International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 5 Issue 1, January - 2021, Pages: 12-15

Information protection supply

Usmonov Makhsud

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

Abstract: *Information security is a set of measures, methods and tools to ensure information security. At the same time, it performs functions such as completeness of information, prevention of unauthorized access to computer objects and programs stored in them, as well as unauthorized use of programs on computers.*

Keywords: Organizational security elements. Technical protection elements. Technical means of protection. Software protection elements.

INTRODUCTION

1. Elements of organizational protection.

2. Technical protection elements.

3. Technical means of protection.

4. Software protection elements.

Information security is a set of measures, methods and tools to ensure information security. At the same time, it performs functions such as completeness of information, prevention of unauthorized access to computer objects and programs stored in them, as well as unauthorized use of programs on computers.

Information security in computer networks refers to technical, software and cryptographic methods and tools, as well as organizational measures to prevent users from owning unauthorized networks, elements and resources.

METHODS

Organizational protection measures are organizational, technical and organizational-legal measures taken in the process of creation and use of telecommunication equipment.

Ethical and ethical safeguards are procedures and arrangements that result from the development of computer technology. While these procedures are not legal, failure to recognize them can damage users' reputations.

Means of legal protection are legal documents developed by the state. They regulate the use, processing and transmission of indirect information and determine the responsibilities of violators of these rules.

Information security. Information security is the observance of standards and requirements for the protection of user information.

There are two approaches to the problem of providing AX: "fragmentary" and complex.

The ‘fragmentary’ approach is aimed at counteracting well-defined threats in the current context. An example of such an approach is some access control tools, specialized antivirus programs.

The advantage of such an approach is that the specific threat is chosen inadvertently. Its significant disadvantage is that it does not have a single secure information processing environment.

The integrated approach is aimed at creating a secure information processing environment in the AX, which combines different measures of countermeasures against threats into a single complex. Creating a secure information processing environment provides a certain degree of assurance of AX, which is an undoubted advantage of a comprehensive approach. The disadvantages of this approach are: limited freedom of movement of AX users, high sensitivity to errors in the installation and adjustment of protection devices, complexity of management.

Security policy is implemented through administrative and organizational measures, physical and software, and determines the architecture of the security system. The security policy for each specific organization should be specially developed and depend on the exact technology of processing the information contained in it and the software and hardware used.

The security policy is determined by the access control method, which determines the order of access to system objects. There are two main types of security policy: selective and authoritative.

Selective security policy is based on the preferred method of access management. A competent security policy refers to the many permissible access relationships provided by the administrator. Typically, a mathematical model based on the application matrix is used to describe the characteristics of selective application management.

The input matrix is a matrix in which the column corresponds to the system object and the row to its subject. At the intersection of the column and row of the matrix, the type of subject's allowed access to the object is indicated. Typically, an object is assigned to a subject as an "application to put in," "apply to write," "apply to execute," and so on. types are used. The input matrix is the simplest approach to modeling access control systems. But it is also the basis for more complex models.

Measures to ensure the security of computer systems are divided into the following groups according to the methods of their implementation: legal (legislative); moral education; administrative; physical; technical and software.

The listed AX is safe These measures can be seen as a series of barriers or barriers to information security. In order to access the protected information, it is necessary to cross several protection boundaries in a row.

Hardware and software tools for information protection

Advances in modern information and communication technologies have made it possible to create a number of necessary tools for protection methods.

Information security tools are programming, software and hardware. Their functional complementarity is effective in addressing the issues of information security posed to security services. To date, a very wide range of network security monitoring techniques has been developed.

RESULTS

MECHANICAL AND TECHENICAL PROTECTION OF INFORMATION BY FUNCTIONAL TASK IS DIVIDED INTO THE FOLLOWING GROUPS:

1. Physical means. These include mechanical, electromechanical, electronic, electron-optical, radio- and radio-technical and other devices. The purpose of these tools is to prevent unauthorized access to information and other possible actions of aggression.

These tools are used to perform the following tasks:

• To protect and monitor the territory of the enterprise;

• uchun To protect and control buildings;

• To protect equipment, products, financial results and information;

• himoyaTo protect access to facilities that control buildings and structures.

Physical means of protection of all objects can be divided into three categories: warning devices (walls around the object); threat detection devices (alarm and surveillance TVs) and threat mitigation systems (fire extinguishers)

In general, these categories can be divided into the following groups:

• Security and fire-fighting systems;

• Security TVs;

• security lights;

• vositalariPhysical protective equipment;

• Hardware.

2. Hardware protection

Information security hardware allows you to perform the following tasks:

• Special inspections of technical means to identify unauthorized leakage channels;

• Identification of unauthorized access to information of various objects;

• Localization (separation) of channels where unauthorized leakage of information is detected

get);

• Search and identification of industrial shipyards;

• Confidentiality of actions against unauthorized access to confidential information and other sources.

3. Software.

Software data protection is a system of special programs that perform the function of information protection. Confidential information security programs are divided into the following areas:

• Protection of information from unauthorized access;

• Protection of information from copying;

• Protection of information from viruses;

• Software development of communication channels.

Functions that software performs to protect information from unauthorized access include:

• Identification of objects and subjects;

• Restricting access to computing and information resources;

• Tracking and recording information and software interactions.

DISCUSSION

The input matrix is a matrix in which the column corresponds to the system object and the row to its subject. At the intersection of the column and row of the matrix, the type of subject's allowed access to the object is indicated. Typically, an object is assigned to a subject as an "application to put in," "apply to write," "apply to execute," and so on. types are used. The input matrix is the simplest approach to modeling access control systems. But it is also the basis for more complex models.

Measures to ensure the security of computer systems are divided into the following groups according to the methods of their implementation: legal (legislative); moral education; administrative; physical; technical and software.

CONCLUSION

Advances in modern information and communication technologies have made it possible to create a number of necessary tools for protection methods.

Information security tools are programming, software and hardware. Their functional complementarity is effective in addressing the issues of information security posed to security services. To date, a very wide range of network security monitoring techniques has been developed.

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.