**Korogod Natalia,**
*associate professor, Head of the Department of Intellectual Property*
*and project management*
*National Metallurgical Academy of Ukraine, Dnipro*
**Popova Natalia,**
*associate professor, Head of the Department of Intellectual Property*
*and civil law disciplines*
*Cherkasy Bohdan Khmelnytsky National University*

# UNODC CYBERCRIME UNIVERSITY TRAINING MODULES AND FEATURES OF THEIR IMPLEMENTATION IN THE EDUCATIONAL PROCESS

The rapid development of information technology expands the freedom and opportunities for people, enriches society, creates a new global interactive market for ideas, research and innovation. At the same time, the benefits of today's digital world and the development of information technology are spreading cases of illegal use of personal data, illegal financial transactions, theft and fraud on the Internet. Cybercrime is becoming transnational and can cause significant harm to the interests of the individual, society and the state [1].

Given the above, for Ukraine, which is at war and constantly suffering from cyberattacks, the issue of cybersecurity is one of the main issues in the field of protection of national interests in cyberspace.

By cybersecurity we mean the protection of vital interests of man and citizen, society and the state during the use of cyberspace, which ensures the sustainable development of the information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to Ukraine's national security in cyberspace [2] .

In order to improve the cyber security situation in Ukraine, the Law on Basic Principles of Cybersecurity in Ukraine and the Cybersecurity Strategy of Ukraine were adopted.

One of the main priorities of the Cybersecurity Strategy of Ukraine is to increase digital literacy and culture of safe behavior in cyberspace, comprehensive knowledge,

skills and abilities that are needed to support cybersecurity goals, implementation of state and public projects to raise public awareness about cyber threats and cyber defense [2].

World best practices show that raising of the level of culture of using the Internet and raising public awareness of cybersecurity is best formed through the introduction of special educational programs in the educational process. Significant progress has been made in this direction by the United Nations Office on Drugs and Crime (UNODC), which has developed for the general public special distance university training modules on Education for Justice (E4J) as part of the Global Program for the Implementation of Justice. Doha Declaration, and part of a series of training modules on cybercrime and is accompanied by a textbook [3].

It should be noted that the textbook and 14 university modules are the result of joint work of leading experts and teachers from more than 25 countries. The modules cover current aspects of cybercrime and include both theoretical concepts and practical knowledge. Also, all modules in the E4J University of Justice series of modules contain of suggestions for special assignments in the classroom, student assessment, slides and other tutorials that teachers can adapt to their context and integrate into the existing curriculum. One Module contains a plan for a three-hour session, but can be used for shorter or longer sessions. The modules are also designed so that the components available in them can be modified by teachers in any country to suit individual educational needs. Each subtopic in the module can be studied in more details and can be transformed into an independent training course [3].

Unfortunately, given modern approaches to curriculum development and adherence to specialty standards, not all higher education institutions in Ukraine can introduce a separate cybercrime course in the educational process, which would include all 14 of the above modules. Given this situation, separate modules were introduced into the educational process at Cherkasy Bohdan Khmelnytsky National University, namely 10 Modules on Personal Data Protection and Processing and 11 Modules on Intellectual Property. Thus, materials from 11 modules were used in the teaching of such a subject as Intellectual Property Law. In particular, the causes,

grounds and alleged motives of infringements related to copyrights and trademarks carried out with the help of cyber technologies, as well as measures to prevent and protect against such offenses were considered [3].

In addition to 11 modules, the study of IT law covered key topics of module 10, such as the right to privacy as a human right, the link between confidentiality and security, the ways in which cybercriminals violate data privacy and security, and the law. relating to the protection of data and reports of damage to data security systems, as well as the ways in which data is protected (and may be protected) to ensure the security of persons, property and information [3].

So, after analyzing the above information, we can conclude that the complete digitalization of all spheres of public life is gaining momentum, and poses new challenges to society related to cybercrime. Increasing the level of digital culture and digital literacy among the civilian population comes to the fore. Education and educational activities are beginning to play a key role in this process. Among the available educational programs on cybercrime, we have identified University modules on cybercrime developed with the support of UNODC, which in our opinion fully cover all key topics on this issue. However, given modern approaches to curriculum development, unfortunately, not all universities in Ukraine can afford to include a whole course on cybercrime in their curricula. Therefore, the best option is the introduction of separate modules in the teaching of related subjects, as we have shown on the example of Cherkasy National University.

## References

1. Cybersecurity strategy of Ukraine. Access model. – [Електронний ресурс] – Режим доступу до ресурсу: https://zakon5.rada.gov.ua/laws/show/96/2016#Text

2. Law of Ukraine On Basic Principles of Cyber Security of Ukraine. Access model. – [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text

3. University Module Series Cybercrime. – [Електронний ресурс] – Режим доступу до ресурсу: https://www.unodc.org/e4j/en/ tertiary/cybercrime.html