Having analyzed the main features of Joe Biden's speeches, the following male features of the selected speeches can be identified: the use of negative forms (104 units), abstract nouns (43 units), terminology (226 units), the quantitative superiority of complex sentences (154 units) over compound ones (31 units), modals for obligation (4 units) and indirect quotations (2 units). The main feminine characteristics of the speeches of the President of the United States include the use of intensifiers (64 units), direct quotation (10 units), "wh"-imperatives (120 units), modal constructions (80 units), "empty" adjectives (9 units), qualifiers (11 units) and polite forms (21 units).

In total, we have analyzed 1 679 linguistic units; the number of masculine markers prevails in the speeches of both politicians, although the amount of lexemes prevails in Joe Biden's speeches (60% in contrast to 51% in the speeches of Kamala Harris). This can be explained by the influence of modern gender trends on the speech of politicians. The main characteristics, which in the past were considered male ones, now can be attributed to those that should be used in the speeches of all politicians, regardless of the gender, as they contribute to better communication with the audience.

Scientific supervisors: Iryna VOROBIOVA
PhD, Associate Professor;
Victoriia LANKINA
English Teacher

UDC 004.056.57 (043.2)

Yurii VERBYTSKYI
National Aviation University, Kyiv

THE PROBLEM OF INFORMATION PROTECTION

The problem of information protection is not new. The initial stage of the development of computer security is strongly connected with cryptography. The main conditions of information security are its availability and integrity. Another task of protection is to ensure the protection of information during its storage or transmission. This is the so-called integrity condition.

Performing encryption and decryption procedures, in any information process system, slows down data transfer because the user will have to wait too long for his "reliably protected" data, which is unacceptable in some modern computer systems.The principle of modern information protection can be expressed as follows – the search for an optimal relationship between availability and security.Protection of information is not limited to technical methods. The main drawback of protection is people. In addition, protection should be constantly improved along with the advancements in the computer network.At this time, the theory of information security has not yet been created. Approaches and tools used in practice often have disadvantages. Necessary to have sufficient training and to be competently oriented in the entire spectrum of information security issues.

The simplest example, when consent is obtained from a person for the processing of personal data, is registration on the website. During such a procedure, large entities are not interested in who and how will process personal data in the future. For many services provided by government bodies, consent to the processing of personal data is also obtained. Unfortunately, it is almost impossible to remember to whom and what personal data is provided, as well as to predict a possible leak of the provided data. There are many problems in this matter, so it is proposed to dwell on the most advanced ones.

Given the number of consents a person provides in today's world, it is impossible to track the transfer of your data to third parties. In this regard, the implementation of the rights granted by the law turns out to be ineffective. In most cases, individuals are often unaware of the distribution of their data and therefore unable to adequately protect it.

The needs of modern information systems have led to the emergence of non-traditional tasks for the protection of electronic information, one of which is the authentication of electronic information under conditions when the parties exchanging information do not trust each other. This problem is related to the creation of electronic digital signature systems. The revolutionary ideas of two-key cryptography led to a sharp increase in the number of open research in the field of cryptography and showed new ways of developing cryptography, its new possibilities, and the unique importance of its methods in modern conditions of mass application of electronic information technologies.

The widespread use of information technologies in information processing and management systems has led to an aggravation of the problem of protection of information from unauthorized access. Information protection in computer systems has several specific features relating to the fact that the information is not rigidly connected to the medium, can be easily and quickly copied and transmitted over communication channels. A very large number of information threats are known, which can be implemented both by external and internal violators.

A separate group of measures to ensure the preservation of information security and the detection of unauthorized requests include programs for detecting violations in real time. Programs of this group send a special signal when violations are detected, which can lead to illegal actions in relation to data. The signal may contain information about the nature of the violation, the place of its occurrence, and other characteristics. In addition, programs can prohibit access to protected information or simulate such a mode of operation that will allow the violator to be identified and detained by the relevant service.

In systems that support several levels of secrecy, the information is accompanied by a special seal indicating the level of secrecy. This requirement is very important.Protection against unauthorized use of software is allocated to a separate group. They become especially important due to the widespread use of computers.

A radical solution to the problems of protecting electronic information can be obtained only based on the use of cryptographic methods that allow solving the most important problems of secure automated data processing and transmission. At the same time, modern high-speed cryptographic conversion methods allow you to preserve the original productivity of automated systems. Cryptographic data transformations are the most effective means of data confidentiality, integrity, and authenticity. Only their use in combination with the necessary technical and organizational measures can provide protection against a wide range of potential threats.

Scientific supervisor: Larysa TEREMINKO,
Associate Professor