УДК 004.738.5:343.53:341.31
DOI: 10.31733/15-03-2024/2/384-385

Аліна СОЛДАТЕНКО
курсант ННІ права та підготовки
фахівців для підрозділів
Національної поліції

Юлія ГАЛЕНКО
старший викладач кафедри
українознавства та іноземних мов
Дніпропетровського державного
університету внутрішніх справ

FEATURES OF COMBATTING CYBERCRIME UNDER MARTIAL LAW

Since the beginning of the military aggression against Ukraine, we have become the target of numerous cyber-attacks. They have affected numerous government institutions, private organizations and civilian population. Critical sectors such as energy, telecommunications, media and financial companies must also be on heightened alert, as these sectors are often considered priority targets during wartime. It is worth noting that Ukraine's legislative framework does not include a separate special act regulating issues related to preventing cybercrime. However, Ukrainian legislation includes some legal acts that address this issue. One of the main sources for preventing cybercrime in the field of information technology is the Law of Ukraine «On the Basic Principles of Cybersecurity in Ukraine». According to this legislative act, a «cyber-attack» is defined as intentional action in cyberspace carried out using electronic communication means and aimed at achieving one or more specific goals [2]. The term «cybercrime» is also defined as a socially dangerous wrongful act in cyberspace or using it, the responsibility for which is provided by the Criminal Code of Ukraine and recognized as a crime by international treaties of Ukraine [2]. The purpose of such actions may include theft or destruction of information in information networks. In a state of war, cybercrimes are committed with the aim of destabilizing the situation in the country through stealing confidential data, disabling technology and causing other material damage.

After the full-scale invasion of russia into Ukrainian territory, the number of criminal offenses in the field of information technology has increased drastically. The aggressor country uses information technology for disinformation about the invasion in Ukraine, propaganda of hostile ideas and more. In connection with this, to reduce the level of cybercrime in the country, the Verkhovna Rada of Ukraine adopted the Law of Ukraine «On Amendments to the Criminal Code of Ukraine to Enhance the Effectiveness of Combatting Cybercrime in a State of War», which came into force on March 24, 2022. Considering the amendments in the Criminal Code of Ukraine, the responsibility for unauthorized interference with the operation of electronic systems has been increased depending on their consequences. Therefore, since the entry of this law into force, unauthorized interference with the operation of information (automated), electronic communication, information and communication systems as well as electronic communication networks (hereinafter referred to as cybercrimes) is punishable by a fine ranging from 17.000 to 51.000 UAH or imprisonment for up to three years. The same actions committed repeatedly or by a conspiracy of a group of persons are punishable by a fine from 51.000 to 119.000 UAH or imprisonment for a term of two to five years [1]. This law also provides punishment for cybercrimes committed specifically during a state of war, namely imprisonment for a term of ten to fifteen years with the deprivation of the right to hold certain positions or engage in certain activities for up to three years.

In my opinion, to build a resilient and reliable system for preventing crime in the field of information technology, it would be advisable not only to strengthen responsibility for committed criminal offenses, but also initiate social-economic, organizational-management and moral-psychological directions aimed at neutralizing factors that contribute to the commission of cyber-criminal offenses.

1. Law of Ukraine «On Amendments to the Criminal Code of Ukraine to Enhance the Effectiveness of Combatting Cybercrime in a State of War» No. 2149-IX as of March 24, 2022.
2. Law of Ukraine «On the Basic Principles of Cybersecurity in Ukraine» No. 2163-VIII as of October 5, 2017.

УДК 004.056.53
DOI: 10.31733/15-03-2024/2/385-386

Vitalie SPINACHI
Master

Serghei OHRIMENCO
D.Sc. in Economics, Professor

*(Laboratory of Information Security,
Academy of Economic Studies
of Moldova)*

ETHICAL HACKING

«Hacking», as a worldwide phenomenon, has emerged relatively recently, has been widely developed in the conditions of the spread of information and communication technologies and the global Internet, as well as in the development and operation of software for personal computing equipment, systems and networks. This activity is the introduction of deliberate changes to the software to achieve certain (most often, selfish) goals. These unauthorized changes are malicious (i.e. capable of causing significant damage) and can pose a serious threat to individuals, society and the state.

Hacker has a double meaning. Encylopedia.com explains: «During the 1960s, the word 'hacker' grew to prominence describing a person with strong computer skills, an extensive understanding of how computer programs worked, and a driving curiosity about computer systems. Hacking, however, soon became nearly synonymous with illegal activity. While the first incidents of hacking dealt with breaking into phone systems, hackers also began diving into computer systems as technology advanced. During the late 1990s and into the new millennium, hacking became a popular term for the act of breaking in, tampering with, or maliciously destroying private information contained in computer networks»[1].

In order to find and eliminate the introduced changes, which are called vulnerabilities deliberately introduced into the software, software testing is performed, which is a process of research, testing of a software product to check the correspondence between the real behavior of the program and its expected behaviour on a finite set of tests. It should be borne in mind that software developers also make mistakes and, thus, it is necessary to check for errors before the programme is handed over to the customer or implemented as part of an information system. Many experts note the importance, complexity and high cost of testing processes not only for software for personal computers and mobile devices, but also for systems and networks in general.

The composition of the hacker community is quite heterogeneous. Some of them specialise in creating special malware for mobile applications, others create encryption software, etc. And these products are sold and exchanged on closed, illegal markets (Dark Markets).

It should be noted that the «hacker community» directs its efforts to the development of a large number of software abuses, which should be conditionally divided into the following groups by purpose: Espionage, Attack, Destabilization [2]; Attacking Web Applications, Advanced Brute-forcing and Password spraying, File Inclusion Attacks, Authentication and Authorization Abuse, Attacking Custom Protocols, Cross-origin Resource Sharing, Social Engineering Attacks Breaking Containers [3], Injection Attacks, Fuzzing, Dynamic Scanning of REST API, and Web Application [4]. Additional analyses can be gleaned from a set of reports from leading computer firms, including The 2023 Faces of Fraud Research Survey Results Report [5], The 2019 Hacker Report. The Survey and Statistics of the Ethical Hacker Community [6], 7th Annual Hacker-Powered Security Report [7], The Evolution of Online Fraud in 2023 and Best Practices to Plug the Gaps [8].

Summarising the intermediate conclusion, two main groups of interaction among hackers should be distinguished. On the one hand, representatives of the first group see the main purpose