

СЕКЦІЯ 8
ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ. КОМП'ЮТЕРНА
ІНЖЕНЕРІЯ. КІБЕРБЕЗПЕКА. ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ
СИСТЕМИ

UDC 37:004:316.772.5

Yury Polukarov, Ph.D, Associate Professor
Olena Zemlyanska, Senior Lecturer
Nataliia Kachynska, Senior Lecturer
Oleksiy Polukarov, Ph.D, Associate Professor
Nataliia Prakhovnik, Ph.D, Associate Professor
National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute»,
polukarov@ukr.net

**MAIN ASPECTS OF CYBER SECURITY AND ITS PLACE IN EDUCATIONAL
INSTITUTIONS**

Emergency situations caused by COVID-19 and the full-scale invasion of Russia into Ukraine have radically changed people's living conditions. In today's conditions, there is an urgent need to speed up the program announced by the government in 2019 for the wide implementation of computer technologies and various online services for the digitalization of the Ukrainian economy and a significant part of the humanitarian sphere. In practice, this primarily involves the creation of technical capabilities to provide all socially significant services in a digital online format while simultaneously providing real opportunities to attract the broad masses of the population of Ukraine to the use of modern digital technologies with the provision of access to high-speed Internet [1].

The special need and relevance of these transformations is also felt in the field of education. It is obvious that without in-depth digitalization and the speedy implementation of modern educational and information technologies based on it, today it is not possible to ensure not only the possibility of increasing, but also the preservation of the existing level of education quality. Of course, first of all, this concerns the study of disciplines related to ensuring human safety. The need for education seekers to develop the necessary competencies to solve various tasks to ensure the highest possible level of life safety and minimize risks to life and health in any spheres and situations in current conditions cannot be provided without the use of modern educational technologies and tools.

One of the priority tasks of modern times is to ensure the safety of human activities in the conditions of rapid development of information technologies and related risks. The Internet and gadgets, which have become an integral part of our lives, hide a whole set of dangers. This should be clearly understood by absolutely everyone who works in the worldwide information and communication network. It is no news to anyone that the modern Internet does not provide for anonymity. Thus, interested parties can easily trace any user by identifying the IP address of his computer [2]. Also, an Internet user may face the problem of cyberbullying – intentional harassment of a certain person that occurs over a long period of time. Do not forget about the excessive passion for computer games.

In order to prevent the aforementioned threats, the educational process requires the introduction of cyber security classes. It is very important to educate applicants about information hygiene, which will allow them to clearly recognize fake information, fraudulent online schemes and take appropriate measures.

In today's conditions, the study of the basic principles of information technology should be the same integral component of the educational process as teaching the basics of a healthy lifestyle, labour protection, environmental and fire safety. It is worth noting that for more effective

formation of competences in information hygiene, the study of its basics should be started as early as possible, that is, at the stage when the younger generation will start using computers, gadgets and gain access to the Internet. It is necessary to be clearly aware of the fact that cyberspace is a modern component of human safety. The child should already at an early age understand that when using the Internet, you need to follow certain clear rules, just like in real life: avoid communication with suspicious people, do not pollute the environment, check the information provided, try to conduct conversations as politely as possible.

Recently, information security has come to the fore. This process accelerated especially quickly after cyberattacks on government sites, banking sites, energy facilities, large companies, closed networks of the defense sector, and others, leaving no one in doubt about the importance of this area of security. That is why it is so important and expedient to expand the study programs of the subject “Basics of health” in schools, and the subject “Occupational safety and life safety” in vocational education institutions with a section on the basics of cyber security.

Today's conditions require all participants in the educational process to understand the impact of cyberspace on personality formation, to assess and consider the dangers that may be encountered. The use of video games in the process of learning cyber literacy will give students the opportunity to practice the rules of safe behavior in the process of the game in believable situations similar to those that can be encountered in real life and will teach them to make the right choices, which will significantly improve the level of protection against cyber threats. Important and relevant are correspondence with unfamiliar adults, the need and feasibility of using a VPN, secure Wi-Fi connection in public places, saving passwords to important resources directly in web browsers, and much more.

In order to preserve confidential information when working with Internet resources, one of the leading developers of the international software antivirus complex has provided a number of basic cybersecurity recommendations for ordinary users [3]:

- regularly check the degree of security of current accounts on various platforms and e-mail accounts;
- monitor the operation of the installed software;
- periodically reinstall the operating system and its components;
- be responsible when setting passwords;
- to observe the regime of double identification on the sites;
- periodically create copies of arrays of important data (for example to the Google Drive environment or to external hard drives);
- use proven licensed anti-virus programs with regularly updated databases.

The proposed approach will allow users of the Internet to identify fraudsters in a timely manner and protect important conference information.

Summing up, we can conclude that the Internet is a unique information environment that unites world achievements. At the same time, this is also a number of dangers that an inexperienced user may encounter. Recognizing potential risks in a timely manner, identifying online fraudsters, saving personal information, learning to distinguish authentic information from fake information is an important task of a modern teacher. This, in turn, requires teachers to regularly attend advanced training courses, including cyber security.

References

1. Barlett C. P. et al. Comparing cyberbullying prevalence and process before and during the COVID-19 pandemic //The Journal of Social Psychology. – 2021. – Т. 161. – №. 4. – С. 408-418.
2. Гончарова І. П. Кібербезпека як складова безпеки життєдіяльності закладів освіти. Матеріали Усеукраїнської науково-практичної інтернет-конференції: (26 жовтня 2022 р.) / Біла Церква: БІНПО ДЗВО «УМО» НАПН УКРАЇНИ. – 2022. – С. 154.
3. Биков В. Ю., Буров О. Ю., Дементієвська Н. П. Кібербезпека в цифровому навчальному середовищі // Інформаційні технології і засоби навчання. – 2019. – №. 70. – С. 313-331.