Олійник Богдан,
здобувач третього (освітньо-наукового) рівня вищої освіти
відділу відкритих освітньо-наукових інформаційних систем
Науковий керівник: ***Олексюк Василь****,*
доктор педагогічних наук, професор, старший дослідник,
провідний науковий співробітник відділу відкритих
освітньо-наукових інформаційних систем,
Інститут цифровізації освіти НАПН України,
м. Київ, Україна

BRIEF ANALYSIS OF DIGITAL TOOLS FOR DEVELOPING INFORMATION SECURITY COMPETENCE OF FUTURE COMPUTER SCIENCE TEACHERS

Introduction

With the active development of digital technologies and students spending more and more time in the digital world, an urgent problem arises - ensuring information security. Because the field of information security is dynamic and new threats and solutions are constantly emerging, it is important for future computer science teachers to stay abreast of new technologies. As noted by Chinese scientists Shen Changxiang, HuangGuo Zhang, Dengguo Feng, and others: “In recent years, momentous accomplishments have been obtained with the rapid development of information security technology. There are extensive theories about information security and technology” [1].

Digital tools help teachers to keep up with modern trends, ensuring that they provide their students with relevant information, and interactivity and practicality make teaching theoretical information more interesting and exciting. And their diversity allows you to choose the necessary digital tool in accordance with a certain educational material. According to Leah Zhang-Kennedy and Sonia Chiasson: “Researchers and practitioners have developed a variety of multimedia educational tools targeted at non-

expert end-users over the last couple of decades to increase awareness and address a knowledge gap in cybersecurity" [2].

Courses for developing information security competence of future computer science teachers

Given the need to ensure information security for both students and schools, more and more computer science teachers understand the importance of improving their skills in this area. In recent years, a large number of different information security courses have appeared on the education market, covering a wide range of topics, from basic knowledge of cyber hygiene to advanced techniques of ethical hacking, cyber threat analysis and infrastructure protection. Cisco courses take a special place among them.

The Cisco company has a special training format - an academic program (or, as it is called more simply, NetAcad - the Cisco network academy). The specificity of this format is that training is not conducted intensively and tightly according to the schedule, as in regular Cisco courses, but in short regular classes, which allows you to combine training with work.

The difference is that NetAcad has a fundamentally different approach to the qualification of students, which assumes that they have a minimum level of ICT competence, respectively, that they have practically no experience working with network technologies.

For example, the creators of the Cisco ICND1 (Interconnecting Cisco Network Devices) 3.0 course program assume that their typical student is an adult who is short-term upgrading his qualifications in his main profession. The developers of the material of the Cisco academic program proceed from the opposite - that a person has absolutely no experience in this field. Let's consider the main courses of the Cisco network academy, which can be used by future computer science teachers in the process of learning the basics of cyber security:

Introduction to Cybersecurity [3].

This course is for people who are just learning about cyber security and have no background in it. Estimated for 15 hours of training and is free. As indicated in the title of the course, the main focus of this course is on the formation of basic concepts in cyber security. After completing this course, the future computer science teacher will be able to:

- get acquainted with the basics of safe work on the Internet;
- learn about different types of malware, vulnerabilities and attacks, and how organizations protect themselves against these attacks;
- to understand the possible directions of career development of specialists in the field of cyber security.

This course forms the basis for future development of own knowledge and training in the field of cyber security.

Cybersecurity Essentials [4]

The course is designed for the student's average level of knowledge. It will be a good choice for people who already have some knowledge in the field of cyber security (ideally after completing the course "Introduction to cybersecurity"). The discipline is

designed for 30 hours of study, which is free. After completing this course, the future computer science teacher will be able to:

- understand procedures for implementing data privacy, integrity, availability, and security controls in networks, servers, and applications;
- determine cyber attacks and their signs, processes and information security countermeasures;
- understand techniques and procedures used by cybercriminals;
- understand how cybersecurity professionals use technologies, processes, and procedures to protect all network components;
- to acquire fundamental knowledge in various fields of security;
- acquire skills in security management, use of control, protection and impact minimization technologies;
- learn about ethical requirements and laws in the field of information security and methods of developing security policies;
- learn about the functions of cyber security specialists and career opportunities.

Digital tools for developing information security competence of future computer science teachers

In order for a future computer science teacher to be able to effectively teach his students about information security, he must have a good understanding of how an attack occurs in practice and what digital tools attackers use when conducting it [9].

Typically, an attack begins by gathering information about a potential "target" from all possible resources. Special tools, such as Maltego, are used to simplify this process. Maltego is an open source (OSINT) platform used for Internet intelligence, data collection and analysis, and for illustrating the connections between devices in a node-based graph [5]. The platform offers a graphical user interface that enables data mining and helps security professionals build a picture of threats in terms of their complexity and severity. This tool can collect information about domains, IP addresses, email addresses, phone numbers, social profiles and other metadata from sources such as search engines, websites, databases and other resources. Gathering information is an important step in conducting an attack, which is why a future computer science teacher, having put this tool into practice, will be able to more effectively explain to his students the importance of not posting personal information in the digital environment.

Let's consider some digital tools that will allow simulating the conduct of an attack for effective understanding, detection and countermeasures.

Gophish is an open source framework used for phishing. It makes it easy to test students' resistance to phishing attacks in the real world. Gophish is written in the Go programming language [6] and offers installation files on Windows, Mac, and Linux, as well as a Docker container for server deployment. With its help, teachers can generate phishing templates using a full-fledged HTML editor. Then, they can set up planned email attacks for student groups and monitor their responses in near real time. It has a user-friendly interface and simplifies the development and tracking of effectiveness of training attacks to increase student phishing awareness.

Ophcrack — is a free, open-source, GPL-licensed program that can help match passwords using LM hashes via rainbow tables [7]. Ophcrack includes an intuitive graphical interface, simplifying its use for individuals with minimal technical experience. Additionally, it has a command-line interface for experienced users who wish to automate processes or incorporate the tool into scripts. Ophcrack gives students a hands-on experience of password vulnerabilities and the importance of using unique, strong, and complex passwords.

Conclusions

The use of digital tools for the development of competence in information security is an urgent problem in the methodology of training future computer science teachers. The modern educational process actively integrates digital technologies, so teachers must not only use them, but also provide a safe learning environment. Knowledge and skills in the field of information security allow computer science teachers to teach students about Internet security, including detecting and countering phishing, password management, and data protection. Using digital tools helps students gain practical experience and be ready to apply their own acquired skills in real situations. “Widely recognized that hands-on exercises are critical for helping students reach course learning objectives”, – highlighted by Jim Marquardson and David Gomillion [8].

It is also worth noting that the use of such tools should correspond to the level of training of students and teachers, as well as the content of the school curriculum. In general, the use of digital tools for the development of information security competence is an important aspect of providing a safe educational space and contributes to the formation of digital skills in both computer science teachers and their students.

References

1. Shen Changxiang, HuangGuo Zhang, Dengguo Feng, ZhenFu Cao, and JiWu Huang. "Survey of information security." Science in China Series F: Information Sciences 50, no. 3 (2007): 273-298, URL: https://www.researchgate.net/publication/225221303_Survey_of_information_security

2. Leah Zhang-Kennedy, and Sonia Chiasson. "A systematic review of multimedia tools for cybersecurity awareness and education." ACM Computing Surveys (CSUR) 54.1 (2021): 1-39, URL: https://dspacemainprd01.lib.uwaterloo.ca/server/api/core/bitstreams/2064298a-2f61-4acb-907e-a96c4415f5ab/content

4. Cisco Networking Academy. Introduction to cybersecurity. Cisco Networking Academy: Learn Cybersecurity, Python & More, URL: https://www.netacad.com/courses/introduction-to-cybersecurity?courseLang=en-US

5. Cisco Networking Academy. Cybersecurity Essentials. Cisco Networking Academy: Learn Cybersecurity, Python & More, URL: https://www.netacad.com/trainings/cybersecurity-essentials?courseLang=en-US

6. Maltego search. Maltego, URL: https://www.maltego.com/search/

7. Gophish. Open-source phishing framework, URL: https://getgophish.com/#features

8. Ophcrack. URL: https://ophcrack.sourceforge.io/

9. Marquardson Jim, and David Gomillion. "Cyber security curriculum development: protecting students and institutions while providing hands-on experience." Information Systems Education Journal 16.5 (2018): 12, URL: https://isedj.org/2018-16/n5/ISEDJv16n5p12.pdf

10. Oleksyuk V.P., Oleksyuk O.R. The state of formation of information security competencies of future informatics teachers. Information technologies and teaching aids. 2017. Vol. 62, No. 6. P. 277. URL: https://doi.org/10.33407/itlt.v62i6.1906