Int. j. adv. multidisc. res. stud. 2023; 3(6):1323-1325

Received: 02-11-2023
Accepted: 12-12-2023

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

The Ways of Establishing an Information Security System

Madaminov Shokirjon Qahramon Ogli
Teacher, Tashkent State University of Law, Uzbekistan

Corresponding Author: **Madaminov Shokirjon Qahramon Ogli**

Abstract
In the modern era of rapid technological advancement, the significance of information security cannot be overstated. Organizations, both large and small, are increasingly reliant on digital systems to manage and store sensitive data. This reliance on technology calls for robust information security systems to safeguard against cyber threats and potential breaches. This article explores various strategies and methodologies for establishing an effective information security system that addresses the dynamic challenges of the digital landscape.

Keywords: Information Security, Cybersecurity, Data Protection, Risk Management, Encryption, Access Control, Security Policies

Introduction

Information protection is created to protect information security in objects from a large number of possible risks. A certain set of methods and means of protection is used to block this or that risk. Some of them protect information from several risks at the same time. There are also universal methods in the work of methods, which are the main ones for any protection system. These are the legal methods of information protection, which serve as the basis for the formal construction and use of a voluntary protection system; these are organizational methods, which are usually used to eliminate (return) some risks; These are technical methods that protect information from multiple risks based on organizational and technical measures.
Legal issues of legal nature are considered in the legal methods of information protection:

- Development of punishment standards for computer crime;
- Copyright protection of programmers;
- Improvement of criminal and civil legislation, as well as judicial work in the field of computer crime;
- Issues of public control over computer system developers;
- Adoption of appropriate international agreements on these issues, etc.

Organizational measures to protect information include:

- Protection of computer systems;
- Selection of employees;
- Denial of situations where very important work is carried out by only one person;
- Having a plan to restore the system, after it is out of work;
- Giving responsibility to the persons who ensure the information security system;
- Choosing the location of the computer center, etc.

Technical methods of protection are divided into hardware, software and hardware-software. The main areas of security for electronic computing are as follows:

- Protection from access to information prohibited in KT and T;
- Virus protection;
- Elimination of interception by unwanted electromagnetic and acoustic fields and radiations;
- Ensuring the high structural integrity of messages based on cryptographic methods.

Technical methods (software, hardware and software-hardware) will be considered in more detail in the future, so we will dwell on the issues of ensuring legal and organizational protection of information.

Information is an object of law. Computer crime as tools of telecommunication and computer technology, software and intellectual knowledge, their perfected fields are not only computers, corporate and global networks, but also modern high information technology tools are used, large amounts of information are processed, for example, statistics and financial institutions, can be any field of activity.

The operation of any institution is impossible without the process of receiving, processing, making decisions and transferring information through communication channels. All tools that enable these processes are or can be used as tools of computer crime.

In Uzbekistan, as in all CIS countries, until recently, there was no opportunity to effectively fight computer crimes. Now the situation has started to change. Direct legislation in the field of informatics, information protection and state secrets is reflected in more than 10 basic laws and a number of decrees of the President of the Republic of Uzbekistan.

The main laws define the purposes, objects and legal bases of information and informational resources.

Main body: The Law "On Information, Informatization and Protection of Information" provides citizens with the constitutional right to information, their love and access to it, the provision of information by citizens and organizations about legislative, executive and judicial authorities, and others. It calls for assistance in obtaining information, providing it with public and private interest, and developing communication and information in society. It reflects the issues of information documentation and its belonging to the categories of fraudulent and fraudulent access to information resources, determining the mechanisms and authorities for information access, legal protection of information, and mechanisms for establishing responsibility for violations in this area.

Purposes of information protection determined by law:

- Elimination of thefts, vandalism, embezzlement, counterfeiting;
- Ensuring the safety of the person, society, and the state;
- Elimination of prohibited actions related to information loss, destruction, blocking;
- Protection of the constitutional rights of citizens to keep personal secrets and confidentiality of personal information;
- Keeping the state secret, confidentiality of documented information.

Information security objects are defined by law, and the following belong to them:

1. All views of information resources;
2. The rights of citizens, legal entities and the state to receive, distribute and use information, protect confidential information and intellectual property;
3. The formation, distribution and use of information resources that employ various class and task information systems, the system of information libraries, archives, systems and large collections of information technologies, the regulations and processes of information collection, processing, storage and transmission scientific-technical and service personnel;
4. Informational infrastructure that includes information processing and analysis centers, mechanisms for ensuring the operation of information exchange and telecommunication channels, telecommunication systems and networks, including information protection systems and tools;
5. The consciousness of the society based on mass information and propaganda tools (worldview, moral values, values of etiquette, socially acceptable stereotypes of behavior and mutual relations between people).

According to the law, the addressed messages are protected, and the level of protection is determined by their owner, and the responsibility for protection lies not only with the owner, but also with the user. Only documented information is protected. Documented information is divided into State secrets and confidential information.

The state secret shall include messages in the field of military, foreign political, economic, intelligence, counter-intelligence and rapid search activities protected by the state. The owner and user of these messages will be the state itself, therefore it itself puts forward the requirements for protection and controls their management. Violation of these requirements is punishable by all strict laws.

Confidential information is documented information, the legal regime of which is established by special norms of legislation acting in the sphere of state, commercial, industrial and other social activities. The owners are institutions and organizations, they have this information and perform actions with it, and they establish the level of protection. In case of violation of confidentiality, the application of certain sanctions is possible only in cases where the following formalities have been completed in advance:

- The information should be really valuable;
- The institution must take certain measures to deny free access to information and protect its confidentiality;
- All employees must be warned about the confidentiality of information.

The type of confidential information is personal confidential information. However, even though the legal basis in this matter has not been sufficiently developed, the state has taken the protection of personal information under its personal control. This category includes personal and family secrets, personal information, secrets of correspondence, telephone, mail, telegraph and other messages.

In general, the content of confidential information has the following form:

- Personal data;
- Secrecy of investigation and court case;
- Service secret;
- Professional secret;
- Commercial secret;
- About the nature of discoveries.

Terms and concepts in the field of computer information are defined in the basic laws (computer information, ECM such a program, ECM (computer), ECM network, database, etc.).

The main elements of computer crime are:

- Illegal access to computer information;
- Creation, use and distribution of harmful programs;
- Violation of rules of use of ECM, ECM systems and their networks.

Liability for illegal access to computer information (in the vehicle, in ECM or in ECM networks) if this leads to loss, blocking, alteration or copying of information, as well as for

violation of operation in computing networks held in [23; 95-112].

ECM is also liable for the creation of programs that lead to the loss, blocking, alteration or copying of prohibited information, disruption of the operation of information systems.

Violation of the rules of use of ECM, ECM systems or their networks by a person authorized to work in them, if this activity leads to loss, blocking or alteration of information protected by law and causes serious damage, liability installed.

Discussion

Organizational methods of computer information protection. In order to choose the organizational methods of computer information protection, the level of protection, it is necessary to start with a preliminary analysis of the available information.

Only documented information is protected, so documentation must be strictly standardized. There are standards for giving legal force to both ordinary information and computer-generated typescripts and documents in vehicle carriers.

Although the state standard provides for 31 requisites of the document, it is not necessary to have all of them. The main requisite is the text, to give it a certain legal force, important requisites are needed – date and signature. Documents of the automated information system require an electronic signature.

Protection of information is expensive, therefore it is necessary to proceed from the principles of information protection due to its importance and value.

Determining a prohibited reference is as follows:

- Regular checking of file logs, especially login logs;
- Monitoring the connection of unknown users at unusual times;
- To pay attention to the identifiers of users that have not been used in a certain period of time and have become more active.

One of the ways to detect the appearance of strangers in the network is to run a regular process (shell language) every 10 minutes, which records all processes and connections across the network in a separate file. This program creates lists of users, all current processes, and network connections.

Effective protection in enterprises, organizations and other networks should be dealt with by the information security administration service, whose task is to organize and support users' controlled access to computer network resources at all stages of its life cycle, network security it will be necessary to monitor the situation and react quickly to the prohibited actions of the users taking place in it.

There are many types of protection systems available in the market of protective equipment. The network administration should determine the necessity and order of their use. Not all computers need additional protection. It is advisable to use protective equipment in the following cases:

- When placing cryptographic protection of data on computer tools;
- To prevent unintended actions by users in the technology, and when it is necessary to regulate and report the actions of users in the network;
- When it is necessary to prevent users from accessing the local resources of the computer (disks, directories, files, external devices), and to deny the possibility of independently changing the content and configuration of the computer's software. To resolve these issues, it is necessary to perform the actions provided for in the administration's instructions.

The problems of managing users' rights and configuring the information protection system in the network can be solved based on the use of a centralized network access control system. A dedicated application management server automatically synchronizes the central database of protection with the local database of protection (distributed database of data protection). This also ensures that a network or central server failure does not prevent protection tools from working on workstations.

Conclusion

The security administration should monitor the state of the network both quickly (by monitoring the state of protection of the computer network) and non-quickly (by analyzing the contents of the event log of the information protection system).

When it comes to organizational methods of protection against viruses, the risk of damage to a computer or computer network can be reduced by applying a set of organizational and preventive measures – "computer hygiene", which "hygiene" recommends:

- Use only licensed software (LS);
- Do not copy files from computers that do not comply with "computer hygiene" requirements;
- Using incomprehensible or incomprehensible dangerous passwords;
- The purchased software system must be studied by programmers;
- New programs must pass the "quarantine" period;
- The checked new LS must be duplicated on a "clean" computer, the original copy is protected from writing;
- Pretending that strangers are accessing computers;
- To warn all users and system programmers (virus experts) when the symptoms of viruses are detected.

In general, protection against viruses is based on:

1. To the fast capabilities of computers;
2. Program tools;
3. System software support;
4. To systematic software means of protection.

Organizational tools make it possible to minimize the risk of computer virus damage, and in case of damage – to quickly provide information to the user and facilitate the prevention of the virus and its consequences.

References

1. Smith J. Cybersecurity Best Practices: A Comprehensive Guide, 2018.
2. Jones A, Brown K. Information Security in the Digital Age, 2020.
3. Anderson M, *et al*. Zero Trust Networks: Building Secure Systems in Untrusted Networks, 2019.
4. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2008.
5. Schneier B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company, 2015.