

УДК 004.056.6

Liza Pikalova¹, Nataliia Zhukova²

¹student of group CST-522 NU “Zaporizhzhia Polytechnic”

²PhD (Philology), associate professor NU “Zaporizhzhia Polytechnic”

COMPUTER SYSTEM SECURITY AND DATA PROTECTION IN THE FACE OF THREATS FROM HACKERS AND VIRUSES

The widespread use of information technology in all spheres of society makes the issue of information protection, its users, information resources, and data transmission channels from criminal attacks of cybercriminals quite relevant. The concentration of information in computers forces some people to intensify their search for ways to access information, while others intensify control over it for the purpose of protection. The complexity of creating an information security system is determined by the fact that data can be stolen from a computer (copied), while remaining in place. Objects of attacks can be both material technical means (computers and peripherals) and software and databases. It is important to preserve such properties of information as availability, integrity, and confidentiality.

The threat to the security of a computer system is an event (impact) that, if realized, will cause a violation of the integrity of information, its loss, or replacement. Threats can be accidental or intentional. Accidental threats include errors of service personnel and users; loss of information due to

incorrect storage of archival data; accidental destruction or alteration of data; equipment and power supply failures; accidental disclosure of confidential information to third parties.

Intentional threats created by malicious actors lead to serious consequences. Intentional threats include unauthorized access to information and network resources, disclosure and modification of data and programs, copying of data, development and dissemination of computer viruses, theft of magnetic media and financial documents, destruction of archival information, and falsification of messages. Depending on their motives, goals, and methods, the actions of information security violators can be divided into four categories: thrill-seekers, ideological hackers, professional hackers, and unreliable (disgruntled) employees.

To properly build a protection system, it is necessary to determine the types of actions taken against information, what an automated system is, the security threats to automated systems, measures to counter security threats, and the principles of building protection systems.

Encryption mechanisms involve the cryptographic protection of information. These protection methods are increasingly being used in the processing and storage of information on magnetic media. This method is the only reliable one for transmitting information over long communication channels. Counteracting attacks by malicious programs involves a complex of various organizational measures and the use of antivirus programs. The goals of these measures are to detect instances of system infection, reduce the consequences of information infections, localize or destroy viruses, and restore information in the information system.

Currently in the USA, there is a developed standard for assessing the security of computer systems - the criteria for evaluating suitability. It takes into account four types of requirements for computer systems: security policy requirements, accounting requirements, trust in computer systems, and documentation requirements.

Protection of data and programs from unauthorized access, copying, and modification is implemented using software-hardware methods and technological techniques. Passwords, electronic keys, electronic identifiers, electronic signatures, data encryption and decoding tools are classified as software-hardware protection tools. Cryptographic methods are used for data encryption, decoding, programs, and electronic signatures.