

[6] O. Burov, et al., Cybersecurity in Educational Networks, Advances in Intelligent Systems and Computing, 359–364, 2020. doi:10.1007/978-3-030-39512-4_56

[7] V. Buriachok, et al., Implementation of Active Cybersecurity Education in Ukrainian Higher School, Information Technology for Education, Science, and Technics, vol. 178 (2023) 533–551. doi:10.1007/978-3-031-35467-0_32

[8] M. Astafieva, et al., Formation of High School Students' Resistance to Destructive Information Influences, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 87-96.

[9] V. Buriachok, V. Sokolov, Implementation of Active Learning in the Master's Program on Cybersecurity, Advances in Computer Science for Engineering and Education II, vol. 938 (2020) 610-624. doi:10.1007/978-3-030-16621-2_57

[10] A. A. A. El-Latif, Y. Maleh, M. A. El-Affendi, S. Ahmad, Cybersecurity Management in Education Technologies: Risks and Countermeasures for Advancements in E learning, 1st ed., CRC Press, Boca Raton, 2023. doi:10.1201/9781003369042

[11] L. Peng, Design of Smart Campus Security Management and Control Platform based on Big Data Technology, in: Educational Innovation and Multimedia Technology, Proceedings of the 2022 Int. Conf., EIMT 2022, Atlantis Press, Dordrecht, the Netherlands, 2022, 586–595. doi:10.2991/978-94-6463-012-1_65

[12] Q. Ni, Y. Zeng, Research on Smart Campus System Architecture Design and Data Security Protection Strategy, Frontiers in Computing and Intelligent Systems 11(3) (2025) 98–100. doi:10.54097/f6sy7t88

[13] S. M. Tahsien, H. Karimipour, P. Spachos, Machine Learning based Solutions for Security of Internet of Things (IoT): A Survey, J. Netw. Comput. Appl. 161 (2020). doi:10.1016/j.jnca.2020.102630

[14] V. Lakhno, V. Malyukov, O. Kryvoruchko, A. Desiatko, Y. Shestak, Smart City Technology Investment Solution Support System Accounting Multi-factories, Software Engineering Perspectives in Intelligent Systems 1 (2020) 1–11. doi:10.1007/978-3-030-63322-6_1

[15] T. Domínguez Bolaño, V. Barral, C. J. Escudero, J. A. García Naya, An IoT System for a Smart Campus: Challenges and Solutions Illustrated over Several Real World Use Cases, Internet of Things 25 (2024). doi:10.1016/j.iot.2024.101099

[16] Y. Li, Application of Big Data Technology in Campus Security Management under the Background of Information Age, J. Physics: Conf. Series 1881 (2021). doi:10.1088/1742-6596/1881/2/022097

[17] Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun, F. Taher, Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research, IEEE Access 10 (2022) 93104–93139. doi:10.1109/ACCESS.2022.3204051

[18] V. Lakhno, M. Lakhno, O. Kryvoruchko, S. Kaminskyi, V. Makaiev, Automation of DDoS Attack Investigation in Industrial Control Systems using Bayesian Networks on Python, in: Cybersecurity Providing in Information and Telecommunication Systems II, 3826, 2024, 282–287.

[19] O. Lytvynov, N. Filipenko, S. Lukashevych, K. Palkova, Cyber Security as a Factor of the Efficiency of Higher Education Institutions, Propylaeum of Law and Security 5 (2024) 15–23. doi:10.32620/pls.2024.5.02

[20] Y. Shestack, Modeling of a Single Information Space Higher Education Institution, Management of Development of Complex Systems 49 (2022) 81–89. doi:10.32347/2412-9933.2022.49.81-89

[21] O. Trofymenko, N. Loginova, S. Manakov, Y. Dubovoi, Cyberthreats in Higher Education, Electron. Professional Sci. J. Cybersecur. Educ. Sci. Tech. 4(16) (2022) 76–84. doi:10.28925/2663-4023.2022.16.7684

[22] A. Ilyenko, S. Ilyenko, O. Yakovenko, Y. Halych, V. Pavlenko, Prospects of Integration of Artificial Intelligence in Cybersecurity Systems, Electron. Professional Sci. J. Cybersecur. Educ. Sci. Tech. 1(25) (2024) 318–329. doi:10.28925/2663-4023.2024.25.318329

[23] T. F. Skumin, R. M. Stasyshyn, Intelektualna systema kiberzakhystu [Intelligent Cyber Defense System], in: Collection of Abstracts IV Int. Sci. Conf. of Young Scientists and Students "Actual tasks of modern technology", TNTU, Ternopil, Ukraine, 2015, 53–54.

[24] M. V. Kostikova, Modern educational process and cybersecurity, in: Materials of the All-Ukrainian Scientific and Practical Internet-Conf. Modelling and Information Technologies in Science, Technology, Cybersecurity and Education, KhNADU, Kharkiv, Ukraine, 2022, 57–59.

[25] S.O. Dotsenko, Cybersecurity of Participants in the Educational Process in the Context of Distance and Blended Learning, in: Proceeding of All-Ukrainian Scientific and Pedagogical Advanced Training Upravlinnia Naukovymy ta Osvitnimy Proiektamy, Helvetyka, Odesa, Ukraine, 2022, 120–123.

[26] D. Dets, A. Barduk, O. Syvolap, Cybersecurity in the Field of Open Access: Principles for Protecting Educational and Scientific Resources, Automation of Technological and Business Processes 17(1) (2025) 17–24. doi:10.15673/atbp.v17i1.3081