*Черкасова В. В.
Харківський національний університет
міського господарства ім. О. М. Бекетова,
м. Харків, Харківська область, Україна*

ASSESSING SUSTAINABILITY OF EDUCATIONAL INFORMATION INFRASTRUCTURE

**Abstract**. Urban information infrastructure is an important element of ensuring the quality of the educational process, as modern educational systems depend on its stable functioning. In the context of growing external threats, such as cyberattacks, man-made disasters and power outages, the assessment of its resilience is of particular importance. The abstracts present an approach to assessing the resilience of the information infrastructure of educational institutions and practical recommendations for improving it, including backup, cloud computing, and the development of continuity plans.

**Keywords**: Information infrastructure resilience, cybersecurity in education, risk-based approach, cloud technologies, educational systems, Internet of Things (IoT).

**Introduction.** Education is one of the most important components of a modern city. The effectiveness of the educational process in educational institutions directly depends on the stable functioning of the digital infrastructure. Under the influence of growing external threats such as pandemics, war, a destroyed power grid, and resulting power outages, the stable operation of information systems significantly affects the quality of educational processes.

In this regard, there is an urgent need to study the resilience of the information infrastructure of educational institutions, as well as to develop a methodology and its evaluation to ensure continuity of operation even in crisis conditions.

The purpose of the study is to investigate the main challenges affecting the sustainability of the information infrastructure of educational institutions and to develop approaches to its assessment and increase of stability in the face of external threats.

**Information infrastructure of educational institutions.** The infrastructure of an educational institution is a set of material objects in an educational institution that ensure the quality implementation of social and educational functions, create comfortable conditions for the stay and activities of all participants in the educational process. [1, p. 183].

The information infrastructure includes hardware (PCs, network equipment), software, this category includes learning platforms (Moodle, Google Classroom), video conferencing services (Zoom, Microsoft Teams), as well as CRM systems for administration (for example, automated schedules, attendance records). Distance learning platforms, which have become critical during the COVID-19 pandemic and with the beginning of the full-scale Russian invasion in February 2022, have become especially important. [2, p. 137-138]

Data storage systems (cloud storage, backups) are an integral part of the information infrastructure; they include educational materials, personal records of students and teachers, and learning outcomes.

Cyber security systems protect the infrastructure from unauthorized access and cyber attacks. This includes anti-virus software and multi-level authentication.

A critical factor in the effective use of infrastructure is the technical staff supporting the infrastructure (network administrators, programmers, IT consultants, trained personnel).

These components interact to create the basis for the implementation of innovative approaches in education and at the same time require careful monitoring and protection from external risks.

**Modern challenges and threats to educational infrastructure.** Modern education is closely linked to information technology, which makes it vulnerable to a wide range of threats. At the beginning of Russia's full-scale invasion of Ukraine, it became apparent that there were significant shortcomings in the approaches and strategies to ensuring intellectual security that must be addressed in the future.

One example of such incidents is the cyberattacks on Ukrainian universities and research institutions in 2022-2023. These attacks were aimed at hacking into information systems, stealing data, and disrupting operations. As a result, the educational process was hampered and significant financial losses were incurred. The theft of personal data created risks for the safety of employees of educational institutions and students. [3, p. 217]

A critical consequence of the Russian-Ukrainian war for the educational environment is the destruction of Ukraine's energy infrastructure. This creates obstacles to distance learning for students, access to digital resources, and maintaining the continuity of the educational process. Educational institutions are forced to adapt by using backup energy sources, cloud technologies, and other measures to ensure the stability of education.

Approaches to assessing resilience. To assess the resilience of this infrastructure, it is necessary to apply comprehensive approaches that combine risk analysis, monitoring of key performance indicators, and the use of modern modeling methods. This allows not only to determine the current state of the system, but also to identify its weaknesses and develop effective measures to improve stability.

To assess sustainability, it is necessary to apply a risk-based approach that includes the following steps:

1. Identification of threats: A detailed analysis of possible threats, such as cyberattacks, natural disasters, technical failures, and human error, is conducted.
2. Impact analysis: For each identified threat, the potential impact on the system is assessed. Parameters such as downtime (how long the system will be unavailable after the incident) and data loss (the amount of data that may be lost or damaged) are taken into account.

The following key indicators are used to quantify the resilience of the information infrastructure:

* MTTR (Mean Time to Recovery): Average system recovery time after a failure. This indicator characterizes the speed of system recovery after an incident.
* Uptime (%): The percentage of time that the system operates without interruption. This indicator reflects the overall reliability of the system.
* RTO (Recovery Time Objective): The time during which the system should be restored after a failure. This indicator determines the allowable downtime for critical functions.

**Practical recommendations for improving resilience**. Ensuring the resilience of information systems is a critical task in today's environment. That is why it is necessary to implement practices that will help reduce the risk of data loss, increase system availability and ensure stability in crisis situations.

The use of backup and redundancy of critical infrastructure components can minimize system interruptions in the event of a system failure. It is also important to implement cloud technologies to reduce recovery time.

Business Continuity Plans (BCPs) for educational institutions involve the development of clear procedures to support operations in crisis situations. Institutions should have a DDoS response plan that outlines the sequence of actions to support the organization's work. [4, p. 19]

Technical approaches to ensuring the security of educational infrastructure play an important role, but it is necessary to take into account raising awareness of students and employees about safe behavior on the Internet and “cyber hygiene.”[5, p. 147]

**Foreign experience in ensuring the sustainability of educational systems**. The experience of countries around the world in this area shows a wide range of strategies, such as the use of distance learning technologies, crisis planning, and modernization of digital infrastructure, which can effectively ensure the continuity and quality of the educational process even in crisis conditions.

In Turkey, the Safe School and Distance Learning project introduced a comprehensive distance learning infrastructure, including improved access to online platforms, new digital resources for teachers and students, and digital skills training. These measures were aimed at strengthening the resilience of education systems and ensuring continuous learning even in emergency situations (for example, during the COVID-19 pandemic)."[6, p. 1-2]

The International Institute for Educational Planning (IIEP) promotes the idea of creating crisis-resilient education systems, including through risk assessment and implementation of risk management programs. For example, Guyana has developed a national risk management policy to minimize the impact of natural disasters and other threats. These measures strengthen the ability of systems to respond to crises while maintaining learning opportunities and the quality of education. [7].

Today, many countries are focusing on ensuring stability by improving their digital learning infrastructure and creating backup systems for data storage and transmission. This helps protect educational processes from interruptions and cyberattacks.

These examples emphasize the importance of a comprehensive approach to ensuring the resilience of education systems. Investments in technology allow not only to introduce innovative teaching methods but also to maintain the stability of systems in the face of external threats, such as pandemics or natural disasters. The development of risk management policies contributes to the systematization of crisis response processes, allowing for quick adaptation to new conditions, minimizing negative consequences for the educational process.

**Prospects for further research.** Artificial intelligence (AI) technologies can be used to develop models to predict possible threats, for example, to analyze the behavior of system users, detect anomalies, or assess risks. By using technologies such as machine learning or neural networks, it is possible to increase the effectiveness of cybersecurity systems and minimize the negative impact of crisis situations on it. [8, p. 366-372]

AI technologies are increasingly being implemented to solve security problems in information systems, including in the education sector. The main goal of such systems is to increase the efficiency of predicting and preventing possible threats through the use of big data analytics and machine learning algorithms.

Key aspects of AI implementation:

1. *Analysis of user behavior*. to detect suspicious actions or deviations from the norm. This helps prevent unauthorized access to data.
2. *Detecting anomalies* such as unusual network activity, a sudden increase in the amount of data transferred, or suspicious database queries.
3. *Risk assessment* by analyzing data on cyber threats, system vulnerabilities, and the likelihood of recurrence of threats.
4. *Predicting attacks* through the use of deep neural networks (Deep Learning). This will allow you to predict potential attack scenarios based on the analysis of large data sets.
5. *Automation of response to attacks*, their blocking, isolation of vulnerable elements of the system or rapid recovery after an incident.

An example of such systems is the integration of AI technologies into SIEM platforms (information security management systems), which allow real-time monitoring and analysis of threats. [9, p. 691-711]

Advantages of using AI to protect educational systems:

* Reduced threat detection time.
* Reducing the number of false positives.
* Efficient management of limited resources as many processes are automated.

The introduction of the Internet of Things (IoT) technology in educational institutions allows for effective monitoring of infrastructure conditions, reducing the risk of technical failures and optimizing the use of resources. To this end, IoT solutions can integrate with network equipment, power supply and climate control systems to automatically collect data, analyze it in real time and predict potential failures. [10]

Main advantages:

* *Energy consumption monitoring*: IoT sensors allow you to track the energy consumption of each device, as well as optimize their use and reduce costs.
* *Alert system:* sensors can detect malfunctions such as server overheating, water leaks, or power outages and send notifications to administrators.
* *Optimized climate control*: the system automatically adjusts the temperature and humidity level in the premises to ensure comfortable conditions for students and staff.

Effective cybersecurity for educational institutions is critical due to the growing number of cyberattacks aimed at stealing data, blocking access to systems, or destabilizing the educational process.

Zero Trust Architecture (ZTA) is a network security concept based on the principle of “never trust, always verify.” This implies that no user or device is assumed to be trustworthy by default, regardless of their location - inside or outside the network.

The main advantages of this approach: [11, p. 2, 11]

* *Unconditional authentication:* all requests for access to network resources must go through an authentication and authorization process that includes verification of identity, device, and context of the request.
* *Dynamic access control:* minimal rights are granted to access resources, they should be necessary to perform specific tasks. This helps reduce the risks associated with excessive access rights.
* *Continuous monitoring:* provides continuous monitoring of all network activity to detect anomalies and potential threats in real time.
* *Traffic visualization:* all network flows should be visible and analyzed, allowing you to detect and respond to suspicious activity.

The Zero Trust Architecture is a response to growing cyber threats and the shortcomings of traditional security models that rely on perimeter defense and can be vulnerable to insider threats. This model offers a more flexible and reliable approach to protecting information systems in today's digital environment.

The development and application of such technologies is an important step towards increasing the resilience of the information infrastructure of educational institutions.

**Conclusions.** The study demonstrates the critical importance of ensuring the sustainability of the information infrastructure of educational institutions in the face of modern challenges. An integrated approach to the assessment and protection of information systems reveals a systematic methodology that combines a risk-based assessment of infrastructure, monitoring of key reliability indicators and the implementation of modern technological solutions.

It is established that the sustainability of information infrastructure is a determining factor in the continuity of the educational process. Adaptive risk management strategies can effectively counteract modern cyber threats, ensuring the stability of educational institutions. Investments in digital technologies and crisis-resistant systems create the necessary foundation for the development of educational institutions in the face of dynamic external challenges.

Research prospects include:

* Development of integrated monitoring systems
* Implementation of artificial intelligence for threat prediction
* Creation of innovative mechanisms for information risk management

**References**

1. Sorochan, T. M. Infrastructure of the educational institution in the theory and practice of education management. Problems of Education, 2015, 2.83: 180-185: https://lib.iitta.gov.ua/id/eprint/26727/1/Інфраструктура%20стаття.pdf (accessed November 26, 2024).
2. Levchuk O., Levchuk K. Digital sustainability: assessing the role of information technology in ensuring the continuity of training in crisis conditions. Computer-integrated technologies: education, science, production. 2024. № 54. С. 137-145. URL: https://doi.org/10.36910/6775-2524-0560-2024-54-16 (accessed November 19, 2024).
3. Economic and political analysis of threats to the intellectual security of Ukraine under martial law. Scientific notes of Lviv University of Business and Law, 2024, 41: 213-224. URL: https://nzlubp.org.ua/index.php/journal/article/view/1250/1202. (accessed November 19, 2024).
4. Cybersecurity in the Information Society, Information and Analytical Digest, No. 7 (July), Kyiv, 2023. URL: https://ippi.org.ua/sites/default/files/2023-7.pdf (accessed November 19, 2024).
5. Cybersecurity and cyber resilience of business: a comparative study of approaches and methods. All-Ukrainian scientific and practical conference: “Cybersecurity strategies: risk management and business continuity”. 2023. С. 147-149. URL: https://duikt.edu.ua/uploads/p\_2626\_38605375.pdf?file=p\_2626\_38605375.pdf (accessed November 19, 2024).
6. Building Back Better: Education Systems for Resilience, Equity and Quality in the Age of COVID-19 (English). Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/497341595425543327/Building-Back-Better-Education-Systems-for-Resilience-Equity-and-Quality-in-the-Age-of-COVID-19 (accessed November 27, 2024).
7. Building resilient education systems | IIEP In Action. IIEP in action | IIEP In Action. URL: https://report.iiep.unesco.org/value-stream/building-resilient-education-systems (accessed November 27, 2024).
8. LOZOVSKY, R., MOROZ, A. (2024). THE IMPACT OF ARTIFICIAL INTELLIGENCE ON STRATEGIES FOR PROTECTING INFORMATION SYSTEMS FROM NEW TYPES OF CYBER THREATS. Herald of Khmelnytskyi National University. Technical Sciences, 337(3(2), 366-372. URL: https://doi.org/10.31891/2307-5732-2024-337-55 (accessed November 28, 2024).
9. López Velásquez, J. M., Martínez Monterrubio, S. M., Sánchez Crespo, L. E., & Garcia Rosado, D. (2023). Systematic review of SIEM technology: SIEM-SC birth. International Journal of Information Security, 22(3), 691-711 (accessed 11/28/2024).
10. Zac Amos. 5 Challenges of Implementing IoT in Rural Schools | IoT For All. IoT For All., 2024 URL: https://www.iotforall.com/5-challenges-of-implementing-iot-in-rural-schools (accessed 11.28.2024).
11. A Survey on Zero Trust Architecture: Challenges and Future Trends / Y. He et al. Wireless Communications and Mobile Computing. 2022. Vol. 2022. P. 1-13. URL: https://doi.org/10.1155/2022/6476274 (accessed November 28, 2024).