COUNTERING CYBER THREATS IN THE CONTEXT OF DIGITAL EDUCATIONAL TECHNOLOGIES IN THE HIGHER EDUCATION SYSTEM OF UKRAINE

Iryna Parfonova
PhD in Economic Sciences,
Associate Professor at the Department of Social Medicine, Organization and Management
in Healthcare, Kharkiv National Medical University, Ukraine
e-mail: Managerhnmi@proton.me, orcid.org/0000-0002-7049-4312

Oleksandra Zinchenko
Postgraduate Student at the Department of Political Science of School of Philosophy,
V. N. Karazin Kharkiv National University, Ukraine
e-mail: alekca.98@ukr.net, orcid.org/0000-0003-1623-957X

Summary

The article is dedicated to analyzing the implementation of distance learning in higher education institutions in Ukraine, as well as the challenges and prospects associated with this process. It discusses the main distance learning platforms used in Ukrainian higher education institutions such as Moodle, Google Classroom, Microsoft Teams, Coursera, EdX, Prometheus, and the National Distance Learning Platform. Each of these platforms has its own features and advantages, ensuring accessibility and flexibility in education for students and educators. In addition to the advantages of distance learning, the article also focuses on cybersecurity issues, which are becoming increasingly relevant with the growth of online education. The main cybersecurity threats are analyzed, including software vulnerabilities, personal data protection, network security, and the low level of user awareness. Approaches to managing innovations for protection against cybercrime and stimulating investments in cybersecurity are discussed, highlighting their effects on educational institutions, the country, and society. The article highlights ways to enhance cybersecurity in HEIs, including implementing modern security technologies, developing strict data access policies, and increasing cyber literacy among students and faculty. The legislative framework of Ukraine regulating data and information protection is also discussed, with particular attention to the laws «On Personal Data Protection» and «On Information Protection in Information and Telecommunication Systems,» as well as recent changes in copyright legislation emphasizing the protection of intellectual property in the digital environment. The article concludes that distance learning in Ukraine has great potential but requires improvements in cybersecurity and updates to legislation for the digital age. The implementation of cybersecurity measures and the modernization of the regulatory framework will help create a safe and effective learning environment.

Key words: distance education; digital educational platforms; professional development of teachers; cybersecurity measures.

DOI https://doi.org/10.23856/6729

1. Introduction

The educational process is a complex system consisting of a large number of disparate subsystems and generally lacking a clear formal definition. A systemic approach allows us to analyse the peculiarities of the functioning and development of the educational system, taking into account the key requirements of the state, society and citizens in both the short and long term.

Digital educational platforms play a key role in modern higher education, providing tools for distance learning, process management and interaction between students and teachers. The digitalisation of education in Ukraine meets modern challenges and trends, improving the quality and accessibility of education. The integration of technologies makes the process more flexible and personalised, which contributes to the competitiveness of Ukrainian universities in the global market.

Implementation of digital solutions requires a systematic approach: training of teachers, modernisation of infrastructure and updating of materials. Ukraine uses international and domestic platforms that support various formats: distance and blended learning, online courses, and virtual laboratories. These forms contribute to the flexibility and accessibility of education, although they require careful organisation and cybersecurity. The Law of Ukraine ‘On Higher Education’ defines distance learning as an individualised process using modern technologies and remote interaction (On Higher Education 2024).

It is worth noting that in recent years, higher education systems around the world, including Ukraine, have been significantly developed under the influence of digital technologies. The rapid development of information and communication technologies (ICTs), as well as recent global challenges such as the COVID-19 pandemic and subsequent martial law in Ukraine, have significantly accelerated the transition to distance learning. Under these conditions, educational institutions were forced to quickly adapt to the new realities by introducing various platforms for organising the distance learning process.

Ukrainian and foreign scholars are actively researching the topic of distance learning. The studies presented in this paper detail the use of modern technologies in vocational education and distance learning.

Ukrainian and foreign scientists are actively researching the topic of distance learning. The presented studies detail the use of modern technologies in vocational education and distance learning. In particular, Desamsetti H. (Desamsetti 2016) identifies the main problems of cloud computing technologies and ways to minimise their impact in the process of education. On the other hand, Reghunadhan R. (Reghunadhan 2022) analyses the historical stages of the development of the global cyber threat, as well as considers the problems and opportunities of cyber defence in the context of global development and deepening international relations. Tytarchuk M. V. (Tytarchuk 2020) compares distance learning in Ukraine and abroad, highlighting its flexibility, accessibility and individual approach. Dudnik V., Tukhtarova T., Kucher R. (Dudnik V., Tukhtarova T., Kucher R. 2020) analyse the peculiarities of organising distance learning under martial law, emphasising the priority of security. Fadziso T., Thaduri U. R., and Desamsetti H. studied aspects of cybersecurity, the main threats and directions of its counteraction in higher education institutions (Fadziso, Thaduri, & Desamsetti 2023). Nashynets-Naumova A., Buriachok V., Korshun N., Zhyltsov O., Skladannyi P., Kuzmenko L. (Nashynets-Naumova, Buriachok, Korshun, Zhyltsov, Skladannyi, & Kuzmenko 2020) analyse the issues of information and cybersecurity in higher education institutions, emphasising the importance of protecting information systems. Kuzmenko O., Kubálek Y., Bozhenko V., Kushneryov O., Vida I. in their works highlighted the main aspects and approaches to managing innovations to protect against cybercrime in various sectors of economic and social life (Kuzmenko, Kubálek, Bozhenko, Kushneryov, & Vida 2021). Yang, A., Kwon, Y. J., and Lee, S. Y. T. investigated the impact of legislative norms in different countries towards effective cybersecurity information sharing (Yang, Kwon, & Lee 2020). Wessels M., Van den Brink P., Verburgh T., Cadet B., & Van Ruijven T. considered the main directions for understanding the incentives for investment in cybersecurity and the subsequent effects of such investment (Wessels, Van Den Brink, Verburgh, Cadet, & Van Ruijven 2021).

In general, the studies cover a wide range of issues related to distance and innovative learning, including the impact of technology on the educational process, problems and prospects for the development of distance education in Ukraine and abroad. At the same time, some aspects, such as the peculiarities of implementing distance learning and cyber threats in the context of digital learning technologies and cybersecurity of the distance higher education system, remain insufficiently disclosed and require further research.

This study aims to provide an analysis of the key platforms for distance higher education used in Ukraine, their functionalities, advantages and disadvantages. Particular attention is paid to the aspects of cybersecurity and learning management in distance learning and the development of a structured system for ensuring cybersecurity of students and teachers when working with distance learning platforms in Ukrainian universities.

2. Digital learning technologies as the future of the educational process and their forms

Today, distance learning opens up many opportunities for students and teachers. It allows access to educational resources regardless of geographical location, provides flexibility in learning, promotes individualisation of the learning process and supports continuous professional development. For Ukraine, as well as for many other countries, these advantages are becoming especially important in the context of constant changes and challenges facing the higher education system. Today, there are many platforms for distance learning, each offering its own unique features and functionality. In Ukraine, as in other countries, educational institutions use different platforms, adapting them to their needs. Let's take a look at the most widely used platforms for distance learning in Ukrainian universities:

– Moodle is the most widely used platform for distance education in Ukrainian universities. It is used to create online courses, conduct tests and organise communication through forums and chats. The main advantage is that it is free, which makes it cost-effective for universities. Moodle can be easily adapted to the needs of institutions, supports various content formats, and is available on different devices and languages. In Ukraine, Moodle is actively used for distance learning, providing quality education even at a distance. It is a powerful and flexible tool that meets the modern requirements of the educational process (BeamStacks Blog).

– Google Classroom is a free web-based learning management platform from Google. It simplifies the creation, distribution and assessment of tasks, improves interaction between teachers and students, especially in distance learning. Key benefits include integration with Google Docs, Sheets, and Drive, a simple interface, and accessibility across devices. Although the platform is less functional than specialised systems such as Moodle and requires a Google account, it is actively used in Ukrainian universities to organise online classes and distribute learning materials (Google Sites). Google Classroom facilitates the learning process by providing convenient access to materials and assignments, as well as effective interaction between participants.

– The third distance learning platform is Microsoft Teams. This is a communication platform designed to organise collaboration, information exchange and interaction in the work environment. Its advantages include ease of use due to its intuitive interface and integration with other Microsoft services, such as Office 365. Users can create group chats, hold video conferences, share files, and work on joint projects in real time. In addition, Teams provides ample opportunities for organising workflows, such as task management and meeting scheduling (Raymond 2023). Microsoft Teams is widely used in higher education institutions in Ukraine, as this platform allows teachers and students to conduct the learning process remotely, share materials, conduct online lectures and seminars, and organise group projects. By integrating with other Microsoft services, such as OneDrive and SharePoint, Teams makes it easy to work with documents and collaborate on them.

– Coursera is one of the most popular online learning platforms founded in 2012 by Stanford University professors. It offers courses, specialisations and certificates from leading universities and companies, providing access to quality education from anywhere. The benefits include high quality content, interactive assignments, video lectures and forums. The platform covers a wide range of topics and allows you to obtain certificates that improve your professional level. Specialisations consist of several courses for in-depth study of specific areas. Coursera cooperates with institutions such as Stanford, Yale, Google, and IBM (Tamm 2023). The disadvantages are paid access to some courses and difficulty for beginners due to the wide range of functionality. Overall, Coursera is a convenient tool for learning at your own pace.

– EdX is a leading online learning platform founded in 2012 by MIT and Harvard that offers courses, certificates, MicroMasters programmes, and online degrees from the world's best universities. It provides access to quality education, regardless of where you live, and promotes professional development. EdX benefits include high-quality content, interactive assignments, forums, and the opportunity to earn a certificate that enhances your professional profile. MicroMasters programmes offer in-depth knowledge in a chosen field and can be counted as credits. The platform cooperates with leading universities such as MIT, Harvard, and Microsoft, guaranteeing high quality education (Review of Coursera, EdX, and Udacity: What's Good and What's Bad). The downside is the high cost of some courses, which can make it difficult for students to pay for them.

– Prometheus is a leading Ukrainian platform for massive open online courses, founded in 2014. It offers free courses from Ukrainian and international universities, experts and companies. The main advantage is the availability of quality education in Ukrainian for a wide audience. Course topics cover business, IT, medicine, law and other disciplines. Learning includes interactive assignments, video lectures, tests, and forums. Prometheus has disadvantages, such as a limited budget and a smaller selection of courses compared to Coursera or EdX (Prometheus). The platform's uniqueness lies in its emphasis on Ukrainian content and partnerships with local universities, which makes the programs relevant to Ukrainian students. The platform also supports civic initiatives by offering civic education courses.

– The National Distance Learning Platform is an initiative of the Ukrainian government to ensure access to quality education. Launched during the COVID-19 pandemic, it offers free resources and courses adapted to the national curriculum, with support for the Ukrainian language. The platform ensures accessibility regardless of place of residence or financial status and covers a wide range of disciplines, from school subjects to university programs. Interactive assignments, video lectures and tests contribute to effective learning. The disadvantages are less interactive content and technical problems compared to international platforms.

Thus, it is important to note that educational platforms play a key role in providing distance and blended learning and offer a large number of benefits. In particular, they enable access to learning material at any convenient time and from any place, facilitate individualised learning and effective communication between teachers and students, encourage independence in learning, and provide access to a wide range of learning resources and tools to improve the quality of education.

It should be emphasised that without the use of software, it is impossible to achieve the ultimate goal of informing the educational and research activities of higher education institutions. At the same time, each higher education institution uses software such as Microsoft Windows operating systems, Microsoft Office document editors, modular object-oriented dynamic learning environment Moodle and ESET anti-virus software in its educational and research activities. In practice, this software is used in different ways (Shapoval, Kotlyaria, Medvedieva, Lishafai, Barabash, & Oleksyuk 2021).

The role of software is to manage the hardware components of various equipment (devices) and to create, process, transmit, store and cyber-secure information (data) circulating in the information space of higher education institutions (Kavak, Padilla, Vernon-Bido, Diallo, Gore, & Shetty 2021). In addition, hardware and software are interdependent and complementary. When analysing software, the following main characteristics (indicators) of its impact on the cybersecurity of higher education institutions can be identified

– software installation (availability);
– adequacy of the software (relevance);
– software maintainability;
– software configuration (Gunduz, & Das 2020).

As in the case of hardware, the inconsistency of at least one of the characteristics of software impact on the cybersecurity of an HEI creates preconditions that reduce the cybersecurity of the HEI, i.e. create vulnerabilities in the information space (Guembe, Azeta, Misra, Osamor, Fernandez-Sanz, & Pospelova 2022).

The decomposition allows us to identify the main characteristics of the impact of external and internal factors on the cybersecurity of higher education institutions:

1) the impact of external factors on the cybersecurity of higher education institutions:

– the implementation of various types of cyberattacks depends on the quality of development and production of hardware and software of the respective foreign manufacturer, i.e. the presence of vulnerabilities (intentional or unintentional);

– in terms of the severity of the impact of external factors on the cybersecurity of higher education institutions, the most dangerous compared to other external factors are emergencies (natural disasters) (it is almost impossible to reduce the effectiveness of their impact) (Guembe, Azeta, Misra, Osamor, Fernandez-Sanz, & Pospelova 2022);

2) the impact of internal factors on the cybersecurity of higher education institutions:

– In particular, the quality of a higher education institution's cybersecurity policy, topology (architecture) of the information space, hardware and software depends on the competence of its specialists. At the same time, the future cybersecurity policy of a higher education institution may also indirectly affect the training (education) of staff through the establishment of legislative requirements for the continuous formation and development of knowledge, skills and competencies in the field of cybersecurity;

– Given the importance of the impact of internal factors on the cybersecurity of higher education institutions, staff training (education) is also of particular importance and should be systematic (without knowledge, it is impossible to solve all existing problems, especially the problem of ensuring cybersecurity in higher education institutions).

Thus, the analysis of external and internal factors is a prerequisite for understanding the current state of cybersecurity in higher education institutions and making appropriate management decisions to improve it (Hina, & Dominic 2020).

3. Cyberthreats and countermeasures

However, along with the benefits, distance learning brings a number of challenges. Key among them is the need to ensure cybersecurity, maintain the quality of education, manage online communications, and effectively use technology to create an interactive learning process. The problem of cybersecurity in Ukrainian universities, especially in distance learning systems, is relevant and urgent. Low user awareness creates significant risks to data and network security. Many students and teachers may not have sufficient knowledge of threats such as phishing attacks or the use of weak passwords. This leaves them vulnerable to cybercriminals. The use of platforms such as Moodle, Google Classroom, Microsoft Teams, Zoom, Coursera, EdX, Prometheus, the national distance learning platform, etc. requires a serious approach to data protection and privacy. Thus, it is important to choose the right platforms that can meet the needs of educational institutions and ensure safe and effective learning. The security of these platforms is critical, as they contain a large amount of personal data and learning materials. Attacks on these platforms can lead to disruption of the educational process, data leakage and financial losses.

Another problem is the vulnerability of e-learning platform software due to outdated versions and security flaws when used in Ukrainian universities. This can lead to attacks by intruders and leakage of confidential information. Insufficient updates of software systems and security flaws can be an easy target for hackers and intruders, threatening the confidentiality and integrity of data. Protecting users' personal data is also critical. A large amount of confidential information stored in e-learning systems can be subject to cyberattacks. Finally, insufficient network security can make it difficult to detect and prevent cyber threats.

Unfortunately, today, a large number of higher education institutions have limited resources to effectively protect their networks, which makes them vulnerable to cybercriminals. As already mentioned, this can lead to the leakage of confidential information and disruption of distance learning systems. We believe that in response to these threats, universities should improve their data protection systems and implement strict access policies. Malware protection is a key aspect of distance learning. Downloading malicious files can corrupt systems, steal data, or gain access to devices. Poor user awareness of cybersecurity issues, such as complex passwords or phishing detection, increases the risk of attack.

Distance learning platforms are also vulnerable to DDoS attacks, which can disrupt services, particularly during exams or thesis defence. Limited resources make it difficult to implement state-of-the-art security measures, increasing the risk of data breaches that could undermine the institution's credibility and violate the law.

The war in Ukraine, which began in 2022, has had a significant impact on higher education, making distance learning critical to ensure continuity. The hostilities forced educational institutions to urgently switch to an online format, accelerating digital transformation. Students and teachers, often displaced by the hostilities, used digital platforms as their primary way of learning, regardless of their location.

Increased risks of cyberattacks required enhanced cybersecurity, including the introduction of two-factor authentication, regular system updates, and user training. Securing communications, such as email and video, has become important to protect information and ensure confidentiality. Adaptation of teaching materials to the new teaching environment took into account the technical and psychological challenges of students, although it also raised issues of copyright and plagiarism.

International organisations support Ukrainian institutions by providing access to platforms and resources, as well as offering exchange programmes. Raising cybersecurity awareness among teachers and students remains important to reduce vulnerability to threats.

4. Conclusions and prospects for further research

Thus, cybersecurity in the Ukrainian higher education system faces many challenges, from protecting personal data and educational materials to ensuring the security of communications and managing IT infrastructure. Despite the many challenges, Ukrainian educational institutions have managed to adapt to the new environment, continuing to provide quality education and support students in this difficult time. Ensuring effective cybersecurity in Ukrainian higher education institutions requires a comprehensive approach that includes user training, software enhancements, personal data protection, the development of strict security policies and strengthening network defences. The 2022 war in Ukraine has had a major impact on the higher education system, making distance learning a vital tool for ensuring the continuity of the educational process. Distance learning platforms such as Moodle, Google Classroom, and Microsoft Teams have played a key role in this transition by providing flexible, affordable, and secure solutions for students and teachers.   Successfully overcoming these challenges requires a comprehensive approach that includes technical, organisational and educational measures.

In general, ensuring cybersecurity for distance learning platforms in Ukrainian universities is a complex task that requires constant monitoring, user education, and the implementation of modern security technologies. This is the only way to guarantee data security and the continuity of the educational process. Therefore, we believe it is necessary to develop a structured cybersecurity system for students and teachers when working with distance learning platforms in Ukrainian higher education institutions (HEIs) that would include several key components. This system should ensure reliable data protection, prevent unauthorised access, and guarantee the confidentiality and integrity of the educational process. We propose the following structure of methods to counter cyber threats in the Ukrainian higher education system:

1. Implementation of a clear cybersecurity policy that covers all aspects of distance learning, this policy should be mandatory for all participants in the educational process. This should include the establishment of clear rules for accessing learning resources, including the use of complex passwords and two-factor authentication;

2. Regular trainings and educational programmes to raise awareness of cybersecurity threats and ways to protect cybersecurity among participants in the educational process, such measures will help maintain an appropriate level of knowledge, skills and abilities to ensure cybersecurity of information and its importance for the educational process. In addition, it is important to create a culture of security among students and teachers through regular reminders and training activities;

3. Technical measures, which include the implementation of tools to protect information systems and data. This includes network security measures, encryption of data transmitted over the Internet, installation, maintenance and timely updates of anti-virus software on all devices, and regular updates of software and operating systems to close known vulnerabilities;

4. Develop organisational procedures to ensure compliance with cybersecurity policies. Here, it is important to pay attention to three components: incident management,

i.e. the creation of procedures for responding to cybersecurity incidents, including a data breach action plan, the implementation of monitoring systems to detect and analyse suspicious activity, as well as regular audits of security systems and evaluation of their effectiveness;

5. Ensuring that the educational process complies with legislation and regulations in the field of cybersecurity, as well as supplementing these documents with the specifics of cybersecurity in the educational environment;

We believe that the implementation of the proposed measures will ensure reliable protection of data and information systems in Ukrainian higher education institutions that use distance learning platforms for the educational process. Only the systematic implementation and support of these measures will help create a reliable and secure educational environment that can effectively withstand modern cyber threats. It is important to regularly review and update security policies and measures in line with new threats and technologies.

References

1. Pro vyshchu osvitu, Zakon Ukrainy № 1556-VII (2024) [On Higher Education, Law of Ukraine No. 1556-VII]. (Ukraine). https://zakon.rada.gov.ua/laws/show/1556-18#Text

2. Desamsetti, H. (2016). Issues with the cloud computing technology. International Research Journal of Engineering and Technology (IRJET), 3(5), 321–323.

3. Reghunadhan, R. (2022). History and Evolution of Global Cyber Technological Threat Landscape: Theoretical Dimensions. Cyber Technological Paradigms and Threat Landscapein India, 1, 21–55.

4. Tytarchuk, M. (2020). Rozvytok dystantsiynoho navchannya za kordonom ta v Ukrayini [Development of Distance Learning Abroad and in Ukraine]. Dystantsiyna osvita v Ukrayini: innovatsiyni, normatyvno-pravovi, pedahohichni aspekty: zb. nauk. prats materialiv I Vseukrayinskoyi naukovo-praktychnoi konferentsiyi, 1, 129-130. doi: http://iro.nau.edu.ua/images/docs/conference/conf_distance/16.06.2020/%D0%97%D0%B1%D1%96%D1%80%D0%BA%D0%B0%20%D1%82%D0%B5%D0%B7_%D0%94%D0%B8%D1%81%D1%82%D0%B0%D0%BD%D1%86%D1%96%D0%B9%D0%BD%D0%B0%20%D0%BE%D1%81%D0%B2%D1%96%D1%82%D0%B0_2020.pdf.

5. Dudnik, V., Tukhatarova, T., & Kuchep, R. (2020). Dystantsiyne navchannya zdobuvachiv osvity Ukrayiny v umovakh voyennogo stanu: orhanizatsiynyy aspekt [Distance Learning for Ukrainian Students in Wartime Conditions: Organizational Aspect]. Visnyk Dniprovskoyi akademiyi neperyvnoї osvity. Seriya: Filosofiya. Pedahohika, 2 (3), 54-60. doi: http://nbuv.gov.ua/UJRN/dnipakmo_2022_2_10.

6. Fadziso, T., Thaduri, R. U., & Desamsetti, H. (2023). Evolution of the Cybersecurity Threat: An Overview of the Scale of Cyber Threat. Digitalization & Sustainability Review, 3(1), 1–12.

7. Nashynets-Naumova, A., Buriachok, V., Korshun N., Zhyltsov, J., Skladannyi P., & Kuzmenko, L. (2020). Technology for information and cybersecurity in higher education institutions of Ukraine. ITLT, 77(3), 337–354. doi: 10.33407/itlt.v77i3.3424.

8. Kuzmenko, O., Kubálek, L., Bozhenko, V., Kushneryov, O., & Vida, I. (2021). An approach to managing innovation to protect financial sector against cybercrime, Polish Journal of Management Studies, 24, 276–291. doi: https://doi.org/10.17512/pjms.2021.24.2.17.

9. Yang, A., Kwon, Y. J., & Lee, S. T. (2020). The impact of information sharing legislation on cybersecurity industry. Industrial Management & Data Systems, 120(9), 1777–1794. https://doi.org/10.1108/imds-10-2019-0536

10. Wessels, M., Van Den Brink, P., Verburgh, T., Cadet, B., & Van Ruijven, T. (2021). Understanding incentives for cybersecurity investments: Development and application of a typology. Digital Business, 1(2), 100014. https://doi.org/10.1016/j.digbus.2021.100014

11. Moodle – Advantages and Disadvantages | BeamStacks Blog. BeamStacks Blog. (n.d.). https://www.beamstacks.com/blog/moodle-advantages-and-disadvantages-learning-system/

12. Google Classroom – Pros and Cons. Google Sites: Sign-in. (n.d.). https://sites.google.com/view/classroom-workspace/new/pros-and-cons. Data zvernennya: Cherv. 19, 2024.

13. Raymond, D. (2023, December 28). Top 10 Cons or Disadvantages of Microsoft Teams. ProjectManagers.net. https://projectmanagers.net/top-10-cons-or-disadvantages-of-microsoft-teams/

14. Tamm, S. (2023, November 22). An honest review of Coursera in 2023: pros, cons & alternatives. E-Student. https://e-student.org/coursera-review/

15. Review of Coursera, EdX, and Udacity: What's good and what's bad. (n.d.). https://www.edukatico.org/en/report/review-of-coursera-edx-and-udacity-what-s-good-and-what-s-bad

16. Prometheus. Let's learn. (n.d.). https://vchymo.com/application/Prometheus.

17. Shapoval, O., Kotlyaria, S., Medvedieva, A., Lishafai O., Barabash, O., & Oleksyuk, O. (2021). Education in Cyberspace: University as Universality. International Journal of Computer Science and Network Security, 21(11), 333–337. doi: http://paper.ijcsns.org/07_book/202111/20211145.pdf

18. Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. Journal of Cybersecurity, 7(1). https://doi.org/10.1093/cybsec/tyab005

19. Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer Networks, 169, 107094. https://doi.org/10.1016/j.comnet.2019.107094

20. Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyber attacks: a review. Applied Artificial Intelligence, 36(1). https://doi.org/10.1080/08839514.2022.2037254

21. Hina, S., & Dominic, P. (2020). Information security policies' compliance: A perspective for higher education institutions. Journal of Computer Information Systems, 60(3), 201–211.