Theoretical exploration of the design of the open university ecosystem and its security challenges within the realm of digital transformation

Oksana Buinytska[1,†], Valeriia Smirnova[1,†], Tetiana Terletska[1,†], Liliia Varchenko-Trotsenko[1,†] and Bohdan Hrytseliak[1,*,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudryavska str., 04053 Kyiv, Ukraine*

Abstract

The paper investigates the theoretical foundations of designing an open university ecosystem for protection against information security threats that meet the requirements of the modern digital society. The authors provide an overview of international and Ukrainian legal acts related to the digital transformation of higher education, which is not limited to and not determined by the introduction of digital technologies into the activities of the university, it involves much deeper changes, namely the formation of a new model of university functioning and activity. The paper discusses international and Ukrainian experiences in designing an open university ecosystem, methodologies, and measures to increase protection against cyber threats and to ensure the safe operation of higher education infrastructure, which is especially relevant in the context of martial law in Ukraine. The key benefits of digital transformation, such as creating opportunities for cooperation, expanding service delivery, and changing approaches to work, individual and group educational needs, are highlighted, which requires the creation of a university ecosystem based on the ideological and methodological principles of openness and continuity of the learning process. The analysis of the ideas of digital transformation and the design of the university ecosystem is based on the research of leading scientists in the world and Ukraine. The authors offer a list of functioning ecosystems that are directly or indirectly related to university education, their features, and strengths are indicated, and the common factors to be taken into account in the process of an educational ecosystem design are defined. Cybersecurity has been identified as one of the important issues to consider in the design of an open university ecosystem The main areas to ensure the reliability and security of the ecosystem include data security and privacy, access control and authentication, and network and infrastructure protection. The digital campus of Borys Grinchenko Kyiv Metropolitan University is described as the current stage of the university's digital transformation and is the basis for designing an open university ecosystem. It includes such main categories as digital education, digital science, digital control, image and leadership, digital space, and infrastructure. The paper also presents the prerequisites for creating an ecosystem of the Grinchenko University in the context of digital transformation as a preparatory stage for the implementation of the study on the design of an open university ecosystem, which was launched by the Digitization of Education Research Lab of Borys Grinchenko Kyiv Metropolitan University. Based on the analysis and considering the requirements and needs of today, an indicative model of the open university ecosystem is presented.

Keywords

open university ecosystem, designing a university ecosystem, open university, cybersecurity, digital transformation

1. Introduction

The rapid development of technologies prompts the digital transformation of all spheres of society's life, which provides an opportunity for the development of education and at the same time creates challenges for universities. The process of digital transformation in the world has been accelerated by the pandemic caused by Covid-19 and the introduction of martial law in Ukraine. Organizations and educational institutions were forced to work in remote mode, not only employees needed to master new digital technologies and tools, but also all citizens—consumers of social services. Digital transformation is not limited to and not determined by the introduction of digital technologies into the activities of the university, it involves much deeper changes, namely the formation of a new model of functioning and activity of the university—an open university, a "university without walls", which will be the

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine
*Corresponding author.
†These authors contributed equally.
o.buinytska@kubg.edu.ua (O. Buinytska);
v.smirnova@kubg.edu.ua (V. Smirnova);
t.terletska@kubg.edu.ua (T. Terletska);
l.varchenko@kubg.edu.ua (L. Varchenko-Trotsenko);
b.hrytseliak@kubg.edu.ua (B. Hrytseliak)

0000-0002-3611-2114 (O. Buinytska);
0000-0001-9965-6373 (V. Smirnova);
0000-0002-8046-423X (T. Terletska);
0000-0003-0723-4195 (L. Varchenko-Trotsenko);
0000-0003-2953-8560 (B. Hrytseliak)

key to success in the next ten years, about which is stated in the Concept of the European Association of Universities "Universities without Walls: A Vision for 2030" [1]. Only with a complete change in the organizational structure of the university, one can realize such benefits of digital transformation as the creation of opportunities for cooperation, the expansion of service delivery, and changes in approaches to work, individual and group educational needs, which require the creation of a university ecosystem based on the worldview and methodological principles of openness and continuity of the process of cognition. The ecosystem itself will ensure the development of a holistic university to achieve its competitiveness, openness, transformation, and transnationality, strategic goals of the university's sustainable development, which is formed as a result of the synergy of education, science, innovation, academic, and business community. However, along with the numerous benefits provided by digital transformation, new challenges arise, among which a special place is occupied by ensuring protection against information security threats, and disruptions in the functioning of the university's digital infrastructure to ensure the continuity of the educational process, increasing the level of security of information resources, protecting confidential data, etc. [2].

To be able to design an open university ecosystem, it is important to study the previous experience of designing educational ecosystems and increasing their security, as well as the legislative framework for this. At the same time, a solution must be planned taking into account the existing infrastructure and available resources of the higher education institution (HEI). Thus, it is necessary to study the prerequisites of the open university ecosystem and modern approaches to ensure its protection. In the context of modern military aggression, which covers not only physical but also cyberspace, higher education institutions (HEIs) are becoming attractive targets for cyberattacks that can lead to the leakage of confidential information, personal data, disruption of the educational process, impact on research results and the overall reputation of the educational institution. The digital transformation of education creates additional challenges, including cybersecurity issues in the open university ecosystem, which must be taken into account in the design process [3, 4]. The main areas of cybersecurity in the open university ecosystem include data security and confidentiality, access control and authentication, and network and infrastructure security. Therefore, the issue of protecting the infrastructure of a higher education institution from cyber threats is a priority.

Problem statement. Modern society requires a profound change in approaches to work, service delivery, problem-solving, and management in various fields. Higher education is no exception and must adapt to the conditions, respond to the challenges of today, and develop to be competitive and effective in the context of digital transformation, which is not limited to the use of digital tools, but requires the development of a new model of functioning to ensure lifelong learning, the introduction of innovative technologies and teaching methods, cooperation with business, government and public structures for high-quality education and research. Designing an open university ecosystem that has a high level of protection against information security threats is an urgent problem and research area.

The purpose of the study. The purpose of the paper is to study the best international, European, and national practices of designing educational and university ecosystems in the context of the digital transformation of society and to ensure their protection. The main tasks are to study the legislative framework for digital transformation, analyze Ukrainian and international experience in various ecosystems related to educational activities and universities in particular, determine the prerequisites for designing an open university ecosystem at Borys Grinchenko Kyiv Metropolitan University in the context of digital transformation, identify key guidelines for the security of the open university ecosystem, and design a model of such an ecosystem.

2. Method description

To achieve the goal of the research several theoretical methods were used: the analysis of the current state of the problem research in scientific publications; the analysis of normative and legislative acts on digital transformation of higher education at national and international levels; generalization of experience in designing open university ecosystems; comparative analysis method; determination of the prerequisites for Borys Grinchenko Kyiv Metropolitan University ecosystem design under the conditions of digital transformation. The research was carried out according to the tasks of the scientific topic "Designing an open university ecosystem in the context of digital transformation of society" (No. 0123U102794), which is being implemented by the Digitization of education research laboratory of Borys Grinchenko Kyiv Metropolitan University.

3. Research results

The paper presents the research carried out at the first and partially second stages of the implementation of the research topic of the Digitization of Education Research Lab of Borys Grinchenko Kyiv Metropolitan University, which includes some tasks, including studying the process of digital transformation based on the world's leading higher education institutions, determining the peculiarities of digital transformation in the management, educational and scientific spheres of higher education institutions, analyzing international experience in designing open university ecosystems; substantiating the prerequisites for the project. The study summarizes the regulatory and legal documents related to the digital transformation of higher education, the experience of ecosystems, and the prerequisites of Borys Grinchenko Kyiv Metropolitan University, which serve as the basis for designing an open university ecosystem.

The study analyzed the use of terminology related to open educational ecosystems and digital transformation in European long-term documents, Ukrainian legislative documents, draft documents submitted for public discussion, articles by leading scholars who study university development, ecosystem building, and digital transformation, etc. (Fig. 1).

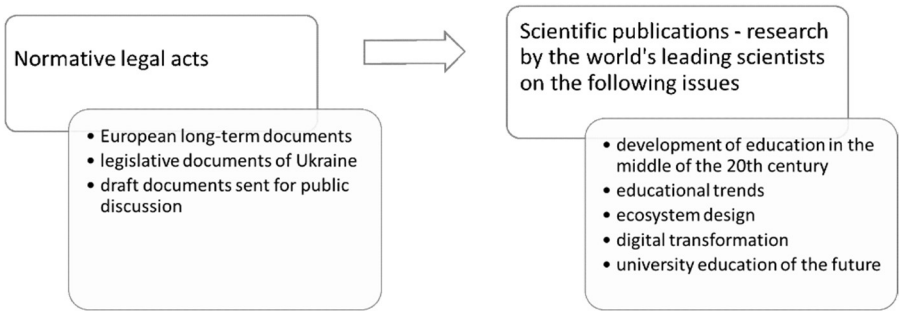

Figure 1: Structure of the analysis

The key issues of digital transformation of university education are reflected in key long-term international documents, including those of the European Commission, the United Nations, the European Association of Universities, and the International Association of Universities.

The main strategic priorities of the Digital Education Action Plan (2021-2027), an updated policy initiative of the European Union (EU), are to promote the development of a high-performance digital education ecosystem. For the implementation of strategic priorities, some measures have been identified, which include the development of a Plan for the digital transformation of higher education institutions, the creation of a European platform for the exchange of higher education content and educational data to support in-depth transnational cooperation between higher education institutions and facilitate the exchange of content and educational data, the development of network infrastructure, the implementation of innovative technologies, development of digital competence of teachers and lecturers, inclusion of artificial intelligence and data-related skills in the European Framework of Digital Competences. The Plan emphasizes the importance of improving ICT skills in areas such as cyber security, big data, quantum technology, and machine learning, as well as improving digital skills for businesses such as web design, digital marketing software development, etc. [5].

Transforming our world: the 2030 Agenda for Sustainable Development [6], one of the key documents of the Department of Economic and Social Affairs, which considers digital technologies as a means of implementing open access to education, global cooperation, and knowledge sharing. Open education is part of an open and socially inclusive world, which means that openness must be visualized as one of the merits of higher education as well and an open university ecosystem can be seen as a way to introduce and fulfil open higher education. In the context of open education, urgent issues include ensuring compliance with international and national standards of cybersecurity in education, ensuring the security and reliability of distance learning platforms, implementing reliable authentication systems to prevent unauthorized access, preserving and protecting educational materials and research results in open access, protecting confidential research data, fostering a culture of cybersecurity among students, faculty, and staff, ensuring the security of data and processes when using cloud technologies [7, 8].

The concept of the European Association of Universities "Universities without Walls: A Vision for 2030" defines the vision of sustainable and efficient universities that serve European societies in a better future. The digital transformation of universities is recognized as an important trend but does not replace a physical presence on campus. As the process of digitization expands, advanced digital technologies must be integrated into university education, the model of which will undergo significant changes for openness and accessibility. However, physical presence on campus should remain a core feature of most educational institutions [1].

The main strategic priority of the International Association of Universities is the digital transformation of higher education. The IAU Strategy (2022–2030) declares that digital transformation affects all aspects of higher education institutions, from governance to teaching and research. It opens up new opportunities but also presents new challenges. HEIs must respond to, interact with, and shape this process to stay current, and modern and correspond to the needs of the society where digital technologies play a crucial role [9].

The strategy for the development of higher education in Ukraine for 2022–2032 is aimed at achieving the Sustainable Development Goals, including the spheres of education and professional training, and is coordinated with other program documents that are conducive to a high standard of living and human progress. The Strategy identifies key priorities for the higher education system at the present stage of social and economic development together with the main characteristics that should be formed by 2032. The Strategy emphasizes that the lack of practice and experience in implementing digital technologies is one of the problems that need to be addressed. Therefore, the digital transformation of educational institutions is an important direction of the development of higher education in Ukraine, which involves the utilization of digital technologies to improve management and monitoring in higher education institutions and the quality of the educational process. The main tasks to achieve the strategic and operational goals of this Strategy are the development of innovation infrastructure based on higher education institutions, promotion of their integration into regional innovation ecosystems and Industry 4.0 clusters, taking into account the SMART specialization of the regions; digital transformation of management, regulation and monitoring processes in higher education institutions and the effective use of digital (distance) technologies in the educational process; development of standardized digital tools for measuring learning outcomes and verifying academic integrity; introduction of IT equipment as part of the digital infrastructure in the updated teaching and research

laboratories of higher education institutions; formation of a fault-tolerant IT infrastructure; encouragement of the use of innovative technologies and teaching and learning tools in the educational process, development of research infrastructure; modernization of networks, secure access and data exchange; search for ways to digitally transform the access of foreign citizens to higher education in Ukrainian universities [10].

Ukraine's Recovery Plan (Education and Science) regulates the key measures for the post-war recovery of the sphere of Ukrainian education. The primary objectives of the Plan encompass several key areas: fostering the creation of personalized educational paths for students, incorporating interdisciplinary educational initiatives, securing acknowledgment from universities for non-formal and informal learning, promoting student-centered learning principles as the cornerstone of educational structuring, and integrating innovative technologies and diverse educational modalities. Additionally, the Plan outlines the integration of digital solutions to reinforce measures for identifying breaches of academic integrity, notably through the development of a standardized digital tool for monitoring academic integrity. The Plan also outlines the need for the digital transformation of management, regulation, and monitoring processes in higher education institutions, the effective use of digital (distance) technologies in the educational process, the creation of a universal methodology for evaluating scientific activity based on world experience in the balance between quantitative and qualitative indicators, the introduction of digital evaluation tools, development a unified information system that will ensure the reliability and relevance of data for analysis and decision making in the field of science [11].

The plan for the implementation of open science in Ukraine provides for measures to ensure open access to scientific results and scientific and technical information; guarantee open access to research infrastructure and promote a favorable environment for the effective use of scientific and technical information and publicly available research infrastructure resources; protect open scientific platforms and data repositories from unauthorized access; ensure security in the exchange of data between different scientific institutions and industries; popularization of science, dissemination of scientific knowledge and involvement of citizens in scientific and technical activities; improvement of the system of quality assessment of scientific and technical activities; raising awareness and building competence in open science. The strategy for advancing open science in Ukraine advocates for the adoption of proper management practices for scientific data (FAIR principles) and the utilization of optimized scientific data (FAIR data). This includes their integration into the research process. Moreover, it entails the establishment of a national scientific information system for open access monitoring, facilitation of data exchange with EU nations, particularly through integration into European data spaces, and the establishment of a unified database documenting scientific and technical accomplishments. Additionally, it aims to refine the criteria for state certification of higher education and scientific institutions, as well as to develop guidelines for these institutions on enhancing institutional policies for evaluating scientific and academic staff, guided by the principles outlined in the San Francisco Declaration on Research Assessment (DORA) and the Open Science Career Assessment Matrix (OS-CAM) [12].

The draft document "Concept of digital transformation of education and science", which is under public discussion, created to bring it into line with the global trends of digital development, highlights the need for the successful realization of each person's potential, including the self-realization of those who choose professions that require acquiring a high level of digital competences and mastering the latest technologies.

In the project of the Ministry of Digital Transformation of Ukraine "Strategy for the Development of the Innovation Ecosystem in Ukraine", where the following innovation areas are prioritized: defense tech, artificial intelligence, FinTech, Green Tech, AgriTech, Cybersecurity, Industry 4.0; the insufficiently developed lifelong education system and weak STEM education, which do not allow the development of innovative entrepreneurship in Ukraine, the low realization of the development potential of the IT sphere due to systemic problems in IT education at every stage of specialist training are noted [13].

The studied documents allow the authors to assert that the digital transformation of university education may result in the construction of an open university ecosystem characterized by a high level of security, compliance with advanced cybersecurity standards, and ensuring reliable protection, integrity, and accessibility of educational resources and data in conditions of increased openness and interaction. The design of an open university ecosystem correlates with the priorities of digital transformation of universities in the documents analyzed above [1, 5, 6, 9–13].

The development of university infrastructure, integration of digital technologies into the educational process, digital transformation of management, regulation and monitoring processes, development of digital competence of teachers and lecturers, ensuring high quality and security standards, open access, dissemination of research results, improvement of institutional policies for the evaluation of research and teaching staff are identified as key strategic priorities of the digital transformation of HEIs in the regulatory documents of the European and national levels. The implementation of the priorities set out in the regulatory documents at the European and national levels plays a significant role in improving the quality of education, increasing the competitiveness of universities, and preparing students who will be successful in the modern digital world. At the same time, these priorities contribute to expanding access to education, ensuring the continuity of the educational process, introducing innovative methods and approaches to teaching, actively involving students in the learning process, expanding research opportunities, and creating a safe and open educational environment conducive to innovation, knowledge sharing, and cooperation. Therefore, we see them as a guideline in designing an open university ecosystem.

Digital transformation has become one of the key aspects of discussions on the development of education in recent years. Scientists are investigating various aspects of the digital transformation of society and education, in

particular, its impact on various spheres of university activity. Among the main tasks of the digital transformation of education, Bykov V., Spirin O., and Pinchuk O. highlight, particularly the formation of a coherent national policy for the digital transformation of education, improving the digital competence of participants in the educational process, conducting research in the field of digitalization of education, etc. [14]. The Ukrainian and foreign experience of the digital transformation of higher education at different stages is summarized by Vakaliuk T., Antoniuk D., Novytska I., and Medvedieva M. It is emphasized that there is no single approach to the digital transformation of higher education, each researcher considers the problem in a separate context and emphasizes that in modern conditions, the digital transformation of higher education institutions is simply necessary to ensure a quality educational process in all its aspects [15].

Cerda Suarez L. M., Nunez-Valdes K., Quiros and Alpera S. [16] highlight a systems perspective to understand the digital transformation in higher education but also expand the range of management decisions about the role of educational ecosystems in this transformation. Recently, considerable attention has been paid by the scientific community to the study of the education ecosystem and the university ecosystem, with an emphasis on the importance of security. In particular, the educational ecosystem as an environment for creating conditions that increase the competitiveness of universities, organizations, areas, and regions is considered by Kovaliuk T. and Kobets N. [17]. The study presents the synergy of education and science with the state-political system, business and economy, and society and proposes the concept of "University 4.0" as part of an innovative educational ecosystem.

The principles of open education are described in the paper by Kyrychenko M., Prosina O., Shven Y., and Kravchynska T. [18]. Among the principles the following ones can be singled out: openness and accessibility, flexibility and adaptability, globalization, and economic efficiency. Identity management options, authorization processes, and access control parameters in public and private universities are studied by Mollakuqe E. and Dimitrova V. [19]. The authors identify key measures aimed at strengthening the overall security of universities against new cyber threats, including continuous monitoring of advanced technologies, user training incident response planning, etc. These measures should be taken into account in the process of designing an open university ecosystem.

Abad-Segura E., Gonz´alez-Zamar M-D., Infante-Moro J.C., Ruip´erez Garc´ıa G. explore the main trends related to the sustainable management of digital transformation, which include Big Data, artificial intelligence, robotics, the use of flipped classroom technologies, digital cooperative learning (DCL), gamification, augmented, virtual or mixed reality, which contributes to increasing the motivation and involvement of students in the educational process, stimulates practical and creative activity, using new didactic models for learning and teaching based on individual learning, personalization of content and development of own skills through social learning [20]. Tungpantong C., Nilsook P., and Wannapiroon P. identify strategy, process, product (service), human factor, data, and technology as the factors that influence the success of the digital transformation of educational institutions. At the same time, the issue of increasing the level of security of the infrastructure and information resources of a higher education institution is particularly important [21]. The study by Dudykevych V., Mykytyn H., Stosyk T., and Skladannyi P. [22] presents a general methodology that allows the implementation of integrated security systems for the safe operation of infrastructure facilities. The methodology includes such key aspects as a multi-level approach to security, ensuring security at all stages of the information life cycle, applying a systematic approach, and using specialized security technologies for each level of architecture.

Ab Jalil H., Ismail I.A., Ma'rof A.M., Lim C.L., Hassan N., Che Nawi N.R. [23] based on an analysis of data from universities, examined the impact of the ecosystem on students' future readiness. Kathleen Mahon, Hannu L. T. Heikkinen, and Rauno Huttunen [24] encourage the inclusion of critical educational practices in the university ecosystems that are now being created. Research work "Towards a Unified Open Education Ecosystem through Generative AI, Blockchain, DAO, MMLA, and NFT" by Dr. Mehmet Firat explores the potential integration of several technologies to create a single educational ecosystem. These technologies include decentralized autonomous organizations (DAOs), blockchain, non-fungible tokens (NFT), generative artificial intelligence, and multimodal learning analytics technologies [25]. Particular attention is paid to information security aspects, including the protection of students' data, ensuring the integrity of educational materials, and creating reliable authentication mechanisms within this innovative ecosystem.

Piazza A., Vasudevan S., and Carr M. examine the cybersecurity ecosystem in higher education, finding very low levels of collaboration and significant opportunities for improving cyber threat information sharing [26]. The research identifies key areas for enhancement, including the need for university management to support collaboration, the potential for coordinating bodies to play a more active role, and the importance of investing in universities' digital estates to improve overall sector resilience. The study by H. Dei, D. Shvets, N. Lytvyn, O. Sytnichenko, and O. Kobus [27] highlights the importance of cybersecurity in educational institutions as part of Ukraine's path to European integration, emphasizing the need for improved legislation, privacy protection, and data security across various sectors. Key challenges include outdated legislation, lack of clear cybersecurity standards, and protection of personal data, while prospects for improvement involve enhancing regulatory frameworks, implementing innovative technologies, and developing tailored cybersecurity mechanisms for educational institutions. Anakhov P., Zhebka A., Popereshnyak S., Skladannyi P., and Sokolov V. [28] present an innovative approach to protecting critical information infrastructure from military cyberattacks, which can be used in part in higher education institutions. The main concept is to decentralize the telecommunications network through its hybridization. This approach is aimed at increasing the resilience of critical information infrastructure to cyber-attacks by diversifying communication channels and dynamically adapting data

transmission parameters. The proposed concept has the potential to significantly increase the level of cybersecurity, which is important in the context of modern military conflicts, where information infrastructure is becoming a key target of attacks.

Kepuska K. and Tomasevic M. [29] propose a simplified cybersecurity framework for e-learning management systems in higher education institutions, considering resource constraints and low cybersecurity awareness.

The design of an innovative and entrepreneurial educational ecosystem of a higher education institution, which takes into account the principle of environmental friendliness and low power consumption of hardware and software, is analyzed by Dan Sheng, Yulong Wang [30].

Cwik S. and Singh C. [31] raise the issue of inclusiveness and equality of participants in the educational process in the scientific education ecosystem. So, we can conclude that the concept of an educational ecosystem or university ecosystem is variably used in scientific literature. However, to consider the issue of designing an ecosystem of an open university in the future, we need to define the legislative background, single out the constitutional components of such an ecosystem, and describe the current state of readiness of the university considering available infrastructure and resources.

The analysis of scientific papers and research on the digital transformation of education, ecosystem design, open university, and approaches to improving the security of educational ecosystems provides a valuable basis for designing a secure, fault-tolerant, flexible open university ecosystem in the context of the digital transformation of society.

The main areas of cybersecurity in the open university ecosystem are focused on such key aspects as protecting the confidentiality of information, ensuring the integrity of the network and infrastructure, protecting personal data, and raising users' awareness of cybersecurity. Integrating cybersecurity principles into the open university ecosystem requires a comprehensive approach that covers all aspects of information security, from data protection to managing risks associated with interactions with external partners. An important aspect is the protection of confidential information stored at the university, in particular, students' personal data and academic records, which includes data encryption, compliance with privacy rules, data backup and recovery, and data loss prevention. Access control ensures that only authorized individuals have access to university systems and data using multi-factor authentication, role-based access control, single sign-on solutions, and privileged access management. Network and infrastructure security is ensured using firewalls, intrusion detection and prevention systems, and secure configuration of network devices, including protection against DDoS attacks and security of computers and mobile devices. A key element of ensuring cybersecurity is raising user awareness through training programs and policies for handling confidential information, which contributes to a culture of awareness of cyber threats.

In addition, the experience of creating various ecosystems was studied, but those related to university education and the digital transformation of education and society were highlighted: innovation, business, university, ICT entrepreneurship, artificial intelligence, digital solutions for education, open science, education, digital education, etc.

The results of the analysis of functioning ecosystems and the features of some of them are shown in Table 1.

Table 1
The analysis of functioning ecosystems

The name of the ecosystem	Proposed/implemented	Features of the ecosystem
Innovative ecosystem of Ukraine	Ministry of Education and Science of Ukraine	Experimental project on the creation based on institutions of higher education, scientific institutions of the Startup-school incubator accelerator network.
All-Ukrainian Innovation Ecosystem "Sikorsky Challenge Ukraine" (SCU)	National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"	Selection, attraction, and training of creative people to create their businesses and startups. Consists of Startup School "Sikorsky Challenge"; Business incubator "Sikorsky Challenge"; Innovative technological environment "Sikorsky Lab"; Center for Intellectual Property; Venture Fund "Sikorsky Challenge".
ICT entrepreneurial ecosystem	EU4Digital	Analysis of the current status of ICT entrepreneurial ecosystem performance. Diagnosis of the performance of the different ecosystem stakeholders: educators, investors, connectors, and facilitators by evaluating 19 indicators. Recommendations for further developing the ICT entrepreneurial ecosystem.
An ecosystem of digital solutions for education	"Institute of Education Content Modernization", Center Educational Consulting, Digital Development Academy LLC, Ed Pro Distribution LLC, Public organization "UkraineActive"	Modern services and tools; Digital Skills and competencies; electronic educational environment of the educational institution; digital transformation of the lesson.
The ecosystem of open science	Boiko A., Kramarenko O., Mayboroda T.	Open source; data/research reproducibility, research data management; open access to publications.
Future Learning Ecosystem	Ab Jalil H, Ismail IA, Ma'rof AM, Lim CL, Hassan N, Che Nawi NR	Characteristics of the educational ecosystem of the future: - Dependence on information and communication technologies.

		- Use of smart learning spaces. - Implementation of innovative pedagogical approaches. - Use of the latest developments, solutions, and technologies that will prepare students for real life. - Searches for new approaches to solving complex problems.
Digital ecosystem of national repositories of academic texts	Ukrainian Institute of Scientific and Technical Expertise and Information	Register of repositories of institutions of higher education and scientific institutions of Ukraine; Digital archives.
Digital education ecosystem	DIGI-HE project research, European Universities Association	Digitally enhanced learning and teaching.
Open access ecosystem	European Universities Association, DIAMAS project	Implementing open access as the default practice for communicating research results. Formation of a coherent high-quality and sustainable institutional ecosystem of open access.
Modern research ecosystem in the conditions of transformational changes	Elsevier	Key trends for librarians to support researchers: - Preprints and open science. - Cooperation in research. - Artificial intelligence technologies. - Changes in the financing system. - Maintaining a work-life balance.
Quantum Technology Education	The QTEdu Project	An educational ecosystem for informing society about quantum technologies.
UNESCO Digital Ecosystem	UNESCO	Structure: - Education - Natural sciences - Social and Human Sciences - Culture - Communication and Information - Ocean - Priority Africa - Priority Gender Equality.
Diamond Open Access ecosystem for scholarly communication	European University Association "Action Plan for Diamond Open Access"	Ensuring the sustainability of the Diamond Open Access scholarly communication ecosystem

The analysis has shown that there is no unified scheme or algorithm for an educational ecosystem design. The ecosystems described above have different structures, various features, and a wide spectrum of services and activities. However, there are common factors taken into account in the process of an educational and innovative ecosystem design. Among them, there are the goals of the organization, the needs of all stakeholders, defined target groups, technical, financial, and human resources that can be involved, the size of the ecosystem, etc.

According to the results of the study "Digital learning ecosystem at educational institutions: A content analysis of scholarly discourse" [32], which relates to the description of the concept of Digital learning ecosystem, four groups are defined, namely: digital learning ecosystem, digital education ecosystem, digital teaching and learning ecosystem. Other terms are classified as parts and are used more frequently (Fig. 2).

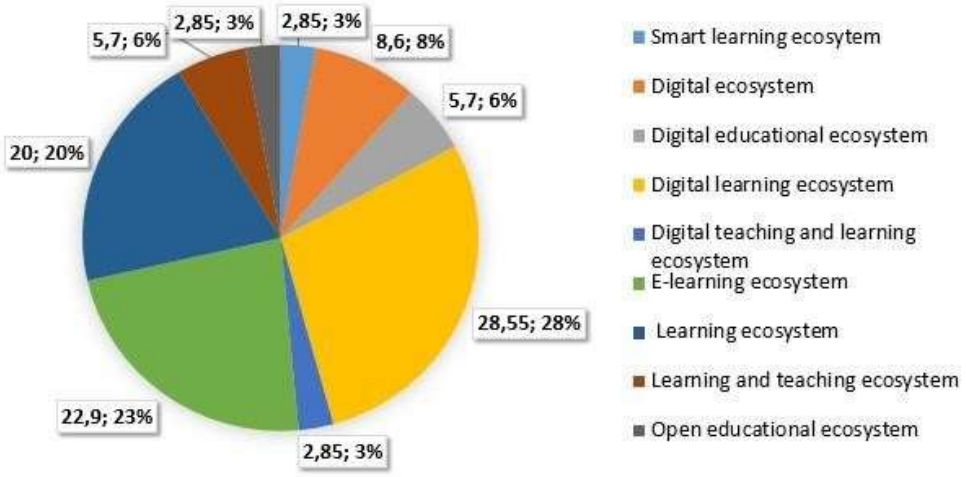

Figure 2: The ratio of the frequency of use of terms (based on research by scientists)

Education can gain a lot more opportunities by facilitating the links of the educational ecosystem, i.e. formal education with non-formal learning from stakeholders: business, politics, etc.

The maturity assessment methodology presented in the Final report of the project "Guide for building the ICT entrepreneurial ecosystems in the Eastern partner countries: Maturity analysis and recommendations" [33] can be adapted for educational and university ecosystems. The main approaches were developed by the results of interviews and consultations with stakeholders of the innovation community in the field of ICT in the Eastern partner countries: representatives of ministries, state institutions, and business support associations, including a wider community of local experts of the entrepreneurial ecosystem in the field of ICT, facilities technology development, education providers, investors, and others.

Digital transformation is affecting all areas of university life: teaching, research, and management, creating new opportunities, but at the same time posing complex challenges that require flexibility, innovation, and openness to change. Universities are facing the need to transform to meet the requirements of the digital era and remain competitive in the global market of educational services. Society wants an open, accessible, flexible, and efficient educational environment aimed at developing the competencies necessary for success in the 21st century and supported by a reliable, powerful IT infrastructure. At the same time, universities play an important role in the digital transformation of society, as they are actively working to provide affordable education, train highly qualified specialists, introduce and develop innovations, and promote lifelong learning. University science contributes to the development of advanced technologies, which, in turn, accelerates the digital transformation of the economy and society towards Economy 4.0 (Fig. 3).

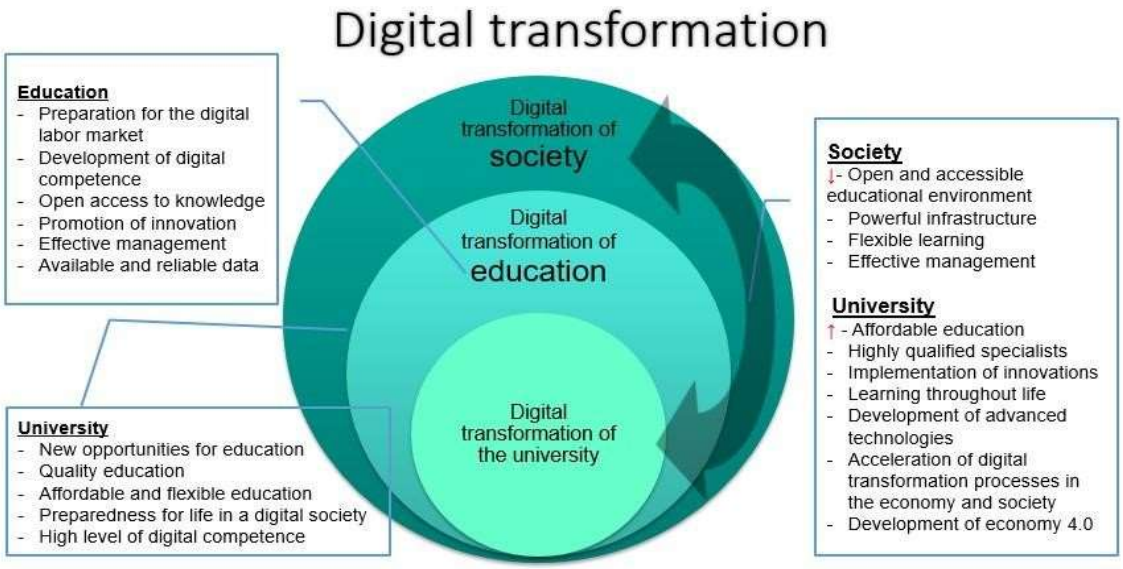

Figure 3: Digital transformation

Digital transformation involves the formation of a new model of functioning and activities of the university—an open university, a "university without walls", which will be the key to success in the next ten years. Realizing the full potential of digital transformation at a university often requires profound changes in the organizational structure, which allows for a more flexible and efficient system, and promotes collaboration, service expansion, and innovation. A prerequisite for meeting the diverse educational needs of modern society is the creation of an open university ecosystem based on the principles of openness and continuous learning.

4. Prerequisites for the creation of the Grinchenko University ecosystem in the conditions of digital transformation

According to the analysis, the process of forming an open university ecosystem in the context of digital transformation involves the formation of a new model of university functioning and activities and a change in the worldview of participants in the educational process. The nature and structure of universities should be hybrid. They should have open, both physical and virtual campuses that will work to interact with society, which will require an integrated system of physical and digital educational, scientific, and management environments to address the demands of the university community and offer versatile and blended methodologies. The traditional campus will remain essential as a hub for social engagement, concentrated learning, and research endeavors. Simultaneously, the virtual campus will extend the university's reach, making it accessible and fostering collaboration, while also pioneering inventive methods to advance the university's mission in research and education.

Borys Grinchenko Kyiv Metropolitan University has thorough studies, which include a formed information and educational environment, a Digital Campus, a System for the development of digital competence of teachers, a system

of ratings, etc. The information and educational environment introduced at the university is a convergence of digital, informational, and educational environments that provide participants in the educational process with free access to digital tools, and informational and educational resources and ensure effective communication and collaboration within the environment. The open information and educational environment of the university includes [34]:

- Platform for the management of training, scientific, and management activities, taking into account the standards.
- Personal digital environment of teachers.
- Personal digital environment of students.
- Communication and collaboration support systems.

To secure the open educational environment of Borys Grinchenko Kyiv Metropolitan University, the University's Cybersecurity Strategy was approved, with the priority areas being improving network protection, data security, and confidentiality, modernizing the remote desktop service for remote work, and creating a single service for managing educational and work processes.

To protect access to the university's open educational environment, a two-stage verification of corporate email accounts was introduced. To ensure secure external access to the university's internal network, we organized the use of a VPN, which provides a secure communication channel and reduces the risk of unauthorized access. Server OSes are updated to versions that support the latest security updates. Each site is equipped with a security certificate (SSL/TLS) that encrypts all transmitted data and protects the confidentiality of user information by creating an encrypted communication channel. The university uses both licensed and free software, choosing the best solutions for educational and scientific tasks. The training and content management systems are regularly updated to the latest versions to ensure their stable operation and compliance with modern requirements. Regular software updates are an integral part of a comprehensive approach to cybersecurity, as they allow us to quickly address identified vulnerabilities that can be used by cybercriminals to gain unauthorized access and compromise data confidentiality. To ensure the security and integrity of information, data is backed up, which ensures reliable data storage and quick access to it in the event of failures or loss of local data, reduces the risk of losing important information, and increases the level of security and data availability for users. Comprehensive protection of workstations and servers is provided by modern anti-virus software, which is constantly updated and includes modules for detecting and neutralizing various types of malware, which creates proactive protection against known and new threats.

An important component of the information and educational environment of Grinchenko University is the electronic learning system, which is constantly being developed and updated following the needs of participants in the educational process. For convenience, the personal digital environment of the teacher and the student, respectively, is organized, which contains all the necessary resources for organizing the educational process, including distance learning, a module for implementing the selective component of the educational program, and an additional block with useful digital tools. The student digital environment contains the study plan, the trajectory of personal development of competencies, the rating of success in each academic discipline and in general, the deadlines for the completion of tasks and their evaluation by the teacher, checking qualification papers for plagiarism, maintain academic integrity in the created university database of qualification papers with the integration of an anti-plagiarism service that checks for plagiarism on the Internet; built-in electronic communication tools among all participants of the educational process. In their digital environment, a student has the opportunity to get acquainted with the activities and ratings of teachers. The teacher's digital environment includes the possibilities of creating and developing electronic educational courses, describing and creating educational disciplines of the student's choice, working programs of educational disciplines, forming performance information, and drawing up and implementing an individual teacher's plan.

Electronic communication between the participants of the educational process is provided by corporate mail on Gmail and related Google services with two-step verification, which creates a reliable secure space for the exchange of educational materials and communication, significantly increases the level of protection against unauthorized access to accounts and prevents the disclosure of confidential information. To implement the program of openness developed an "E-portfolio", "Activity register database", "Institutional repository", a functioning Wiki, etc. [35] Grinchenko University's Internet portal, social network pages of the university and faculties, electronic scientific professional journals are functioning to present and popularize the university's activities on the Internet, informational support of the educational process of scientific, social and humanitarian, publishing activities, and international cooperation.

To display a complete picture of the activity of a teacher at Grinchenko University, the "E-portfolio" system has been developed, which allows not only to creation of an e-portfolio of a teacher but also for building rating tables of indicators for evaluating the main types of activities of each teacher and all departments to objectively analyze the quality of personnel ensuring professional activity and quality of higher education (Fig. 4).

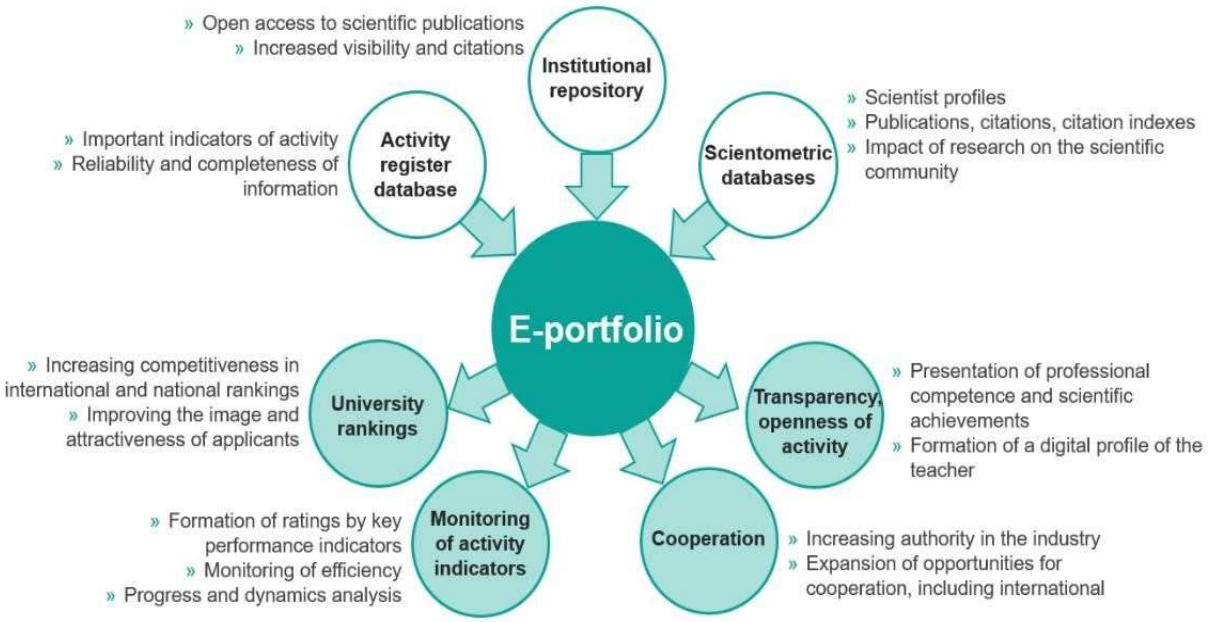

Figure 4: E-Portfolio System

A unified database of employees' professional performance indicators was created with the possibility of forming ratings for certain types of activities. To monitor the effectiveness of the scientific activity of teachers, a rating based on the indicators of research activity defined by corporate standards of scientific activity and digital competence—the Transparency Rating (Fig. 5)—has been introduced. The indicators of the publication activity of teachers (number of publications, citation, h-index, i10-index), in particular in influential scientometric databases, are taken into account in the methodologies of the most authoritative international and Ukrainian educational ratings.

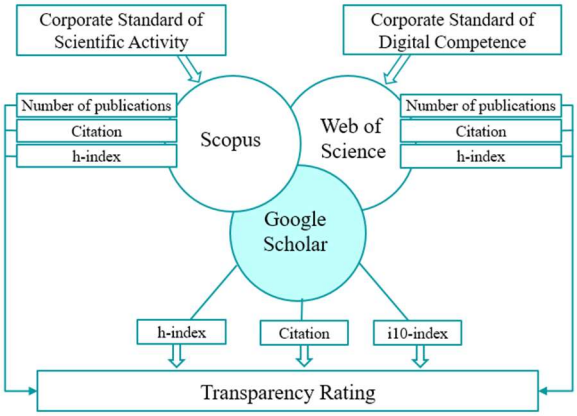

Figure 5: Scheme of Transparency Rating at Borys Grinchenko Kyiv Metropolitan University

The rating is based on the citation rates of scientific publications in the three most important scientometric databases—Scopus, Web of Science, Google Scholar and is a motivating factor for teachers to update their own e-portfolio profiles, create profiles in scientometric databases, in case of absence, update information in profiles, in particular Google Scholar, supplementing profiles with indexed publications, disseminating research results, discussing them in the international network scientific community, thus developing skills in the use of digital technologies in the organization of research and dissemination of research results [36].

All available digital resources of the university form an integral information infrastructure—the Digital Campus, which provides safe and convenient access to all necessary digital resources, protecting the personal data of users and ensuring uninterrupted operation of systems. Information resources in the Digital Campus are presented in the following categories (Fig. 6):

- Digital education
- Digital science
- Digital control
- Image and Leadership
- Digital space
- Infrastructure.

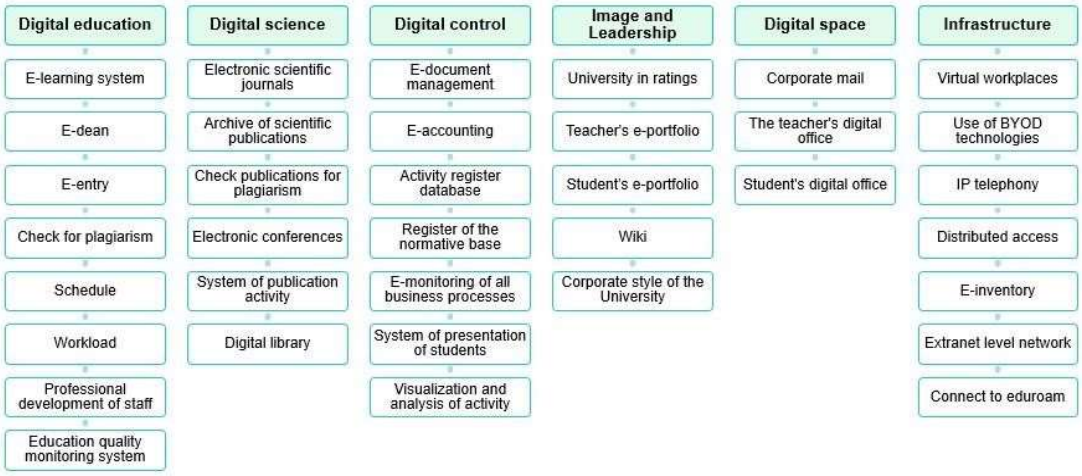

Figure 6: Digital Campus Components

Digital Campus is proven to provide sufficient support for all educational process participants. According to the survey of scientific and pedagogical staff members at Borys Grinchenko Kyiv Metropolitan University (https://forms.gle/DGiF8cg9tXcBhrYbA) aimed at studying current aspects of the university teachers' professional activities, 74,3% of the respondents estimate the Digital Campus as a very convenient digital environment. The level of sufficiency of resources in Digital Campus estimated as Excellent and Very Good by the university staff members reaches the following indicators: Digital education—95,7%; Digital science—87%; Digital control—80%; Image and leadership—87%; Digital space—92,8%; Infrastructure—84,3% (Fig. 7).

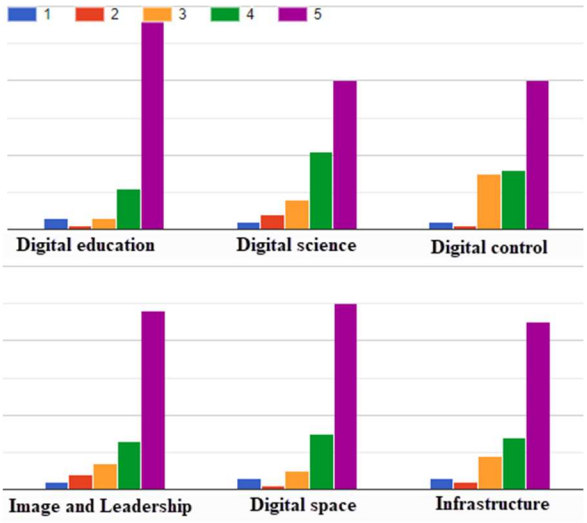

Figure 7: The level of resource sufficiency in Digital Campus

Although there is a high level of satisfaction with Digital Campus, there is room for development. Among the requests by research and teaching staff are the implementation of artificial intelligence and virtual reality, improvement of current research presentation on the university chairs/departments, strengthening of opportunities for research and conference activities presented in Digital Campus, and digital projects. This proves the need for the further development and expansion of the Digital campus and its integration with all the university resources including human, digital, and physical. In the future, there is a strategic vision of how the Digital Campus in the process of its development is transformed as a component of the open university ecosystem which is going to include human resources, systems, and equipment and ensure security, accessibility, sustainability, implementation of innovations, etc.

Therefore, we see the next important stage as the development of the already implemented and bringing it to a new stage—the stage of designing the open university ecosystem, which is a complex of interacting human and material resources, physical and virtual campuses, which ensures the development of the university as a system as a whole to achieve the strategic goals of the university's sustainable development, which is formed as a result of the synergy of education, science, innovation, the state, business, investors, academic community to create a value proposition, openness, transformability and transnationality, which corresponds to the vision "Universities without walls: vision for 2030" of the European Association of Universities [1], which member is also Grinchenko University. In the context of digital transformation, the design of the open university ecosystem should be based on an integrated approach to cybersecurity, considering the requirements for information security and data privacy. Ensuring a high level of information security is facilitated by the use of multi-level protection systems, such as data encryption, limited access to resources, information backup, and the introduction of modern cybersecurity tools such as antivirus programs, firewalls, intrusion detection and prevention systems (IDS/IPS), the implementation of a privacy policy that includes the use of data anonymization and minimization mechanisms, ensuring the rights of users to protect personal information following the requirements of the law.

An indicative model of the open university ecosystem is shown in Fig. 8.

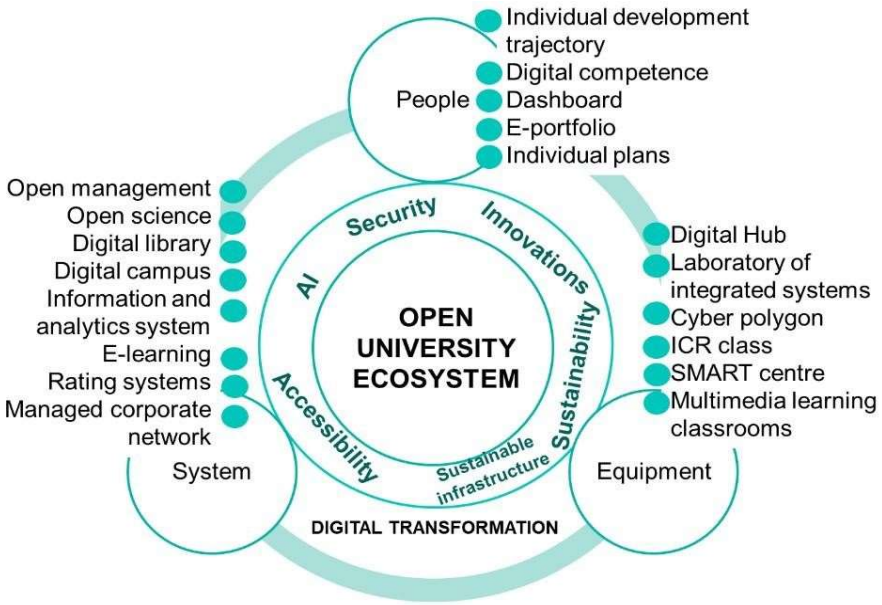

Figure 8: Open University Ecosystem Model

The open university ecosystem model involves the interaction of people, systems, and resources, and envisages the creation of a safe, innovative, sustainable, and integrated environment that actively uses the capabilities of artificial intelligence. It is expected that the system will be constantly evolving under the influence of digital transformation, while remaining secure and ensuring sustainable development, considering environmental, social, and economic aspects. The open university ecosystem is a dynamic structure that combines innovative solutions and advanced technologies to create an effective, safe, and accessible educational environment.

Human resources as a part of the ecosystem are addressed not only as people who provide the ecosystem operation but also as ecosystem development potential. That means the ecosystem must include both tools to ensure high-quality work of human resources and to give opportunities for professional development. Equipment refers to the physical resources of the ecosystem including infrastructure, networks, computer equipment, etc. The system includes all digital resources of the university ecosystem. In the process of open university ecosystem design the main features of its operation must be kept in focus: innovation, sustainability, accessibility, and security. Innovations are the driving force of ecosystem development. They imply technical resources, software, pedagogical approaches, and managerial solutions. In this context, AI should be mentioned as one of the most impactful technologies of today. The development of such technologies as AI would influence higher education and universities must learn how to manage it and get a use of it rather than ignore it. Sustainability includes the environmental, social, and economic dimensions of the open university ecosystem development. It ensures the long-term and cost-effective functioning of the ecosystem and its positive impact on all stakeholders, society, and the environment. Accessibility considers both physical and digital spaces of the university and provides equal opportunities for study and work for people with different abilities and backgrounds. Security refers to the physical security of campuses and all material resources and digital space security. Cybersecurity is one of the highest priority issues in the open university ecosystem design as it ensures personal information security, ecosystem information security, and the provision of a smooth educational process in the digital environment.

5. Conclusions

The strategic priorities for the digital transformation of higher education set out in European and national regulations include infrastructure development, technology integration, managerial digitalization, teacher competence and quality assurance, and the creation of a safe and open educational environment. The implementation of these priorities is key to improving the quality of education, the competitiveness of universities, and the readiness of students for the digital era, which will promote wider access to education, innovative teaching methods, active student participation, enhanced research opportunities, and a favorable environment for cooperation and innovation. Designing an open university ecosystem in the context of digital transformation requires an integrated approach to cybersecurity, constant monitoring, and adaptation to new threats. This involves not only the implementation of technical solutions but also the development of a cybersecurity culture among all participants in the educational process, the development of security policies, and regular training. Thus, key components such as security, innovation, sustainability and sustainable infrastructure, accessibility, and integration of artificial intelligence serve as the basis for the formation of an open university ecosystem.

After analyzing the experience of creating various ecosystems, including university ecosystems, which are formed in the context of educational transformation, the strengths, and demand for university ecosystems, the authors found the lack of a sustainable algorithm for designing a

university ecosystem, an unambiguous definition of concepts related to the process of designing ecosystems, variability in the use of names, different approaches to presenting the structure of the ecosystem, etc.

Digital transformation calls for the establishment of an open university ecosystem, which involves changes in organizational structure and educational paradigms. Borys Grinchenko Kyiv Metropolitan University uses the integration of physical and virtual campuses to improve collaboration and provide greater accessibility. A Digital Campus, a System for the development of digital competence of teachers, a system of ratings, an electronic learning system, information, and an educational environment will serve as a sufficient basis for the university's digital transformation and for building an open university ecosystem.

The cybersecurity of the open university ecosystem is a strategic priority that ensures the sustainability, innovation, and competitiveness of the university in the digital age. The protection of information resources, including academic data, research, and intellectual property, is the key to the successful functioning of a higher education institution and its reputation.

The current study is aimed at and limited to theoretical results. Given the feasibility and relevance of the study, it is planned to further substantiate and design the ecosystem, defining the principles and criteria for its success.

References

[1] Universities Without Walls—A Vision for 2030 (2021).

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

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

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

[5] Digital Education Action Plan (2021–2027). URL: https://education.ec.europa.eu/focus-topics/digital-education/action-plan

[6] Transforming Our World: The 2030 Agenda for Sustainable Development. URL: https://sdgs.un.org/2030agenda

[7] P. Skladannyi, et al., Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 97–106.

[8] H. Hulak, et al. Formation of Requirements for the Electronic RecordBook in Guaranteed Information Systems of Distance Learning, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, CPITS 2021, vol. 2923 (2021) 137–142.

[9] IAU Strategy (2022–2030). URL: https://www.iau-aiu.net/IMG/pdf/iau_strategy_2030.pdf

[10] On the Approval of the Strategy for the Development of Higher Education in Ukraine for 2022-2032. URL: https://www.kmu.gov.ua/npas/pro-shvalennya-strategiyi-rozvitku-vishchoyi-osviti-v-ukrayini-na-20222032-roki-286-

[11] National Plan for the Recovery of Ukraine: Education and Science. URL: https://mon.gov.ua/static-objects/mon/sites/1/gromadske-obgovorennya/2022/08/19/HO.proyekt.Planu.vidnovl.Osv.i.nauky-19.08.2022.pdf

[12] On the Approval of the National Plan for Open Science. URL: https://zakon.rada.gov.ua/laws/show/892-2022-%D1%80#Text

[13] Ukraine's Innovation Ecosystem Development. URL: https://drive.google.com/drive/folders/1BsqTijFWycOQUmUhZvbFmwZSUMT4HmlB

[14] V. Bykov, O. Spirin, O. Pinchuk, Modern Tasks of Digital Transformation of Education, UNESCO Chair Journal "Lifelong Professional Education in the XXI Century", 1 (2020) 27–36. doi: 10.35387/ucj.1(1).2020.27-36.

[15] T. Vakaliuk, et al., Digital Transformation of Higher Education: Foreign and Domestic Experience, Scientific Journal of the National Pedagogical Dragomanov University. Series 5: Pedagogical Sciences: Realities and Prospects, 90 (2022) 24–28. doi: 10.31392/NPU-nc.series5.2022.90.05.

[16] L. Cerda Suarez, K. Nunez-Valdes, S. Quiros y Alpera, A Systemic Perspective for Understanding Digital Transformation in Higher Education: Overview and Subregional Context in Latin America as Evidence, Sustainability 13 (2021) 12956. doi: 10.3390/su132312956.

[17] T. Kovaliuk, N. Kobets, The Concept of an Innovative Educational Ecosystem of Ukraine in the Context of the Approach "Education 4.0 for Industry 4.0", in: ICTERI-2021, Vol I: Main Conference, PhD Symposium, Posters and Demonstrations, vol. 3013 (2021) 106–120.

[18] M. Kyrychenko, et al., Open Distance Education for Teachers in Ukraine: the Case of the Ukrainian Open University of Postgraduate Education, CTE Workshop Proceedings, 11 (2024) 134–157. doi: 10.55056/cte.661.

[19] E. Mollakuqe, V. Dimitrova, Comparative Analysis of Identity Management, Access Control, and Authorization Practices in Public and Private Universities, Open Res. Europe 4(23) 2024. doi: 10.12688/openreseurope.16634.2.

[20] E. Abad-Segura, et al., Sustainable Management of Digital Transformation in Higher Education: Global Research Trends, Sustainability, 12(5) (2020) 2107.

[21] C. Tungpantong, P. Nilsook, P. Wannapiroon, A Conceptual Framework of Factors for Information Systems Success to Digital Transformation in Higher Education Institutions, in: 9th International Conference on Information and Education Technology (ICIET) (2021) 57–62.

[22] V. Dudykevych, et al., Platform for the Security of Cyber-Physical Systems and the IoT in the Intellectualization of Society, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3654 (2024) 449–457.
[23] H. Ab Jalil, et al., Predicting Learners' Agility and Readiness for Future Learning Ecosystem, Education Sciences, 12 (2022) 680. doi: 10.3390/educsci12100680.
[24] K. Mahon, H. Heikkinen, R. Huttunen, Critical Educational Praxis in University Ecosystems: Enablers and Constraints, Pedagogy, Culture & Society, 27(3) (2019) 463–480. doi: 10.1080/14681366.2018.1522663.
[25] M. Firat, Towards a Unified Open Education Ecosystem through Generative AI, Blockchain, DAO, MMLA and NFT, OSF Preprints (2023). doi: 10.31219/osf.io/rkpt4.
[26] A. Piazza, S. Vasudevan, M. Carr, Cybersecurity in UK Universities: Mapping (or Managing) Threat Intelligence Sharing within the Higher Education Sector, Journal of Cybersecurity, 9(1) (2023). doi: 10.1093/cybsec/tyad019.
[27] H. Dei, et al., Legal Challenges and Perspectives of Cybersecurity in the System of State Governance of Educational Institutions in Ukraine, Journal of Cyber Security and Mobility, 13(5) (2024) 963–982. doi: 10.13052/jcsm2245-1439.1357.
[28] P. Anakhov, et al., Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 240–245.
[29] K. Kepuska, M. Tomasevic, A Lightweight Framework for Cyber Risk Management in Western Balkan Higher Education Institutions, PeerJ Computer Science (2024). doi: 10.7717/peerj-cs.1958.
[30] D. Sheng, Y. Wang, Design of Innovation and Entrepreneurship Education Ecosystem in Universities based on User Experience, Mathematical Problems in Engineering, (2022) 1–9. doi: 10.1155/2022/3266326.
[31] S. Cwik, C. Singh, Developing an Innovative Sustainable Science Education Ecosystem: Lessons from Negative Impacts of Inequitable and Non-Inclusive Learning Environments, Sustainability, 14(18) (2022) 11345. doi: 10.3390/su141811345.
[32] L. Nguyen, K. Tuamsuk, Digital Learning Ecosystem at Educational Institutions: A Content Analysis of Scholarly Discourse, Cogent Education, 9 (2022) 2111033. doi: 10.1080/2331186X.2022.2111033.
[33] Guide for Building the ICT Entrepreneurial Ecosystems in the Eastern Partner Countries: Maturity Analysis and Recommendations. URL: https://eufordigital.eu/library/guide-for-building-the-ict-entrepreneurial-ecosystems-in-the-eastern-partner-countries-maturity-analysis-and-recommendations/
[34] O. Buinytska, The System of Pedagogical Design of Information and Educational Environment for the Training of Future Social Educators: Monograph, Borys Grinchenko Kyiv University (2021). URL: https://elibrary.kubg.edu.ua/id/eprint/39617/
[35] O. Buinytska, L. Varchenko-Trotsenko, B. Hrytseliak, Digitization of Higher Education Institution, Educological discourse, 1(28) (2020) 64–79. doi: 10.28925/2312-5829.2020.1.6.
[36] N. Morze, O. Buinytska, V. Smirnova, Designing a Rating System based on Competencies for the Analysis of the University Teachers' Research Activities, in: Cloud Technologies in Education, vol. 3085 (2022) 139–153.