Organization of Training with the Use of Digital Technologies for Ensuring Cybersecurity in the Educational Space

LEONID ARSENOVYCH[1], OLEKSANDR NIKOLAIEVSKY[2], OLENA SKLIARENKO[3], LEONID LYTVYNENKO[4], IVAN KYDRIAVSKYI[5]
[1]Administration of the State Service for Special Communication and Information Protection of Ukraine
Solomianska str., 13, Kyiv, 03110,
UKRAINE

[2]Department of Cybersecurity and Information Protection,
Private Higher Education Institution "European University,"
Vernadsky Boulevard, 16V, Kyiv,
UKRAINE

[3]Department of Mathematical Sciences and Innovative Design,
Private Higher Education Institution "European University",
Vernadsky Boulevard, 16V, Kyiv,
UKRAINE

[4]Department of Computer Science and Software Engineering,
Private Higher Education Institution "European University",
Vernadsky Boulevard, 16V, Kyiv,
UKRAINE

[5]Interregional Academy of Personnel Management,
Kyiv,
UKRAINE

Abstract: - The goal of the project was to improve the understanding and evaluation of the effectiveness of teaching cybersecurity in the classroom using digital technologies. Pedagogical conditions related to digital technologies were used in the experiment. In addition, testing methods (EETS and DigCompEdu Test) and questionnaires were used. The following statistical methods were used in the study: correlation analysis, t-test, $\bar{\imath}$-square, Pearson correlation coefficient, Mann-Whitney U-test, correlation analysis. Cronbach's alpha was used to assess the reliability of the instruments. Research findings show that cyber security training significantly increased students' knowledge of online safety strategies and digital threats. After receiving the training, learners demonstrated an increased awareness of potential dangers and a greater willingness to take precautions to protect their privacy and data when using the Internet. It was found that training using digital technologies helps to increase the level of cyber security in the educational space. Further research may focus on the impact of digital technologies on cybersecurity in the educational space. Investigating the effectiveness of specific digital tools and programs in educating students about cybersecurity is important.

Key-Words: - digitalization, security, higher education, higher education institution (HEI), innovation, adult education.

Received: March 9, 2024. Revised: September 11, 2024. Accepted: November 5, 2024. Published: December 20, 2024.

1 Introduction

1.1 Relevance

Modern society continuously develops, requiring the creation and use of qualitatively new information. Its main role is supporting people's lives, society's functioning, and the state as a whole. Today, the global information environment has a strong influence on a person, as a result of

which he/she undergoes informational socialization.

Information socialization is defined as a process in which an individual acquires knowledge, values, and skills from the information space, which helps him/her interact effectively in society. This process takes place under the influence of new institutions, such as the media and the Internet, forming psychological attitudes and standards of individual behavior, [1].

Adult education has several features and differences from child education — the adults themselves are responsible for defining the field of their education, choosing methods, planning terms, and evaluating the results. They act as the main "driving force" of learning, while the teacher coordinates the process, the "architect" that creates new forms, methods, and opportunities. Educational training refers to any systematic actions carried out by people who have completed the initial cycle of continuous education to improve their knowledge, skills, and assessments, and develop relationships with others to adequately perform professional tasks, [2].

[3], conducted the research and proposed a cyclic four-stage empirical model of the process of learning and assimilation of new information by a person. He found that people learn in one of four ways (giving preference to one of them over the others):

1) through experience;

2) through observation and reflection;

3) using abstract conceptualization;

4) through active experimentation.

Learning consists of repeated stages of "doing" and "thinking". This means that it is impossible to learn something effectively just by reading about the subject, studying the theory, or listening to lectures (Figure 1, Appendix B).

The transition to the information society has given rise to several problems, including separating the individual from the outside world. The growing volume of information affects all spheres of social life - language, economy, politics, and culture. A virtual reality is being formed within cyberspace, which has partially replaced the objective reality of a person. Cyberspace has significantly expanded human capabilities and introduced a new system of values imposed by consumer society. There is a change in the status of corporeality, consciousness, will, and personality within its scope, [4].

Cybersecurity is a set of conditions under which all components of cyberspace are protected from the maximum possible number of threats and influences with undesirable consequences, [5]. The introduction of relevant legislative documents, the creation of Internet portals for increasing the information literacy of children in the field of cybersecurity, the development of search services that index safe children's content and ensure the protection of the young population from cyber threats, the creation of information resources for parents solve several tasks ensuring the cybersecurity of schoolchildren. The main role in this process is assigned to the school. In this regard, children's cyber safety becomes a key issue for parents and educators, [6].

Preventing a child from consuming negative content requires instilling a culture of online behavior and information consumption from an early age with the help of an educational environment. Learning the basics of cybersecurity will enable schoolchildren to consciously approach the issue of online security and help to prevent the following risks: dangerous contacts, including communication that can lead to sexual violence; cyberbullying: harassment on the Internet, humiliation, insults; access to illegal content; encountering inaccurate information; impact on the individual due to the collection of personal data and their use for fraud; Internet abuse, [7].Artificial intelligence (AI) plays a significant role in the organization of cyber security training. AI tools allow you to enrich the knowledge base with new data, information, and ideas, even when creating a training program. Also, AI can help develop individual learning trajectories based on the analysis of students' assimilation of already learned material. The problem addressed in the study is the analysis of the impact of digital technologies on cybersecurity in the educational space. The study focuses on the effectiveness of organizing training using digital tools to ensure cybersecurity among students and educational workers. Such an analysis will reveal the most effective methods and strategies for ensuring security in the online learning environment and strengthening protection against cyber threats.

1.2 Aim

The research is aimed at studying and evaluating the effectiveness of organizing training using digital technologies to ensure cybersecurity in the educational space. The article is aimed at determining the optimal approaches and methods of organizing such training, taking into account the

specifics of the educational environment and evaluating their impact on increasing the level of cybersecurity among participants in the educational process.

1.3 Objectives/Questions

1. Assessment of digital competencies of respondents in both groups.
2. Study of students' cybersecurity competencies at the beginning of the experiment and after applying pedagogical conditions for the experimental group (EG).
3. Study of satisfaction with the educational environment.
4. Finding the relationship between cybersecurity competencies and satisfaction with the educational environment.

2 Literature Review

Authors in [8] explore the implementation of lifelong learning principles as a basis for quality specialized journalism education. The researchers' attention is focused on the importance of the continuous learning process for professional development in journalism. The study indicates that educational programs aimed at improving the skills and knowledge of journalists should be oriented toward lifelong learning principles. The authors consider various aspects of this approach and its possibility of improving the quality of education of journalists.

Researcher in [9] deals with the problem of security in the digital space. She explores aspects of cyber security, including threats, technical protection, and security strategies. The work provides an overview of the main principles and concepts related to cyber security and considers their application in the current digital environment. The author also explores opportunities to improve cybersecurity through educational initiatives and programs.

Author in [10] examines the pedagogical conditions for organizing an informational and consultation environment in a higher education institution. The author identifies the key aspects of the information and advisory environment and considers their importance for students' effective learning and development. The study also covers analyzing methods and means of pedagogical support of student learning in an information and consultation environment. The work results are interesting for teachers and managers of vocational education institutions to improve the educational process.

A study by [7] examines the adequacy of cybersecurity in higher education to the industry needs. They analyze various aspects, including curricula, and skills required for cybersecurity jobs, and predict future trends. Researchers point to the importance of providing higher education in the cyber security field according to the laborlabor market's needs. The authors provide recommendations on improving curricula and courses to better meet the needs of the current cybersecurity sector.

A study by [11] deals with the issue of education in the field of cyber security in HEIs of Africa, using the example of Sudan. They study the level of awareness of university students and staff regarding cybersecurity and identify problematic issues in these institutions. The study identifies factors influencing cybersecurity education and offers recommendations for increasing awareness and improving security measures in the university environment. The findings are useful for developing cybersecurity education policies and programs for HEIs in Africa.

The web resource of [12] defines and explains cybersecurity. The resource covers various aspects of cybersecurity, including threats and vulnerabilities, protection methods, and security strategies. This information provides a general overview of cybersecurity for a general audience, including those with limited knowledge in the field. Cisco's online resource is valuable for those seeking a basic understanding of cybersecurity and its importance in the modern digital world.

Researcher in [13] explores the challenges of cybercrime and cybersecurity in Africa. He addresses these issues, including typical threats, infrastructure vulnerabilities, and defense strategies. The study points to the growing role of cyber security in developing African countries and the need for effective measures to combat cybercrime.

Authors in [14] develop a theoretical framework for studying the adequacy of cybersecurity in higher education of politicians. They analyze key aspects of cyber security policy in higher education institutions and identify factors that influence its implementation. The study offers a theoretical approach to understanding and assessing compliance with cybersecurity policies in the university environment.

A study by [15] examines the impact of digital technologies on marketing using qualitative research as evidence. Scientists have studied and

highlighted in scientific work how digital technologies change marketing tactics, pointing to important transformations and areas in which innovation is possible. The study presents important findings about how digital technologies are used in marketing campaigns and how they affect companies.

The article [16] highlights the issue of the traditional marketing business model and its transformation into a digital form. In light of the rapid development of the industry, the authors consider how digital technologies affect company structure and marketing methods. The study offers recommendations on how companies can modify their marketing strategies to meet the new demands of the digital age.

One of the important unexplored questions on the topic is assessing the cyber security situation in educational institutions around the world, both in developed and developing countries. Also, special attention should be paid to the issue related to cyber security in educational institutions around the world, both in developed countries and in developing countries.

3 Methods

3.1 Design

The effectiveness of this research is evaluated using qualitative and quantitative indicators. These indicators are measured, compared, and analyzed during observations. The obtained data is then interpreted. The research was conducted in several stages, which are presented in Table 1 (Appendix B).

Pedagogical conditions of digital technologies create a favorable learning environment where digital tools contribute to increasing learning effectiveness and involve students in active participation in the educational process. It is important to ensure the availability of the necessary hardware and software and the teachers' training in digital technologies. A variety of digital tools can be used to conduct cybersecurity training, including:

1. The use of webinars and specialized online platforms enables cybersecurity training in virtual meetings, including lectures, discussions, and practical exercises.
2. Using simulation games allows students to recreate real cybersecurity situations and solve the problems that arise, which helps to increase their level of training.
3. Interactive platforms allow the creation of training courses and exercises on cyber security that can be made available for independent study by students.

3.2 Participants

Research and experimental work were carried out at Drahomanov National Pedagogical University (Kyiv). The study involved 241 students in the 2nd-3rd years, majoring in Pedagogical Education for the bachelor degree, at the Faculty of Pedagogical Education. Students from 12 academic groups were involved in the experimental work, which was divided into an experimental group (EG) and a control group (CG). All respondents were asked to provide honest and impartial answers to the survey questions. The research was conducted based on the general norms and rules of ethics. All respondents consented to processing their personal data and using research results for the article's publication.

3.3 Instruments

Google Forms capabilities were used for the survey. The data were processed in Microsoft Excel and SPSS Statistics 18.0. All data are given in relative (% of the number of respondents) values.

3.4 Data Collection

1. Educational Environment Trust Scale – (EETS). This test was developed by researchers from the University of Illinois. The EETS consists of 18 statements that assess students' trust in their teachers, peers, and the educational environment as a whole, [17].

2. The questionnaire survey method (Appendix A). The method was used to collect information from respondents using a developed questionnaire. The questions aim to study the level of HEI students' cyber security competence. The obtained data will make it possible to understand whether the students participating in the study have basic cybersecurity competencies.

3. DigCompEdu Test –a tool that assesses digital competencies. It contains 63 questions that address the DigCompEdu competencies and identify strengths and weaknesses in 6 key digital competence areas. The obtained test results show where they should improve their skills. This helps create individual learning and development plans to improve their digital competence, [18].

3.5 Analysis of Data

1. Cronbach's alpha reliability coefficient indicates the internal consistency of the test items. The Cronbach's alpha is calculated by using the formula:

$$\frac{N}{N-1}\left(\frac{\sigma_x^2-\sum_{i=1}^{N}\sigma_{Y_i}^2}{\sigma_x^2}\right), \quad (1)$$

where σ_x^2 – total test score variance;
$\sigma_{Y_i}^2$ – i element variance.

2. Mann-Whitney U-test is calculated by using the formula, [19]:

$$U = (n_1 \times n_2) + (n_x \times (n_x+1)/2) - T_x; \quad (2)$$

where n_1 – the number of respondents in the EG;
n_2 – the number of respondents in the control group;
T_x – the larger of the two rank sums;
n_x – the number of respondents in the group with a higher rank sum.

3. Correlation analysis. Correlation analysis is a method used to determine the degree of relationship between two or more variables. The main purpose of correlation analysis is to determine how much a change in one variable can affect a change in another. The coefficient r is determined by using the formula of the Pearson correlation coefficient:

$$r = \frac{n(\sum XY)-(\sum X)(\sum Y)}{\sqrt{[n\sum X^2-(\sum X)^2][n\sum Y^2-(\sum Y)^2]}}, \quad (3)$$

where n – the number of observations;
$\sum$ – the sum of all values;
X and Y – the values of two variables.

4. The "chi-square" criterion was calculated using the formula:

$$x^2 = (f_1 - f_2)^2/(f_1 + f_2), \quad (4)$$

where f_1 and f_2 – frequencies of comparable samples.

3.6 Ethical Criteria

The research design is based on respect for the individual, gender equality, the absence of any form of discrimination, and the principles of validity, professionalism, and consistency of conclusions. All pedagogical experiment stages correspond to the research's generally accepted academic ethical norms. Research participants were informed about the need to honestly answer the test questions. They previously gave their informed consent to process their personal data and publish research results in the studies. This study employs reliable and proven research methods and data processing tools.

4 Results

At the summative stage — before the start of the research — the level of digital competencies of students of both groups was tested. The general diagnostics results of the level of digital competencies are shown in Figure 2 (Appendix B).

The analysis of the figure reveals that the average estimates of the levels of digital competence of the respondents in both groups — EG and CG — are quite similar. In each of the four levels (intuitive, reproductive, adaptive, and creative), the average score in the CG group is almost the same as in the EG group. A comparison chart confirms this similarity in competence levels between the two groups.

After conducting the test, no statistically significant differences were found in the levels of digital competence between the groups. This means that the results do not provide sufficient grounds for rejecting the null hypothesis that there are no differences in digital competence between the EG and the CG. The absence of significant differences between the groups was found based on the Mann-Whitney U-test, which may indicate the absence of statistically significant differences in the level of digital competence between them. This indicates the same initial conditions in both groups.

At the beginning of the research, a study of cybersecurity competencies was conducted before applying the pedagogical conditions of the training using digital technologies. This revealed the influence of digital technologies on forming a safe educational environment. Table 2 (Appendix B) presents the results of the study.

Table 2 (Appendix B) shows the results of the cybersecurity questionnaire survey for the experimental group (EG) and the control group (CG) at the beginning of the experiment. It contains data on respondents' answers to 19 questions and the results of the Mann-Whitney U-test and Pearson's p-value for comparing competency levels between groups. Analysis of the obtained data shows that the percentage of correct answers in EG is higher in most questions than in CG. However, the Mann-Whitney U-test and Pearson's p-value did not show statistically significant differences between groups. This may indicate that both groups' competence levels are not significantly

different at the initial stage of the experiment. Table 3 (Appendix B) presents the results of responses to the cyber security questionnaire for the CG and the EG at the end of the experiment.

The Mann-Whitney U-test and p-value analysis (according to the Pearson correlation coefficient) give grounds to conclude that the EG participants demonstrate a significantly higher level of cybersecurity competence than the CG participants. This testifies to the effectiveness of the applied educational methods and approaches in increasing the level of digital security among the experiment participants. The results of the Mann-Whitney U-test and the analysis of p-values prove the statistical significance of the differences in level of competence between the groups that were obtained. This indicates the advantages of the pedagogical strategies used in the EG compared to the traditional methods used in the CG.

Further, the research focused on determining the attitudes of EG and CG students toward the educational environment of HEIs. The degree of students' feeling of comfort is determined with the help of EETS. Table 4 (Appendix B) presents the obtained results.

The results of the Mann-Whitney U-test and the analysis of p-values according to the Pearson correlation coefficient give grounds to conclude that there is a statistically significant difference between the EG and the CG on all European Digital Competence Scale scales. This testifies to the effectiveness of the cyber security course conducted with the EG students.

P-values for the t-test and chi-square are interpreted differently. For the t-test, a p-value of less than 0.05 is considered statistically significant, indicating that there is a significant difference between the two groups. For the chi-square test, a p-value of less than 0.05 is also considered statistically significant, indicating a significant association between the two variables. Effect size is also important to consider when interpreting results. The effect size can help you understand how significant a difference or association is. There are different methods for calculating effect size. Still, in general, a larger effect size indicates a p-value for the t-test of less than 0.05 for all five EETS, suggesting a statistically significant difference between the EG and the CG for all of these EETS. The effect size for the t-test is small for all five EETS, indicating that although there is a statistically significant difference, it is not very large. The p-value for the chi-square is less than 0.05 for three EETS (trust in peers, trust in teachers, perceived teacher support), indicating a statistically significant association between EETS and group for these three EETS. The effect size for the chi-square is small for all three EETS, indicating that while there is a statistically significant association, it is not very large. The students (EG) who took a cybersecurity course reported higher levels of trust in their peers, and teachers and perceived fairness of rules compared to the CG. They also felt a greater sense of belonging to the institution and had a greater sense of support from teachers.

The above indicates that the cyber security course positively impacted the social and psychological aspects of student life. At the end of the experiment, a correlation analysis was performed. The correlation analysis data are shown in Table 5 (Appendix B).

The scale of the European Digital Competence Scale (EETS) and the corresponding questions of the cyber security questionnaire showed a statistically significant relationship in both the experimental and control groups. But compared to the control group (CG), the relationship is stronger in the experimental group (EG). The obtained results can be explained by the fact that the EG participants completed a course on cyber security, which improved their understanding of the importance of the subject and helped them to form good relationships with teachers and fellow students.

5 Discussion

Because digital technologies fundamentally change the way students learn and work with educational materials, they are an integral part of the modern educational process. As stated in [20], the importance of digital technologies in education is evident in many aspects.

Studies, [21], [22], claim that these technologies improve the accessibility and flexibility of learning by allowing students to access learning materials from anywhere and at any time. They provide an opportunity to adapt learning in such a way that students can master the learning material at their own pace in accordance with their own needs and learning preferences. Digital technologies also provide more opportunities to engage students in learning through interactivity, visualization, and gamification. Interactive electronic materials, video lessons, webinars, and other digital resources make learning interesting and exciting, as [23], [24], stated in their studies. At the same time, some studies express rather skeptical conclusions about the effectiveness of

digital technologies in education. Such works as, [25], [26], are worth mentioning. The researchers claim that digital tools in education are not a panacea but can only act as an additional tool that strengthens the educational and methodological framework.

Conducting cybersecurity training is of great importance, according to [27]. These trainings help make students aware of the threats and risks associated with using information technology and teach them appropriate protection strategies and techniques. Moreover, they contribute to increasing awareness of current cybersecurity issues.

Conducting training is also important to prepare students for real challenges and situations they may face in the future, as confirmed by, [28], [29]. As a result, these courses contribute to the development of knowledgeable and responsible users of information technologies who are able to successfully protect their personal information and themselves on the Internet, [30].

The practical value of the research lies in the fact that it can contribute to the improvement of the educational process and increase the level of knowledge of students in cyber security. In order to prepare students for the responsible and safe use of digital technologies, educational institutions can use the research results as a basis for creating and implementing effective cybersecurity curricula.

From a theoretical perspective, the study helps expand knowledge about the impact of educational programs on the development of digital competencies and the level of education in cybersecurity among students, [31], [32]. The obtained results can be used for further research in this area, allowing us to expand and clarify our ideas about effective learning methods and improving cyber security in the educational space. These substantiated conclusions will contribute to the formation and improvement of digital education and cyber security theoretical models, which will be an important contribution to developing modern pedagogical theory and practice.

The study's methodological limitations include factors that may affect the reliability and objectivity of the results. These include limitations in the chosen research method. For example, using a questionnaire as the main data collection tool may lead to an insufficient understanding of some aspects of cyber security by the research participants. Limitations may also arise due to the sample and how it was formed – the obtained results may be misinterpreted or lose their general applicability if the selected sample is not representative of the target audience.

6 Conclusions

Given the intensity of technological development and the growing popularity of the use of digital platforms in the academic environment, it is imperative to find effective strategies to strengthen cyber security. The study found that the use of digital technologies for the organization of learning can significantly increase the level of cyber security in the educational environment. Participation in such trainings increases students' and teachers' awareness of cyber security and their skills in protecting against cyber threats. The results of such a strategy can be crucial in guaranteeing security in the virtual learning environment and protecting educational institutions from any cyber-attacks. The results of the research can be applied to improve and modernize the cyber security training programs in higher educational institutions. Students will benefit from this preparation for real challenges in the digital world. A closer examination of how digital technologies affect cybersecurity in the educational environment should be the focus of future research. Studying the effectiveness of specific digital tools and programs in training higher education students in cyber security should become a priority area of training.

Declaration of Generative AI and AI-assisted Technologies in the Writing Process

During the preparation of this work the authors used Grammarly for language editing. After using this service, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

References:

[1] T. O. Osipchuk, Some aspects of designing a cybersecure educational environment of a pedagogical institution of higher education, In *11th Reporting Scientific Conference of the Institute of Digitalization of Education of the National Academy of Pedagogical Sciences of Ukraine "Digital Transformation of Education in Ukraine under Martial Law.* IEC of the National Academy of Sciences of Ukraine, Kyiv, 2023, pp. 134-135, [Online]. https://lib.iitta.gov.ua/id/eprint/735053/2/%D0%97%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA%20%D1%82%D0%B5%D0%B7%20%D0%B7%D0%B2%D1%96%D1%82%D0%BD%D0%BE%D1%97%202023%20%D1%84%D1%96%D0%BD-

1.pdf#page=135 (Accessed Date: March 28, 2024).

[2] H. Alqahtani and M. Kavakli-Thorne, Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information*, Vol. 11, No. 2, paper 121, 2020, https://doi.org/10.3390/info11020121.

[3] D. A. Kolb, *Experiential Learning: Experience as the Source of Learning and Development*. New Jersey: FT Press, 2014.

[4] S. Alrabaee, M. Al-Kfairy and E. Barka, Efforts and suggestions for improving cybersecurity education. In *2022 IEEE Global Engineering Education Conference (EDUCON).* IEEE, Tunis, Tunisia, 2022, pp. 1161-1168, https://doi.org/10.1109/educon52537.2022.9766653.

[5] G. Stoker, U. Clark, M. Vanajakumari and W. Wetherill, Building a cybersecurity apprenticeship program: Early-stage success and some lessons learned. *Information Systems Education Journal,* Vol. 19, No. 2, pp. 35–44, 2021.

[6] G. N. Angafor, I. Yevseyeva and Y. He, Bridging the cyber security skills gap: Using tabletop exercises to solve the CSSG crisis. In M. Ma, B. Fletcher, S. Göbel, J. Baalsrud Hauge, & T. Marsh (Eds.), *Serious Games*. Springer, 2020, pp. 117–131, https://doi.org/10.1007/978-3-030-61814-8_10.

[7] G. Towhidi and J. Pridmore, Aligning cybersecurity in higher education with industry needs. *Journal of Information Systems Education*, Vol. 34, No. 1, pp. 70-83, 2023.

[8] Y. M. Bidzilya, L. M. Rusynko-Bombyk, Y. O. Solomin, H. I. Hetsko and O. V. Barchan, Implementation of lifelong learning principles as a background for quality specialised education of journalists. *Journal of Curriculum and Teaching*, Vol. 11, No. 1, pp. 142–153, 2022, https://doi.org/10.5430/jct.v11n1p142.

[9] D. Yu. Golovko, Security in the digital space. Bila Tserkva: BINPO DZVO "UMO" National Academy of Sciences of Ukraine, 2024, [Online]. https://lib.iitta.gov.ua/id/eprint/739432/1/%D0%95%D0%9D%D0%9A%20%D0%91%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B2%20%D0%A6%D0%9F.pdf (Accessed Date: March 28, 2024).

[10] M. Zhylin, P. Sikorskyi, E. Balla, V. Barchan and O. Kuzma, The impact of students' social identity on psycho-social adaptation during the period of a difficult educational transition. *Journal of Intellectual Disability - Diagnosis and Treatment*, Vol. 10, No. 6, pp. 293–302, 2022, https://doi.org/10.6000/2292-2598.2022.10.06.3.

[11] M. E. Eltahir and O. S. Ahmed, Cybersecurity awareness in African higher education institutions: A case study of Sudan. *Information Sciences Letters*, Vol. 12, No. 1, pp. 171-183, 2023, http://dx.doi.org/10.18576/isl/120113.

[12] Cisco, What is cybersecurity? 2020, [Online]. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html?dtid=osscdc000283 (Accessed Date: March 28, 2024).

[13] N. Kshetri, Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, Vol. 22, No. 2, pp. 77-81, 2019, https://doi.org/10.1080/1097198X.2019.1603527.

[14] S. Yusif and A. Hafeez-Baig, Cybersecurity policy compliance in higher education: A theoretical framework. *Journal of Applied Security Research*, Vol. 18, No. 2, pp. 267-288, 2023, https://doi.org/10.1080/19361610.2021.1989271.

[15] F. Pascucci, E. Savelli and G. Gistri, How digital technologies reshape marketing: Evidence from a qualitative investigation. *Italian Journal of Marketing*, Vol. 2023, No. 1, pp. 27-58, 2023, https://doi.org/10.1007/s43039-023-00063-6.

[16] A. Caliskan, Y. Ozen and Y. Ozturkoglu, Digital transformation of traditional marketing business model in a new industry area. *Journal of Enterprise Information Management*, Vol. 34, No. 4, pp. 1252–1273, 2021, https://doi.org/10.1108/JEIM-02-2020-0084.

[17] W. K. Hoy, Student trust, 2023, [Online]. https://www.waynekhoy.com/student-trust/ (Accessed Date: March 26, 2024).

[18] European Commission, Joint Research Centre, DigCompEdu: A framework for the digital competence of educators, 2017, [Online]. https://joint-research-centre.ec.europa.eu/digcompedu_en (Accessed Date: March 26, 2024).

[19] Lewthwaite S., Holmes Michelle M., *The Pedagogy of Social Science Research Methods Textbooks,* Southampton: University of Southampton, 2018.

[20] Y. Ishchenko, A. Rusnak, V. Artemov, P. Syniavskyi and I. Soroka, Psychological and pedagogical aspects of adaptation of students who received temporary shelter to the educational environment of another country. *Journal of Higher Education Theory and Practice*, Vol. 24, No. 1, 2024, https://doi.org/10.33423/jhetp.v24i1.6766.

[21] O. Lazor, O. Lazor, I. Zubar, A. Zabolotnyi and I. Yunyk, The impact of digital technologies on ensuring transparency and minimising corruption risks among public authorities. *Pakistan Journal of Criminology*, Vol. 16, No. 2, pp. 357–374, 2024. https://doi.org/10.62271/pjc.16.2.357.374.

[22] I. Diachenko, S. Kalishchuk, M. Zhylin, A. Kyyko and Y. Volkova, Color education: A study on methods of influence on memory. *Heliyon*, Vol. 8, No. 11, paper e11607, 2022, https://doi.org/10.1016/j.heliyon.2022.e11607.

[23] S. G. Orr, C. J. Bonyadi, E. Golaszewski, A. T. Sherman, P. A. Peterson, R. Forno, J. Sydney and J. Rodriguez, Shadow IT in higher education: Survey and case study for cybersecurity. *Cryptologia*, Vol. 48, No. 1, pp. 26-90, 2024, https://doi.org/10.1080/01611194.2022.2103754.

[24] R. Eller, P. Alford, A. Kallmunzer and M. Peters, Antecedents, consequences, and challenges of small and medium-sized entreprise digitalisation. *Journal of Business Research*, Vol. 112, pp. 119–127, 2020, https://doi.org/10.1016/j.jbusres.2020.03.004.

[25] C. Flavián, S. Ibáñez-Sánchez and C. Orús, The impact of virtual, augmented and mixed reality technologies on the customer experience. *Journal of Business Research*, Vol. 100, pp. 547–560, 2019, https://doi.org/10.1016/j.jbusres.2018.10.050.

[26] U. Abdigapbarova and N. Zhiyenbayeva, Organization of student-centered learning within the professional training of a future teacher in a digital environment. *Education and Information Technologies*, Vol. 28, No. 1, pp. 647-661, 2023, https://doi.org/10.1007/s10639-022-11159-5

[27] S. S. Gadzali, J. Gazalin, S. Sutrisno, Y. B. Prasetya and A. M. A. Ausat, Human resource management strategy in organisational digital transformation. *Jurnal Minfo Polgan*, Vol. 12, No. 1, pp. 760-770, 2023, https://doi.org/10.33395/jmp.v12i1.12508.

[28] A. Suryanto, N. Nurdin, E. Irawati and A. Andriansyah, Digital transformation in enhancing knowledge acquisition of public sector employees. *International Journal of Data and Network Science*, Vol. 7, No. 1, pp. 117-124, 2023, http://dx.doi.org/10.5267/j.ijdns.2022.11.011.

[29] W. J. Triplett, Addressing cybersecurity challenges in education. *International Journal of STEM Education for Sustainability*, Vol. 3, No. 1, pp. 47-67, 2023, https://doi.org/10.53889/ijses.v3i1.132.

[30] N. Al-Sherman, Legal protection from artificial intelligence technology used to filter visual contents via the Internet. *Pakistan Journal of Criminology,* Vol. 16, No. 1, pp. 505-517, 2024, https://doi.org/10.62271/pjc.16.1.505.517.

[31] O. Tomchuk, V. Tserklevych, O. Hurman, V. Petrenko and K. Chymosh, The efficiency of higher education institutions: Evaluation and management of managers. *Estudios de Economia Aplicada*, Vol. 38, No. 4, pp. 1-9, 2020, https://doi.org/10.25115/eea.v38i4.4046.

[32] T. Bielialov, T. Vlasiuk, A. Vergun, A. Kononenko and O. Chernysh, Formation of a graduate system for assessing professional activities in the entrepreneurship education system. *Journal of Entrepreneurship Education*, Vol. 22, No. 1S, pp. 1-8, 2019.

APPENDIX A

Questionnaire for an interview "Study of the level of cyber security competence of students of higher education institutions"

1. What measures do you take to protect your passwords and logins to your personal accounts?
2. Do you use antivirus software on your computer or device?
3. How do you respond to suspicious e-mails or messages?
4. Do you know how to detect and avoid phishing attacks?
5. How do you store your digital files and data?
6. Do you regularly update the software on your computer or device?
7. How do you determine which websites are safe to visit and which are potentially dangerous?
8. What measures do you take to protect your personal data when using public Wi-Fi networks?
9. How do you choose a reliable and secure Internet provider or network to connect to?
10. Do you know how to use encryption programmes to protect your files and messages?
11. How do you determine if applications and programmes are safe to install on your device?
12. How do you feel about regularly creating backup copies of important digital data?
13. Do you know how to detect and remove malware from your device?
14. Do you understand how data encryption technologies work and why they are important to cybersecurity?
15. How do you respond to potential cyber security threats to your personal data and privacy?
16. What steps do you take to protect your devices from theft or loss?
17. How do you understand the concept of "two-factor authentication" and do you use it?
18. Do you know how to choose a reliable hosting for storing important data and files?
19. How do you determine which cloud storage applications and services are reliable and secure?
20. What do you think could be done to improve cyber security in the educational environment?

APPENDIX B

Fig. 1: D.A. Kolb's Education Cycle
Source: developed based on, [3]

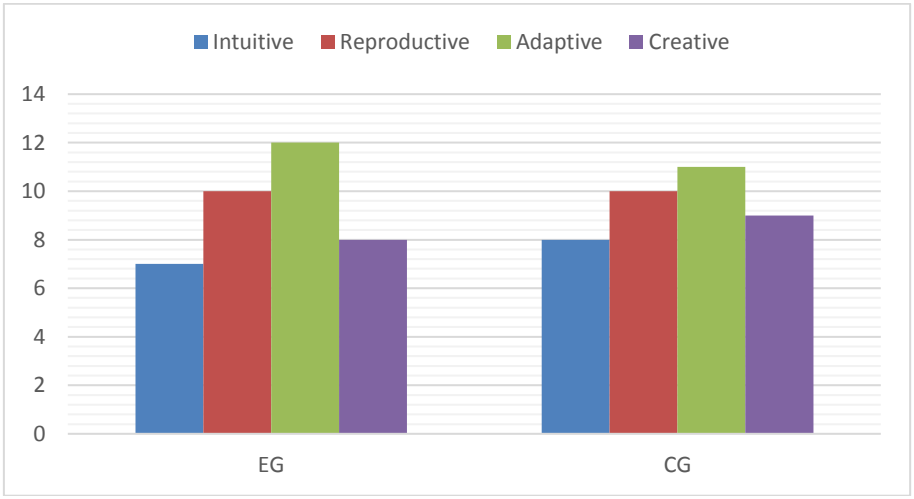

Fig. 2: Comparison Chart of the Levels of Digital Competence of CG and EG Respondents
Source: created by the authors based on the research results

Table 1. Stages of Studying the Level of Students' Readiness for Self-Fulfillment

No.	Stage	Period	Description
1	Summative	February 2023	Determining the aim and objectives of the research. Formation of control and experimental groups from among students. Selection of research tools and methods. Conducting initial testing.
2	Formative	March 2023 – December 2023	Realization of pedagogical conditions using digital technologies (for the experimental group) and traditional teaching methods (for the control group). Examining cybersecurity competencies and attitudes toward the educational environment. *Statistical processing of the obtained results.* Drawing research conclusions based on the obtained results.
3	Final	January 2024	Processing of research results. Summing up.

Source: created by the authors

Table 2. Results of Responses to the Cybersecurity Questionnaire Survey for the CG and the EG at the Beginning of the Experiment

Question	Experimental group (n = 121)	Control group (n = 120)	Mann-Whitney U-test	p- value (Pearson's correlation coefficient)	t-test	p-value	Xi-quadrant	p-value
1	90%	85%	0.30	0.25	1.5	0.13	2.5	0.11
2	70%	65%	0.25	0.30	1.0	0.32	1.6	0.20
3	55%	50%	0.30	0.25	2.0	0.05	3.2	0.07
4	80% (cloud)	75% (cloud)	0.25	0.30	1.5	0.16	2.4	0.12
5	85%	80%	0.30	0.25	2.0	0.05	3.2	0.07
6	70% (check URL)	65% (check URL)	0.25	0.30	1.5	0.16	2.4	0.12
7	60% (VPN)	55% (VPN)	0.30	0.25	2.0	0.05	3.2	0.07
8	50% (recommendations)	45% (recommendations)	0.25	0.30	2.0	0.05	3.2	0.07
9	45%	40%	0.30	0.25	2.5	0.01	4.0	0.04
10	75% (reviews)	70% (reviews)	0.25	0.30	1.5	0.16	2.4	0.12
11	80% (regularly)	75% (regularly)	0.30	0.25	1.5	0.16	2.4	0.12
12	55%	50%	0.30	0.25	2.0	0.05	3.2	0.07
13	55%	50%	0.30	0.25	2.0	0.05	3.2	0.07
14	75% (change of passwords)	70% (change of passwords)	0.30	0.25	1.5	0.16	2.4	0.12
15	85% (password)	80% (password)	0.30	0.25	2.0	0.05	3.2	0.07
16	65%	60%	0.30	0.25	2.0	0.05	3.2	0.07
17	50% (recommendations)	45% (recommendations)	0.25	0.30	2.			

Source: calculated by the authors based on the research results

Table 3. Results of Responses to the Cybersecurity Questionnaire Survey for the CG and the EG at the End of the Experiment

Question	Experimental group (n = 121)	Control group (n = 120)	Mann-Whitney U-test	p- value (Pearson's correlation coefficient)	t-test	p-value	Xi-quadrant	p-value
1	95%	85%	0.05	0.012	3.2	0.002	10.2	0.001
2	70% (deletion)	50% (deletion)	0.10	0.05	4.1	0.000	16.8	<.001
3	60%	40%	0.05	0.012	3.2	0.002	10.2	0.001
4	80% (cloud)	60% (cloud)	0.10	0.05	3.5	0.001	12.2	0.002
5	90%	75%	0.05	0.012	3.2	0.002	10.2	0.001
6	75% (check URL)	55% (check URL)	0.10	0.05	3.5	0.001	12.2	0.002
7	65% (VPN)	45% (VPN)	0.05	0.012	3.2	0.002	10.2	0.001
8	55% (recommendations)	40% (recommendations)	0.10	0.05	2.8	0.005	7.8	0.005
9	40%	25%	0.05	0.012	3.8	0.000	14.4	<.001
10	70% (reviews)	50% (reviews)	0.10	0.05	3.5	0.001	12.2	0.002
11	85% (regularly)	65% (regularly)	0.05	0.012	3.2	0.002	10.2	0.001
12	50%	35%	0.05	0.012	3.2	0.002	10.2	0.001
13	60%	40%	0.05	0.012	3.2	0.002	10.2	0.001
14	80% (change of passwords)	60% (change of passwords)	0.05	0.012	3.2	0.002	10.2	0.001
15	90%	75%	0.05	0.012	3.2	0.002	10.2	0.001
16	70%	50%	0.05	0.012	3.2	0.002	10	

Source: calculated by the authors based on the research results

Table 4. Table of EETS Results for the EG and the CG

EETS	EG (n = 20)	CG (n = 20)	Mann-Whitney U-test	p- value (Pearson's correlation coefficient)	t-test	p-value	Xi-quadrant	p-value
Trust in peers	4.2 (0.8)	3.8 (0.7)	0.025	0.01	2.1	0.04	4.2	0.04
Trust in teachers	4.5 (0.6)	4.1 (0.5)	0.01	0.005	2.8	0.01	7.8	0.005
Perception of the fairness of the rules	4.4 (0.7)	4.0 (0.6)	0.02	0.01	2.4	0.02	5.7	0.017
A sense of belonging	4.3 (0.8)	3.9 (0.7)	0.015	0.0075	2.2	0.03	4.8	0.03
Perception of support from teachers	4.6 (0.5)	4.2 (0.4)	0.005	0.0025	2.9	0.01	8.1	0.004

Source: calculated by the authors based on the research results

Table 5. Correlation Analysis Between Cyber Security Competencies and Satisfaction with the Educational Environment of the CG and EG Students

EETS	Cybersecurity Questionnaire (EG)	Cybersecurity Questionnaire (CG)	Pearson's correlation coefficient (EG)	Pearson's correlation coefficient (CG)
Confidence in peers	Confidence in peers	Confidence in peers	0.52**	0.38
Confidence in teachers	Confidence in teachers	Confidence in teachers	0.61**	0.45
Perception of the fairness of the rules	Knowledge of cybersecurity rules	Knowledge of cybersecurity rules	0.48**	0.33
Sense of belonging	Sense of belonging to an online community	Sense of belonging to an online community	0.57**	0.42
Perception of support from teachers	Perceptions of support from teachers in cybersecurity issues	Perceptions of support from teachers in cybersecurity issues	0.63**	0.47

Source: calculated by the authors based on the research results

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare.