EUROPEAN JOURNAL OF LIFE SAFETY AND STABILITY (EJLSS)
ISSN2660-9630
www.ejlss.indexedresearch.org Volume 25, January-2023 ||

Modern Information Security

Tlemisov Ilham Kongratbay, Jangabaev Muxtar Faxratdinovich, Janxojaev Asqar Ayxoja uli, Qallibekov U'mitbek Òserbay uli
3 years students, Undergraduate degree Karakalpak State University named after Berdakh
(Nukus, Republic of Karakalpakstan)

Abstract: *This article is about information security.*

Keywords: *Information, communications, security, data integrity, modern society.*

Date of Submission: 29-12-2022 ***Date of Acceptance: 30-01-2023***

The information society, to which humanity is steadily striving, radically changes the status of information, expanding its potential as a positive resource, and revealing its sharply negative possibilities. Information has always surrounded a person, so any society can be considered informational. However, the study of information as a strategic resource for the development of mankind has shown that it can be reliable and relevant, new and outdated, but it cannot be transmitted, received or stored in its pure form, any information has its own carrier and is transmitted through communication channels. In the most general form, information is information, regardless of the form of their presentation, perceived by a person or special devices as a reflection of the facts of the material world in the process of communication. Consequently, by exposing both the individual and society to information, it is possible to govern the state. The well-known expression of Nathan Mayer Rothschild "who owns information, owns the world" shows how those who own the largest amount of information on any issue can deform the mechanisms of communication, destabilize the mechanisms of functioning of the main systems of society, deprive the possibility of realizing the information component of the individual. Therefore, the problem of information security and information security, ensuring its integrity, reliability and accessibility comes to the fore in modern society.

In accordance with the Law on Security and the content of the Concept of National Security of Uzbekistan, information security will be understood as the state of protection of vital interests of the individual, society and the state in the information sphere. In order to ensure information security, the state is constantly fighting against internal and external threats to the country's information space. As a result, the basic principles and basic information security measures are formulated, which should ensure:

Section "Fundamental and applied problems of the humanities"

- data integrity - protection against failures leading to loss of information, as well as unauthorized creation or destruction of data;
- confidentiality of information and at the same time its availability to all authorized users.

In the process of implementing these principles, the States identified the most vulnerable areas of possible violations: banking and financial institutions, information networks, public administration systems, and defense and special structures. These structures of the State require special security measures, since they ensure the sovereignty of the country. As the main information security measures, information encryption tools are used, up to the use of file systems with data encryption. Modern information security breach detection systems include virtualization systems, sandboxes with built-in anti-virus protection systems and knowledge management systems about cyber threats and vulnerabilities.

The main problem in ensuring information security is the protection of the information itself. The state ensures the protection of information at the legislative level, but it cannot protect us from the human factor. The authors note changes in the approaches used by cybercriminals to carry out attacks:

- sending emails with malicious attachments to employees of the organization;
- distribution of malware through Internet resources;
- physical penetration into the office;
- Penetration into the corporate network of the organization through the external perimeter - complemented by a new sophisticated method in the form of introduction into the supply chain.

Recently, there have been problems of information protection in Uzbekistan related to the use of foreign software. So, according to E.A. Razumovskaya, the main one is "a significant, decades-long emerging import dependence of the country in the computer field." There is a situation in our country when all products that are exported are accompanied by documentation, diagrams, drawings prepared exclusively on licensed software that is produced in Western countries; enterprise management systems are installed at factories. Thus, Uzbekistan in the banking sector is already ready to ensure the security of information about bank customers, settlements, transactions, etc. But the problem of protecting information about people - personal data and personal information is considered more serious. The fashion for using cloud services, in most cases foreign, leads to the fact that user information is physically stored on the servers of foreign corporations and any commercial and industrial secrets, military secrets remain virtually unprotected.

Conclusion: Information protection is a guarantee of security, the task of the state. But both users and enterprises are able to carry out measures to improve information security and information protection. To do this, fairly simple but effective measures are used: building a system of differentiation of critical powers in business systems, restricting access to information resources exceeding the minimum sufficient level. But success in the field of information security can only bring an integrated approach that combines proper management, the company's efforts to convince employees of the need to improve information security, create legislation and state control over the level of information security, and the use of domestic software and information technologies. Adaptation of traditional measures - network solutions, improvement of the quality of operational information collection, threat modeling, increased responsibility, also expand the boundaries of the "safe perimeter" and create conditions for the effective and safe use of information in real time.

References

1. Abashev A., Jedrin I., Akupov V. Global'nye tendencii rynka informacionnoy bezopasnosti // Informacionnaya bezopasnost'. 2015. № 5. 16-17 p.
2. Belov E. B., Los' V. P. Osnovy informacionnoy bezopasnosti. M.: Goryachaya liniya: Telekom, 2006.
3. Mel'nikov V. P., Kleymenov S. A., Petrakov A. M. Informacionnaya bezopasnost' i zashita informacii. 3rd ed. M.: Academiya, 2008.