4. Типове положення про службу захисту інформації в автоматизованій системі: НД ТЗІ 1.4-001-2000 / Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України. Київ. 2000. URL: https://tzi.com.ua/downloads/1.4-001-2000.pdf
5. Large Language Models for Cyber Security: A Systematic Literature Review / H. Xu та ін. arXiv.org e-Print archive. URL: https://arxiv.org/html/2405.04760v5

INNOVATIVE PEDAGOGICAL TECHNOLOGIES FOR DEVELOPING LEARNERS' CYBERSECURITY CULTURE

Hlushych Valentyna
Ph.D., Associate Professor
Department of Business Journalism and Digital Media
S. Kuznets Kharkiv National University of Economics,
Kharkiv, Ukraine
Hlushych Vitalii
IT Teacher Second Qualification Category
Slobozhansky State Lyceum
with Enhanced Military and Physical Training,
Kharkiv, Ukraine

In the context of the digital transformation of contemporary society, education is increasingly integrating information and communication technologies into all aspects of the educational process. E-learning platforms, cloud services, digital learning materials, distance and blended learning systems, interactive environments, electronic documents and online communication have become integral components of learners' educational activities. On the one hand, these technologies create new opportunities for personalised learning, broaden access to educational content, and support the development of independence, mobility and professional readiness. On the other hand, the active use of digital technologies generates new risks related to the protection of personal data, the security of user accounts, the reliability of information, digital ethics and responsible behaviour in the online environment.

In this regard, the issue of fostering a cybersecurity culture among learners is of particular importance. In contemporary scholarly and pedagogical discourse, digital competence is understood not merely as a set of technical skills required to use digital devices, software or electronic resources, but as an integrated personal quality. It combines knowledge, practical skills, value orientations, critical thinking, the ability to communicate safely in digital environments and the responsible use of information technologies in educational, professional and social activities.

Cybersecurity is one of the key components of digital competence, as it determines learners' ability to act safely and responsibly in the digital environment. Its content is not limited solely to the technical aspects of protecting digital devices or

software. Cybersecurity also includes the ability to protect personal accounts, personal data, learning materials and the results of educational activity, as well as the ability to recognise potential digital threats, critically evaluate information and make responsible decisions when working online.

The main components of a cybersecurity culture among learners include cyber hygiene skills, such as creating strong passwords, using multi-factor authentication, working safely with email, recognising phishing messages, exercising caution when using open networks, updating software in a timely manner and following privacy rules when using digital platforms. Equally important are the ability to verify the reliability of information sources, share digital content responsibly, adhere to the principles of academic integrity and understand the possible consequences of one's own behaviour in the digital environment.

The development of a cybersecurity culture among learners should not be episodic, but systematic, consistent and pedagogically purposeful. It is not sufficient merely to acquaint learners with a list of rules for safe online behaviour. It is necessary to create conditions for the practical application of these rules in real or simulated educational situations. For this reason, innovative pedagogical technologies have significant potential, as they stimulate cognitive activity, develop critical thinking, independence, communication skills and a responsible attitude towards the use of digital resources.

One of the key directions in fostering a cybersecurity culture is the use of interactive learning technologies. These technologies involve active interaction among participants in the educational process, discussion of problem-based situations, analysis of digital risks, group work, completion of practical tasks and collaborative decision-making. For example, when studying email security, learners may analyse examples of phishing emails, identify signs of fraud, formulate rules for secure communication and discuss the possible consequences of opening suspicious links or attachments without due caution.

Project-based learning is also an effective means of fostering a cybersecurity culture. It enables the combination of theoretical knowledge with practical activity and the creation of a concrete educational product. Learners may develop cyber hygiene guidelines, information leaflets, digital posters, video tutorials, presentations or mini-campaigns devoted to safe online behaviour. Such projects contribute not only to a deeper understanding of cybersecurity issues, but also to the development of skills in searching for, analysing, structuring and presenting information, as well as teamwork and digital creativity.

Simulation-based learning methods play an important role in this process, as they make it possible to model real-life situations involving cyber threats. It is advisable to use educational scenarios related to phishing attacks, personal data breaches, attempts at unauthorised access to accounts, violations of privacy rules or the unsafe use of open Wi-Fi networks. In analysing such situations, learners acquire the ability to identify a problem, assess risks, choose a safe course of action and predict the possible consequences of their own decisions.

Adaptive learning technologies make it possible to take into account learners' individual levels of digital competence. This is particularly important because participants in the educational process may have different experiences of using digital tools and different levels of awareness of cyber threats. Through an adaptive approach, teachers can select tasks according to learners' needs and abilities, gradually increase the complexity of learning material, provide individual support and create conditions for the progressive development of digital competence.

An interdisciplinary approach is especially important in fostering a cybersecurity culture. Issues of information security and cybersecurity should be integrated not only into computer science or digital technology courses, but also into the content of professionally oriented disciplines. This is due to the fact that, in their future professional activities, learners will work with sector-specific information systems, electronic databases, digital documents, online services and communication platforms. Therefore, the safe use of digital tools should be regarded as an integral component of a future specialist's professional responsibility.

A practice-oriented approach ensures that the content of education is connected with real digital situations. Within this approach, learners should not only master theoretical concepts, but also perform practical tasks, such as creating secure passwords, configuring privacy settings, verifying the reliability of information sources, analysing digital risks and identifying safe methods for storing and transmitting data. This format of learning contributes to the formation of stable patterns of responsible digital behaviour.

The competence-based approach to fostering a cybersecurity culture focuses the educational process on the learner's ability to act independently, critically and responsibly. It is not only a matter of knowing individual rules, but also of being prepared to apply them in various educational, professional and everyday situations. This orientation makes it possible to consider a cybersecurity culture as an important outcome of modern education.

Thus, fostering a cybersecurity culture among learners is an essential component of developing their digital competence in the context of the digital transformation of education. This process should be systematic, consistent, interdisciplinary and practice-oriented. Innovative pedagogical technologies create effective conditions for the development not only of technical skills, but also of critical thinking, responsibility, digital ethics and the ability to behave safely in the digital environment. A promising direction for further research is the development of methodological models for integrating the cybersecurity component into educational programmes, taking into account the specific features of learners' professional training.

References

1. Batsurovska I. V., Kashyna H. S., Makiievskyi O. I. Methodological approaches to the development of didactic materials for vocational education: from theory to practice. Modern aspects of science: XLVIII volume of the international collective monograph. Czech Republic: International Economic Institute s.r.o., 2024. P. 172–191.

2. Bondarenko V. I. Conditions and means of formation of information security skills of future teachers. Information Technologies and Learning Tools. 2019. Vol. 74, no. 6. P. 294–306. URL: https://journal.iitta.gov.ua/index.php/itlt/article/view/2550/1603
3. Kovalchuk A. Development of digital competence of future vocational education teachers in the context of digitalisation. Youth and Market. 2024. No. 2. P. 148–152.
4. Voloshanivska T. V. Improving the quality of cybersecurity specialists' training in the context of the digital transformation of education. Pedagogical Sciences. 2023. No. 7. P. 88–94.

РОЗРОБКА МЕТОДОЛОГІЇ ТА КОНЦЕПТУАЛЬНОЇ МОДЕЛІ ПЗ ДЛЯ РОЗПІЗНАВАННЯ DEEPFAKE КОНТЕНТУ

Нехороших Д.М.
асистент
Скрильник В.Ю.
здобувач вищої освіти бакалаврського рівня
Кафедра безпеки інформаційних технологій
Харківський національний університет радіоелектроніки, Україна

Анотація. У цій роботі розглядаються процеси виявлення синтетичного (Deepfake) медіаконтенту в контексті розвитку сучасних генеративних нейронних мереж та кіберінформаційних загроз. Обґрунтовується необхідність переходу від мономодальних рішень до багаторівневих мультимодальних методів розпізнавання. Розроблено архітектуру системи підтримки прийняття рішень, яка інтегрує структурний, візуальний, частотний та акустичний аналіз медіа. Програмне забезпечення гарантує точність ідентифікації та вирішує проблему «чорного ящика» процесів прийняття рішень штучним інтелектом.

Ключові слова: Deepfake, машинне навчання, мультимодальний аналіз, розпізнавання, штучний інтелект.

Вступ. Сучасна архітектура технологій ШІ, таких як генеративно-суперечливі мережі (GAN), варіаційні автоенкодери (VAE) та дифузійні моделі, слугує основою для розробки «діпфейків». Ці загрози включають різноманітні атаки за допомогою соціальної інженерії, обхід механізмів біометричної двофакторної аутентифікації та здійснення фінансового шахрайства. Існуючі методи розпізнавання втрачають актуальність через антикриміналістичний вплив каналу передачі: під час завантаження у соціальні мережі відео піддаються інтенсивному стисненню, внаслідок чого необхідний високочастотний шум остаточно знищується. Сучасні генератори також здатні маскувати свою присутність у спектральній та просторовій областях.