# Technical means of information security

**Aghayeva Shabnam**

## Abstract

This article examines the information security techniques that are essential to protect the confidential information of companies, governments, and individuals from the growing number of hacking, data theft, malware, and other online attacks. It also examines cryptography, firewalls, intrusion detection, identity and access management, and other security measures. measures, including tools, techniques and strategies used to protect sensitive data from attack. The article also highlights information security issues and risks, as well as external risks such as targeted attacks and security vulnerabilities. Information security information is also shown, including having strong security policies, continuously monitoring systems and networks, and responding quickly to security incidents. The article provides recommendations for strengthening information security in an ever-changing technology environment, such as implementing comprehensive security measures as well as developing personalized and effective security. Some of the most common technical tools used to protect data are shown to include firewalls, antivirus, intrusion detection software, encryption systems, multi-factor authentication, virtualization, and network segmentation. was done. Multi-factor authentication requires two or more forms of authentication before accessing a system or application to increase security. Virtualization has been reported to help create isolated computing environments to protect sensitive systems and data.

**Key words**: information, information security, attacks, technical means

The history of the creation of technical means of information protection began long before the computer era. One of the first examples of technical information security is the encryption system used by the ancient Greeks. They used a technique called a "wanderer," a mechanical device to encrypt and decrypt text.With the development of technology, the technical means of information security are becoming more and more complex and diverse. In the 19th century, the first telegraphs were invented and there was a need to protect messages transmitted through them from interception and eavesdropping. This led to the creation of the first cryptographic systems.

Enigma, an electromechanical encryption system used by the Germans to protect their messages during World War II, was created. But thanks to the efforts of Allied cryptographers, the system was cracked. With the development of computer technology in the 1950s, the technical means of protecting information became much more sophisticated and effective. The concept of user authentication and information access control was introduced in the early 1960s. In the 1970s, the first antivirus programs were created, and in the 1980s, the first programs to protect against hackers and intruders appeared. Now, technical means of information protection are one of the most important aspects of information security, and their development and improvement are continued.

Information security is a discipline that aims to protect information and computer systems from internal and external threats. Information can be stolen, lost, corrupted, or misappropriated, which can have serious financial, legal, and reputational consequences for organizations or individuals. To prevent these incidents, information security techniques have been developed to protect sensitive data and ensure data confidentiality, integrity and availability.

Information security tools are tools and software designed to protect the confidentiality, integrity, and availability of information. Some of the main technical means of information protection include:

1. Antivirus software: Protects computers and other devices from harmful programs such as viruses, trojans, and spyware.
2. Firewall: a program or device that controls incoming and outgoing traffic on a computer network, blocks unwanted connections, and prevents unauthorized access to information.
3. Cryptographic protection means: it allows information to be encrypted in a way that is inaccessible to

outsiders. Some cryptographic tools include data encryption, electronic signatures, and digital certificates.
4. Backup systems: data backup to external media such as hard drives, USB drives or the cloud. This allows you to quickly restore data in case of loss or damage.
5. Authentication tools: allows to determine the legitimacy of the user and prevent unauthorized access to information. These include passwords, biometrics (such as a fingerprint scanner) and access cards.
6. Monitoring tools: allows you to monitor the activity of users and devices on the network to identify unusual access attempts or attacks. These can be software tools such as access systems or hardware tools such as surveillance cameras and motion sensors. Antivirus programs (antiviruses) are designed to protect computers and other devices from malicious programs such as viruses, trojans, rootkits, spyware, and other threats. They work by scanning files and the system for malware, blocking threats and deleting already infected files.

The main functions of antivirus programs:
- Blocking threats and deleting already infected files
- Preventing viruses and other threats from updating the database
- Protection from new and unknown threats
- Protection from phishing and other online threats
- Monitors and blocks network attacks on the device

A firewall is a security tool that provides network access control as well as traffic management between networks with different trust levels. A firewall is used to protect computers and networks from unauthorized access, viruses, hacking attacks, and other threats.

Main functions:
- Access Blocking - Denying access to certain ports, protocols or IP addresses to prevent unauthorized access to the network.
- Port Scanning Protection - blocking of port scanning that can be used by attackers to identify vulnerabilities in the network and subsequent attacks.
- Intrusion detection - detection and prevention of unauthorized network access attempts or hacker attempts.
- Network partitioning - dividing networks into several subnets with different levels of trust. This increases the security of the network and protects it from unauthorized access.

There are two types of firewalls: software and hardware. Software firewalls operate at the operating system level and control traffic passing through the computer on which they are installed. Hardware firewalls are separate devices that operate at the network level and monitor traffic passing through them.

Cryptographic security measures are used to protect data from unauthorized access, as well as to ensure data confidentiality and integrity. Cryptography is the science of methods for ensuring the confidentiality and integrity of data by encrypting and decrypting it. Cryptographic security tools include various encryption algorithms and keys, as well as software and hardware used to create secure communication channels, store data, and exchange data.

The main methods of cryptographic protection:
- Symmetric encryption An encryption method in which the same key is used to encrypt and decrypt messages. This method is quick and simple, but vulnerable to man-in-the-middle attacks.
- Asymmetric encryption is an encryption method where different keys are used to encrypt and decrypt messages. One key is used to encrypt messages and the other to decrypt them. This method provides a higher degree of security than symmetric encryption.
- Electronic signature is a cryptographic security method that creates a digital signature that confirms the authenticity and integrity of a document. This method is used to protect electronic documents by digitally signing them.
- Digital certificates are electronic documents that confirm the authenticity of identification data and cryptographic security keys. They are used to protect electronic transactions and keep email secure.

In addition, an important aspect of cryptographic protection is the management of encryption keys. Encryption keys should be stored in a safe place and regularly.

Backup systems are designed to back up data to protect against data loss or damage. Backup can be performed both on local media and on a remote server.

There are several types of backup systems:

1. A full backup is a copy of all data to media. A full backup is used to create a master copy of data or when you need to transfer all data to a new server.
2. An incremental backup only copies data that has changed since the last full or incremental backup. An incremental backup takes less time and space than a full backup.
3. A differential backup is copying only data that has changed since the last full backup. A differential backup takes up more space than an incremental backup, but takes less time than a full backup.
4. A snapshot backup is a copy of all data at a specific point in time. A snapshot can be created on a local or remote server. A snapshot can be used to restore the system in the event of a crash or attack.
5. Online backup is a real-time data backup process. Online backup is used to protect data in real-time and allows for quick data recovery.
6. Offline backup is the process of backing up data when a server or computer is disconnected from the network. Offline backup is used to create archival copies of data or when a server or computer cannot connect to a network.

Authenticators are mechanisms used to authenticate users and devices to a system. Verification can be done using various methods and technologies:

1. Login and password is the most common authentication method used to authenticate users in the system. Login and password ensure access to the system only by users who know the appropriate credentials.
2. Access keys are an authentication method used to authenticate devices on a network. Access keys can be used to enable communication between devices on a network.
3. Biometrics is an authentication method that uses a person's biological parameters, such as fingerprint, voice or face recognition, to authenticate users to a system.
4. Tokens are an authentication method that uses electronic devices such as USB keys or smart cards to authenticate users to the system.
5. Network authentication is an authentication method that uses protocols such as RADIUS or TACACS+ to authenticate users trying to access the network.
6. One-time passwords are an authentication method that uses temporary passwords that are given to users for one-time use and provide an additional level of security.
7. Multi-factor authentication is an authentication method that uses multiple authentication methods to provide a higher level of security. For example, login may require a username and password, as well as a fingerprint or passkey.

Monitoring tools are software or hardware used to collect, analyze, and display information about system or network activity. They can be used to monitor various parameters such as performance, availability, resource usage, and to detect and prevent security breaches.

Monitoring tools can be classified according to different criteria, such as the type of data or application they monitor. Some of the more common monitoring tools include:

1. Performance monitoring is a type of monitoring used to monitor the performance of a system or network. This may include monitoring CPU usage, memory, disk space, network connections, and other parameters that may affect system performance.
2. Availability monitoring is a type of monitoring used to monitor the availability of a system or network. This may include monitoring the availability of websites, applications, servers and other resources, as well as detecting and automatically notifying you of failures.
3. Security monitoring is a type of monitoring used to detect and prevent security breaches in a system or

network. This may include inbound and outbound traffic monitoring, attack and malware detection, resource access monitoring, and other functions.

4. Event monitoring is a type of monitoring used to track events on a system or network. This may include event log monitoring, configuration change monitoring, user activity monitoring, and other functions.

5. Network monitoring is a type of monitoring used to monitor network activity and detect network problems. This may include monitoring the speed and load on the network, monitoring the detection of corrupted packets.

**Conclusion**

Technical means of information protection are necessary means to ensure information security in the modern digital world. They protect sensitive data from various types of threats, including viruses, hacking attacks, data leaks, and more. used to protect Antivirus programs, firewalls, cryptographic protection tools, monitoring and auditing tools, authentication tools, and content filters are used for various aspects of information security. It should be noted that there is no universal tool for information protection, and the use of only one of the listed tools does not guarantee complete protection from threats. Instead, it is advisable to use a comprehensive protection system that will include several tools and technologies. Technical means of information protection play a key role in ensuring information security, but it is also necessary to remember that the human factor is also an important aspect of protection. Employee training, establishing and monitoring security policies, and regular security testing are also required to ensure data security.

**References**

[1] Buzov G.A. Protection of limited access information from leakage through technical channels // M.: GLT, 2016. 586 p.

[2] Zapechnikov S.V., Miloslavskaya N.G., Tolstoy A.I., Ushakov D.V. Information security of open systems // M.: GLT, 2018. 558 p.

[3] Konakhovich G.F., Klimchuk V.P., Pauk S.M., Potapov V.G. Protection of information in telecommunication systems // K.: MK-Press, 2005. 288 p.

[4] Semenenko V.A. Information security: учеб. пособие // M.: МГИУ, 2017. 277 p.

[5] Partyka T.L., Popov I.I. Information security: учеб. пособие // M.: Forum, 2016. 432 p.

[6] Titov A.A. Engineering and technical protection information: учеб. пособие // Tomsk: ТГУСУР, 2010.

[7] Torokin A.A. Engineering and technical protection information: учеб. manual // M.: Helios ARV, 2005. 960