UDC 004.8:378.147

Yurii V. Shchavinsky
PhD in Technical Sciences, Associate Professor of Information and Cyber Security Department
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID 0000-0002-2319-8983
yushchavinsky@ukr.net

Tetiana M. Muzhanova
PhD in Public Administration, Associate Professor,
Associate Professor of Information and Cyber Security Department
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID 0000-0002-7435-0287
muzanovat@gmail.com

Yuriy M. Yakymenko
PhD in Military Sciences, Associate Professor,
Associate Professor of Information and Cyber Security Department
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-6848-852X
yakum14@ukr.net

Mykhailo M. Zaporozhchenko
Assistant of the Department of Information and Cyber Security Management
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0003-0182-9497
zaporozhchenkomm@gmail.com

APPLICATION OF ARTIFICIAL INTELLIGENCE FOR IMPROVING SITUATIONAL TRAINING OF CYBERSECURITY SPECIALISTS

Abstract. The article identifies the problem of the need for continuous development and improvement of practical skills for cybersecurity professionals due to the constant growth and evolution of threats to information and cyber security for organizations, businesses, society, and the state. The relevance of implementing innovative technologies to improve the methods of developing technical and managerial competencies of cybersecurity specialists in higher education institutions is justified in accordance with the strategic direction of education reform in Ukraine. The relevance of developing the ability and skills for cybersecurity professionals to respond promptly to threats is associated with the use of artificial intelligence by cybercriminals. The analysis conducted in this work allowed us to conclude the need for improvement of the situational teaching method as one of the main ways to develop the competencies of students majoring in Cybersecurity and Information Security in higher education institutions. One of the ways to improve the method is to use artificial intelligence tools in creating various types of tasks for classes. To create educational situations and options for resolving conflicting situations in cybersecurity management and cyber incidents with the aim of developing skills in future cybersecurity managers to make timely, correct, and effective decisions, it proposed to use the artificial intelligence tool - the ChatGPT language model. Thanks to its excellent capabilities, which include summarizing and analyzing articles, encoding, debugging, and generating thematic blocks of situations, it represents significant progress in the field of artificial intelligence. The application of ChatGPT allowed the creation of the necessary number of situational tasks with options for correct solutions in a short time, covering all areas of activity for cybersecurity specialists. However, during the research, there was a need for critical evaluation and verification of the information provided by the model for compliance with the context and rules, laws, and ethical norms that apply in each specific situation. This issue addressed by refining and specifying the request to the ChatGPT language model to generate situations.

Keywords: information technologies; cyber security; professional competencies in cyber security; situational learning; artificial intelligence.

© Yurii. Shchavinsky, Tetiana Muzhanova, Yuriy. Yakymenko, Mykhailo Zaporozhchenko 2023.

1. INTRODUCTION

The problem statement. A strategic direction of the education reform in Ukraine is the modernization of the structure, content, and organization of education based on a competency approach, fostering the utilization of innovative technologies and state-of-the-art teaching methods in the educational process [1]. The integration of information technologies into all spheres of human life requires the adoption of new approaches to shaping the abilities, knowledge, and skills of graduates from higher education institutions, which they will need in their professional activities. The essence of these new approaches lies in orienting educational programs toward a competency-based approach in the training of professionals, necessitating the implementation of innovative teaching technologies aligned with contemporary advancements in science and technology.

In today's context, the training of cybersecurity professionals is particularly relevant due to the need for fast response to the challenges associated with information and cybersecurity in the rapidly growing and ever-changing digital world. The advancement of technology and the increased utilization of digital systems have led to a rise in the number and complexity of cyber threats. The emergence of new technologies such as artificial intelligence, the Internet of Things (IoT), blockchain, and cloud computing requires proficiency in responding promptly to hacker attacks, data breaches, malicious software, and other forms of cybercrime that are becoming more widespread and intricate.

Equipping cybersecurity experts with these competencies involves a dynamic combination of knowledge, skills, practical expertise, modes of thinking, professional, philosophical, and civic qualities, as well as moral and ethical values. These attributes define an individual's capacity effectively engage in professional and lifelong learning activities and are the outcomes of education at a certain level of higher education [2]. This process executed through educational programs during various forms of classes.

During lectures, seminars, practical sessions, internships, one of the ways to develop the necessary students' skills and abilities of cybersecurity management in various situations is the application of the situational learning method. Despite its numerous advantages, the implementation of situational learning does come with certain challenges. One of the main challenges is the limited immediate access to real-life situations that constantly arise in the cyber space. The widespread implementation of situational learning requires significant efforts, time, and financial investments to prepare realistic scenarios, develop specialized simulators, or engage experts to conduct practical sessions.

In some cases, there may be a lack of a standardized approach to situational learning, particularly in specific professional domains, which could influence the quality and consistency of the learning process. To address these mentioned challenges and to ensure the need for developing technical and managerial skills of cybersecurity professionals during their studying at higher institutions, new approaches to the application of situational learning need to be developed.

Analysis of recent studies and publications. Analysis of the literature indicates that there is a significant body of both international and domestic scientific publications dedicated to the method of situational learning using information technologies.

As asserted by authors [3]-[6] in their works, the emergence of the Internet over the last few years has substantially transformed the forms and content of traditional education, giving rise to various learning systems such as computer-assisted and web-based learning. These electronic learning systems enable educators to create meaningful content with diverse scenarios for practical sessions, prepare tasks for simulating situations, engage in discussions, and manage distance-learning activities.

The research paper [7] explores the possibility and practical approach to integrating Ukrainian higher education standards with the best international practices in training professionals in the specialty 125 "Cybersecurity and Information Protection," considering the constant transformation and development of the global information society. To facilitate active learning conditions for students of technical sciences, the CDIO 3.0 (Conceive - Design - Implement - Operate) engineering educational standard approach is proposed, encompassing the sequential steps of conception, design, implementation, and operation of products, processes, systems, and services. This approach has been piloted in two higher education institutions in Ukraine: the State University of Information and Communication Technologies and the Boris Grinchenko Kyiv University.

In the study [8], the significance of utilizing modern information and communication technologies, particularly interactive ones, during professional training at higher education institutions is substantiated. The specificity and educational goals of the interactive educational technology Case Study are outlined, the structure and principles of creating case studies are described, and the features of implementing Case Study based on information and communication technologies are identified.

The necessity to address the challenges of preparing highly skilled cybersecurity professionals has led researchers to seek new methods of practical education that would ensure the effective development of competencies necessary for professional activities. One of such approaches is the proposal to apply a cyber resilience framework in the training of professionals. This framework integrates models of system resilience and human behavior, providing organizations with diagnostic capabilities to better prepare for emerging cyber threats. It ensures the viability of the human aspects of cybersecurity, which are critically important for the continuity of their business [9]. Additionally, as noted in the research [10], it is especially important when shaping the managerial competencies of future cybersecurity managers to consider the role of the human factor and social engineering in the training of cybersecurity professionals.

In the research works [11], [12], functional schemes of virtual educational laboratories for simulating cybersecurity processes have been proposed. The implementation of these schemes provides extensive opportunities for creating diverse learning situations in the field of cybersecurity. The authors also identified the advantages of using virtual educational laboratories for simulating cybersecurity processes to meet the educational needs of both public and private cybersecurity sectors.

In the case study [13], the procedure for the development and application of test benches for cyber security training to provide skills and competencies to specialists using cloud technologies is defined. At the same time, the authors note the difficulty in their maintenance.

The works [14], [15] provide arguments for the application of the practical cybersecurity platform to create a comprehensive learning environment for professionals in managing cognitive situations in cyber ranges. In these works, researchers focus solely on personalized learning.

The use of a cybersecurity education structure based on the ADDIE model version (Analyse – Design – Develop – Implement - Evaluate) is proposed in the study [16]. This model defines the following sequence of actions: analysis; design; development; implementation; evaluation. The authors, however, note the complexity and lack of flexibility in structures created on the base of this model and suggest its implementation in the final course of cybersecurity professionals' training at higher education institutions.

The challenges of forming cybersecurity competencies are identified in research [17]-[20]. In the works [17], [18], it is proposed to shape competencies using the integrated cybersecurity educational structure called CyTrONE (Cybersecurity Training and Operation Network Environment), developed by the company Cyber Range Organization and Design.

Based on instructor input data obtained from the educational database, CyTrONE loads educational content into the Learning Management System (LMS) via the auxiliary tool CyLMS and creates a related learning environment using the Cyber Range Instance System (CyRIS) (Figure 1).

The third module of CyPROM can be used to manage the processes of incorporating dynamic elements into the educational activities, such as real-time attacks, etc. The participants can access these elements through the LMS MOODLE. To familiarize themselves with the training content, conduct necessary investigations, and provide responses through LMS, participants need to connect to the cyber range.

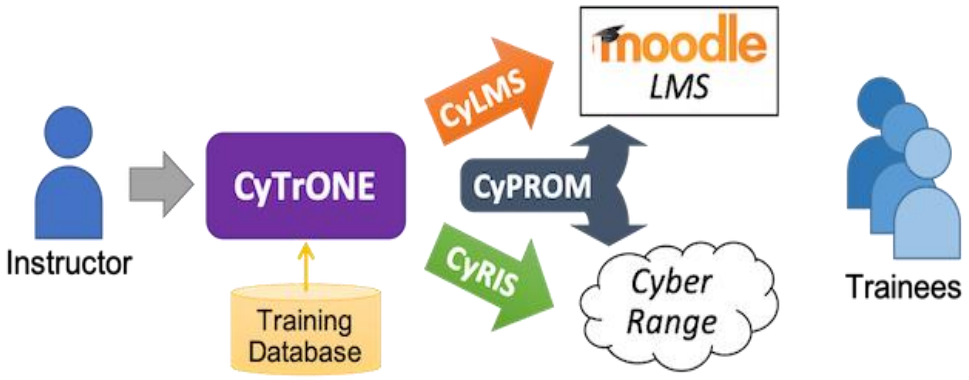

Figure 1. Scheme of the CyTrONE training structure

The CyTrONE distribution is freely available on the GITHUB website at the following link «https://github.com/crond-jaist/cytrone», and already includes some selective training modules. According to the authors, CyTrONE is well-suited for real educational events in terms of functionality, usability, and performance. However, the need for continuous enrichment of the training database due to the evolving nature of threats was noted.

In the work [19], various methods of informing about information and cybersecurity are discussed and evaluated. These methods are used to enhance the awareness of cybersecurity professionals. The need for employing combined methods, such as textual, gamified, and video-based methods, is emphasized. The author also points out the complexity of developing educational content that accurately reflects the current state of cyber threats.

The author of the article [20] has developed a Decision Support System (DSS) in cybersecurity, based on models describing cybersecurity tasks in conceptual and functional aspects. The DSS aims to facilitate the effective execution of loosely formalized cybersecurity tasks and enhance the understanding of situations to be analysed during computer systems' cyber protection.

Based on the analysis of Ukrainian legislation in the field of information and cybersecurity, as well as the NATO Cybersecurity Curriculum Framework, the research [21] provides examples of competency models for cybersecurity professionals within the national cybersecurity system. The article proposes models of professional competencies that can serve as a basis for improving educational programs and curricula for training professionals in the field of cybersecurity, primarily at the undergraduate level of higher education. Additionally, these models could be used for adjusting higher education standards for the specialty 125 "Cybersecurity and Information Protection," including the third (educational and scientific) level.

In the work [22], examples of professionally oriented tasks are provided for higher education students majoring in 'Cybersecurity,' which involve the utilization of information and

communication technologies and expand the possibilities of applying software tools in the educational process, including during situational method sessions.

However, despite the positive outcomes of fundamental and applied research, many proposals have been subject to criticism due to their limited adaptability to the real-time changes of modern cyber threats [23]. Current educational programs are centered around manually configuring tasks for practical sessions, which is both exhaustive and error-prone. Also, these programs allocate minimal attention to the integration of artificial intelligence.

The research goal. The purpose of the article is to study the use of artificial intelligence to improve the method of situational learning in the formation of the competences of cyber security specialists and to provide practical recommendations for the further development of the system of personnel training in the field of cyber security.

2. THE ESSENCE OF THE SITUATION METHOD

The situational method of learning, known worldwide as the case method (Case Study – studying a situation), is one of the most effective teaching approaches in cybersecurity. It is employed to provide practical education to students and prepare them for real-world situations they might encounter in their professional careers. Through this method, the most effective development of competencies occurs as a dynamic fusion of knowledge, skills, and practical abilities [2].

When applying the situational method, students are provided with opportunities to solve real tasks related to threat detection and analysis, cybersecurity problem-solving depending on the type of cyberattacks, and the development of strategies to prevent future incidents. Students can explore system vulnerabilities, conduct security audits, develop protection plans, and security policies. Through role-playing games, they can assume different roles (hackers, system administrators, or cybersecurity analysts) and simulate scenarios that involve the application and formation of knowledge and skills related to system defense or security breach detection. The main stages of applying the situational method are illustrated in Figure 2.

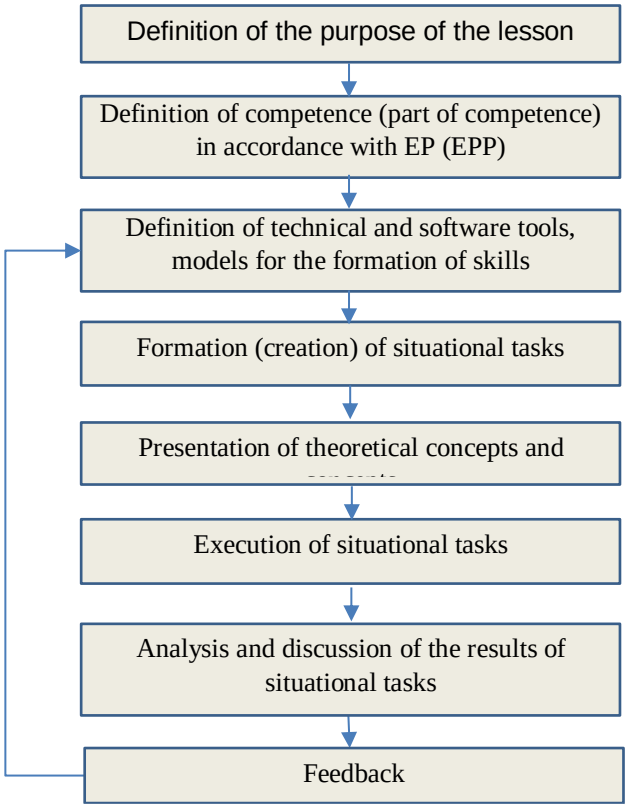

Figure 2. The main stages of applying the situational method

The application of this method allows students to gain practical experience and develop crucial skills in the field of cybersecurity, preparing them for real-world challenges they will encounter in their future professional careers. A key stage in this sequence involves designing situational tasks, the completion of which ensures the formation of necessary competencies and learning outcomes in line with the educational (educational-professional) programs for training cybersecurity professionals. Therefore,

implementing the method requires the prompt development of scenarios that reflect the current state of cyber threats.

3. RESEARCH METHODS

To study ways of enhancing the situational teaching method in developing competencies of cybersecurity professionals, interactive action research is successfully used. This approach combines research with practice, allows to learn and improve research methods based on practical outcomes. The core idea is that the researcher collaborates closely with practitioners, studies practical issues and implements improvements in real environment. One of the models of this method is the model of operational (or technical) action research (Figure 3), typically visualized as a cycle of steps: 'Plan → Act → Observe → Reflect'.

In the context of improving the method of situational training in cyber security, Action Research has the following stages (Figure 4):

Figure 3. Functional diagram of the technical action research model

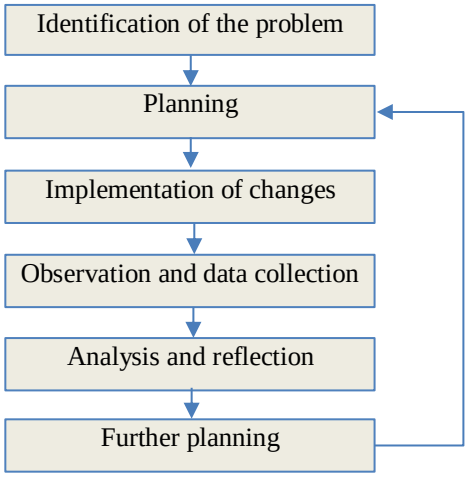

Figure 4. Stages of application of the action

With the aim of creating a more effective learning structure, the plan developed in accordance with the research stages (Figure 4) included:

1. Defining competencies to be developed by the situational teaching method within a specific academic discipline in line with the curriculum;
2. Searching for technical teaching tools;
3. Creating tools to automate the generation of learning situations;
4. Designing scenarios and evaluating program effectiveness;
5. Adjusting obtained results;
6. Formulating recommendations.

4. THE RESULTS AND DISCUSSION

The training of masters in Cybersecurity under the educational-professional program of the second (master's) level of higher education, "Information and Cybersecurity Management" [24], at the State University of Information and Communication Technologies involves obtaining the qualification of a "Master in Cybersecurity with specialization in Information and

Cybersecurity Management." This qualification is based on the competencies acquired during the learning process.

Critical managerial competencies that masters in Cybersecurity should possess include those associated with adhering to corporate and professional ethics in cybersecurity. This encompasses the ability to identify, articulate, and resolve teamwork-related issues, as well as the capability to plan and implement training, supervise and support personnel, and make effective decisions regarding information and cybersecurity issues.

Due to the multitude of positions in various fields where information and cybersecurity professionals can work after completing higher education, it's essential to create a significant number of situations during practical sessions (18 classroom hours) to cultivate the necessary students' competencies and achieve the planned learning outcomes. This approach improves their managerial skills in problem-solving and decision-making within the realm of cybersecurity.

To enhance the situational teaching method by rapidly generating scenarios for learning material development, an artificial intelligence tool developed by OpenAI, ChatGPT (Generative Pre-Trained Transformer), was utilized. Using ChatGPT, a language model, in response to specific prompts, generated 12 thematic situations along with decision options, tailored to each student, within a 25-minute timeframe. Each situation variant, generated by the language model, along with its corresponding correct solution, ranged from 2500 to 4000 characters including spaces. Upon evaluation, it was observed that the context of the generated situational tasks by ChatGPT didn't fully correspond to the given instructions, indicating the need for editing prompts to guide the language model in forming precise situational tasks.

The evaluation of the relevance of the created situational tasks was conducted with the involvement of cybersecurity experts to determine the degree of correspondence between the generated text and the goal of fostering managerial competencies based on the criteria of content, structure, style, and completeness. The evaluation scale for correspondence to the competency-forming goal ranged from 0 (no correspondence) to 1 (complete correspondence). The initial evaluation of the correspondence of the generated tasks was performed by three experts.

The improvement of the second prompt to ChatGPT involved specifying the content of the request regarding the correspondence with the goal of cultivating managerial competencies in fields of cyber tools application (banking, industry, military, government administration). Adding the sentence "Let's work this out in a step by step way to be sure we have the right answer" at the end of the prompt allowed to break down the task into two to three steps, reduce the time for generating situational tasks, and obtaine better responses.

For the second evaluation of situational tasks, aimed at ensuring objectivity, five experts were engaged. The evaluation results for two generations of situational tasks are presented in Table 1.

Table 1

The result of the evaluation of situational tasks

No	Evaluation criterion	First evaluation experts			Second evaluation experts				
		1	2	3	1	2	3	4	5
1	Content	0,6	0,5	0,5	1	1	1	1	1
2	Structure	0,5	0,4	0,5	0,9	0,9	0,9	0,9	0,9
3	Style	0,5	0,7	0,6	1	0,9	0,9	0,9	0,9
4	Completeness	0,7	0,6	0,7	0,9	0,9	0,9	0,9	1

To measure the consistency between different experts in evaluating correspondence of the generated situational tasks to the goal of fostering managerial competencies, the

Krippendorff's alpha coefficient was applied [25]. The calculation of this coefficient was implemented in the Python programming language using the Krippendorff module within the Microsoft Visual Studio environment. The program listing is as follows:

```
import krippendorff
# first evaluation data
data1 = [
    [0.6, 0.5, 0.5, 0.7],
    [0.5, 0.4, 0.7, 0.6],
    [0.5, 0.5, 0.6, 0.7],
 ]
# Calculation of Krippendorff's Alpha of the first estimate
alpha = krippendorff.alpha(data1)
print("Krippendorff's Alpha 1:", alpha)
# second evaluation data
data2 = [
    [1, 0.9, 1, 0.9],
    [1, 0.9, 0.9, 0.9],
    [1, 0.9, 0.9, 0.9],
    [1, 0.9, 0.9, 0.9],
    [1, 0.9, 0.9, 1]
 ]
# Calculation of Krippendorff's Alpha of the second evaluation
alpha = krippendorff.alpha(data2)
print("Krippendorff's Alpha 2:", alpha)
```

The result of the calculation of the Krippendorff alpha coefficient (Figure 5) allows us to state that there is a fairly strong (0.41 - 0.6) consistency of the experts' evaluation of the first (0.484375) and second (0.5824175824175823) generation of situational tasks.

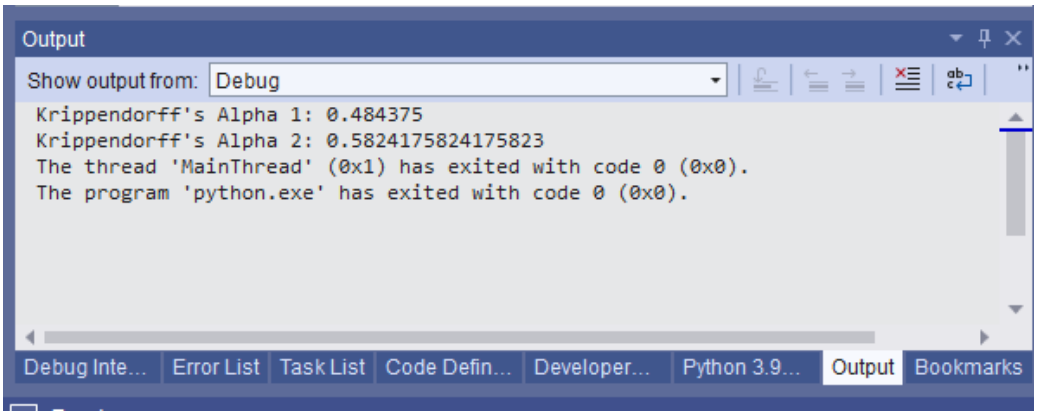

Figure 5. Calculation results Krippendorff's Alpha

The result of experts' evaluation of the relevance of the generated tasks (Table 1) confirms the effectiveness of using artificial intelligence to improve the method of situational learning. After editing the queries, the time spent on generating 12 thematic situations amounted to 9 minutes (Figure 6). In manual mode, creating such a quantity of variants would require a

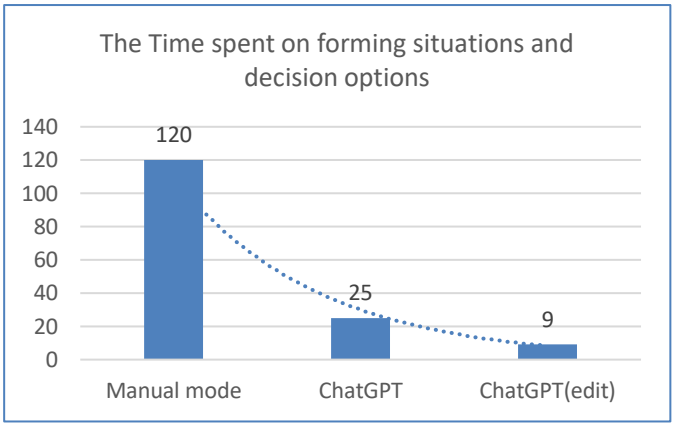

Figure 6. Effectiveness of using artificial intelligence

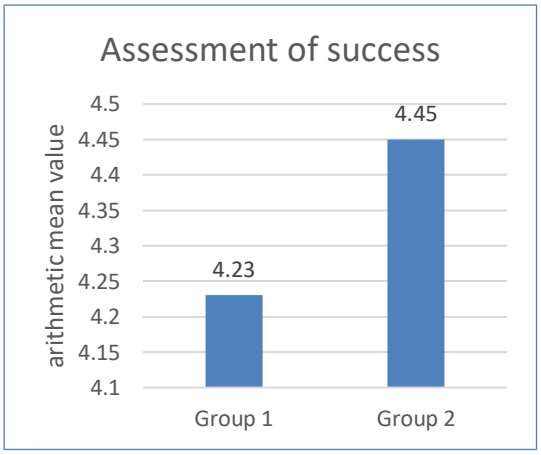

Figure 7. Comparison of success

significant amount of time (120 minutes or more), therefore, time savings has also been taken into account as a criterion for the effectiveness of applying ChatGPT.

Another important criterion for evaluating the use of artificial intelligence to enhance the situational teaching method is its impact on the quality of skill acquisition and managerial competencies of students. The indicator for this criterion is learning success. To determine this indicator, the performance results of an educational group (Group 1), where only one situation was considered, were compared to those of an educational group (Group 2) where a large number of situations generated by the ChatGPT language model were considered. The comparison of performance based on the arithmetic mean (Figure 7) confirms the effectiveness of the proposed enhancement method.

Thus, the method of enhancing situational learning through the application of artificial intelligence allows creating situational tasks almost in real time for the development of the competencies of cyber security specialists that meet modern requirements.

4. CONCLUSIONS AND PROSPECTS FOR FURTHER RESEARCH

The introduction of the latest IT in all areas of society's life, as well as the use of artificial intelligence technologies by cybercriminals, leads to the fact that cyber threats are constantly evolving, and the consequences of incidents are becoming more and more tangible. In such conditions, the demand for professionals with skills to prevent and counter cyber security threats is very high. And it will continue to grow as more companies and industries seek to protect their data and reputation. In order for cyber security specialists to be able to effectively perform their functions, it is necessary to constantly update their management competencies in accordance with the development trends in the field of IT and cyber security.

Designing various cybersecurity problem scenarios and defining the options of their solution using artificial intelligence can be an effective approach to foster managerial skills of cybersecurity professionals. The process of developing situational tasks on information and cyber security should inherently consider legal and ethical norms, as well as industry specifics. This pedagogical approach empowers students and cybersecurity practitioners to gain practical experience and skills essential for effectively addressing actual challenges in the field.

The investigation of the application of ChatGPT as an artificial intelligence tool to enhance the situational teaching method has confirmed its effectiveness. However, it is important to note that ChatGPT is a language model that generates text based on learned templates, examples, and rules, lacking personal experience or real-world interactions. Therefore, it's crucial to critically evaluate and verify the information provided by the system, with particular attention to context and adherence to the rules, laws, and ethical norms applicable in each specific situation.

A direction for further research will involve developing a specialized model using established Python programming language libraries in conjunction with the LMS MOODLE for automated assessment of correct solution variations in the form of textual blocks based on their comparison with a benchmark answer by the method of vector text representation.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] Decree of the Cabinet of Ministers of Ukraine of February 23, 2022, No. 286. "*On the approval of the Strategy for the Development of Higher Education in Ukraine for 2022-2032*". [Online]. Available: https://www.kmu.gov.ua/npas/pro-shvalennya-strategiyi-rozvitku-vishchoyi-osviti-v-ukrayini-na-20222032-roki-286- . Accessed on: Apr. 08, 2023. (in Ukrainian).

[2] Verkhovna Rada of Ukraine. (2014), *Law of Ukraine* "*On Higher Education*"*dated July 1, 2014 No. 1556 – VII, Gazette of the Verkhovna Rada (GVR),* [Online]. Available: https://zakon.rada.gov.ua/laws/show/1556-18#Text. Accessed on: Apr. 10, 2023). (in Ukrainian).

[3] Rawat, B. and Dwivedi, S.K, "An Architecture for Recommendation of Courses in E-learning System". *International Journal of Information Technology and Computer Science (IJITCS)* Vol.9, No.4, Apr. 2017, pp.39-47. doi: https://doi.org/10.5815/ijitcs.2017.04.06 (in English).

[4] Sonali Sharma and Shilpa Mahajan, "Design and Implementation of a Security Scheme for Detecting System Vulnerabilities". *International Journal of Computer Network and Information Security (IJCNIS)* Vol.9, No.10, Oct. 2017, pp. 24–32 doi: https://doi.org/10.5815/ijcnis.2017.10.03. (in English).

[5] Yu. Nosenko, M. V. Popel, M. P. Shishkina, "Cloud services and technologies in scientific and pedagogical activity: Methodological recommendations", Under the editorship M. P. Shishkina. - K.: IITZN National Academy of Sciences of Ukraine, 2016, 73 p. (in Ukrainian).

[6] A. Nashynets-Naumova., V. Buriachok., N. Korshun, O. Zhyltsov, P. Skladannyi, and L. Kuzmenko, "Technology for information and cyber security in higher education institutions of ukraine", *Information Technologies and Learning Tools (ITLT),* vol. 77, no. 3, pp. 337–354, Jun. 2020. doi: https://doi.org/10.33407/itlt.v77i3.3424. (in Ukrainian).

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

[8] S. Loboda and S. Denisenko, "Use of information and communication. interactive technologies in the professional training of publishing and printing specialists", *Information Technologies and Learning Tools (ITLT),* 2017. pp. 58-69. doi: https://doi.org/10.33407/itlt.v62i6.1939 . (in Ukrainian).

[9] van der Kleij, R., Leukfeldt, R. "Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security". In: *Advances in Human Factors in Cybersecurity. AHFE 2019. Advances in Intelligent Systems and Computing, vol 960.* Ahram, T., Karwowski, W. (eds) Springer, Cham. 2020. pp. 16-27. https://doi.org/10.1007/978-3-030-20488-4_2 (in English).

[10] O. Burov, et al. "Cybersecurity in educational networks*". Intelligent Human Systems Integration 2020: Proceedings of the 3rd International Conference on Intelligent Human Systems Integration (IHSI 2020): Integrating People and Intelligent Systems,* February 19-21, 2020, Modena, Italy. – Springer International Publishing, 2020, pp. 359-364. (in English).

[11] L. Arsenovych, "Further development of the system of professional training of cyber security specialists in the conditions of the development of digital technologies", *public*, vol. 3, September 2022, pp. 3-13, doi: https://doi.org/10.32851/tnv-pub.2022.3.1. (in Ukrainian).

[12] V. Buryachok, S. Shevchenko and P. Skladannyi, "A virtual laboratory for modeling processes in information and cyber security as a means of forming students' practical skills". *Cyber security: education, science, technology*. 2018. № 2, pp. 98–104. doi: https://doi.org/10.28925/2663-4023.2018.2.98104 . (in Ukrainian).

[13] M. Frank, M. Leitner and T. Pahi, "Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education". *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing*

and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, USA, 2017, pp. 38-46, doi: https://doi.org/10.1109/DASC-PICom-DataCom-CyberSciTec.2017.23. (in English).
[14] M. Kianpour, S. Kowalski, H. Øverby and E. Zoto, "From Cyber Incidents to Training Cognitive Situation Management: Work in Progress". *2020 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA),* Victoria, BC, Canada, 2020, pp. 163-166, doi: https://doi.org/10.1109/CogSIMA49017.2020.9216102. (in English).
[15] C. Pham, D. Tang, K. Chinen and R. Beuran, "CyRIS: a cyber range instantiation system for facilitating security training". *SoICT '16: Proceedings of the 7th Symposium on Information and Communication Technology*. December 2016, Pages 251–258, doi: https://doi.org/10.1145/3011077.3011087 . (in English).
[16] N. Chowdhury, S. Katsikas and V. Gkioulos, "Modeling effective cybersecurity training frameworks: A delphi method-based study". *Computers & Security*, Volume 113, 2022, doi: https://doi.org/10.1016/j.cose.2021.102551. (in English).
[17] R. Beuran, D. Tang, C. Pham, K. Chinen, Y. Tan, and Y. Shinoda, "Integrated framework for hands-on cybersecurity training: CyTrONE". *Computers & Security*. Volume 78, 2018, Pages 43-59, doi: https://doi.org/10.1016/j.cose.2018.06.001. (in English).
[18] H. Aldawood and G. Skinner, "Reviewing Cyber Security Social Engineering Training and Awareness Programs–Pitfalls and Ongoing Issues, *Future Internet*, vol. 11, no. 3, p. 73, Mar. 2019, doi: https://doi.org/10.3390/fi11030073 . (in English).
[19] J. Abawajy, "User preference of cyber security awareness delivery methods". *Behaviour & Information Technology*. 33:3, 2014, pp. 237-248. doi: https://doi.org/10.1080/0144929X.2012.708787. (in English).
[20] B. Akhmetov, V. Lakhno, Y. Boiko, and A. Mishchenko, "Designing a decision support system for the weakly formalized problems in the provision of cybersecurity", *EEJET*, vol. 1, no. 2 (85), pp. 4–15, Feb. 2017. (in English).
[21] V. Buriachok, V. Bogush, Y. Borsukovsky, P. Skladnannyi, and V. Borsukovskaya, "Model of training specialists in information and cyber security in higher education institutions of Ukraine", *ITLT,* VOL. 67, NO. 5, pp. 277–291, Oct. 2018. doi: https://doi.org/10.33407/itlt.v67i5. (in Ukrainian).
[22] N. Rotanova, T. Shabelnyk, S. Krivenko and Yu. Lazarevska, "The problem of training cyber security specialists: applied direction of mathematical disciplines". *Cyber security: education, science, technology*. № 1 (13), 2021, pp. 123-132. doi: https://doi.org/10.28925/2663-4023.2021.13.123132. (in Ukrainian).
[23] R. Gurnani, K. Pandey and S. K. Rai, "A scalable model for implementing Cyber Security Exercises," 2014 International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2014, pp. 680-684, doi: https://doi.org/10.1109/IndiaCom.2014.6828048. (in English).
[24] Management of information security, Educational and professional program of the second (master's) level of the higher world of the State University of Telecommunications. [Electronic resource]. Available: https://www.dut.edu.ua/uploads/p_1826_51261889.pdf. Accessed on: Apr. 10, 2023). (in Ukrainian).
[25] A. Zapf, S. Castell, L. Morawietz, Measuring inter-rater reliability for nominal data – which coefficients and confidence intervals are appropriate?. *BMC Med Res Methodol* 16, 93, 2016. doi: https://doi.org/10.1186/s12874-016-0200-9. (in English).

Text of the article was accepted by Editorial Team 21.08.2023

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ УДОСКОНАЛЕННЯ СИТУАТИВНОГО НАВЧАННЯ ФАХІВЦІВ КІБЕРБЕЗПЕКИ

Щавінський Юрій Віталійович
кандидат технічних наук, доцент кафедри управління інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних технологій, м. Київ, Україна
ORCID ID 0000-0002-2319-8983
yushchavinsky@ukr.net

Мужанова Тетяна Михайлівна
кандидат наук з державного управління,
доцент, доцентка кафедри управління інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних технологій, м. Київ, Україна
ORCID ID 0000-0002-7435-0287
muzanovat@gmail.com

Якименко Юрій Михайлович
кандидат військових наук, доцент,
доцент кафедри управління інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних технологій, м. Київ, Україна
ORCID ID 0000-0002-6848-852X
yakum14@ukr.net

Запорожченко Михайло Михайлович
асистент кафедри управління інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних технологій, м. Київ, Україна
ORCID ID 0000-0003-0182-9497
zaporozhchenkomm@gmail.com

Анотація. У статті визначена проблема необхідності постійного розвитку та вдосконалення практичних навичок спеціалістів кібербезпеки з огляду на постійне зростання кількості загроз інформаційній та кібернетичній безпеці організацій, підприємств, суспільства і держави та їх еволюцію. Обґрунтована актуальність впровадження інноваційних технологій з метою вдосконалення методів формування технічних і управлінських компетентностей фахівців кібербезпеки в закладах вищої освіти у відповідності із стратегічним напрямом реформування освіти в Україні. Актуальність формування у фахівців кібербезпеки вмінь і навичок оперативного реагування на загрози пов'язана із застосуванням кіберзлочинцями штучного інтелекту. Проведений у даній роботі аналіз наукових досліджень дозволяє зробити висновок про необхідність удосконалення ситуативного методу навчання як одного з основних способів формування компетентностей студентів спеціальності Кібербезпека та захист інформації в закладі вищої освіти. Одним із шляхів удосконалення методу є застосування інструментів штучного інтелекту при створенні різного роду завдань для проведення занять. Для створення навчальних ситуацій та варіантів розв'язання конфліктних ситуацій в управлінні кібербезпекою та кіберінцидентами з метою формування навичок прийняття своєчасних, правильних і ефективних рішень майбутніми менеджерами кібербезпеки запропоновано використовувати інструмент штучного інтелекту – мовну модель ChatGPT, яка своїми чудовими можливостями: узагальненням та аналізом статей, кодуванням, налагодженням, генерацією тематичних блоків ситуацій – свідчить про значний прогрес у галузі штучного інтелекту. Застосування ChatGPT дозволило за короткий час створити потрібну кількість ситуативних завдань з варіантами правильних рішень, якими було охоплено всі напрямки діяльності фахівців кібербезпеки. Разом з тим, при проведенні дослідження виявилась потреба в критичному оцінюванні та перевірці інформації, що надається моделлю, на відповідність контексту та правилам, законам та етичним нормам, які діють у кожній конкретній ситуації. Цю проблему вдалося вирішити шляхом уточнення та конкретизації запиту до мовної моделі ChatGPT для генерації ситуацій.

Ключові слова: інформаційні технології; штучний інтелект; ситуативне навчання; професійні компетентності; кібербезпека.

This work is licensed under Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.