INFORMATION AND WEB TECHNOLOGIES

Umarova Zhanat
Associate Professor, PhD,
South Kazakhstan University named after M. Auezov, Republic of Kazakhstan

Yessirkepov Nurzhan
Master's student,
South Kazakhstan University named after M. Auezov, Republic of Kazakhstan

ADVANTAGES OF USING INFORMATION TECHNOLOGIES IN MODERN SOCIETY

***Abstract**: The issue of information security of economic objects requires multidimensional and further study. In today's world, informatization is a strategic national resource, one of the main assets of an economically developed state. Improvement of rapid informatization, its penetration into all spheres gives rise to a number of important problems and unavoidable advantages in the vital interests of the individual, society and the state. Methods of protection of information from the system position It is necessary to use all available arsenals in all structural elements of the economic object and all stages of the technological cycle of information processing. The effectiveness of information security should not exceed the costs of implementation and the potential costs of implementation. Information security planning is the process which each service develops detailed information security plans to ensure that users have the authority and rights to achieve specific goals, to monitor protection tools, and to respond immediately to failures.*
***Keywords**: Information technology, computer, global networks, telecommunications, Information security*

Modern society is called informational. The extensive development of the Information Society offers the possibility of collecting, storing, processing computer technologies and means of communication and transmitting information in such a volume and with such efficiency. Thanks to new information technologies, the sphere of communication, both industrial and non-productive activities of a person, through the involvement of his daily experience, is expanding indefinitely. The

current stage of informatization is associated with the use of an individual electronic computer equipment, telecommunications systems, and the creation of computer networks. There is an increasing need to develop and apply effective solutions in the field of the information industry.

Telecommunications systems include wired and wireless local and global networks, as well as hardware and software that allow systems to communicate with each other or with users. The set of telecommunications systems that support many federal government agencies includes network infrastructure and other components of technical solutions owned by commercial telecommunications service providers and managed on behalf of the government.

Emergency planning for telecommunications systems should be aimed at preventing single failure points by introducing redundant communication channels, network devices, and even service providers. In addition to network and provider redundancy, the capabilities offered by telecommunications systems for normal operation can provide unexpected solutions in the absence of primary processing sites or infrastructure sub-components. Such features include remote access services for system administrators and other authorized employees, as well as wireless network technology as an alternative or backup communication mechanism in case of failure affecting the local network or other components of the wired network.

Telecommunications systems include wired and wireless local and global networks, as well as hardware and software that allow systems to communicate with each other or with users. The set of telecommunications systems that support many federal government agencies includes network infrastructure and other components of technical solutions owned by commercial telecommunications service providers and managed on behalf of the government.

Emergency planning for telecommunications systems should be aimed at preventing single failure points by introducing redundant communication channels, network devices, and even service providers. In addition to network and provider redundancy, the capabilities offered by telecommunications systems for normal operation can provide unexpected solutions in the absence of primary processing

sites or infrastructure sub-components. Such features include remote access services for system administrators and other authorized employees, as well as wireless network technology as an alternative or backup communication mechanism in case of failure affecting the local network or other components of the wired network.

Long-term communication technologies in the twentieth and XXI centuries usually include electrical and electromagnetic technologies such as telegraph, telephone, television and teleprinter, networks, radio, microwaves, optical fibers and communication satellites. The Internet of Things (IoT), advertised as one of the most important trends affecting the telecommunications industry, started 2020 as no one expected. IoT is the connection of devices, endpoints, and resources that have never been able to communicate with the network. Telecommunications is considered a good career path, as the industry develops and grows with the growth of new technologies. Wireless equipment provides more reliable services, and companies compete to provide the fastest internet and the best deals. We are moving to digitalization through future-generation technologies, and all this is possible only through high-speed networks and data exchange services that the next-generation mobile networks of the telecommunications sector (5G and beyond) can offer. This is the future of telecommunications. Information technology and the ability to interact and communicate are a fundamental part of the functioning of our society. In today's digital ecosystem, telecommunications has become the basis for easy communication and sharing between businesses, governments, communities, and families. Many companies that want to hire telecommunications technicians choose people with a technical school certificate or an additional degree in electronics or computer science. Some require special certificates from certain equipment manufacturers or professional organizations.

Telecommunications networks are information transmission systems that allow you to transmit information between different objects in analog or digital form using electromagnetic or optical signals. Information may consist of audio or video data, or some other data types.

Information security threats include distorting events or actions, unauthorized use, or even destruction of information resources of a managed system, as well as

software and hardware. If we consider any cybernetic model from the classical point of view of a managed system, the impact on it can be random. Therefore, the types of threats to information security are accidental or unintentional. Their way out can be the construction of hardware, incorrect actions of employees, careless errors in the software of the information system (is) or its users, and so on. Such risks should also be taken into account .The damage caused by them can be significant. However, the situation in which much attention is paid to this work is a deliberate threat. Unlike an accidental threat, the purpose of the application is to cause damage to the managed system or users. A person who tries to disrupt the operation of an Information System or gain unauthorized access to information is usually referred to as a "computer hacker" (hacker). Information security includes:

– Information space and the state of its protection;

– Formation and development of the interests of citizens, organizations and the state;

– The state of the infrastructure in which information is strictly used;

– State of information that is excluded or significant;

– The state of security of the economic component of information (production structures, including systems for collecting, accumulating and processing information for the management structure in the economic sphere, analysis and forecasting of overall economic development, management system and coordination in industry and transport, centralized supply of management systems, decision-making system and coordination of actions in emergency situations, information and telecommunications systems);

– Security of the information part of the financial component (i.e. security of the system of information networks and databases of banks and the system of financial exchange and financial settlements).

Ensuring information security should begin with determining security. Subjects of relations related to the use of Information Systems. Their interests can be divided into the following main categories: accessibility (the ability to receive the necessary information service at a convenient time), information integrity (relevance and consistency of information, protection from its and unauthorized changes).

Thus, the implementation of information security threats is a violation of the confidentiality, integrity and availability of information. A hacker can be acquainted with confidential information. In addition, information security may be compromised due to accidental, careless errors of employees.

Information threats can be caused by:

Natural factors (natural disasters-fire, flood, storm, lightning and other causes);

human factors.

The latter (Human Factors), in turn, are divided into:

Threats that occur accidentally, unintentionally. These risks are associated with errors in the process of preparing, processing and transmitting information (scientific and technical, commercial, currency and financial documentation); not directed "leakage of intelligence", knowledge, information (for example, Population migration, departure to other countries, family reunification, etc.). These are risks associated with errors in the process of designing, developing and manufacturing systems and their components (buildings, structures, premises, computers, communication facilities) (operating systems with errors in the operation of hardware, application programs, etc. B.) due to its poor-quality production; information with errors in the preparation and processing process (errors of programmers and users qualification and poor-quality service, errors of operators in training, data input and output, correction and processing of information);

Threats caused by deliberate actions arise from the influence of people. These are risks associated with the transmission, distortion and destruction of scientific research (new technologies, disclosure of production secrets, invention and other anti-social motives ,documentation, drawings, discoveries and other materials); official and other scientific, technical and commercial conversations; targeted "leakage of intelligence", knowledge of information (for example, reasons related to obtaining other citizenship). These are risks associated with unauthorized access. Introduction to the resources of an automated information system (making changes to technical computer equipment and means of communication computer equipment and communication channels, theft of Information Media: floppy disks, descriptions, prints, etc.).

Information protection is currently relevant at one time. We live in an information society and absorb it on a daily basis. Sometimes information is more expensive than the material goods themselves. Accordingly, there is a need for protection. Each company is interested in competitors with its own databases. Now the security of the enterprise is not only physical, material security, but also information security. Protection should be done individually for each system, but in accordance with the general rules. Protective construction includes:

Risk analysis and protection, continuous operation and recovery plans, which will end with the development of the protection system project;

Implementation of the protection system based on the results of risk analysis;

Constant monitoring of the operation of the M Protection System and the AIS in general (software, system and administrative).

At each stage, certain protective requirements are implemented. Their peculiarity is that compliance with the requirements leads to the creation of a secure system. Today, the protection of AIS is an independent direction. Therefore, it is easy and inexpensive to use to perform protective work.

The problem of information security of economic objects is multidimensional and requires further study. In the modern world, informatization is a resource of a strategic national character, one of the main wealth of an economically developed state. The improvement of rapid informatization, its penetration into all spheres, creates undeniable advantages and a number of important problems in the vital interests of the individual, society and the state. Given that there is a need to protect one information, the economic potential is currently increasingly determined by the level of development the potential vulnerability of the information infrastructure is growing proportionally. Ways to protect information from the system position it is necessary to use the entire arsenal available in all structural elements of the economic object and stages of the technological cycle of processing all information. Methods and means of protection should reliably cover possible ways of illegal access of protected persons. The effectiveness of information security its costs should not exceed the potential costs of implementation and implementation.

Information security planning through the development of detailed information protection plans by each service, it is necessary to ensure control over the means of protection and immediately respond to their failure, which is a reality in the exercise of the powers and rights of users to achieve certain goals.

References:

1. Ageev, A. S., comp. Organization and modern methods of information protection: Method. manual for hands. and employees of security services Ageev A. S. and others; Under the general editorship of S. A. Diev, A. G. Shavaev . - M.: Concern " Bank. Business Center", 1998
2. Aleshin, L. I. Information Protection and information Security: A course of lectures by L. I. Aleshin; Moscow State University of Culture, Moscow: Moscow State University of Culture, 1999
3. Yastrebov, D. A. Information security: terms and definitions / D. A. Yastrebov. - M.: TISSOT, 2002
4. Security systems: Intersectoral topic. cat. - M.: Groteck, 2001
5. Special equipment and information security: Textbook / [Auth. Study: Zhenilo R., Kirillychev A. N., Kirin V. I., etc.]; Ed. by V. I. Kirin; Akad. department of the Ministry of Internal Affairs of Russia. Vol. 1., 2000
6. Torokin, A. A. Fundamentals of engineering and technical protection of information". - Os-89 Publishing House, 1999
7. Stepanov, E. A. Information security and information protection: Textbook for university students studying in the specialty " Documentology and documentation. ensuring upr. " E. A. Stepanov, I. K. Korneev. - M.: INFRA-M, 2001
8. Tsvetkov, V. Ya. Technologies and information security systems: Analit. review of V. Ya. Tsvetkov;
9. Shakovets, A. N. Fundamentals of computer information protection and information security: Lecture by A. N. Shakovets, N. V. Rymareva;
10. Yakovlev, V. V. Information security and information protection in corporate networks of railway transport: Textbook for university students zh. - D. transp. V. V. Yakovlev, A. A. Kornienko. - M., 2002