UDC 004.056.5 (043.2)

Maksym YAKHYMOVYCH
National Aviation University, Kyiv

DEVELOPMENT OF COMPUTER SECURITY

With the advent of computers and a new fragment of the service sector, activity has increased significantly, as it is easier for anyone to rob a person without having to be in physical contact with them.

People who were unfamiliar with computer technology but discovered the World Wide Web very quickly encountered a lot of fraudsters looking for easy money. But this issue really became a widespread problem when government, military, financial, and medical organizations were at risk. A lot of important information could have fallen into the hands of malicious actors until the government began to take cybersecurity more seriously and introduced this concept into legislation. According to the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine," the following definition follows: "Cybersecurity is the protection of the vital interests of a person and a citizen, society and state when using cyberspace, which ensures the sustainable development of information society and digital communication environment, timely detection, prevention and neutralization of real and potential threats to Ukraine's national security in cyberspace."

Ukraine has developed a cybersecurity system that includes academic cybersecurity, state cybersecurity, commercial cybersecurity, and non-profit volunteers and public organizations. The cyber police works closely with the Government's Cyber Incident Response Team (CERT-UA), the SSU's Situation Center for Cybersecurity (MISP-UA), and under the supervision of the NSDC, threats are neutralized to avoid the escape of confidential information. Despite such a system, Ukrainian cyberspace is still vulnerable to powerful hacker attacks, due to the lack of competence of government specialists and the frequent neglect of information security.

There are several ways to make mistakes in security systems, the main one being the system design. This, in turn, is due to unstable ciphers, unreliable client-server architecture, or poor authentication mechanisms. Configuration errors and operator errors (negligence, weak

password, access control, opening links from unknown users, changing settings) also lead to data breaches.

Hackers are also improving their resources and hacking methods: DoS-attack (used to completely deny access to information instead of obtaining it); Backdoor (an algorithm for bypassing the authentication process, gaining access to a computer or information).

In addition to government agencies, ordinary Internet users also need to protect their personal information, and there are plenty of ways to do so; using primary protection methods (updating the system, performing program and system breaks, performing cleanups) and systems with secure design.

Thus, information security is an important component of maintaining order, without it, all systems on the planet would cease to function properly. For every action. There is a counteraction, and as the quality of information protection improves, new, more powerful ways of hacking will appear, so the development of cybersecurity remains very important.

Scientific supervisor: Nataliia DENYSENKO,
Senior Lecturer