DOI: 10.32347/2412-9933.2026.65.194-203
UDC 004.94:378.4

Olena Kryvoruchko
ORCID: https://orcid.org/0000-0002-7661-9227
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
DSc (Eng.), Professor, Professor of the Department of Computer Systems, Networks and Cybersecurity
Yaroslav Shestak
ORCID: https://orcid.org/0000-0002-5102-9642
State University of Trade and Economics, Kyiv, Ukraine
Director of the Information and Computing Centre – the Main Centre for Information Technology,
PhD, Senior Lecturer, Department of Software Engineering and Cybersecurity
Oleh Kulinich
ORCID: https://orcid.org/0000-0002-0643-6898
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
PhD, Associate Professor, Associate Professor at the Department of Computer Systems, Networks and Cybersecurity
Elizaveta Zavhorodnya
ORCID: https://orcid.org/0000-0003-0549-7020
State University of Trade and Economics, Kyiv, Ukraine
Head of Library Department, PhD

Article history:
Received: 30.01.2026
Accepted: 12.02.2026
Published: 26.03.2026

INTELLECTUALIZATION OF INFORMATION FLOW MANAGEMENT AS A MEANS OF ENSURING THE CYBER RESILIENCE OF A HIGHER EDUCATION INSTITUTION'S INFRASTRUCTURE

Abstract. *At present, higher education institutions (HEIs) employ a model of software-based protection and resource load auditing, the key feature of which is the ability to independently manage automated educational systems in manual mode with direct access. At the same time, this advantage actually turns into a significant disadvantage, since the operation of such a model requires considerable human resources. It necessitates the availability of specialists responsible for administering individual automated systems, as well as coordinating their operation with other internal and external information systems. This article is devoted to studying approaches to the intellectualisation of information flow management within HEI's infrastructure from the perspective of ensuring their cyber resilience. The growth in volumes of asynchronous and unstructured data, the increasing complexity of information system architectures, and the widespread adoption of blended and distance learning formats significantly increase the load on the information infrastructure environment of higher education institutions and highlight the need for adaptive management mechanisms. The limitations of conventional administration and monitoring systems are examined, as these systems predominantly focus on controlling individual resources and do not provide comprehensive analysis of infrastructure states and proactive responses to dynamic changes in environmental parameters. In this context, the feasibility of employing an intelligent management centre as an integration layer capable of ensuring coordinated interaction among heterogeneous components of the information infrastructure is substantiated. The methodological framework of the study is a combination of systems analysis of the HEI information infrastructure, a neural network-based approach to processing asynchronous and unstructured data, and modelling of the prospective infrastructure development based on the concept of the target current state. This approach creates the prerequisites for a transition from fragmented resource management to intelligent analysis of information flows and the formation of adaptive management decisions, taking into account the contextual parameters of the educational institution's operation. The proposed concept of intelligent management contributes to increasing the level of automation of management processes, optimising the use of information resources, and strengthening the cyber resilience of HEI infrastructure in the context of escalating digital threats and dynamic transformation of the educational environment.*

Keywords: information system; intelligent management centre; information flows; information infrastructure of HEI; neural network-based approach; support system for managerial decisions; intelligent interaction centre; UML diagrams; resource management; digital transformation of education

Introduction

The current stage of development of higher education institutions (HEIs) is characterised by rapid increase in information flows, growing complexity of information infrastructure architectures, and higher requirements for its cyber resilience. The digitalisation of educational, managerial and scientific processes necessitates a transition from fragmented automated solutions to integrated intelligent management systems capable of providing continuous monitoring, analysis and adaptive resource management under conditions of dynamic cybersecurity threats.

A distinctive feature of the information infrastructure environment of HEIs is the combination of heterogeneous hardware and software components, a multiplicity of users with different access levels, and a variable format of the educational process (full-time, distance and blended learning). Under such conditions, traditional approaches to information flow management and cyber security prove insufficiently effective, as they do not provide centralised data analysis, prompt incident response and system status forecasting.

In this context, the task of intellectualising information flow management as a means of improving the cyber resilience of HEI's infrastructure becomes increasingly relevant. The use of artificial intelligence methods, especially neural network models, opens up opportunities for automated processing of large volumes of unstructured data, identification of hidden dependencies in the operation of network components, and generation of well-founded managerial decisions in real time.

The aim of the study is to substantiate the feasibility of establishing an intelligent centre for information flow management in HEIs and to develop an approach to its operation as a key element in ensuring the cyber resilience of the information infrastructure. Achieving this aim involves analysing the current state of HEI's information systems, identifying their functional limitations, and modelling a target infrastructure state, taking into account security, adaptability, and management efficiency requirements.

Literature review

The issues of digital transformation of HEI infrastructure and the implementation of intelligent traffic management systems are the focus of attention for many Ukrainian scholars. The theoretical foundations for the development of a modern information and educational environment and cloud-oriented systems in HEIs are presented in the works of V. Yu. Bykov and S. Y. Hohonyants et al. [1; 2]. At the same time, the technical aspects of intelligent resource management and flow optimisation in distributed networks have been studied in detail in the works of O. Y. Sova et al. and O. Kolomiitsev et al., who propose mathematical models of adaptive routing and quality of service assurance [3; 4].

However, despite significant achievements, the issue of integrating these two areas within a single intelligent interaction centre capable of synchronising asynchronous data from all components of the HEI infrastructure remains insufficiently studied. The scientific novelty of this article lies in the development of an algorithm for the operation of an intelligent interaction centre which, unlike existing solutions, provides comprehensive processing of unstructured data and the generation of adaptive recommendations for participants in the educational process based on neural network modelling of interactions among network components.

Research methods

The study employs a set of general scientific and specialised methods aimed at analysing, modelling and substantiating the intellectualisation of information flow management in HEI's information infrastructure.

System analysis methods were used to assess the current state of HEI's information infrastructure, identify its structural components, information interconnections and functional limitations that affect the level of cyber resilience. This made it possible to identify key vulnerabilities in existing approaches to resource management and user access control.

A neural network-based approach was applied to develop an intelligent management centre, which ensures the implementation of tasks for classifying the states of network components, predicting changes in information flow parameters, and supporting management decision-making under conditions of uncertainty and dynamic changes in system characteristics. The use of neural network models allows for the consideration of unstructured and asynchronous data received from various elements of the HEI infrastructure.

The modelling of the information infrastructure operation was carried out based on the concept of the target current state, which made it possible to substantiate the feasibility of implementing an intelligent management centre and assess its impact on the level of automation of management processes, the efficiency of information resource utilisation, and the improvement of cyber security of the HEI.

Results

The management of HEI activities using information systems remains insufficiently automated and requires a significant amount of technical coordination. Additional difficulties arise in the development of a comprehensive cyber security system, due to different configurations, access settings and actual user privileges across individual automated systems.

The disadvantages of such solutions include the use of heterogeneous database management systems and automated system administration mechanisms, which do

not provide the possibility of centralised data analysis and flexible adjustment of access to resources depending on the physical or remote presence of participants in the educational process (academic staff and higher education students). Information resources are managed mainly in manual mode, which complicates the control of the implementation of management decisions due to limited and complex feedback. In particular, the functioning of the information environment of the HEI infrastructure requires the involvement of a considerable number of IT professionals with different competencies to administer all its components [6].

At the same time, access to resources may change due to malfunctions in managed switches or power outages, which negatively affects the stability of the institution as a whole. The connection of gadgets, laptops, and other wireless equipment is performed using switching devices that ensure constant control and monitoring of the network status.

Fig. 1 presents the set of information resources of the database infrastructure used in the system, clearly demonstrating the insufficient level of security of the databases with which users of the HEI information infrastructure interact. Under such conditions, coordination of information flows requires direct intervention in system operation in order to formulate proposals for management decisions and solve typical tasks in a interactive mode. An additional drawback is the lack of information regarding the actual physical presence of users in the HEI information infrastructure system.

These shortcomings can be eliminated through the implementation of an intelligent management centre for the HEI's information infrastructure, built on the basis on a neural network-based approach. The proposed system provides for the existence of an intelligent interaction centre, which uses neural network algorithms to analyse the state of the infrastructure, formulate recommendations for decision-making, and generate tasks in accordance with the current operating conditions of the system.

Fig. 2 illustrates a model of the information infrastructure using the example of the State University of Trade and Economics (SUTE) in its target state after the proposed changes, in which the use of an intelligent management centre is implemented as a key element of the management system [7].

The proposed intelligent management centre differs fundamentally from traditional monitoring and administering systems of HEI information infrastructure. Unlike conventional solutions, which primarily perform functions of data collection, visualisation and resource status notification, the intelligent interaction centre implements functions of analysis, forecasting and managerial decision support in semi-automated and automated modes.

A key component of the proposed approach is the use of neural network algorithms that classify the states of the information infrastructure, detect anomalies in the operation of databases and network resources, as well as forecast loads and possible failures. Based on the analysis results, the intelligent interaction centre generates recommendations regarding the optimal resource distribution, adjustment of user access rights and response to potential cyber threats.

A distinctive feature of the proposed system is its ability to take into account contextual information, including the physical or remote presence of participants in the educational process, which enables dynamic adaptation of access policies and enhances cybersecurity of the HEI information infrastructure. Thus, the intelligent management centre performs not only control functions, but also acts as a tool for intelligent support of management decisions, which determines its scientific novelty and practical significance.

Fig. 2 presents a model of the HEI information infrastructure with controlled data flow management processes and intelligent resource allocation according to current user needs. The proposed model provides the ability to analyse the need for information and network resources, verify access rights and grant them on request, as well as differentiate access in a wireless network into controlled and guest segments.

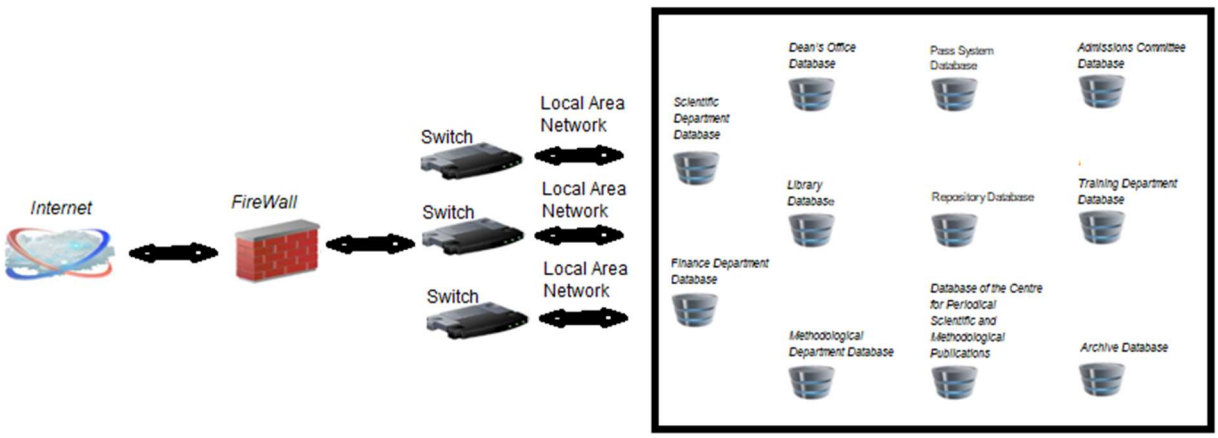

Figure 1 – Model of HEI's information infrastructure (current cybersecurity systems for protecting information resources) Source: developed by authors

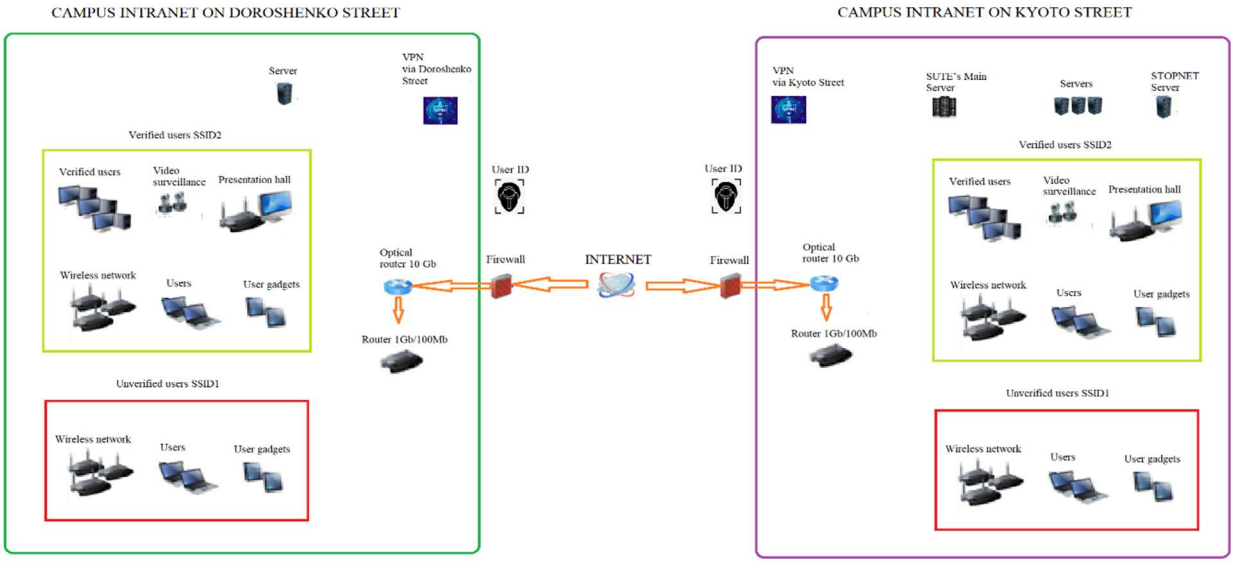

Figure 2 – Model of HEI's information infrastructure after changes (system of electronic communication networks, means of communication, access to information resources using an intelligent management centre, based on the example of SUTE)

At the user identification stage within the access control system, an individual pool of available resources is formed in order to ensure its uninterrupted and convenient operation. If interaction with other information systems is required, the corresponding access rights are granted without interrupting the user's session in the current environment. To ensure integration between information systems, electronic communication requests are generated, and the intelligent management centre produces a data structure adapted to the requirements of a specific consumer system.

Information infrastructure resources are distributed according to the actual user needs, while the flexibility of the proposed system allows adjusting the database load, forecasting peak loads, and generating recommendations for their redistribution or optimisation. Support is provided for authentication and operation both within local networks with defined access to resources and within virtual networks using specialised electronic digital keys for remote work [9].

Fig. 3 illustrates the physical connections and switching changes resulting from the implementation of the intelligent management centre. The proposed centre provides complete control over resource allocation, increases the efficiency of resource use, analyses the state of the infrastructure and generates recommendations for management decisions using artificial intelligence tools.

Analysis of the models presented in Fig. 2 and Fig. 3 indicates a significant improvement in the management of information flows and resources for different categories of users. The intelligent management centre implements authentication, assessment of the consequences of user authorisation, forecasting of system usage scenarios and the corresponding optimal allocation of resources, including computing capacity, databases, access to automated systems and HEI's Internet resources. In addition, the intelligent management centre monitors failures in the operation of automated systems, detects unauthorised access attempts, and initiates corrective actions by information infrastructure administrators.

To increase the level of management automation, it is proposed to include an intelligent management centre in the information infrastructure of the SUTE, which interacts with all automated systems and cybersecurity subsystems. The functions of the intelligent management centre include centralised control of user administrative rights based on a description of standard access profiles, enabling automation of the processes of granting, modifying or revoking access rights in various information systems.

An important element of the intelligent management centre operation is the detection of a user's physical presence on the campus through access cards reading by the access control system, with the possibility of additional verification using video surveillance systems. The potential use of biometric identification methods, in particular voice or fingerprint recognition, is also considered; however, their implementation requires additional financial costs and modernisation of the access control infrastructure.

After confirming the user's physical presence, the intelligent management centre ensures the provisions of the full range of resources according to user's category and access level. In addition, the intelligent management centre can analyse the individual needs and behavioural characteristics of users to create personalised services, including information about new library acquisitions by research profile, changes in class schedules, planned scientific events, as well as automated recording of on-site attendance for financial, economic and human resources management purposes.

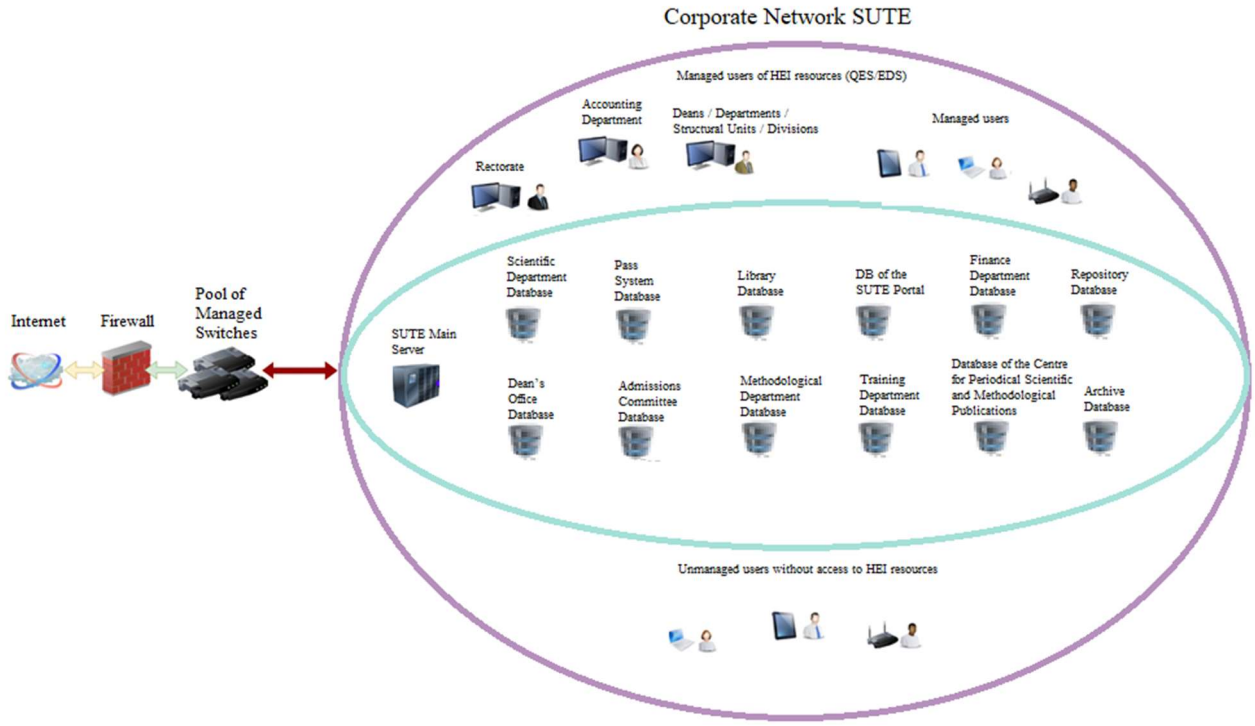

Figure 3 – Model of the information infrastructure of higher education institutions after changes (systems and mechanisms for protecting information resources using an intelligent management centre, based on the example of SUTE)
Source: developed by authors

The primary tasks of the intelligent interaction centre for information components of the HEI's infrastructure are the coordination and harmonisation of information flows from all HEI subsystems in order to form a coherent relationship among them in accordance with the Concept of a Unified Harmonious Open Digital Space of the HEI. The implementation of this approach ensures effective management of educational activities and the educational process both within the institution as a whole and at the level of its structural units (institutes, faculties and departments), personalisation of access to information resources, taking into account the mobility of participants in the educational and scientific environment, as well as the adaptability of educational information flows to individual user needs.

Within the proposed intelligent management centre, the neural network module processes a set of input parameters, including data on server and network load, databases states, user activity, access parameters, as well as information about the physical or remote presence of participants in HEI's information infrastructure.

Based on the analysis of the input data, the neural network classifies the current state of the information infrastructure, identifies anomalous operating modes, and generates forecasts of potential overloads or failures. The output parameters of the neural network module are recommendations for optimal resource allocation, adjustment of access policies, initiation of protective mechanisms, and generation of tasks for administrative personnel or automated subsystems.

These goals are achieved through the implementation of modern information technologies and the corresponding material and technical base, which includes software and hardware, global, local and corporate computer networks, advanced communication facilities, as well as hardware and software mechanisms for protecting the components of the HEI's information infrastructure.

Information flows received by the intelligent interaction centre from various subsystems of the HEI's infrastructure are represented by both structured and unstructured data. These data are processed using data analysis algorithms, logical inference methods and intelligent information processing techniques, resulting in personalised recommendations for users with the possibility of subsequent monitoring of their implementation, in particular in cases involving the execution of management decisions and administrative documents of HEI leadership.

The functional capabilities of the intelligent interaction centre include the provision of personalised information and analytical services, such as automated selection of scientific literature according to professional orientation; information about new arrivals of professional journals, articles and materials from scientific conferences; display of the spatial structure of the university campus with geolocation of educational buildings and classes; access to the electronic resources of the SMART library and management of their ordering and reservation; checking scientific and educational

materials for textual borrowings and plagiarism; displaying the class schedule for the current period and semester; supporting electronic document management; displaying individual academic and teaching workloads; as well as access to information on academic groups according to the user's access rights.

The combination of these functional capabilities forms HEI's information infrastructure as a single harmonised open digital space, adapted to the individual needs of participants in the educational and scientific process through personalised access to information resources and analytical flows. This ensures the harmonisation of the educational and scientific environment in accordance with the professional and educational orientation of each participant in the HEI.

The intelligent interaction centre for the components of HEI's information infrastructure is implemented in the form of a neural network-based system designed to coordinate and manage information flows in the educational space in order to improve the efficiency of the organisation and harmonisation of the educational process and educational activities.

In designing the architecture of the intelligent interaction centre, a modular principle of system design was employed, which increases the level of portability, scalability and mobility of its components. The use of a modular structure allows for the replacement or modernisation of individual components without disrupting the overall architecture of the system and inter-module interaction mechanisms.

The main modules of the intelligent interaction centre include:

– a remote management, monitoring and neural network training process configuration module;

– a training environment module which, in addition to supporting the training of neural networks with variable topology for specific applied tasks, serves as a demonstrative example of such environments and is characterised by structured documentation and clear source code;

– a tool for server-side execution of modelling and training processes for neural networks with variable topology;

– a network security module that ensures cybersecurity of local and wireless networks of HEI and plays a key role in protecting neural network server resources and end-user devices from unauthorised interference;

– interaction modules integrated into the core functional components of the system.

As an instrumental tool for server-side execution of machine learning processes, the use of the *nlab* library, implemented in the C++ programming language is proposed. This library provides the mathematical framework for constructing neural networks with variable topology, as well as interaction protocols with management modules and the training environment.

To ensure the correct operation of the neural network core, it is necessary to define a set of attributes and training parameters that correspond to the selected type of neural network and the specifics of the applied tasks related to management of HEI's information infrastructure. The selection of training parameters is carried out with due regard to the features of the mathematical framework of the *nlab* library and the requirements for accuracy, adaptability and stability of the intelligent interaction centre.

All components of the developed system, including the *nlab* library, management and monitoring tools, and the neural network training environment, operate in close interaction with one another. The *nlab* library defines the basic protocols and interfaces for intercomponent communication. The JSON-RPC protocol, which operates on top of the TCP transport protocol, is used to implement management influences. Interaction between the library and the training environment is carried out using TCP protocols or Windows operating system named pipes, which is due to the specifics of the software platform.

UML deployment diagrams were used to describe the architecture and visualise the placement of hardware and software components of the intelligent interaction centre of HEI's information infrastructure. This type of diagram enables representation of the physical level of the system, including computing nodes, software modules, communication channels between them, and the deployment of software artefacts on hardware resources.

The use of deployment diagrams facilitates modelling of the system's software and hardware topology and provides a clear representation of the physical-level interrelationships among its components, which is essential for analysing the scalability, reliability, and cyber security of the intelligent interaction centre. At the same time, only the part of the hardware infrastructure that is directly or indirectly involved in the operation of the system software is modelled.

Based on the defined requirements and architectural solutions, a structural deployment diagram was developed to represent the software and hardware topology of the intelligent interaction centre of the information infrastructure blocks of HEI (Fig. 4).

Fig. 4 shows the structural diagram of the software and hardware topology of the intelligent interaction centre of HEI's information infrastructure blocks, which reflects the deployment of the system's core components and the mechanisms of their interaction.

The central element of the diagram is a neural network server, which includes a data centre and a neural network learning centre [8]. Within the learning centre, machine learning processes are implemented using supervised and unsupervised methods, which allows for

both training on labelled data sets and automatic classification and generalisation of input information. The neural network training process is iterative and includes stages of forward signal propagation and backward error propagation in order to minimise the deviation between predicted and actual outcomes.

The training environment can be deployed either on a dedicated computing device or jointly with a training server, thereby enhancing training performance. The *nlab* library, implemented in the C++ programming language, is used as a tool for server-based machine learning. It provides the mathematical framework for constructing neural networks with variable topology and supports interaction protocols with management modules and the training environment.

To implement the mathematical apparatus of learning, the TWEANNs (Topology and Weight Evolving Artificial Neural Networks) software module is used. This module performs the evolution of both the topology and the weights of the neural network using fitness functions that determine the optimality of the obtained solutions. Specific fitness functions are defined in accordance with the characteristics of the training environment, in particular *traffic_env* [11].

Interaction between the *nlab* library, the training environment, and management tools is implemented using the JSON-RPC protocol over TCP, as well as through Windows operating system pipes. System components can be managed both in local and remote modes. The modular architecture of the system ensures scalability and enables the reuse of individual interaction components.

The administrative part of the system is deployed on a separate computing device and provides management, monitoring, and configuration of the intelligent interaction centre. The training server can be deployed either on a single physical device or as a clustered solution using operating systems from the Windows, Linux, or macOS families. The client-side component of the system operates on individual user devices according to their access level and may be implemented on desktop computers, laptops, tablets, mobile devices, and other wireless gadgets [11].

A dedicated security module constitutes a separate component of the system that protects software and hardware resources by controlling applications installation, verifying digital signatures, using sandboxing technology, restricting access to critical system resources, and verifying DRM licences. This module contributes to increasing the level of cyber security of the intelligent interaction centre and the entire information infrastructure of the HEI [10].

To describe the dynamics of system component interaction, a UML activity diagram of the ‘system launch’ subprocess is used, which reflects the sequence of key operations and the control flows between the modules of the intelligent interaction centre.

Fig. 5 shows the algorithm for launching the intelligent interaction centre of the higher education institution’s information infrastructure blocks.

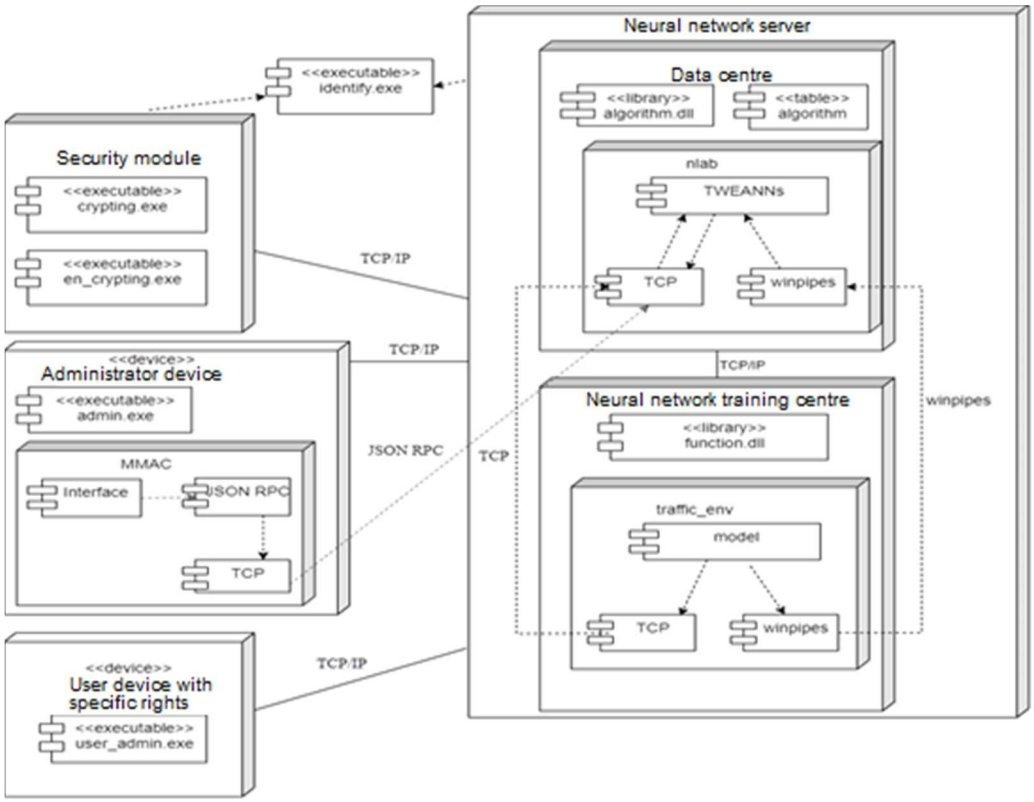

Figure 4 – Model of the software and hardware topology of the intelligent interaction centre of HEI’s information infrastructure blocks Source: developed by authors

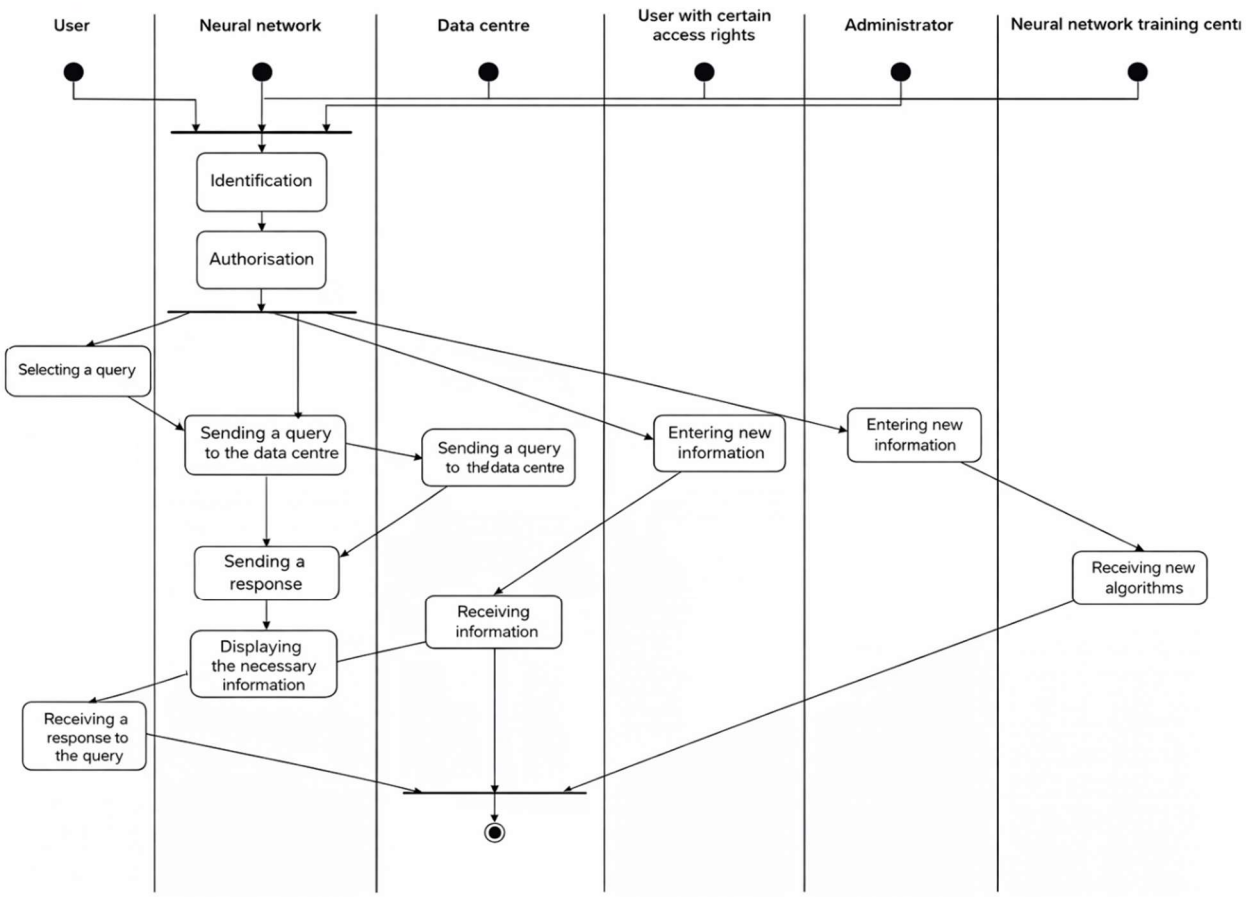

Figure 5 – Algorithm for the functioning of the intelligent interaction centre of HEI's information infrastructure blocks. Source: developed by authors

The initial stage of the centre's operation involves mandatory user identification and authorisation (administrator or staff members with the appropriate access rights) [5; 11]. The subsequent algorithm encompasses the stages of neural network training, as well as mechanisms for managing information flows between individual elements of the HEI's information infrastructure. The final result is the complete synchronisation of all environment components with the intelligent interaction centre. Such a system ensures the transformation of incoming asynchronous and unstructured data into systematised, structured information and provides expert recommendations aimed at optimising the educational process for all participants within the information space of the HEI's information infrastructure.

Conclusions

The study proposes and scientifically substantiates an algorithm for the operation of an intelligent interaction centre for the components of the information infrastructure of a higher education institution, aimed at improving the efficiency of information flow management and ensuring the cyber resilience of the infrastructure. It is demonstrated that the use of a neural network-based approach to the processing of asynchronous and unstructured data allows synchronising interactions among disparate subsystems of the HEI information space and transforming input data into actionable recommendations to support management decisions.

In contrast to conventional monitoring and administration systems, the proposed approach offers not only control over the current state of information resources, but also intelligent support for management decision-making by classifying infrastructure states, forecasting loads, and adaptively adjusting user access to information resources with due consideration of contextual parameters, in particular, the physical or remote presence of participants in the educational process.

The implementation of an intelligent management centre is regarded as a key stage in the digital transformation of higher education institutions, ensuring the transition from fragmented data accumulation to intelligent analysis and proactive resource management. The proposed approach establishes the prerequisites for increasing the level of management processes automation, improving the efficiency of information infrastructure use, and strengthening the cyber security of higher education institutions in the context of growing digital threats.

Prospects for further research

Future research prospects in this area are related to the development and refinement of the proposed approach to the intellectualisation of information flow management in higher education institutions. In particular, it is advisable to further detail the architecture of the neural network modules of the intelligent interaction centre and conduct simulation modelling to evaluate the performance and stability of the proposed algorithm under peak network loads conditions.

The next stage of research involves practical testing of the developed intelligent interaction centre in the real conditions of a higher education institution, as well as expanding its functional capabilities, particularly in terms of automated formation of individual educational trajectories based on the analysis of large volumes of asynchronous and unstructured data.

In future research, we plan to focus on integrating the proposed algorithm with existing cyber protection systems at higher education institutions, which will increase the resilience of the intelligent interaction centre to external destructive influences, unauthorised access, and threats to the integrity of information processing.

Conflict of Interest. The authors confirm that there are no financial, personal, or other interests that could be considered a potential conflict of interest regarding the publication of this article.

Funding. The research was conducted without financial support.

Data Availability. All data are available in digital or graphical form within the main text of the manuscript.

Use of Artificial Intelligence. The authors confirm that no artificial intelligence tools were used in the creation of this work.

References

1. Bykov, V. Yu. (2019). Digital transformation of society and development of a computer technology platform for education and science in Ukraine. *Information and Digital Educational Space of Ukraine: Transformational Processes and Development Prospects*, 21–27. URL: https://lib.iitta.gov.ua/id/eprint/718707/6/Збірник%202019.pdf

2. Hohonyants, S. Y., Klochko, A. O., Salash, O. A., & Rudenko, Y. G. (2020). Structure of the information and educational environment in the distance learning system. *Telecommunication and Information Technologies*, 69 (2). https://doi.org/10.31673/2412-4338.2020.025245

3. Sova, O. Y., Romanuk, V. A., Zhuk, P. V., & Umanets, Y. L. (2012). Methodology of Intellectual Control Systems Synthesis for Perspective Mobile Radio Networks with Dynamic Topology. *Scientific Works of Kharkiv National Air Force University*, 4 (33), 112–116. URL: https://journal.viti.edu.ua/public/romanuk/2012/7_2012.pdf

4. Kolomiitsev, O., Bulba, S., Nosko, S., Lytovchenko, D., Slobodeniuk, Yu., Kobets, Yu., & Shabanov, D. (2025). Adaptive Mathematical Model of the Graph of Request Routing in Side Car Components. *Grail of Science*, 57, 532–551. https://doi.org/10.36074/grail-of-science.17.10.2025.057

5. Kryvoruchko, O., Kostiuk, M., & Tsiutsiura, M. (2017). Architectural Solution of Time Management System in Test Driven Development Approach. *International Journal of Science and Research (IJSR)*, 6 (6), 1217–1219. URL: https://www.ijsr.net/archive/v6i6/ART20174430.pdf

6. Tsiutsiura, M. I., Kryvoruchko, O. V., & Tsiutsiura, S. V. (2020). *Divergent methodology for harmonising decisions in the management of higher education institutions*. Sole Proprietor Yamchynskyi O. V.

7. Shestack, Y. (2022). Modeling of A Single Information Space Higher Education Institution. *Management of Development of Complex Systems*, 49, 81–89. https://doi.org/10.32347/2412-9933.2022.49.81-89

8. Toliupa, S., Lukova-Chuiko, N., Nakonechnyi, V., Saiko, V., & Kulinich, O. (2020). Formation of a Strategy for Managing the Operating Modes of Security Systems Based on the Game Control Model. *Information Systems and Technologies Security*, 1 (3-4), 37–46. https://doi.org/10.17721/ists.2020.4.38-47

9. Shestack, Y. (2023). Case technologies in information design infrastructure of the institution of higher education. *Management of Development of Complex Systems*, 55, 141–157. https://doi.org/10.32347/2412-9933.2023.55.141-157

10. Shestack, Y., & Zavhorodnya, E. (2025). Ensuring cybersecurity in a trading company: challenges, standards and solutions. *Marketing of the Future: Challenges and Realities*, 55–59. URL: https://duikt.edu.ua/uploads/p_2779_55525382.pdf

11. Biloshchytskyi, A., Omirbayev, S., Mukhatayev, A., Kuchanskyi, O., Biloshchytska, S., Andrashko, Y., Toxanov, S., & Faizullin, A. (2023). A structural model for building a system for the development of methodological competence and methods for evaluating its effectiveness. *Eastern-European Journal of Enterprise Technologies*, 5 (3 (125)), 6–22. https://doi.org/10.15587/1729-4061.2023.289045

12. Cabinet of Ministers of Ukraine. (2025). *On approval of the Procedure for assessing the state of cyber protection of information, electronic communication and information and communication systems, critical infrastructure facilities, critical information infrastructure facilities* (Resolution № 1799). URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-poriadku-otsiniuvannia-stanu-kiberzakhystu-informatsiinykh-s1799311225

13. Kryvoruchko, O., Kulynich, O. M., Shestack, Y., & Zavhorodnya, E. (2026). Conceptual approaches to creating a sustainable information infrastructure for higher education institutions. *Science, Technology and Global Challenges*, 166–173. URL: https://sci-conf.com.ua/wp-content/uploads/2026/01/SCIENCE-TECHNOLOGY-AND-GLOBAL-CHALLENGES-11-13.01.26.pdf

Криворучко Олена Володимирівна
ORCID: https://orcid.org/0000-0002-7661-9227
Національний університет біоресурсів і природокористування України, Київ, Україна
Доктор технічних наук, професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки
Шестак Ярослав Іванович
ORCID: https://orcid.org/0000-0002-5102-9642
Державний торговельно-економічний університет, Київ, Україна
Директор Інформаційно-обчислювального центру – головного центру інформаційних технологій, PhD, старший викладач кафедри інженерії програмного забезпечення та кібербезпеки
Кулініч Олег Миколайович
ORCID: https://orcid.org/0000-0002-0643-6898
Національний університет біоресурсів і природокористування України, Київ, Україна
Кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки
Завгородня Єлизавета Олександрівна
ORCID: https://orcid.org/0000-0003-0549-7020
Державний торговельно-економічний університет, Київ, Україна
Завідувач відділу бібліотеки, PhD

ІНТЕЛЕКТУАЛІЗАЦІЯ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ ІНФРАСТРУКТУРИ ЗАКЛАДУ ВИЩОЇ ОСВІТИ

Анотація. *На сьогодні у закладах вищої освіти (ЗВО) використовується модель програмного захисту та аудиту навантаження ресурсів, ключовою особливістю якої є можливість самостійного керування автоматизованими освітніми системами в ручному режимі з прямим доступом. Водночас ця перевага фактично перетворюється на суттєвий недолік, оскільки функціонування такої моделі потребує значних людських ресурсів. Це зумовлює необхідність наявності фахівців, відповідальних за адміністрування окремих автоматизованих систем, а також координацію їхньої роботи з іншими внутрішніми та зовнішніми інформаційними системами. Дана стаття присвячена дослідженню підходів до інтелектуалізації управління інформаційними потоками в інфраструктурі ЗВО з позиції забезпечення їхньої кіберстійкості. Зростання обсягів асинхронних та неструктурованих даних, ускладнення архітектури інформаційних систем та широке впровадження змішаного та дистанційного форматів навчання значно збільшують навантаження на інформаційне інфраструктурне середовище закладів вищої освіти та підкреслюють потребу в адаптивних механізмах управління. Розглянуто обмеження традиційних систем адміністрування та моніторингу, оскільки ці системи переважно зосереджені на контролі окремих ресурсів і не забезпечують комплексного аналізу стану інфраструктури та проактивного реагування на динамічні зміни параметрів середовища. У цьому контексті обґрунтовано доцільність використання інтелектуального центру управління як інтеграційного рівня, здатного забезпечити узгоджену взаємодію між гетерогенними компонентами інформаційної інфраструктури. Методологічною основою дослідження є поєднання системного аналізу інформаційної інфраструктури ЗВО, підходу на основі нейронних мереж для обробки асинхронних та неструктурованих даних, а також моделювання перспективного розвитку інфраструктури на основі концепції цільового поточного стану. Такий підхід створює передумови для переходу від фрагментарного управління ресурсами до інтелектуального аналізу інформаційних потоків та формування адаптивних управлінських рішень з урахуванням контекстуальних параметрів функціонування освітнього закладу. Запропонована концепція інтелектуального управління сприяє підвищенню рівня автоматизації управлінських процесів, оптимізації використання інформаційних ресурсів та зміцненню кіберстійкості інфраструктури ЗВО в умовах ескалації цифрових загроз та динамічної трансформації освітнього середовища.*

Ключові слова: інформаційна система; інтелектуальний центр управління; інформаційні потоки; інформаційна інфраструктура ЗВО; підхід на основі нейронних мереж; система підтримки управлінських рішень; інтелектуальний центр взаємодії; UML-діаграми; управління ресурсами; цифрова трансформація освіти

Link to publication

APA Kryvoruchko O., Shestack Y., Kulinich O., & Zavhorodnia E. (2026). Intellectualization of information flow management as a means of ensuring cyber resilience of higher education institution infrastructure. *Management of Development of Complex Systems*, 65, 194–203, dx.doi.org\10.32347/2412-9933.2026.65.194-203.

ДСТУ Криворучко О. В., Шестак Я. І., Кулініч О. М., Завгородня Є. О. Інтелектуалізація управління інформаційними потоками як засіб забезпечення кіберстійкості інфраструктури закладу вищої освіти. *Управління розвитком складних систем.* Київ, 2026. № 65. С. 194 – 203, dx.doi.org\10.32347/2412-9933.2026.65.194-203.