PERIODICA
Journal of Modern Philosophy, Social Sciences and Humanities
ISSN NO:2720-4030 Volume 46 September 2025

On Modern Methods And Means Of Protection In Computer Networks

A.T. Utepbergenova
Nukus State Institute named after Ajinyoz

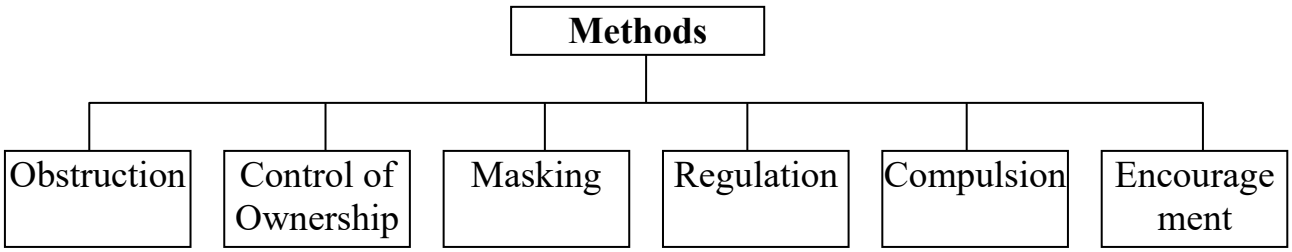
ABSTRACT
This article discusses modern methods and tools for protecting information in computer networks. Technical, software, cryptographic and organizational measures used to ensure information security are covered in detail. Also, unauthorized access methods, methods for their prevention, the importance and practical application of cryptographic protection mechanisms are analyzed. The article provides a detailed classification of information protection tools - formal, informal, technical, software, organizational, ethical and legal aspects.

ARTICLE INFO
Received: 28th June 2025
Accepted:26th July 2025

KEYWORDS:
Information security, computer networks, protection methods, cryptography, software tools, technical tools, organizational measures, unauthorized access, information protection.

Information protection in computer networks refers to technical, software and cryptographic methods and means, as well as organizational measures, to prevent unauthorized users from accessing the network, its elements and resources.

Methods and means of ensuring information security in direct telecommunication channels can be classified as follows:



It is acceptable to describe the above methods as follows.

Interception is defined as the physical means of preventing access to devices, media, etc.

Ownership management is a method of regulating the use of system resources. This method consists of the following functions:

- • identify each object, element of the system, for example, users;
- determine the authenticity of the object or subject by identification;
- create working conditions and allow work according to the adopted regulations;
- record access to protected resources;
- respond to unauthorized actions, for example, signal, disable, refuse to execute the request, etc.

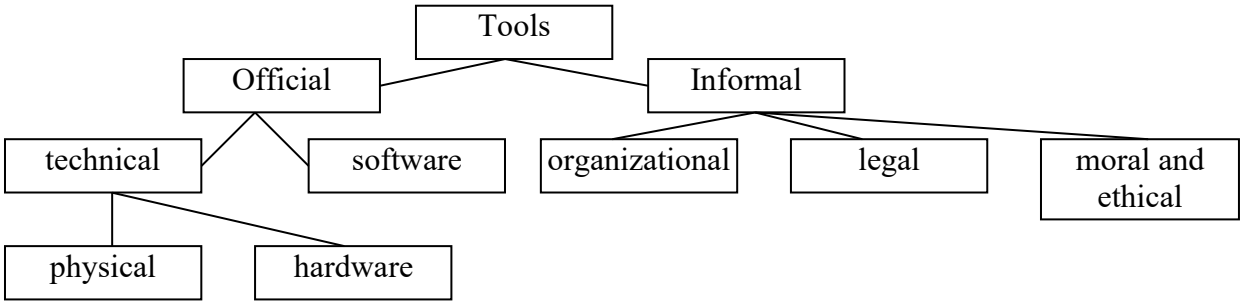
Masking - encoding data using cryptography to make it difficult to read.

Sorting - creating conditions when working with data that reduce the likelihood of unauthorized access to the system.

Coercion - processing data in accordance with accepted rules, otherwise users will be subject to material, administrative and criminal penalties.

Enforcement - aimed at enforcing accepted procedures in accordance with ethical and moral rules.

In the implementation of the above-mentioned methods, they apply the tools classified as follows.



Official means — are tools that perform information protection functions without the participation of individuals.

Unofficial means — are regulations that directly determine the activities of individuals or their functioning.

Technical means refer to electrical, electromechanical, and electronic devices. Technical means, in turn, can be physical and hardware-based.

Hardware-technical means are devices integrated into telecommunication equipment or connected to it via an interface. For example, a parity check scheme for data control, which is used to detect errors in transmitted data, automatically checks the parity of the number of units (together with the control bit).

Physical technical means — are devices and systems that operate autonomously. For example, ordinary door locks, metal bars installed on windows, and security electrical equipment belong to physical technical means.

Software means — are specialized software designed to perform information protection functions.

In information protection, software means were initially the most widely used, but today they are considered secondary protection tools. An example of this is the password system.

Organizational protection means — are organizational-technical and organizational-legal measures adopted during the creation and operation of telecommunication equipment. As a direct example, the following processes can be mentioned: building construction, system design, installation of equipment, testing, and commissioning.

Ethical and moral protection means — are rules and agreements arising as a result of the development of computer technology. Although these rules are not legally binding, failure to comply with them may damage the reputation of users.

Legal protection means — are legal documents developed by the state. They directly regulate the use, processing, and transmission of information, and determine the responsibilities of those who violate these rules.

For example, the rules developed by the Central Bank of the Republic of Uzbekistan clearly define the organization of information protection groups, their powers, obligations and responsibilities.

The development of methods and means of ensuring security can be divided into three stages: 1) development of software tools; 2) development in all directions; 3) at this stage, developments are observed in the following areas:

-hardware implementation of protection functions;

-creation of tools that cover several protection functions;

-generalization and standardization of algorithms and technical means.

Currently, the ways of unauthorized data leakage include the following:

• remote reading of electronic beams;

• irradiation of communication cables with electromagnetic waves;

• use of covert listening devices;

• remote imaging;
• reading of acoustic waves emanating from a printer;
• theft of data carriers and production waste;
• reading of data stored in the system's memory;
• copying of data by overcoming protection;
• entering the system under the guise of a registered user;
• use of software traps;
• exploitation of flaws in programming languages and operating systems;
• presence in programs of subroutines that can be launched under specially defined conditions;
• illegal connection to communications and devices;
• intentional disabling of protection devices;
• introduction and use of computer viruses into the system.

Almost all of these methods can be prevented, but no satisfactory means of protection against computer viruses have yet been developed.

In order to protect data transmitted directly over a network, the following measures should be taken:
- prevent the transmission of transmitted data from being opened and read;
- prevent the transmission of transmitted data from being analyzed;
- prevent the transmission of transmitted data from being altered and detect attempts to alter it;
- prevent the detection of software interceptions used to transmit data;
- prevent fraudulent connections.

These measures are mainly implemented using cryptographic methods.

Literature

1. Aripov M. Informatics and information technologies. Uchebnik dlya studentov vuza T. 2005.
2. Alaminov M.Kh., Utemuratov T.R. Computer networks.-T.: "Science and technology", 2018, 164 p.
3. M.Alaminov, T.Utemuratov Configuring IPsec VPN server for VPN connection for clients in Kerio Control (on the example of Windows operating system). A collection of scientific articles by scholars devoted to the importance of valuing the elderly. Nókis-2015 j.
4. M. Alaminov, T. Utemuratov. How to connect to the Internet. Science Society, 2017 vol.