Edukacja zawodowa i ustawiczna. № 8, 2023. С. 93-107

Larysa Petrenko

ORCID ID: 0000-0002-7604-7273

DIGITAL SECURITY IN THE PROFESSIONAL ACTIVITIES OF FUTURE TEACHER OF A HIGHER EDUCATION PEDAGOGICAL INSTITUTION IN THE REALITIES OF THE MARTIAL LAW

Introduction. Access to the Internet is a fundamental right of every person, in particular, of the participants of educational process, and the use of this open free space, in which the exchange of ideas, information and knowledge, social interaction and communication of people takes place, remains unrestricted. In the context of the digital transformation of society, the scope of threats has expanded significantly and new challenges have grown, that require adapted and innovative responses. In this regard and awareness of the profound changes caused by the transition to digital technologies, the convergence and globalization of computer networks, which continues, the member states of the Council of Europe and other states signed the Convention on Cybercrime in 2001, which was ratified by the Verkhovna Rada of Ukraine in 2005 (Cybercrime Convention, 2001).

Since then, the number of cyberattacks has continued to grow; they are becoming increasingly sophisticated and coming from a wide range of sources. In this regard, the EU has developed and adopted a Cybersecurity Strategy aimed at increasing resistance to cyberthreats and ensuring that citizens and businesses benefit from reliable digital technologies. This document divides responsibility for ensuring a cybersecure digital transformation between governments, businesses and citizens.

The European Declaration on Digital Rights and Principles for the Digital Decade (The European Declaration on Digital Rights and Principles for the Digital Decade, 2022) emphasizes that digital transformation affects all aspects of people's

lives - expanding opportunities to improve the quality of their lives, introducing innovations, significant economic growth and sustainability. It also formulated new tasks for the structure, security and stability of national societies and economies. The main purpose of the mentioned Declaration on Digital Rights and Principles of the Digital Decade is to clarify (determine the rules) regarding the observance of European values and basic human rights in the online world (Europe's Digital Decade: Digital Targets for 2030, 2021).

In response to the Russian Federation's application of hybrid warfare technologies, the National Security and Defense Council of Ukraine decided in January 2016 to approve the draft Cybersecurity Strategy of Ukraine. Its main goal is "to create conditions for the safe functioning of cyberspace, its application in the interests of the individual, society and the state" (About the Cybersecurity Strategy of Ukraine, 2016).

The Information Security Doctrine of Ukraine was adopted in order to counter threats aimed at the consciousness of citizens, incitement of national and religious enmity, propaganda of aggressive war, change of the constitutional order by violent means, violation of sovereignty and territorial integrity, which turned the information sphere into a key arena of confrontation. One of the priorities of the state policy in the information sphere is defined as "increasing the media literacy of society by promoting the training of professional personnel for the media sphere with a high level of competence" (About the Information Security Doctrine of Ukraine, 2016).

New challenges (the development of information technologies and their convergence with artificial intelligence technologies; the recognition of cyberspace, together with other physical spaces, as one of the possible theaters of war; the destructive activity of the Russian Federation - committing acts of cyberterrorism and cybersabotage against the national information infrastructure; the increase in the intensity of interstate confrontation and intelligence subversive activities in cyberspace; constant improvement and development of new tools and mechanisms for the implementation of cyberthreats; strengthening of the tendency

to use cyberattacks as a tool for special information operations, manipulation of public opinion, influence on the processes of elections; transition to 5G networks, which functioning fundamentally depends on the correct operation of software, and due to the novelty of this technology, may undergo through new, unforeseen threats; the COVID-19 pandemic, which will obviously have a long-term impact on the world order, strengthening the role of electronic communications in everyday communication and work, that increases the degree of vulnerability of information processing processes, in particular, personal data, etc.) and the rapidly changing digital world led to "the formation of a more balanced and effective national cybersecurity system that can flexibly adapt to changes in the security environment, guaranteeing the safe functioning of the national segment of cyberspace to the citizens of Ukraine, foreseeing the new opportunities for digitalization of all spheres of public life" (About the Strategy of Cybersecurity of Ukraine, 2021).

Among the priorities of national interests, outlined in the Cybersecurity Strategy of Ukraine (2021), attention should be focused on "creating conditions for the safe functioning of cyberspace, its implementation for the interests of the individual, society and the state" (About the Cybersecurity Strategy of Ukraine, 2021). This document envisages "the involvement of a wide range of participants in solving tasks in the field of cyber security, including economic entities, public associations and individual citizens of Ukraine. It is planned to develop a National Cyberliteracy Program. It should be aimed at increasing the level of digital literacy of the population of Ukraine, in particular, by including questions to the curricula of general secondary, professional (vocational and technical), professional pre-higher and higher education" on the formation of digital skills, cyberawareness of modern cyberthreats and countering them (About the Strategy cyber security of Ukraine, 2021). The main provisions of this document are specified in the Implementation Plan of the Cybersecurity Strategy of Ukraine, approved on December 30, 2022 (About the Implementation Plan of the Cybersecurity Strategy of Ukraine, 2021).

Therefore, the relevance of the formation of digital security skills of all citizens, including future teachers of pedagogical higher education institutions in the process of professional training, is substantiated in a number of documents adopted both in the EU and at the state level in Ukraine.

A comprehensive systemic strategic vision of the digital transformation of the sphere of education and science, which corresponds to the principles of implementation by the executive authorities of the principles of the state policy of digital development, is outlined in the draft Concept of Digital Transformation of Education and Science for the period until 2026. Unfortunately, in connection with the large-scale Russian aggression in Ukraine, the mentioned document was never adopted at the state level and is currently at the stage of public discussion.

As M. Fedorov noted, "from the night to the morning of February 24, 2022, there was an attack on the basic information resources of Ukraine" on such a scale that no country in the world has experienced. Teams of specialists defended cyberspace all night. Owing to their continuous work, the information systems of the Ukrainian infrastructure survived (Fedorov, 2022).

As a result of the military actions, the universities displaced from the occupied territories faced the problem of maintaining databases, lack of technical resources, establishing a safe information and educational space for the renewal of the educational process. Therefore, "the servers that contained library information resources, materials for distance learning, documentation of the educational process, etc., remained in the temporarily occupied territory" (Nikolayev, Riy, Shemelinets, 2022). The solution of the mentioned problems took place by using the computer capacities of universities that accepted higher education institutions displaced from the occupied territories on their premises, or by contacting third-party organizations for the provision of such services. For example, the EPAM company provided an opportunity to transfer information to cloud services, owing to which conditions were created for the full use of platforms for the organization of distance learning.

However, this problem has been solved only partially. A wide range of security issues, the quality of the Internet and communication remain unresolved for students and teachers who could not leave the temporarily occupied territories. Some of the students, teachers, and other employees of higher education establishments found themselves outside of Ukraine. Many have had difficulties with providing computer equipment to perform current organizational work. Therefore, the complex of these problems actualized the need to study the issue of digital security in the professional activity of a future teacher of pedagogical institution of higher education in the realities of martial law.

This problem was reflected in the dissertations of domestic scientists. For the period 2000-2023, in the database of the National Repository of Academic Texts (NRAT) under the key term “digital security”, 2 documents (2021) were found, which highlighted the results of the study of the information security management of the enterprise in the conditions of digital transformation (O. Urdenko) and economic security of business activity in the conditions of the development of digital activity (O. Onofriychuk). Therefore, there are currently no completed studies on the problems of formation (development) of digital security skills (competencies) among future specialists, in particular teachers of pedagogical higher education, in the national dissertations database.

At the same time, the results of research on the problem of information security are highlighted in 142 dissertations, among which it is necessary to highlight those made in the field of knowledge 01 Education/Pedagogy. These are: the scientific works of S. Voskoboinikov (2016), which developed and experimentally tested pedagogical conditions for the formation of professional readiness of future information security specialists for the protection of information with limited access; Yu. Ivanchuk (2013), who investigated the issue of the formation of professionally significant qualities in future information security specialists in the process of studying scientific and natural disciplines; M. Koliada (2012), which scientifically substantiates the theoretical and methodological foundations of the professional training of future specialists in

information protection and information security management. The result of the study by L. Konoplenko (2016) was a method of teaching oral English communication by using a business game of future information security specialists, and in the dissertation of O. Synekop (2011) - a method of interactive teaching of English written communication of future information security specialists using computer technologies. V. Kovalchuk (2012) studied the problem of ensuring information security of high school students in a computer-oriented educational environment. Thus, the topic of digital security in the professional activities of future teachers of pedagogical institutions of higher education remains outside the attention of domestic scientists.

According to OUCI (Open Ukrainian Citation Index), the term “digital security” is used by researchers in 9 journal publications. Thus, V. Bondarenko (2019) presented the results of a study of the conditions and means of forming information security skills of future teachers; O. Budnyk (2020) outlines positions important for the digital literacy of the teacher in the context of security in the digital society. H. Henseruk (2021), L. Kanishevska (2022), V. Plaksienko (2020), L. Sultanova (2022) study digital security within the framework of digital competence. A set of different types of resources and services of the hybrid cloud-oriented environment of the university, that are important to use for the effective training of future economists, in particular, services for digital security, is considered in the scientific work of O. Hlazunov. The publication by M. Drushliak presents infomedia literacy and its characteristics through a set of markers: critical thinking, resistance to influences, fact-checking, digital security, the ability to prevent risks in communication, etc. T. Yermak substantiates the list of students’ leadership skills, which includes digital literacy and security.

The scientific interests of foreign scientists in the study of digital security are also quite different. When studying scientific works in the unified bibliographic and reference database of scientific literature Scopus, we singled out the following works: S. Schinagl, A. Shahim, S. Khapova (2022) on a dual approach to digital security management; G. D. R. Castro, M. C. G. Fernandez, Á. U. Colsa (2021)

regarding the interaction between digitalization and sustainability, which opens up wide opportunities for the development of the economy and society in achieving the sustainable development goals. Pathways to the development of professional digital competence through transformational agencies are revealed by L. M. Brevik, G. B. Gudmundsdottir, A. Lund, T. A. Strømme (2019); features of digital security in Estonia were studied by A. K. Saleh, A. D. S. Yuliana, G. W. Pramudian. F. A. Ghauri paid attention to the study of the problem of private digital security. The human factors on digital security are in the spotlight of Avijit Dutta (2021) and others.

The purpose of the study is to determine the essence of the digital competence of the future teacher of a pedagogical institution of higher education and outline the content of digital security in their professional activities.

Presentation of the main research material. The full-scale war in Ukraine unleashed by Russia became the loudest event in 2022, which affected all economic sectors and people's daily life. The field of education was no exception. Today, the scientific-pedagogical teams of pedagogical institutions of higher education (PHEE) have to search for answers and those challenges that faced the national education system in extreme conditions: mass forced migration; destroyed infrastructure; data storage; unfinished programs and reforms; COVID-19; unequal opportunities in communities and regions; the advent of Industrial 4.0, etc.

However, the started war of the aggressor country against the Ukrainian people cannot stop reforms in the field of higher education. In this incredibly difficult wartime, the efforts of scientific and scientific-pedagogical staff is aimed at solving such urgent issues as: formation of high-quality human capital; training of innovative specialists with developed critical thinking, inner freedom, ability to be creative, willingness to learn throughout life. In digital society, these qualities and the formed digital competence of a teacher of vocational education and training are an indispensable condition for the successful development of his or her professional and scientific career.

Organization of the educational process for the training of specialists in modern digital educational environment, integration into the European space of higher education and the European research space, interaction with scientists of different countries within the framework of research projects, require scientific and pedagogical staff to possess a wide range of new professional competencies. The target and content guidelines for the development of digital competencies of a teacher are reflected in a number of international and domestic documents that provide a development strategy and normative regulation of the educational environment based on digital technologies (Vuorikari, Punie, Carretero, Brande, 2016; Description of the Framework of Digital Competence for Citizens of Ukraine, 2021; Draft Plan for the Recovery of Ukraine, 2022; On the approval of the Strategy for the Development of Higher Education for 2022-2032, 2022).

In the context of the adopted normative documents, the digital competence of scientific and pedagogical staff can be interpreted as a meaningful application of digital skills, including technological, technical, social, organizational skills, as well as ethical values in the context of educational activities or professional and personal development, performance of functional duties. It should be emphasized that digital competence is included in a number of key competences (Vuorikari, Punie, Carretero, Brande, 2016), and is related to all types of literacy and is often used as a synonym for the concept of "digital literacy".

Based on the analysis and generalization of 15 frameworks of digital competences of education staff adopted in different countries, A. Ferrari notes: "Digital competence is a set of knowledge, skills, attitudes, abilities, strategies and awareness that are necessary when using ICT and digital media to perform tasks; problem solving; communication; information management; cooperation; creating and sharing content; accumulation of knowledge for effective and autonomous work and leisure, as well as effective participation in meaningful learning and relevant, critical, flexible and ethical communication" (Ferrari, 2012, p. 29). The need for a modern person to possess the digital competence "for personal fulfillment and development, employment, social inclusion and active citizenship"

is emphasized in the recommendations of the European Commission on lifelong learning (European Commission, 2018).

The issue of developing the content and structure of digital competence and digital culture of pedagogical staff is highlighted in scientific works, in particular: N. Morze, O. Bazeliuk, I Vorotnykova and others (2019). According to the results of the study of these modern socio-cultural phenomena, the authors indicate the need for constant improvement of the ability to navigate the large volumes of information, which today is a requirement for specialists in any field, in particular for teachers of vocational education and training. A set of studies, conducted by the scientists of the Institute of Digital Technologies of the National Academy of Pedagogical Sciences of Ukraine for the period from 2018 to 2020, was dedicated to the problem of digitalization of education and the development of digital competences among the subjects of the educational process, the summarized results of which were highlighted by V. Bykov in a scientific report. The scientist drew attention to the complex nature of the formed digital competencies of participants in the educational process (Bykov, 2021).

There are different concepts of the development of a teacher's professional digital competence in European countries and, accordingly, different approaches to determining the level of their formation. Thus, scientists A. Cattaneo (A. Cattaneo), C. Antonietti (C. Antonietti) and M. Rauseo (M. Rauseo) attribute the concept of "digital competence" to complex concepts, which gradually replaced the term "digital literacy" and developed into the "historically linked stratified transversal and multidimensional concept" (Cattaneo, Antonietti, & Rauseo, 2022) according to which digital competence, from the point of view of different researchers, can reflect the interaction of a different number of components, in particular, technological, ethical and cognitive or other (Cattaneo, Antonietti, & Rauseo, 2022.). It should be noted, that this point of view reflects the modern competence paradigm of education, but it is different from the point of view of L. Havrilova (2017), who believes that "digital literacy" is more complex concept. Therefore, in the scientific pedagogical literature there is a discrepancy regarding

the essence of the concepts “digital competence” and “digital literacy”, which indicates the need for their further research.

In conclusion, we note that the digital competence of a teacher of higher vocational education institution should be understood as his ability to meaningfully applied digital skills, including technological, technical, social and organizational skills necessary when using ICT and digital media in order to: perform tasks; problem solving; communication; information management; cooperation; creating and sharing content; accumulation of knowledge for effective and autonomous work, adherence to ethical values in the context of educational activities or professional and personal development and performance of functional duties.

The use of modern digital technologies changes the nature of the teachers’ professional activity and puts new demands on them. Continuous improvement of digital competence becomes the norm of everyday life and its improvement is a condition for professional growth of those who will provide professional training for future specialists and those who will teach new generations of teachers of the New Ukrainian School (Petrenko, 2013). In their professional activities, they will deal with large volumes of information. IT technologies will reveal the new opportunities in organization of research activities in the scientific and methodological work. Moreover, they will create conditions for constant access to electronic educational resources that will provide an opportunity to improve analytical knowledge and skills in practice, expand communication channels for exchanging information with colleagues and scientists from different countries of the world (Petrenko, Shevchenko, Zelikovska, 2020).

However, rapid digitalization poses threats to the field of education. Currently, scientists consider information security in two aspects - technical and technological and socio-humanitarian (Kudlai, 2015). From the point of view of V. Kudlai, the technical and technological aspect of information security reflects the ability of an individual to use information protection programs, awareness of the danger of saving information from the network, etc. The socio-humanitarian sphere of danger is associated with non-compliance with norms of behavior in the

Internet: posting (searching) compromising information, hating (negative comments and messages, irrational criticism of another person) in social networks, social groups and comments. To this should be added sexting, flaming, griffing, cyberbullying, etc. as separate types of cyberviolence (Educational Marker, 2020). From the point of view of A. Nashynets-Naumova, who studies the issue of information security in the context of legal protection, methods of information protection "can be divided into two groups: organizational and technical. Organizational methods provide for the restriction of "possible unauthorized physical access to information systems", and technical methods "presuppose the use of software and technical means aimed, first of all, at limiting the access for the user, who works with the information systems of the enterprise to the information, that he or her has no right to access" (Nashynets-Naumova, 2012).

Defining the content of the concept "digital security" requires a detailed analysis. V. Bondarenko points out its ambiguity and prefers the term "information security", arguing this with a broader definition of the essence, which reflects "the state of protection of the vital interests of an individual, in which harm is not allowed due to: incompleteness, untimeliness and implausibility of information that is used; negative information impact; negative consequences of the use of information technologies; unauthorized distribution, use and violation of the integrity, confidentiality and availability of information (Bondarenko, 2019, p. 298). Such a point of view is quite legitimate, as it is based on the results of other scientific studies of domestic scientists. But the scientific works of O. Urdenko (2021) and O. Onofriychuk (2021), which were found in the National Repository under the keywords "digital security", also talk about the information security of enterprises and business activities in the conditions of digital transformation. We suppose, that it is the definition of terms in the topic of dissertation that can be explained by the authors' introduction of the definition of "digital security" to the key concepts, which, it is worth noting, remained unformulated by the named authors.

Therefore, there are reasons to believe that digital security differs from information security in technological features of information processing in digital form when its institutional transformation takes place, but the socio-humanitarian and organizational aspects remain similar.

Conclusions. In the context of the digital transformation of society, the threat landscape is constantly expanding and new challenges are emerging that require adapted and innovative responses. In this regard, the EU has developed and adopted a number of documents aimed at increasing resistance to cyberthreats and ensuring that citizens and businesses benefit from reliable digital technologies. This document divides responsibility for ensuring a cybersecure digital transformation between governments, businesses and citizens. In Ukraine, which during the war is subject to constant cyberattacks on basic information resources, a regulatory and legal framework is also being formed for the safe functioning of cyberspace, its use in the interests of the individual, society and the state, in particular, it is envisaged to involve a wide range of participants in solving tasks in the field of cybersecurity.

The author defined the essence of the concept of "digital security of the future teacher of a pedagogical institution of higher education" as the ability to meaningfully apply digital skills, including technological, technical, social, organizational skills, necessary when using ICT and digital media for: performing tasks; problem-solving; communication; information management; cooperation; creating and sharing content; accumulation of knowledge for effective and autonomous work, adherence to ethical values in the context of educational activities or professional and personal development and performance of functional duties. Based on the study of various aspects (technological, socio-humanitarian, organizational) of information security, its difference from the digital security of the future teacher of a pedagogical institution of higher education was revealed. It consists in the technical and technological features of information processing in digital form when its institutional transformation takes place, but the socio-humanitarian and organizational aspects remain similar. It was found that the

content of digital security of the future teacher of a pedagogical institution of higher education is complex and is considered by scientists as a multidimensional concept, since it can reflect the interaction between different set of components: cognitive, organizational, technical, technological, ethical, value, etc.

Abstract. The essence of the concept of "digital security of the future teacher of a pedagogical institution of higher education" is defined as the ability to meaningfully apply digital skills, including technological, technical, social, organizational skills, necessary when using ICT and digital media for: performing tasks; problem-solving; communication; information management; cooperation; creating and sharing content; accumulation of knowledge for effective and autonomous work, adherence to ethical values in the context of educational activities or professional and personal development, performance of functional duties. The difference between information security and digital security of the future teacher of a pedagogical institution of higher education, which consists in the technical and technological features of information processing in digital form when its institutional transformation occurs, but the socio-humanitarian and organizational aspects and remain similar, is revealed. It was found that the content of digital security of the future teacher of a pedagogical institution of higher education is complex and is considered by scientists as a multidimensional concept, since it can reflect the interaction of a different number of components: cognitive, organizational, technical, technological, ethical, value, etc.

Keywords. Digital security, information security, teacher, pedagogical institution of higher education, martial law.

Bibliography

1. Bondarenko B. I. (2019). Conditions and tools for developing future teachers' information safety skills. *Information Technologies and Learning Tools, 74*(6), 294–306. https://doi.org/10.33407/itlt.v74i6.2550.

2. Bykov, V. (2021). Developing the educational process participants' competencies on the basis of cloud-oriented information and educational systems: Scientific report at the meeting of

the Presidium of the National Academy of Educational Sciences of Ukraine, March 18, 2021. *Herald of the National Academy of Educational Sciences of Ukraine*, *3*(1), 1-6. https://doi.org/10.37472/2707-305X-2021-3-1-2-3.

3. Cattaneo, A. A., Antonietti, C., & Rauseo, M. (2022). How digitalised are vocational teachers? Assessing digital competence in vocational education and looking at its underlying factors. *Computers & Education*, *176*, 104358. Взято з: https://doi.org/10.1016/j.compedu.2021.104358.

4. Drushlyak M. H., Semenog O. M., Hrona N. V., Ponomarenko N. P., and Semenikhina O. B., «Typology of internet resources for the development of youth's infomedia literacy», *ITLT*, vol. 88, no. 2, pp. 1–22, Apr. 2022.

5. Europe's Digital Decade: digital targets for 2030. Взято з: Europe's Digital Decade: digital targets for 2030 (europa.eu).

6. European Commission. Proposal for a Council Recommendation on Key Competences for Lifelong Learning. Brussels, 17.1.2018. Взято з: resource.html (europa.eu).

7. Glazunova O. H., Sayapina T. P., Kasatkina . O. M., Korolchuk V. I., & Voloshyna T. V. (2021). Formation of digital security skills of future specialists in economics. *Information Technologies and Learning Tools*, *82*(2), 93–108. https://doi.org/10.33407/itlt.v82i2.4308.

8. Havrilova, L. H., & Topolnik, Y. V. (2017). Digital culture, digital literacy, digital competence as the modern educational phenomena. *Information Technologies and Learning Tools*, *61*(5), 1–14. https://doi.org/10.33407/itlt.v61i5.1744.

9. Joint Research Centre, Institute for Prospective Technological Studies, Ferrari, A. (2012). *Digital competence in practice : an analysis of frameworks*, Publications Office. https://data.europa.eu/doi/10.2791/82116.

10. Kanishevska, L. (2022). Scientific and practical implementation of digitalisation of the educational process in modern conditions: Scientific report to the general meeting of the National Academy of Educational Sciences of Ukraine "Scientific and Methodological Support for the Digitalisation of Education in Ukraine: State, Problems, Prospects", November 18-19, 2022. *Herald of the National Academy of Educational Sciences of Ukraine*, *4*(2), 1-6. https://doi.org/10.37472/v.naes.2022.4224

11. Kremen, V., Sysoieva, S., Bekh, I., Voznesenska, O., Havrysh, N., Honchar, L., Zhurba, K., Ilin, V., Kanishevska, L., Kyrychenko, V., Komarovska, O., Korniienko, A., Kunytsia, T., Kurbatov, S., Lytovchenko, O., Malynoshevskyi, R., Machuskyi, V., Naidonova, L., Reipolska, O., Tolochko, S., Fedorchenko, T., Kharchenko, N., Chaplinska, Y., & Shakhrai, V. (2022). The concept of education of children and youth in the digital space. *Herald of the National Academy of Educational Sciences of Ukraine*, *4*(2), 1-30. https://doi.org/10.37472/v.naes.2022.4206

12. Morze, N., Bazeliuk, O., Vorotnikova, I., Dementiievska, N., Zakhar, O., Nanaieva, T., Pasichnyk, O., & Chernikova, L. (2019). Description of educator's digital competence. *Electronic Scientific Professional Journal "Open educational e-environment of modern university"*, 1-53. https://doi.org/10.28925/2414-0325.2019s39

13. Petrenko L. M., Shevchenko V. P., & Zelikovska O. O. (2020). Leveraging crowd-based technologies for education in it-students professional training. *Information Technologies and Learning Tools*, *76*(2), 213–235. https://doi.org/10.33407/itlt.v76i2.3378

14. Stef Schinagl, Abbas Shahim, Svetlana Khapova (2022). Paradoxical tensions in the implementation of digital security governance: Toward an ambidextrous approach to governing digital security. *Computers & Security*, 122, 102903.

15. Sultanova, L., & Prokofieva , M. (2022). Digital security in higher education. *Adult education: theory, experience, prospects*, *21*(1), 106-117. https://doi.org/10.35387/od.1(21).2022.106-117

16. Vuorikari R, Punie Y, Carretero Gomez S. and Van Den Brande G. DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model. EUR 27948 EN. Luxembourg (Luxembourg): Publications Office of the European Union; 2016. JRC101254

17. Diia. Digital Education. National online platform for developing digital literacy. Дія. Цифрова Освіта (diia.gov.ua)).

18. Cybercrime Convention. Verkhovna Rada of Ukraine. Document 994_575 (valid), current edition, ratified on 07.09.2005. Main source: Конвенція про кіберзлочинність | від 23.11.2001 (rada.gov.ua)

19. Kudlai V. O. (2015). Digital competence of the individual in the context of development of information society. *Bulletin of Mariupol State University*. 10, 97-104.

20. Nashynets-Naumova A. Yu. (2012). The issue of insuring the information security of the enterprise. *Juridical Bulletin*, # 3(24), 58-62.

21. Nikolayev Ye., Riy H., Shemelynets I. Within the foreign walls: how displaced universities overcome problems. Vox Ukraine. July 12, 2022. Main source: У чужих стінах: як долають проблеми переміщені університети (voxukraine.org)

22. Onofriychuk O. P. (2021). Economic security of business activity in conditions of the development of the digital economy : diss., Candidate of Economic Sciences : (2021). Academician Stepan Demianchuk International University of Economics and Humanities, Rivne, 252.

23. Description of the framework of digital competence for the citizens of Ukraine. Main source: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/3/mintsifra-oprilyudnyue-

ramku-tsifrovoi-kompetentnosti-dlya-gromadyan/%D0%9E%D0%A0%20%D0%A6%D0%9A.pdf.

24. Educational Marker. Main source: (10) Facebook.

25. Petrenko L. M. (2013). Training of the Head of Vocational Educational Institution for Analytic Activities: an Innovative Approach. *Science and Education*. 3, 124–128.

26. On the implementation plan of the Cybersecurity Strategy of Ukraine. Resolution of the National Security and Defense Council of Ukraine, dated December 30, 2021. Main source: Про План реалізації Стратегії кібербез... | від 30.12.2021 (rada.gov.ua).

27. On the Resolution of the National Security and Defense Council of Ukraine, dated May 14, 2021 “On the Cybersecurity Strategy of Ukraine”. Decree of the President of Ukraine No. 447/2021. Main source: Про рішення Ради національн... | від 26.08.2021 № 447/2021 (rada.gov.ua)

28. On the Resolution of the National Security and Defense Council of Ukraine, dated May 14, 2021 “On the Cybersecurity Strategy of Ukraine”. Decree of the President of Ukraine No. 96/216. Main source: УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №96/2016 — Офіційне інтернет-представництво Президента України (president.gov.ua)

29. On the Decision of the National Security and Defense Council of Ukraine dated December 29, 2016 “On the National Security Doctrine of Ukraine”. Decree of the President of Ukraine No. 47/217. Main source: УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №47/2017 — Офіційне інтернет-представництво Президента України (president.gov.ua)

30. On the approval of the Higher Education Development Strategy for 2022-2032 Decree of the Cabinet of Ministers of Ukraine dated February 23, 2022. No 286-p. Main source: Про схвалення Стратегії розвит... | від 23.02.2022 № 286-р (rada.gov.ua).

31. Urdenko O. H. (2021). Modeling and management of information security of the enterprise in the conditions of digital transformation: diss. Dr. of Phil., Kyiv National University of Economics named after Vadym Hetman, 280.

32. Fedorov M. All basic information resources of Ukraine are being attacked from night to day - Ministry of Digital Affairs. Economic Truth. February 24, 2022. Main source: З ночі й досі атакують усі базові інформаційні ресурси України – Мінцифри | Економічна правда (epravda.com.ua)