International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 5 Issue 1, January - 2021, Pages: 1-4

Information Protection and Its Types

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract**:** *Ensuring the physical integrity of information while preventing the destruction or destruction of information elements Avoiding falsification (alteration) of information while maintaining its integrity; Prevent unauthorized access to information from the network by unauthorized persons or processes; It is understood that the information and resources provided (sold) by the owner will be used only on the basis of agreements between the parties.*

Keywords: Privacy, Confidentiality, Integrity, Authentication, Reliability, Accuracy, Identification Control, Prevention of Intentional Violations

INTRODUCTION

1. Information security and its categories.

2. Technical means of network security control.

3. Risks to data in automated information systems.

4. The need for protection in automated information systems.

Information security means:

Ensuring the physical integrity of information, while preventing the destruction or destruction of information elements;

Avoiding falsification (alteration) of information while maintaining its integrity;

Prevent unauthorized access to information from the network by unauthorized persons or processes;

It is understood that the information and resources provided (sold) by the owner will be used only on the basis of agreements between the parties.

METHODS

Tasks of information protection

Utility is the ability to get the information you need over a period of time. Integrity is the relevance of information to protect it from destruction and unauthorized alteration. Privacy is the protection of information from unauthorized access. From the point of view of information security, information can be categorized as follows: • Confidentiality - a guarantee that certain information can be accessed only by relevant persons, ie its use is restricted and documented in accordance with the law. Violation of this clause is called theft or disclosure of information; • Confidentiality - a guarantee of reliability, non-disclosure, confidentiality; • Integrity - a guarantee that the information is in its original form, ie no unauthorized changes have been made to its storage and transmission; violation of this clause is called falsification of information; • authentication - a guarantee that the person declared the owner of the information resource is in fact the owner of the information; a violation of this clause is called forgery of the author of the message; • Appeals are a fairly complex category, but are widely used in e-business. Guarantee that the author of the message can be identified if necessary. As mentioned above, the information system can be classified as follows: • reliability - a guarantee that the system will behave as planned in normal and unnatural situations; • accuracy - a guarantee of accurate and complete execution of all orders; • access control - a guarantee that different groups of individuals have different access to information sources and that restrictions on such access are always enforced;

• control - a guarantee that at any time you can fully inspect any part of the software package; • authentication control - a guarantee that the customer who is currently connected to the system is exactly who he or she is; • Prevention of intentional violations - the system's preconceived notion of intentionally erroneous information within the limits of pre-agreed norms The objectives of information protection are: - unauthorized leakage, theft, loss, alteration of information, prevention of counterfeiting; - prevention

of threats to the security of individuals, society and the state; - prevention of unauthorized actions to delete, change, falsify, copy, block information; - prevention of any illegal interference with information storage and information systems, ensuring law and order as the amount of documented information; - protection of the constitutional rights of citizens to the protection of privacy and confidentiality of personal data contained in the information system;

- protection of state secrets, confidentiality of documented information in accordance with the law; - Ensuring the rights of subjects in the creation, development and use of information systems, technologies and their means.

Ensuring information security is becoming more complex and important due to the massless paperless automated management of information and communication technologies. That's why it's automated According to DataQuest, the volume of sales of information security tools in 1996-2000 amounted to 13 billion. Was equal to USD.

A set of organizational, technical, software, technological and other means, methods and measures that reduce the vulnerabilities of information and prevent unauthorized access to information, its exit and loss - is called an information security system.

Owners of information and the competent public authorities should personally determine the required level of information protection and the type of system, methods and means of protection, based on the value of the information, the damage caused by its loss and the cost of the protection mechanism. The value of information and the reliability of the protection required are directly related.

The protection system must be continuous, planned, centralized, purposeful, precise, reliable, complex, easy to improve and quick to change appearance. It usually needs to be effective in all extreme conditions.

In organizations with a small amount of information, it is advisable and effective to use simple methods of information protection. For example, the segregation and masking of readable securities and electronic documents, the appointment and training of staff working with these documents, the organization of security of the building, the obligation not to distribute valuable information to employees, control over visitors, computer use the simplest methods of protection, etc. Generally, the simplest methods of protection are effective.

In organizations with a complex structure, a large number of automated information systems and a large amount of information, a comprehensive system of information protection is created. But this method, as well as simple methods of protection, should not interfere too much with the work of the servants.

The complexity of the protection system is achieved by the presence of legal, organizational, engineering, technical and software-mathematical elements. The ratio of elements and their content ensures the uniqueness of the information security system of organizations and its uniqueness and difficulty of breaking.

It is possible to imagine that a definite system consists of many different elements. The content of the elements of the system determines not only its specificity, but also the level of protection, taking into account the value of the information and the value of the system.

The element of legal protection of information means the legitimacy of the protection of legal relations between the organization and the state, as well as the observance of the order of protection of valuable information of the organization and the responsibility of the staff for violation of this order.

Protection technology includes management and restrictive measures that encourage employees to adhere to the rules of protection of valuable information of the organization.

The external protection element is a factor that connects all other elements to a single system. According to many experts, organizational protection in information security systems is 50-60%. This depends on many factors, including the selection, placement and training of personnel who will implement the principles and methods of protection of information in practice.

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

The element of technical protection of information is designed for the organization of security of the territory, buildings and devices with the help of a complex of technical means and slow and active struggle against means of technical inspection. Although the cost of technical protection is high, this element is important in the protection of information systems.

The software-mathematical element of information protection is designed to protect valuable information that is processed and stored on a computer, local area network and various information systems.

Conditions, actions and processes that can damage a computer system (network) are considered threats to the computer system (network).

Reasons for accidental exposure to automated information systems include (Figure 2.1).

Figure 2.1. Causes of accidental exposure to automated information systems

It is known that the main components of a computer system (network) are hardware, software and data.

RSULTS

Theoretically, there are four types of risks to these components: disruption, retention, modification and falsification.

Interruption is the temporary stopping of the current shafts by the central processing unit to perform external actions (works, processes), after which the processor returns to the previous state and resumes the suspended operation. Each interrupt has a serial number, based on which the CPU device searches for a partition program for processing. Processors can create two types of interrupts: software and hardware. If a device needs emergency maintenance, there will be a technical interruption. Typically, such a delay is an unexpected event for the CPU. Program interrupts are performed using special processor commands within the main program. In the event of a program interrupt, the program automatically pauses and performs the interrupt process.

Capture is the process by which malicious individuals gain access to software and various magnetic media. Examples of illegal copying of programs and data, unauthorized readings from computer networks, and so on.

DISCUSSION

Owners of information and the competent public authorities should personally determine the required level of information protection and the type of system, methods and means of protection, based on the value of the information, the damage caused by its loss and the cost of the protection mechanism. The value of information and the reliability of the protection required are directly related.

The protection system must be continuous, planned, centralized, purposeful, precise, reliable, complex, easy to improve and quick to change appearance. It usually needs to be effective in all extreme conditions.

In organizations with a small amount of information, it is advisable and effective to use simple methods of information protection. For example, the segregation and masking of readable securities and electronic documents, the appointment and training of staff working with these documents, the organization of security of the building, the obligation not to distribute valuable information to employees, control over visitors, computer use the simplest methods of protection, etc. Generally, the simplest methods of protection are effective.

In organizations with a complex structure, a large number of automated information systems and a large amount of information, a comprehensive system of information protection is created. But this method, as well as simple methods of protection, should not interfere too much with the work of the servants.

CONCLUSION

Modification - this process allows a malicious person not only to gain access to the components of a computer system (data sets, programs, hardware), but also to change their content (appearance). For example, a change is a change in the data in a database by a malicious person, or a change in the files of a computer system in general, or a change in the code of a program used to perform some additional illegal processing. .

Counterfeiting is the process by which malicious individuals explore situations that are not accounted for in the system, identify deficiencies, and then send a fake process or fake records to the system and other users in order to take action.

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

3 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

4Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

5 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.