DEVELOPING CYBER HYGIENE SKILLS IN CHILDREN AS A FOUNDATION FOR THEIR INFORMATION SECURITY UNDER MARTIAL LAW

Olha HABORETS

The active use of digital technologies by children significantly increases the risks associated with information security, particularly during martial law, when information attacks become an integral part of hybrid warfare. Children often become targets of manipulation, harmful content, and psychological pressure online. Key threats include cyberbullying, where children are subjected to harassment on social media; phishing attacks aimed at stealing their personal data; and harmful content that can affect their psycho-emotional state and shape distorted perceptions of reality. Disinformation is another powerful factor used to manipulate public opinion, necessitating the education of children on mechanisms for its recognition.

To minimize these risks, it is essential to implement educational programs on the fundamentals of cyber hygiene, teach children how to verify information, and properly utilize digital protection tools. Parents and teachers play a crucial role, as they must possess a sufficient level of cyber security awareness and actively engage with children during their internet use. State and public initiatives should also focus on fostering digital literacy among young people, strengthening the protection of their personal data, and creating a safe online environment.

Recommended measures include developing national educational initiatives that integrate digital security courses into school curricula, enhancing the digital competence of parents, and establishing mechanisms for monitoring threats to children in cyberspace. Another critical aspect is international cooperation and the implementation of innovative methods for preventing cyber threats, including the use of artificial intelligence technologies to detect harmful content.

Special attention should be given to the rise of new types of digital threats, such as deepfakes, which can be used to create manipulative content, and cyber grooming—techniques employed by criminals to build trust with children for exploitative purposes. Developing skills to counter digital fraud schemes, which are becoming increasingly

sophisticated, is also crucial. Integrating modern analytical methods and machine learning algorithms for monitoring and preventing such threats can be a key step in ensuring the cyber security of the younger generation.

In the context of digitalization and growing cyber threats, fostering a culture of cyber hygiene among children must become a fundamental component of the overall education and security system of the state. Only a comprehensive approach that includes educational, technological, and legal measures will effectively protect children from information threats and equip them with the ability to use digital technologies safely.

REFERENCES

1. Габорець О. А., Горелов Ю. П., Кобзев І. В. Методичні аспекти викладання кібергігієни у рамках дистанційного навчання. Протидія кіберзлочинності та торгівлі людьми: матеріали міжнар. наук.-практ. конф., м. Кам’янець-Подільський, 23 трав. 2024 р.: ХНУВС, 2024. С. 159-161.

ПСИХОЛОГО-ПЕДАГОГІЧНІ АСПЕКТИ ФОРМУВАННЯ ЦИФРОВОЇ БЕЗПЕКИ У ДІТЕЙ З ОСОБЛИВИМИ ОСВІТНІМИ ПОТРЕБАМИ

Захар ДОЛГОВ, Владислав КОСЮЧЕНКО

Сучасне суспільство характеризується стрімким розвитком цифрових технологій, що значно впливає на всі аспекти життя, зокрема на освіту дітей з особливими освітніми потребами (ООП). Однак цифрове середовище містить не лише можливості, а й ризики, пов'язані з безпекою дітей. Такі діти можуть мати різноманітні специфічні когнітивні відхилення, що значною мірою впливає на їхню реакцію та адаптацію, здатність до критичного мислення, розпізнавання загроз та на фоні цього підвищення тривожності.

Проблема забезпечення цифрової безпеки дітей з ООП є актуальною через їхню підвищену вразливість до кіберзагроз. Через специфічні когнітивні спотворення діти з ООП частіше стикаються з неприйняттям в мережі, кібербулінгом, маніпуляціями, соціальними сигналами людей та труднощами в соціальних комунікаціях. Це вимагає розробки спеціальних психолого-