THE MAIN FACTORS OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN INFORMATION PROTECTION SYSTEMS

Samandarov Javlon Iskandarovich
Doctoral student of Tashkent State Pedagogical University
https://doi.org/10.5281/zenodo.7677380

Abstract. *This article talks about security of state confidential information and general information protection technologies by improving information security training.*
Keywords: *information, computer, virtual entity, technology, electronic documents, mechanism, protection, courier.*

Problems of compliance with group ergonomic indicators during the design and construction of the "Human-Computer" system, the role and importance of modern media in spreading high culture to the masses; aggravation of moral problems in the process of informing society, improvement of computer etiquette, computer literacy and computer culture and ending dehumanization in order to put an end to the issues of moral crisis, computerization of society, illegal use of information, that is, the rise of computer crime, virtual existence and its application in various spheres of human cultural activity, advantages of computer use in the field of medicine indicate that information technologies cover all areas of our society.

It is the basis of all automated information processing systems that store and process information, present it to consumers, and use the most modern information technologies. Along with the development and complexity of information technology tools and methods, the level of society's dependence on the information security used in it increases.

Problems of ensuring information security have been worrying mankind since ancient times. The need to protect information arose from the need to transmit both military and diplomatic information. For example, the ancient Spartans encrypted their military information. The simple writing of information using hieroglyphs in Chinese makes it mysterious for foreigners. Until now, the most reliable and simple channel - the courier channel - has been used to ensure the safety of information transmission.

The security of such communication systems depends on the reliability of the courier and the ability to avoid situations where information can be exposed. Ensuring information security is becoming more complex and important as information and communication technologies are managed on a mass, paperless, automated basis. Therefore, a new modern technology of information protection is emerging in automated information systems. According to DataQuest, the sales volume of information protection tools in 1996-2000 was equal to 13 billion US dollars.

The complex of organizational, technical, software, technological and other tools, methods and measures that reduce the weaknesses of information and prevent unauthorized access to information, its exit and loss is called an information protection system.

Owners of information and authorized state bodies must determine the necessary level of information protection and the type of system, protection methods and means based on the value of information, the damage caused by its loss, and the price of the protection mechanism. The value of information and the reliability of the required protection are directly related to each other.

In organizations with a small volume of information, it is appropriate and effective to use simple methods to protect information. For example, separating and masking readable valuable papers and electronic documents into separate groups, appointing and training an employee who works with these documents, organizing security of the building, imposing an obligation on employees not to distribute valuable information, controlling outsiders, the use of the simplest methods of computer protection, etc. Usually, using the simplest methods of protection gives a significant effect.

In organizations with a complex content, a large number of automated information systems and a large amount of information, a complex system of protection is established to protect information. But this method and the simple methods of protection should not interfere too much with the work of the employees.

The complexity of the protection system is achieved by the presence of legal, organizational, engineering-technical and software-mathematical elements in it. The proportion of elements and their content ensure the uniqueness of the organization's information protection system and its non-repeatability and difficulty in breaching.

A concrete system can be thought of as consisting of many different elements. The content of the system elements determines not only its uniqueness, but also the level of protection set, taking into account the value of the information and the value of the system.

In the sense that the element of legal protection of information is the right of protective measures, it is imagined the legal strengthening of mutual relations between the organization and the state and the compliance of the personnel with the procedure for protecting the valuable information of the organization and the responsibility for the violation of this procedure. Protection technology includes management and restrictive measures that encourage personnel to comply with the organization's valuable information protection rules.

The element of organizational protection is considered to be the factor connecting all other elements to a single system. According to most experts, organizational protection makes up 50-60% of information protection systems.

Organizational measures of information protection are reflected in normative methodological documents of the organization's security service. In this regard, they often use the single name of the system elements seen above - the element of organizational and legal protection of information.

The element of technical protection of information is intended for the organization of protection of territory, buildings and devices with the help of a complex of technical tools, as well as passive and active struggle against technical inspection tools. Although the price of technical protection means is high, this element is important in protecting the information system.

The software-mathematical element of information protection is designed to protect valuable information processed and stored in computers, local networks and various information systems.

Conditions, actions and processes that can damage the computer system (network) are considered risks for the computer system (network) [8].

The protection system should be continuous, planned, centralized, targeted, accurate, reliable, complex, easily perfected and quickly changed in appearance. It generally needs to be flexible in all extreme conditions.

Information protection refers to a strictly regulated dynamic technological process that ensures the information security of management and production activities and ensures the

integrity, reliability, ease of use and confidentiality of the organization's information reserves. Any documented, i.e., information recorded on a material body with the requisites that allow identification must be protected from illegal treatment intended to harm the owner, user of the information, and other person. From the point of view of information security, information can be categorized as follows:

• **secrecy** — a guarantee that specific information can be accessed only by the relevant persons, that is, its use is restricted and documented in accordance with legal documents. Violation of this clause is considered theft or disclosure of information;

• **confidentiality** — guarantee of reliability, non-distribution, confidentiality;

• **integrity** — a guarantee that the information is in its original form, that is, no unauthorized changes were made during its storage and transmission; Violation of this clause is called falsification of information;

• **authentication** — a guarantee that the person declared as the owner of the information reserve is really the owner of the information; Violation of this clause is called falsification of the author of the message;

• **appealling** — rather complex category, but widely used in e-business. Guarantee that the author of the message can be proven if necessary.

As above, the information system can be classified as follows:

• **reliability** — guarantee that the system will behave as planned in normal and abnormal situations;

• **precision** — guarantee of exact and complete execution of all orders;

• **system access control** — ensuring that different groups of individuals have different access to information sources and that restrictions on such access are always enforced;

• **being controlled**— a guarantee that any part of the program complex can be fully checked at any time;

• **identification control** — a guarantee that the currently logged-in client is exactly who he says he is;

• **prevention of intentional violations** — pre-agreed behavior of the system in relation to intentionally entered erroneous data within pre-agreed limits [9].

The purposes of information protection are as follows:

- prevention of unauthorized leakage, theft, loss, alteration, and falsification of information;
- prevention of danger to personal, society, state security;
- prevention of unauthorized actions to destroy, change, falsify, copy, block information;
- prevention of any illegal interventions in the information reserve and information system as the amount of documented information that ensures the legal order;
- protection of the constitutional rights of citizens who maintain personal privacy and confidentiality of personal information available in the information system;
- maintaining state secrets, confidentiality of information documented in accordance with the law;
- ensuring the rights of subjects in the creation, development and use of information systems, technologies and the tools that provide them.

Currently, the urgency of solving the problem of information protection is confirmed by the growing costs of protection measures. Building a reliable system of protection requires large

material and financial costs. And this justifies itself, because the damage to the reliability and integrity of information can have the most serious consequences.

The modern stage of the development of new information technologies, computer systems and networks, and the Internet has made it clear that a systematic study of the problem of ensuring information security is absolutely necessary. In this regard, higher demands are placed on specialists, their information potential and culture. The efficiency of the organizations and institutions, as well as the success and development of the specialist depend on how well the users of computer tools know and can use modern methods and tools of new information technologies.

Thus, in the modern information society, in the society of market relations, information remains a special commodity (product). The legality of the development of computer systems observed in recent times leads to the fully legal development of the information protection system. The problem of organizing adequate information protection in a computer system is undoubtedly a difficult one. In addition to the reasons that cause the problem of affordability, it is possible to highlight the ever-increasing expenses allocated to the formation of information protection (in the USA and Western European countries alone, these expenses amount to 6 billion dollars).

To sum up, fully ensuring information security, releasing state decisions and information, appointing and training an employee who works with these documents, organizing the security of the building, obligation of employees not to distribute valuable information, controling visitors from outside doing, replacing the teaching of the simplest methods of computer protection with modern methods are the most necessary fields in the information age.

REFERENCES

1. O‘zbekiston Respublikasi Prezidentining 2017 yil 70fevraldagi “ O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida”gi PF-4947-son Farmoni
2. Axborot-kommunikatsiya texnologiyalari izohli lug‘ati. Copyright@2004 UNDP Digital Development Initiative Programme. –Toshkent, 2004.
3. Axrarov B.S. Axborot xavfsizligi. // O‘quv qo‘llanma. –Toshkent: KURO PRINT, 2009.
4. Saltzer, J and Schroeder, M., “The Protection of Information in Computer Systems”, Proceedings of the IEEE 63(9), Sep. 1975, pp. 1278-1308.
5. https://www.law.cornell.edu/uscode/pdf/lii_usc_TI_44.pdf
6. Филатова О. Социология массовой коммуникации: краткий глоссарий. М: Гардарики, 2006.
7. Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью» (ГОСТ Р ИСО /МЭК 17799-2005) http://www.g-ost.ru/2262.html.
8. Статьев В.Ю., Тиньков В.А. Информационная безопастность распределенных информационныц систем/Информационное общество, 1997, вып.
9. Шудегов, В.Е. Нормативно-правовое обеспечение стандартов общего образования/ В.Е. Ш удегов, Е.В. Буслов // Стандарты и мониторинг в образовании. - 2006. - № 1. - С. 26-36.; № 2. - С. 16-22