UDC 004.491

Vladyslav Yu. Kyva
PhD of Pedagogical Sciences, Senior Research Fellow of General and Resource Planning Research Staff
The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID ID 0000-0002-6689-7530
kyvavlad30101991@gmail.com

Olha V. Zastelo
PhD of Pedagogical Sciences, Staff member
The Foreign Intelligence Service of Ukraine, Kyiv, Ukraine
ORCID ID 0000-0002-3443-4523
zolga777@ukr.net

Oleksandr M. Nakonechnyi
Head of the Information and Analytical Support Department – Deputy Head of the Administrative Management
The National Defence University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine
ORCID ID 0000-0002-7124-9431
o.m.nakonechnyi@gmail.com

FORMATION OF CYBER SECURITY SKILLS THROUGH METHODS OF HACKING, BYPASSING AND PROTECTING THE PROCEDURE FOR GRANTING ACCESS IN MICROSOFT WINDOWS OPERATING SYSTEM

Abstract. The article looks into the problematic issue of forming/developing teaching staff's cyber security skills (a case study of the teachers from the National University of Defence of Ukraine named after Ivan Cherniakhovskyi). The importance of this issue is fueled by the analysis of cyber security of user information on personal computers through the prism of vulnerabilities in the security mechanisms implementation for Microsoft Windows operating system (versions 7, 10), including access procedures. The key steps and specificities of the procedure for granting access (identification, authentication and authorization) in Microsoft Windows operating system are described. A survey among the teachers-respondents was conducted to figure out whether they understand the essence of the procedure for granting access and have some idea about methods of hacking, bypassing and protecting this access. The survey revealed that the teaching staff totally misunderstand the concepts and procedures. The issue of forming/developing teaching staff's cyber security skills becomes even more relevant amid the implementation of basic cyber security principles in Ukraine, adopted by the Verkhovna Rada in 2017. Accordingly, the authors describe typical modern tools of hacking, bypassing and protecting the procedure for granting access in Microsoft Windows operating systems (versions 7, 10), which will enable everyone to master some practical steps in order to realize the importance and necessity of key tools and techniques of ensuring personal cyber security. In doing so, the authors intended to visualize possible ways of cyber security violation and increase awareness about them with the aim of preventing cyber risks. In addition, the authors seek to inform different categories of people that contemporary information and communications technologies not only expand the capabilities of our global digital society, but also increase exponentially the number of objects vulnerable to cyber threats. In addition, our task was to promote the issues of forming/developing teachers' skills in supporting their cyber security by training them to implement some cyber security tools and techniques aimed at reducing cyber risks. Our attention is also paid to some ethical aspects in reviewing the outlined outcomes, presented for educational purposes in an effort to raise public awareness of the described vulnerabilities, which pose cyber risks to those involved in information sphere.

Key words: tools and techniques; hacking; bypassing; cyber security skills; identification; authentication; authorization; Microsoft Windows.

1. INTRODUCTION

The problem statement. The issue of ensuring Ukraine's cyber security 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 EU and NATO countries is countering the threats of misinformation and cyber influence.

It should be noted that today the Russian Federation is using Ukraine as a testing ground for testing not only new weapons and military equipment, but also new cyber warfare tactics and techniques. 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" [1] 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 cyber security sphere.

Article 10 of this Law reflects one of the most important aspects: improvement of the citizens' digital literacy and culture of safe behavior in cyberspace, their knowledge, skills and abilities needed to support cyber security, implementation of state and public projects to raise public awareness of cyber threats and cyber defence [1], calling attention to the importance of cyber training of various categories of Ukraine's citizens in order to combat external and internal cyber influence of 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 at the state level aimed at forming/developing people's awareness and skills required to support cyber security. Currently, there is only a declaration of such intentions reflected in the laws [1] – [2], but there are not enough practical actions taken to implement these intentions.

In order to find a solution to this problem, we analysed most typical tools and techniques of cyber influence on various information environment elements. The Ukrainian citizens are expected to become familiar with these real and hypothetically possible cyber threats in their daily activities. At the same time, this study seeks to take the first practical steps to raise awareness of Ukrainian society about cyber threats and cyber defence, which will help reduce cyber risks in the security and defence sector of Ukraine.

It is a well-known fact that today any teacher of a higher military institution is a user of a personal computer (PC), which is or may be an object of sensitive information (data) processing and storage. Therefore, a PC may be a target of cyber influence by the enemy, for instance, the Russian Federation agents [3], who are eager to steal any data necessary to destabilize Ukraine. Thus, the primary task is the formation/development of cyber skills of teachers of the National Defence University of Ukraine named after Ivan Cherniakhovskyi, as they need the relevant basic knowledge and skills in their professional activities.

Analysis of the recent research and publications. The issues of cyber hygiene and cyber security skills formation/development are covered in the works of the following foreign and Ukrainian scholars: A. A. Cain, M. E. Edwards and J. D. Still [4]; J. Esparza, N. Caporusso and A. Walters [5]; F. E. Eboibi [6]; K. Maennel, S. Mäses and O. Maennel [7]; Ken Modeste [8]; J. Nicholson and J. McGlasson [9]; J. A. Oravec [10]; S. Panda, E. Panaousis, G. Loukas and C. Laoudias [11]; P. Pusey and W. A. Sadera [12]; J. M. Such, P. Ciholas, A. Rashid, J. Vidler and T. Seabrook [13]; V. Yu. Bykov, O. Yu. Burov and N. P. Dementiievska [14]; O. Yu. Burov, O. Butnik-Siverskyi, O. Orliuk and K. Horska [15]; V. L. Buriachok, V. M. Bohush, Yu. V. Borsukovskyi, P. M. Skladannyi and V. Yu. Borsukovska [16]; V. P. Oleksiuk and O. R. Oleksiuk [17].

In addition, different aspects of operating system vulnerabilities, hacking detection, assessing software vulnerabilities and pen-testing were research topics of B. Cannoles and A. Ghafarian [18]; A. Gorbenko, A. Romanovsky, O. Tarasyuk and O. Biloborodov [19]; Y. Khera, D. Kumar and N. Garg [20]; Y. Kolli, T. K. Mohd and A. Y. Javaid [21]; A. Luse, A. Al Marzooqra J. Burkman [22]; R. Mahajan, M. Singh and S. Miglani [23]; S. Samtani, H. Zhu and H. Chen [24]; S. Shrivastava and T. K. Ramesh [25]; D. Stiawan, M. Y. B. Idris, A. H. Abdullah, M. Al Qurashi and R. Budiarto [26]; H. Y. Xiao and B. B. Zhao [27].

Thus, A. A. Cain, M. E. Edwards and J. D. Still [4] studied the influence of age, gender, experience and level of education in cyber hygiene. They note that users' cyber hygiene is a key element that plays a major role in combatting cyber threats. In addition, they argue that there is a need to constantly update the knowledge, skills and abilities to use different software in order to increase the level of cyber security in daily activities. Accordingly, those users who follow cyber hygiene measures have lower cyber risks.

J. Esparza, N. Caporusso and A. Walters [5] point out that cyber threats are becoming more complex and diverse, and therefore there is a need to update measures to counter different types of cyberattacks.

S. Panda, E. Panaousis, G. Loukas and C. Laoudias [11] argue that cyber hygiene measures are necessary to strengthen the level of cyber security of an organization, especially to protect against cyber attacks of social engineering, which are aimed at the human factor. In addition, they note that the relevant measures (recommendations) are usually superficial and do not take into account all the nuances of the use and operation of different purpose software.

P. Pusey and W. A. Sadera [12] studied the level of teacher training, in particular their ability to integrate different information technologies into the learning process and cyber security issues during their implementation. Accordingly, the researchers evaluated 318 teachers. The results showed that the teachers were not ready to implement and use information technology.

The research of V. L. Buriachok, V. M. Bohush, Yu. V. Borsukovskyi, P. M. Skladannyi and V. Yu. Borsukovska [16], who analyzed the most critical threats to global security in the information sphere, results in a conclusion about the growing information confrontation and increasing tensions between different countries. In addition, they emphasize the need to develop a quality model for training cyber security professionals.

In turn, H. Y. Xiao and B. B. Zhao [27] share important knowledge about cyber protection of Adobe Reader from cyberattacks. In particular, their study analyzed in detail the functionality, various technical means and limitations of the Adobe Reader sandbox.

R. Mahajan, M. Singh and S. Miglani [23] demonstrate how a hacker can exploit a vulnerability in the NTFS file system to hide malicious code on a victim's machine in order to carry out a cyberattack.

Also very interesting are the studies of Y. Khera, D. Kumar and N. Garg [20], who emphasize that the increasing number of different information technologies has enhanced the efficiency of various software, including mobile and Windows applications. However, this has made it difficult to use these systems and gave rise to potential cyber vulnerabilities that can be used by attackers (hackers) to carry out various types of cyber attacks and exploit hacked users' systems. In addition, the researchers emphasize that over the last 10 years, hacking has expanded dramatically. Accordingly, any organization finds itself in complex cyber uncertainty about the cyber protection of its systems and confidential data from the growing number of cyber attacks. Therefore, the researchers emphasize that it would be better to detect and identify these vulnerabilities in advance before a hacker could exploit them. Therefore, the authors focus on the analysis of the life cycle of testing for penetration into an information system, in order to assess the degree of its cyber security and further improvement.

V. Yu. Bykov, O. Yu. Burov and N. P. Dementiievska [14] analyzed the problem of cyber security of participants in the educational process and emphasized that it is not limited to technical aspects of information resources protection, but should include such types of protection as legal, technical, informational, organizational and psychological. In addition, the researchers emphasize that the most common cyber attack on participants in the educational process, including users, is the method of social engineering. At the same time, the authors also emphasize the constant need for the formation and development of cyber hygiene in the digital world.

Unresolved aspects of the problem. However, taking into consideration these significant scientific developments, it should be noted that currently there are no scientific studies explaining and illustrating some specific and, in some sense, undocumented vulnerabilities of security tools of Microsoft Windows operating systems (versions 7, 10), in particular, procedure for granting access.

The aim of the article is to analyze the existing methods of hacking, bypassing and protecting the procedure for granting access in Microsoft Windows operating system and to feature the results of a training conducted at the National University of Defence of Ukraine named after Ivan Cherniakhovskyi specifically with the aim of forming cyber security skills of the teaching staff.

2. RESEARCH RESULTS

Cyber security is an important aspect of today's world, as government, military, corporate, financial, and medical organizations collect, process, and store vast amounts of data on digital devices. As intellectual property, financial data, personal information, or other types of data may be confidential, unauthorized access to these data, their disclosure, or leakage may have a negative impact on security and defence sector of Ukraine. In the digital age, people depend greatly on the Internet and storage devices in many aspects of our daily lives, so they should stay vigilant and protect their activities from cyber threats. To ensure cyber security, people need to pay attention to the current cyber hygiene strategy, i.e., they are expected to apply their cyber security skills to protect and maintain their digital devices and systems properly. Thus, cyber security implies maintaining security of equipment, software and information technology infrastructure, permanent network monitoring, briefing and training of various categories of information and communication technology (ICT) users. Cyber security can be effective only if ICT users develop their essential cyber security skills in their daily work.

According to the development and rapid spread of various types of cyber threats, there is a need to develop skills in cyber security of users, namely the acquisition of knowledge and practical experience in cyber security of PC. In particular, we propose to consider the protection mechanisms of the Microsoft Windows operating system, the procedure for granting user access to the PC: what it is and why it is needed in the context of user's cyber security.

Digital globalization has made it possible to receive, store and transmit information without restrictions, but at the same time, a considerable part of this information needs protection. One of the most important tools of information protection is the restriction of access to a PC (where confidential data is stored) by means of the procedure for granting access. The access to information (data) can be obtained by the person who has the right to do so, and this right can be obtained through the procedure for granting access, i.e., through the process of identification, authentication and authorization, without which no information protection system is available in modern operating systems, including Microsoft Windows. Let's define the key concepts: identification, authentication and authorization.

Authorization is granting a certain user or a group of users the right to perform certain actions, and the procedure of verification (confirmation) of the rights granted while performing these actions [28]. From the point of view of any information system, authorization is a procedure for granting access to a person (user) to perform appropriate actions (operations) based on the person's (user's) knowledge.

By this time, the person (user) should already be identified (pass identification – we need to know who it is) and authenticated (pass identification – confirmation of identity). Thus, the procedure for granting a user access to the PC is implemented through the mechanisms of identification, authentication and authorization.

These processes are integrated in the procedure for granting access to a PC (Fig. 1).

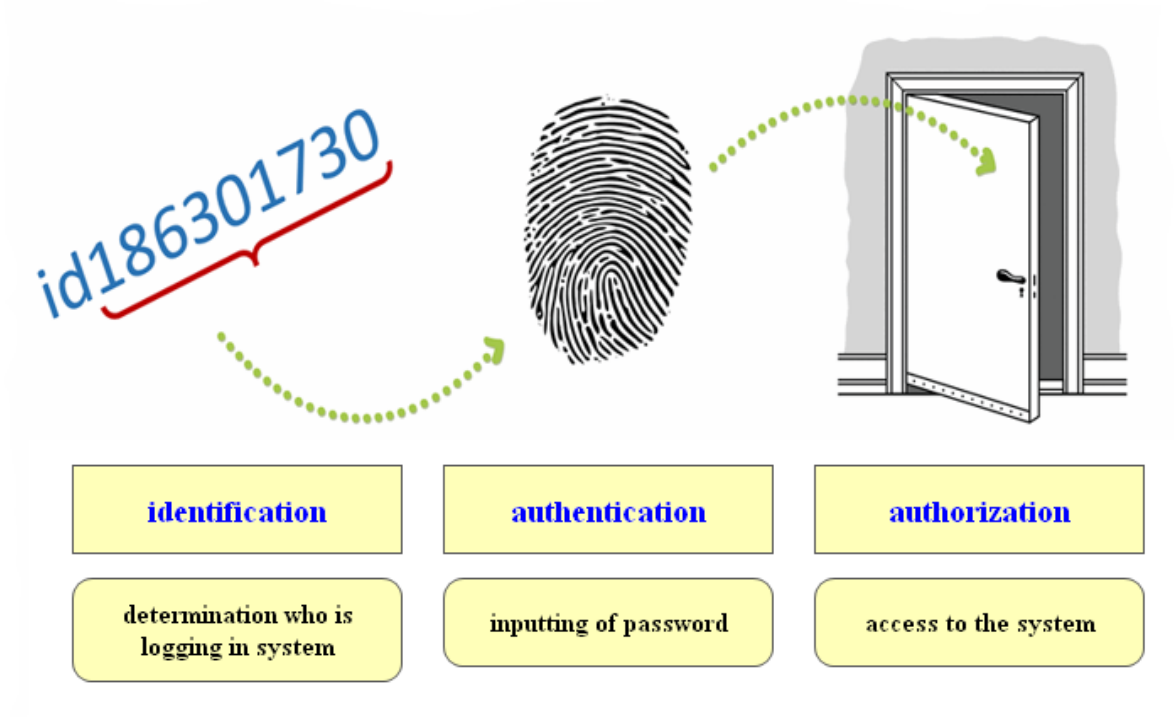

Fig. 1. Procedure for granting a user access to the PC

One of the most common and simplest ways of granting access to a PC is by entering a login and a password. This procedure has already been built into operating systems and information services. The use of passwords is generally accepted to be a rather weak tool of verifying the access rights granting and the main password reliability factor is its complexity. One of the specific features of the human brain is that a person is unable to remember unique, long and complex passwords, though such passwords are considered the most reliable in terms of cyber security. In turn, simple passwords become cyber vulnerable.

We conducted a survey among teachers (235 people) of the National Defence University of Ukraine named after Ivan Cherniakhovskyi in order to determine their awareness in the context of protection of personal data stored on their PCs, their understanding of "identification", "authentication", "authorization" concepts and their awareness of hacking, bypassing and protecting the access procedure. The survey revealed that 83% of the teachers (195 people) have an ambiguous idea of these concepts, misunderstanding cyber risks and threats posed by the methods of hacking and bypassing the procedure for granting access to PCs. Consequently, there is an urgent need for these teachers to become aware of hacking and bypassing tools and techniques of protecting the procedure for granting a user access to a PC.

After considering the essence and content of access procedures in PC and given the results of the teachers' survey, we thought it essential to analyze tools and techniques of hacking, bypassing and protecting access procedures in Microsoft Windows operating system (versions 7, 10) and present them in the article in order to provide a wide range of PC users with this important information.

2.1. Hacking the procedure for granting a user access to a PC in Microsoft Windows operating system (versions 7, 10).

Security Accounts Manager (SAM) is a registry file in Windows, used from Windows NT to the latest versions of Microsoft Windows. SAM stores hashed user passwords (LM hash or NTLM hash). Passwords are relatively secure due to the fact that the hash function is one-way. Obtaining a hash of the operating system users' passwords is usually the initial step leading to compromising the system in the future. Access to hashed passwords gives the "green light" for cracking the password and its decryption (brute force).

Thus, let us consider the way of obtaining hashed passwords from SAM. An attacker can simply take advantage of the user's absence at the PC and gain access to the system and data, i.e., obtain hashed passwords from SAM. Therefore, if an attacker has gained physical access to the system, for example, when they have got your PC, or when social engineering has worked successfully, they usually take the following steps:

1. The attacker uploads from a USB drive with the GNU-Linux operating system installed, which allows him/her to bypass the internal security system of the Microsoft Windows operating system to block access to SAM hash passwords, both ordinary users and even system administrators for security.

2. After uploading, the attacker copies the following files: SAM and SYSTEM (system encryption key), located at «C:\Windows\System32\config».

3. An attacker can use various utilities, such as: SAMInside, John the Ripper, RainbowCrack, LCP. They enable him/her to decrypt two files (SAM and SYSTEM), previously copied from the attacked PC and, accordingly, to further dictionary attack in the full search or hybrid hacking mode. Accordingly, in the dictionary attack mode, the program takes the hashes of words from the dictionary and compares them to the hash copied from the attacked PC. Words from the dictionary can be modified according to the configured system of rules. Programs usually come with a dictionary of 4 million lines. When in brute-force mode, the program goes through all possible combinations of passwords, i.e., applies the probabilistic approach, which first checks the statistically more popular combinations of characters. Thus, the probability of how fast his password can be cracked (decrypted) depends on the complexity and length of the password created by a PC user.

2.2. Bypassing the procedure for granting user access to a PC in Microsoft Windows operating system (versions 7, 10).

During the procedure of granting access in the Microsoft Windows operating system it is possible to activate the Sticky Keys feature on the prompt screen while entering the user's password by pressing the Shift key 5 times (Fig. 2) or activating the accessibility feature (Fig. 3).

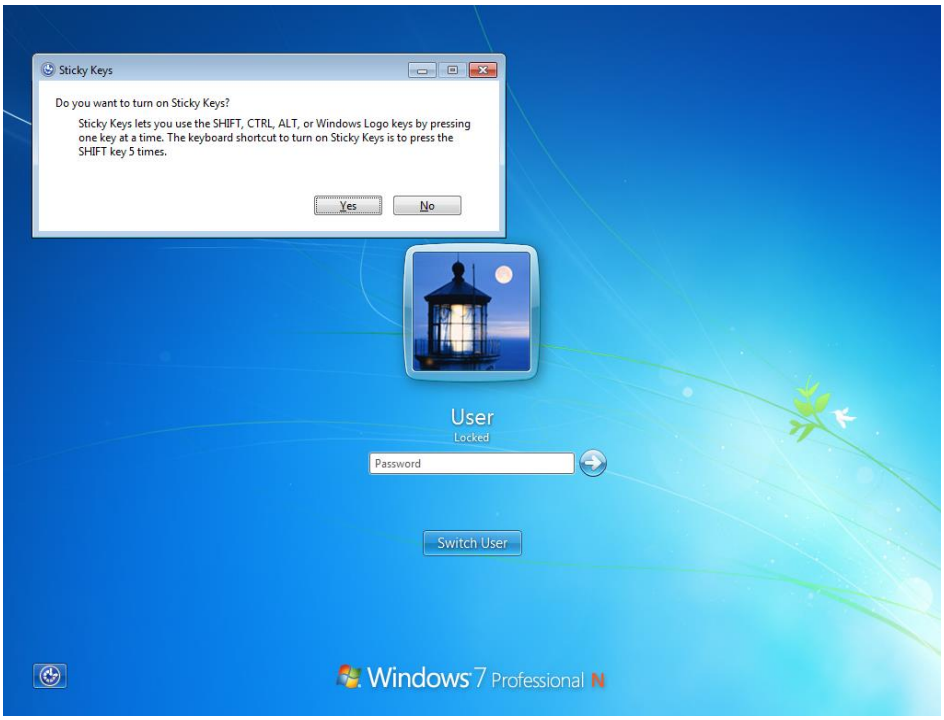

Fig. 2. Activating the Sticky Keys feature

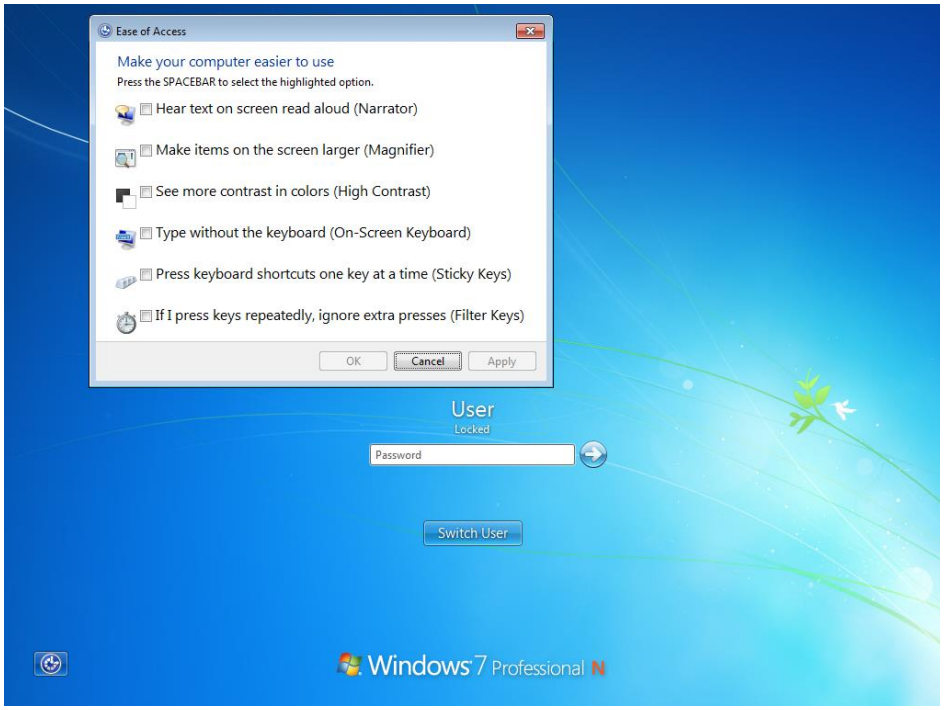

Fig. 3. Activating the accessibility features

The Sticky Keys and accessibility features are activated by sethc and utilman software, respectively, which are indirectly related to the vulnerability of the Microsoft Windows operating system itself, i.e., the ability to gain administrator access to these files. Let's have a look at how an attacker can exploit this vulnerability to gain access to a user's PC by performing these steps:

1. When booting the Microsoft Windows operating system, an attacker forcibly restarts the PC by pressing the RESET key or holding down the power button for 5 seconds.

2. The appropriate reaction of the operating system to such manipulations is to launch it into the selecting mode for further launching (Fig. 4).

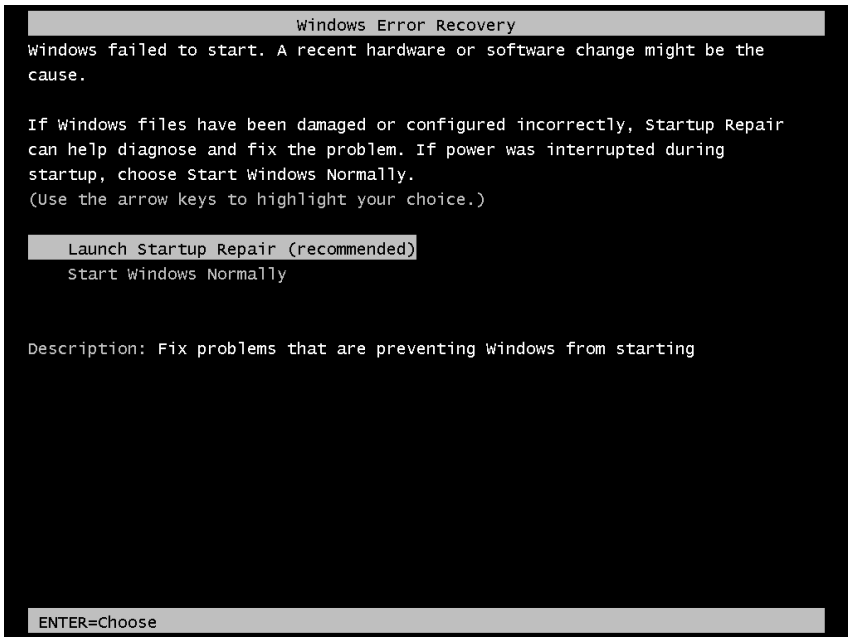

Fig. 4. Selecting the mode for further launching of the operating system

In this case, we choose the "Launch Startup Repair (recommended)" mode and wait for the appropriate download to restore, the waiting time can vary from 5 minutes to 2 hours.

3. After restoring the operating system, a dialog box will appear with information about the lack of ability to automatically restore the operating system (Fig. 5).

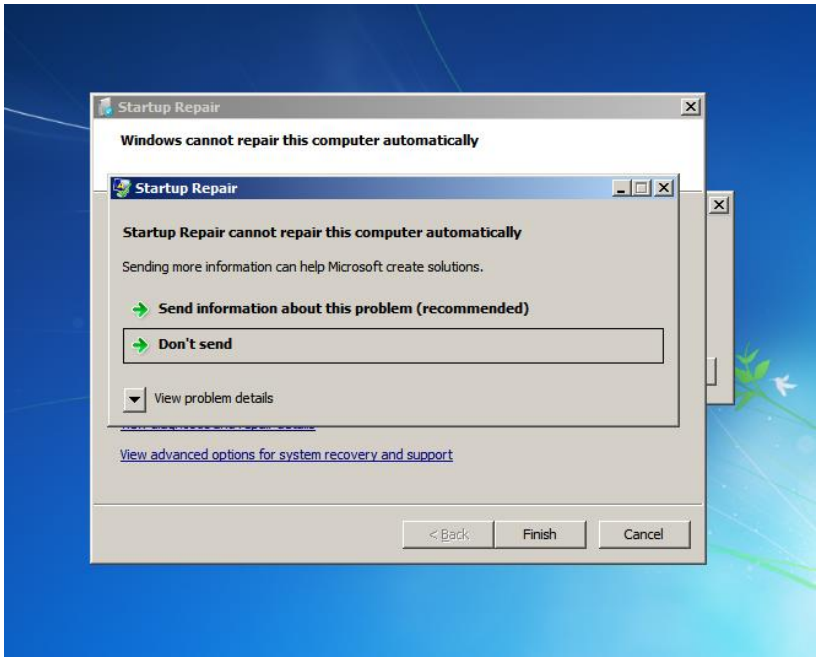

Fig. 5. Dialog box with information about the lack of automatic repair

Then we click on the "View problem details", go to the bottom of the window using the scroll bar and click on the link "X:\windows\system32\ru-RU\erofflps.txt" (Fig. 6). In doing so, we run the Microsoft Windows Notepad with Administrator access to Microsoft Windows system files. The attacker intends to gain access to the system files sethc, utilman and cmd. In order to access, you follow certain sequence of steps through a text notebook: file → open → my computer → select the system drive → file type, select all files → go to → "Windows\system32\".

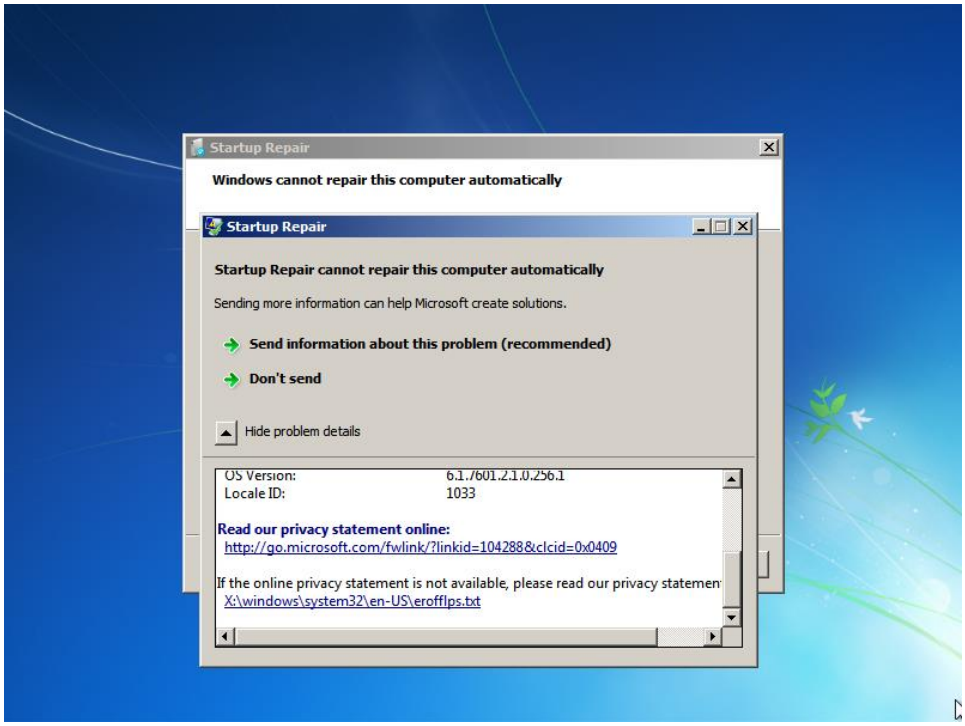

Fig. 6. Switching to operating system vulnerabilities

4. After successfully navigating to the specified directory address "Windows\system32\" you need to find the sethc, utilman and cmd software files, make copies of these files and rename them in the following order:

– sethc → to sethc_temp (just rename the file);
– utilman→ to utilman_temp (just rename the file);
– cmd → to cmd_temp1 and cmd_temp2 (first we make a copy of the file 2 times);
– cmd_temp1 → to sethc (rename the file);
– cmd_temp2 → to utilman (rename the file).

When completing all these steps, you can restart the PC for further actions.

5. The operating system reboots, but we already know that a vulnerability has been used to reassign the administrator in order to run the appropriate software during the procedure for granting access to the PC. We press the Shift key 5 times and watch the result of our previous actions on the screen, how the command line with the administrator's privileges starts running instead of the Sticky Keys feature (Fig. 7). The same thing happens, when you launch the accessibility feature.

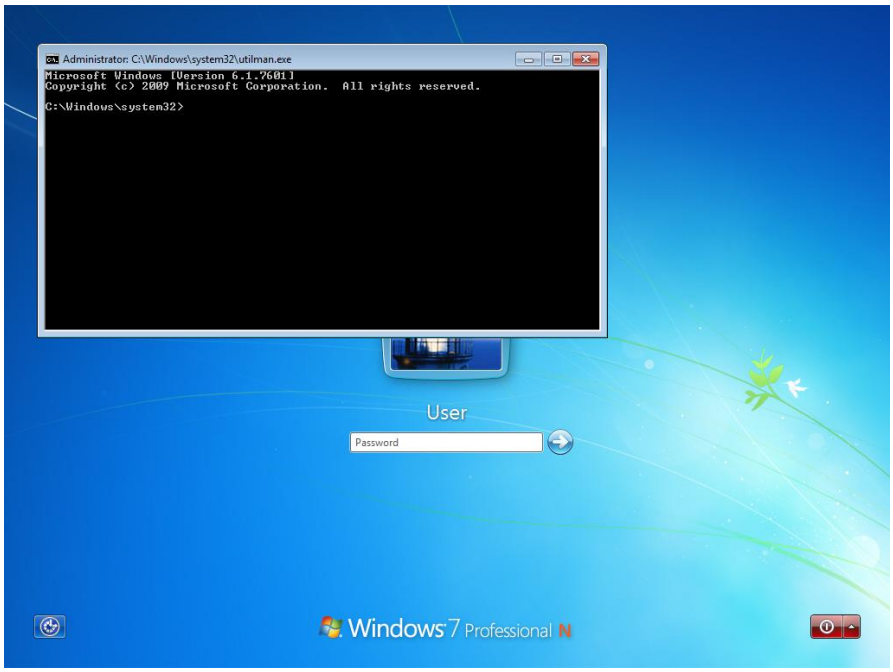

Fig. 7. Running the command line instead of the Sticky Keys feature

6. When an attacker gains access to the command line with administrator privileges, they may use the command net user to delete (replace) the old password or create a new user with administrator privileges.

The described technique of bypassing the access procedure can be applied to both Microsoft Windows versions 7 and 10. The only difference will be the order of transition to recovery mode, described here:

1. When booting the Microsoft Windows 10 operating system, you must forcibly restart the PC by pressing the RESET key or pressing and holding the on/off key for 5 seconds and doing so two times. As a result, the operating system launches the automatic repair (Fig. 8).

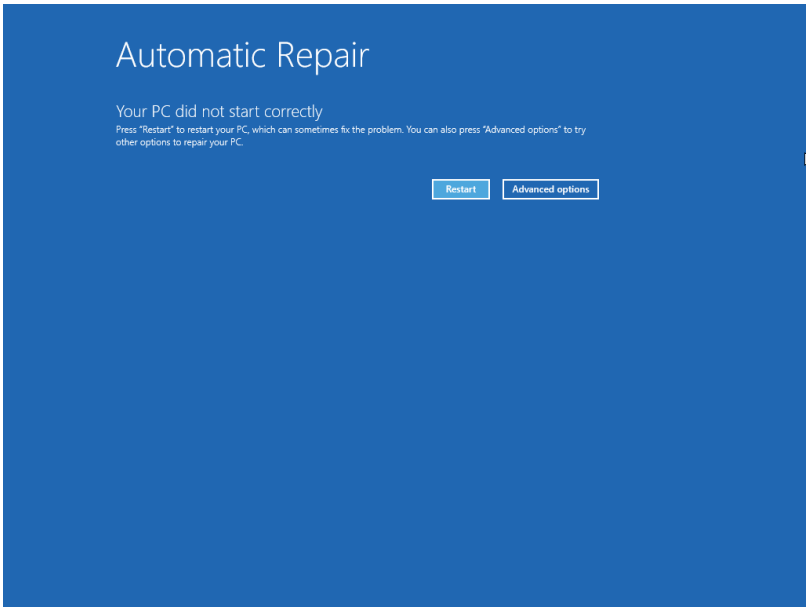

Fig. 8. Launching the automatic repair of the operating system

Then we move on to advanced options, troubleshoot, advanced options, command prompt (Fig. 9).

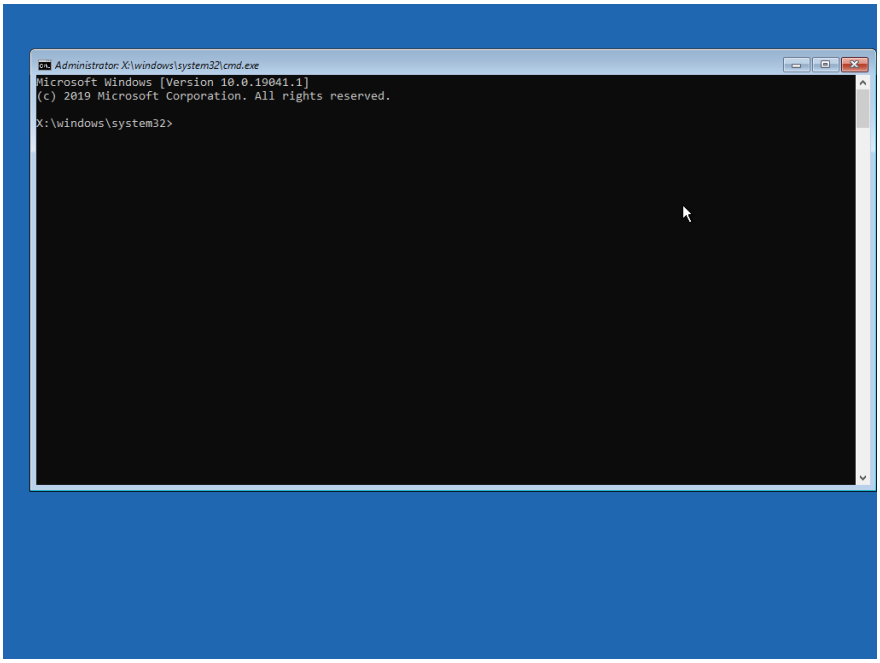

Fig. 9. Going to the command prompt with administrator privileges

2. After that, we run a text notebook from the command line using the notepad command and repeat the steps as described above for Microsoft Windows 7 operating system.

2.3. Protection of the procedure for granting access to the PC in Microsoft Windows operating system (versions 7, 10).

The analysis of tools and techniques of hacking and bypassing the procedure for granting access to a PC reveals vulnerabilities in Microsoft Windows, which is a prerequisite for violating access confidentiality to relevant data (information) by an attacker. Consequently, there is an urgent need to counter these tools and techniques of bypassing and hacking the procedure for granting access to a PC. Most users may immediately say that you just need to set a password for a Microsoft Windows user account, but we already know that this method does not work.

Therefore, we offer the most reliable technique of counteraction to bypassing or hacking called the hard disk encryption technique in the Microsoft Windows operating system. It is worth noting that there is already a built-in BitLocker software in Microsoft Windows. However, like other software, it has some vulnerabilities, described in [29].

Let’s consider other software VeraCrypt [30], which is free of cyber vulnerabilities and is currently the most reliable software for hard disk encryption. We will consider this software capabilities and its key idea to ensure cyber security of data (information), in particular the protection of the procedure for providing user access to a PC in Microsoft Windows.

VeraCrypt is a cross-platform software used to encrypt data (information) on your hard drive (or any drive) for different types of operating systems: Unix; Linux and Windows. The main idea of this software is that when encrypting data (information) on a PC hard drive, the user will need to enter a password before booting the operating system. That is, the attacker will not be able to use the methods of hacking or bypassing the procedure for granting access to a PC by blocking the operating system booting with a password and data (information)

encryption, which will not allow the attacker to manipulate already encrypted files. Information on the installation procedure on a PC can be found in [30].

2.4. Outcomes of the formation/development of cyber skills of the teaching staff of the National University of Defence of Ukraine named after Ivan Cherniakhovskyi

In order to form/develop teachers' cyber security skills in tools and techniques of hacking, bypassing and protecting the procedure for granting access to a PC in Microsoft Windows, we conducted a training at the National University of Defence of Ukraine named after Ivan Cherniakhovskyi. The outcomes of this training are presented in tables 1-3.

Table 1

Teachers' knowledge of the identification, authentication and authorization concepts

Concept	Before the training		After the training	
	Teachers who had an idea about the concept	Teachers who did not have any idea about the concept	Teachers who had an idea about the concept	Teachers who did not have any idea about the concept
Identification	16	219	235	0
Authentication	9	226	235	0
Authorization	16	219	235	0

At the beginning and at the end of the training conducted for 235 teachers, the input and output controls were performed, revealing the following (Table 1):

1. Before the training:

– 7% (16 teachers) had an idea about the identification concept, whereas 93% (219 teachers) lacked this knowledge;

– 4% (9 teachers) had an idea about the authentication concept, whereas 96% (226 teachers) lacked this knowledge;

– 7% (16 teachers) had an idea about the authorization content, whereas 93% (219 teachers) lacked this knowledge;

2. After the training:

– 100% of the participants (all 235 teachers) understood the concepts of identification, authentication and authorization.

At the same time, we tested the teachers' knowledge about tools and techniques of hacking, bypassing and protecting the procedure for granting access to a PC in Microsoft Windows and we found the following (Table 2):

Table 2

Teachers' knowledge about tools and techniques of hacking, bypassing and protecting the procedure for granting access to a PC in Microsoft Windows

Tools and techniques related to the procedure for granting access	Before the training		After the training	
	Teachers who had some knowledge of the methods	Teachers who did not have any knowledge of the methods	Teachers who had some knowledge of the methods	Teachers who did not have any knowledge of the methods
Hacking	0	235	235	0
Bypass	0	235	235	0
Protection	0	235	235	0

The outcomes revealed the following:

1. Before the training:

– 0% (0 teachers) had an idea about the tools and techniques of hacking, bypassing and protecting the procedure for providing access to a PC or, in other words, 100% (235 teachers) knew nothing about these tools and techniques.

2. After the training:

– 100% (235 teachers) knew about the tools and techniques of hacking, bypassing and protecting the procedure for providing access to a PC.

Finally, we checked the teachers' acquired knowledge and helped them practice in order to form/develop their cyber security skills in applying tools and techniques of hacking, bypassing and protecting the procedure for granting access to a PC in Microsoft Windows operating systems (Table 3).

Table 3

Teachers' skills in applying tools and techniques of hacking, bypassing and protecting user access procedures in Microsoft Windows

Application of tools and techniques related to the procedure for granting access	Before the training		After the training	
	Teachers who could apply these tools and techniques	Teachers who could not apply these tools and techniques	Teachers who could apply these tools and techniques	Teachers who could not apply these tools and techniques
Hacking	0	235	235	0
Bypass	0	235	235	0
Protection	0	235	235	0

The outcomes revealed the following:

1. Before the training:

– 0% (0 teachers) had skills in applying the tools and techniques of hacking, bypassing and protecting the procedure for providing access to a PC in Microsoft Windows before the training or, in other words, 100% (235 teachers) had no knowledge about these tools and techniques.

2. After the training:

– 100% (235 teachers) acquired skills enabling them to apply the tools and techniques of hacking, bypassing and protecting the procedure for providing access to a PC in Microsoft Windows.

Thus, as a result of the conducted teaching staff training there remained no teachers who did not know how to apply in practice the tools and techniques of hacking, bypassing and protecting the procedure for granting access to a PC in Microsoft Windows.

3. CONCLUSIONS AND PROSPECTS OF FURTHER RESEARCH

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 explains the importance of forming and developing personal cyber security skills for Ukrainian citizens, in particular, the teachers of the National University of Defence of Ukraine named after Ivan Cherniakhovskyi, as these skills are essential for their military, professional, and daily activities.

Secondly, we conducted a cyber security 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 in applying tools and techniques of hacking, bypassing and protecting user access procedures in Microsoft Windows operating system. If before the training the teachers had almost no understanding of the basic concepts and no skills and abilities to support their cyber security, after the training 100% of the participants (all 235 teachers) showed the development of their cyber security skills.

Thirdly, by conducting this cyber security training, the authors took the first step to put into practice the law of the Verkhovna Rada of Ukraine "On the implementation of the basic principles of cyber security of Ukraine", namely to implement the goal of improvement of the citizens' digital literacy and culture of safe behavior in cyberspace, their knowledge, skills and abilities needed to support cyber security, implementation of state and public projects to raise public awareness of cyber threats and cyber defence [1].

Promising areas of further research:

1. Development of a methodology and a specialized training course to form and/or develop teachers' competences in cyber security.

2. Search, analysis and publication of other cyber vulnerabilities to further inform various categories of people in order to form and/or develop their cyber security awareness.

REFERENCES (TRANSLATED AND TRANSLITERATED)

[1] Law of Ukraine «On Basic Principles of Cyber Security of Ukraine». [Online]. Available: https://zakon.rada.gov.ua/laws/show/2163-19#Text. Accessed on: 12.02.2022. (in Ukrainian).

[2] Decree of the President of Ukraine «On Cyber Security Strategy of Ukraine». [Online]. Available: https://zakon.rada.gov.ua/laws/show/447/2021#n12. Accessed on:12.02.2022. (in Ukrainian).

[3] Spy games. Why did Groysman's ex-translator come out of the pre-trial detention center?[Online]. Available: https://www.radiosvoboda.org/a/ezgov-derzgzrada-sud-shpygun/30038712.html. Accessed on:12.02.2022. (in Ukrainian).

[4] A. A. Cain, M. E. Edwards, J. D. Still,"An exploratory study of cyber hygiene behaviors and knowledge",*Journal of information security and applications*, vol. 42, pp. 36-45, 2018. (in English).

[5] J. Esparza, N. Caporusso, A. Walters, "Addressing Human Factors in the Design of Cyber Hygiene Self-assessment Tools", *International Conference on Applied Human Factors and Ergonomics*, Springer, Cham, pp. 88-94, 2020. (in English).

[6] F. E. Eboibi,"Cybercriminals and coronavirus cybercrimes in Nigeria, the United States of America and the United Kingdom: Cyber hygiene and preventive enforcement measures",*Commonwealth Law Bulletin*, pp. 113-142, 2020. (in English).

[7] K. Maennel, S. Mäses, O. Maennel, "Cyber hygiene: The big picture",*In Nordic Conference on Secure IT Systems*, Springer, Cham, pp. 291-305, 2018. (in English).

[8] Ken Modeste, "Current Standards for Cyber-Hygiene in Industrial Control System Environments",*Industrial Control Systems Security and Resiliency*, Springer, Cham, pp. 3-15, 2019. (in English).

[9] J. Nicholson, J. McGlasson,"CyberGuardians: improving community cyber resilience through embedded peer-to-peer support",*In Companion Publication of the 2020 ACM designing interactive systems conference*, pp. 117-121, 2020. (in English).

[10] J. A. Oravec,"Emerging "cyber hygiene" practices for the Internet of Things (IoT): professional issues in consulting clients and educating users on IoT privacy and security",*In 2017 IEEE International Professional Communication Conference (ProComm)*, pp. 1-5, 2017. (in English).

[11] S. Panda, E. Panaousis, G. Loukas, C. Laoudias,"Optimizing investments in cyber hygiene for protecting healthcare users",*In From Lambda Calculus to Cyber security Through Program Analysis*, Springer, Cham, pp. 268-291, 2020. (in English).

[12] P. Pusey, W. A. Sadera,"Cyberethics, cybersafety, and cyber security: Preservice teacher knowledge, preparedness, and the need for teacher education to make a difference",*Journal of Digital Learning in Teacher Education*, vol. 28(2), pp. 82-85, 2011. (in English).

[13] J. M. Such, P. Ciholas, A. Rashid, J. Vidler, T. Seabrook, "Basic Cyber Hygiene: Does It Work?",*Computer*, vol. 52(4), pp. 21-31, 2019. (in English).

[14] V. Yu. Bykov, O. Yu. Burov, N. P. Dementievska, "Cyber security in a digital learning environment",*Information Technologies and Learning Tools*, vol. 70(2), pp. 313-331, 2019. (in Ukrainian).

[15] O. Burov, O. Butnik-Siversky, O. Orliuk, K. Horska,"Cyber security and innovative digital educational environment",*Information Technologies and Learning Tools*, vol. 80(6), pp. 414-430, 2020. (in English).
[16] V. L. Buriachok, V. M. Bogush, Yu. V. Borsukovskii, P. M. Skladannyi, V. Yu. Borsukovska, "Training model for professionals in the field of information and cyber security in the higher educational institutions of Ukraine",*Information Technologies and Learning Tools*, vol. 67(5), pp. 277-291, 2018. (in Ukrainian).
[17] V. P. Oleksiuk, O. R. Oleksiuk, "The status of information security competence formedness of future computer science teachers",*Information Technologies and Learning Tools*, vol. 62(6), pp. 277-291, 2017. (in Ukrainian).
[18] B. Cannoles, A. Ghafarian, "Hacking Experiment by Using USB Rubber Ducky Scripting",*Journal of Systemics*, vol. 15(2), pp. 66-71, 2017. (in English).
[19] A. Gorbenko, A. Romanovsky, O. Tarasyuk, O. Biloborodov, "From analyzing operating system vulnerabilities to designing multiversion intrusion-tolerant architectures",*IEEE Transactions on Reliability*, vol. 69(1), pp. 22-39, 2019. (in English).
[20] Y. Khera, D. Kumar, N. Garg, "Analysis and Impact of Vulnerability Assessment and Penetration Testing",*In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, pp. 525-530, 2019. (in English).
[21] Y. Kolli, T. K. Mohd, A. Y. Javaid, "Remote desktop backdoor implementation with reverse tcp payload using open source tools for instructional use",*In 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*,pp. 444-450, 2018. (in English).
[22] A. Luse, A. Al Marzooq, J. Burkman, "Windows ME: Using Antiquated Software to Learn About Security",*IEEE Potentials*, vol. 37(2), pp. 10-12, 2018. (in English).
[23] R. Mahajan, M. Singh, S. Miglani, "ADS: Protecting NTFS from hacking",*In International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014)*, pp. 1-4, 2014. (in English).
[24] S. Samtani, H. Zhu, H. Chen, "Proactively identifying emerging hacker threats from the dark web: A diachronic graph embedding framework (d-gef)",*ACM Transactions on Privacy and Security (TOPS)*, vol. 23(4), pp. 1-33, 2020. (in English).
[25] S. Shrivastava, T. K. Ramesh, "Integration of SDN Controller, Time-Sliding Window, and Quantum Key Distribution with Resource Allocation Strategy in Optical Networks for High Security",*In 2019 Global Conference for Advancement in Technology (GCAT)*, pp. 1-5, 2019. (in English).
[26] D. Stiawan, M. Y. B. Idris, A. H. Abdullah, M. AlQurashi, R. Budiarto, "Penetration Testing and Mitigation of Vulnerabilities Windows Server",*Int. J. Netw. Secur.*, vol. 18(3), pp. 501-513, 2016. (in English).
[27] H. Y. Xiao, B. B. Zhao, "Analysis on sandbox technology of adobe reader x",*In 2013 International Conference on Computational and Information Sciences*, pp. 137-140, 2013. (in English).
[28] Authentication. [Online]. Available: https://en.wikipedia.org/wiki/Authentication. Accessed on: 12.02.2022. (in English).
[29] We study and discover BitLocker. How to protect Windows drives and how to crack it. [Online]. Available: https://xakep.ru/2017/02/23/bitlocker-hacking/. Accessed: 12.02.2022. (in Russian).
[30] VeraCrypt. [Online]. Available: https://www.veracrypt.fr/en/Home.html. Accessed on: 12.02.2022. (in English).

Text of the article was accepted by Editorial Team 17.04.2022 p.

ФОРМУВАННЯ НАВИЧОК З КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ МЕТОДІВ ЗЛОМУ, ОБХОДУ ТА ЗАХИСТУ ПРОЦЕДУРИ НАДАННЯ ДОСТУПУ В ОПЕРАЦІЙНІЙ СИСТЕМІ MICROSOFT WINDOWS

Кива Владислав Юрійович
доктор філософії,
старший науковий співробітник наукового відділу загального та ресурсного планування штабу
Національний університет оборони України імені Івана Черняховського, м. Київ, Україна
ORCID ID 0000-0002-6689-7530
kyvavlad30101991@gmail.com

Застело Ольга В'ячеславівна
кандидат педагогічних наук, співробітниця
Служба Зовнішньої розвідки України, м. Київ, Україна
ORCID ID 0000-0002-3443-4523
zolga777@ukr.net

Наконечний Олександр Михайлович
начальник відділу інформаційно-аналітичного забезпечення – заступник начальника адміністративного управління
Національний університет оборони України імені Івана Черняховського, м. Київ, Україна
ORCID ID 0000-0002-7124-9431
o.m.nakonechnyi@gmail.com

Анотація. У статті розглянуто проблемне питання формування/розвитку кібербезпекових навичок і умінь у педагогів (на прикладі викладачів Національного університету оборони України імені Івана Черняховського). Важливість цього питання підкріплюється аналізом кібербезпеки персональних даних користувачів на їх власних комп'ютерах крізь призму вразливостей у реалізації механізмів захисту операційних систем Microsoft Windows (версії 7, 10), зокрема процедури доступу. Описано основні етапи і особливості процедури надання доступу (ідентифікації, аутентифікації та авторизації) в операційних системах Microsoft Windows. Наведено дані опитування, проведеного серед респондентів-викладачів, щоб з'ясувати, чи розуміють вони суть процедури надання доступу, чи мають вони уявлення про способи зламу, обходу і захисту цього доступу. Опитування виявило, що викладачі не розуміють ні ці поняття, ні ці процедури. Відповідно, питання формування/розвитку кібербезпекових навичок і умінь педагогічних кадрів набуває актуальності на тлі впровадження основних принципів кібербезпеки в Україні, прийнятих Верховною Радою в 2017 році. Автори дослідження описали типові методи зламу, обходу та захисту процедури надання доступу до операційної системи Microsoft Windows (версії 7, 10), які дозволять кожному освоїти деякі практичні кроки, щоб усвідомити важливість і необхідність ключових заходів і методів забезпечення особистої кібербезпеки. Водночас автори мали на меті візуалізувати можливі шляхи порушення кібербезпеки та підвищити обізнаність громадян з метою запобігання кіберризикам. Крім того, автори прагнуть донести до різних категорій громадян, що сучасні інформаційно-комунікаційні технології не лише розширюють можливості нашого глобального цифрового суспільства, а й експоненціально збільшують кількість об'єктів, уразливих до кіберзагроз. Разом із цим завданням було вирішення питань формування/розвитку навичок і умінь педагогів щодо підтримки їх кібербезпеки шляхом проведення тренінгу з вивчення основних понять, методів і прийомів кібербезпеки, спрямованих на зниження кіберризиків. Увага також приділяється деяким етичним аспектам при розгляді окреслених результатів, представлених з освітньою метою, щоб підвищити обізнаність громадськості про описані вразливості, які становлять кіберризики для суб'єктів інформаційної сфери.

Ключові слова: методи і прийоми; злам; обхід; кібербезпекові навички і уміння; ідентифікація; автентифікація; авторизація; Microsoft Windows.