Vladyslav Kyva, PhD
The National Defence University of Ukraine
named after Ivan Cherniakhovskyi
Kyiv, Ukraine
DOI: https://doi.org/10.30525/978-9934-26-222-7-34

ACQUISITION OF CYBER DEFENCE KNOWLEDGE BY TEACHERS OF HIGHER MILITARY EDUCATIONAL INSTITUTIONS

The issue of ensuring Ukraine's cybersecurity is becoming more and more vital regarding the hybrid war waged by the Russian Federation since the beginning of 2014. This issue is equally relevant for the EU and NATO member-countries and other countries setting a course for membership in these organizations. Therefore, one of the prioritized national security tasks for both Ukraine and other EU and NATO countries is countering the threats of misinformation and cyber influence.

It should be noted that today the Russian Federation is constantly trying to use Ukraine as a testing ground not only for testing new weapons and military equipment in the east of Luhansk and Donetsk

regions, but also for testing new cyber warfare tactics and techniques throughout Ukraine. In response to the Russian aggression and cyber influence on Ukraine's information systems (e.g., Petya/NotPetya virus and others), the Verkhovna Rada of Ukraine passed an important law «On Basic Principles of Cyber Security of Ukraine» [3] in October 2017, which takes into account modern European expertise and principles of the cooperation among state institutions, private sector and civil society in the cybersecurity sphere.

Article 10 of this Law reflects one of the most important aspects: "improving the digital literacy of citizens and culture of safe behavior in cyberspace, comprehensive knowledge, skills and abilities needed to support cybersecurity, state and public projects to raise public awareness of cyber threats and cyber defense [3], actualizing the cyber training of various categories of Ukraine's citizens in order to combat external or internal cyber influence by cybercriminals.

There is a social problem of very little knowledge of various categories of citizens about possible cyber threats and countering tools and techniques. This is due to the lack of training programs for citizens aimed at forming/developing the awareness and skills to support citizens' cybersecurity functioning at the state level. Currently, there is only a declaration of such intentions reflected in the laws [1; 3], but there are not enough practical actions taken to implement these intentions.

This problematic issue also concerns teachers of the military education system [2]. Therefore, the author have performed a study which serves as the basis for the training on the formation of cyber security skills in the National University of Defence of Ukraine named after Ivan Cherniakhovskyi teachers. In particular, the training considered modern methods of hacking, bypassing and protecting the access granting procedure in the Microsoft Windows operating system.

It should be noted that knowledge of these methods is a preventive cyber hygiene measure, as in everyday activities, any PC user can fall victim to a cyberattack implemented via the access granting procedure.

Thus, the results of the performed training indicate the following:

– firstly, our analysis of some tools and techniques of hacking, bypassing and protecting the procedure for granting access to a PC

proves the fact of their diversity and the need for constant monitoring. This fact was a prerequisite for forming and developing personal cybersecurity skills of Ukrainian citizens, in particular, the teachers of the National University of Defence of Ukraine named after Ivan Cherniakhovskyi, which are essential for their military, professional, and daily activities;

– secondly, there was introduced a cybersecurity training for teachers of the National University of Defence of Ukraine named after Ivan Cherniakhovskyi with input and output control of their knowledge of the identification, authentication and authorization concepts and their awareness and skills of applying tools and techniques of hacking, bypassing and protecting user access procedures in Microsoft Windows operating systems. When before the training the teachers had almost no understanding of the research concepts on the subject and no skills and abilities to support their cybersecurity, then after the training 100% of participants (all 235 teachers) showed the development of their cybersecurity skills;

– thirdly, the author took the first step to put into practice the law of the Verkhovna Rada of Ukraine «On the implementation of the basic principles of cybersecurity of Ukraine», namely «increasing digital literacy and culture of safe behavior in cyberspace, comprehensive knowledge, skills and abilities needed to support cybersecurity and public projects to raise public awareness of cyber threats and cybersecurity» [3], introducing this cybersecurity training.

References:

1. Decree of the President of Ukraine «On Cyber Security Strategy of Ukraine». Available at: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (accessed 12.02.2022). (in Ukrainian)

2. Kyva V. Yu. (2022) Analysis of factors affecting cyber security of a higher military educational institution. *Cybersecurity: Education, Science, Technique*. Vol. 3(15). pp. 53–70.

3. Law of Ukraine «On Basic Principles of Cyber Security of Ukraine».Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text (accessed 12.02.2022). (in Ukrainian)