pISSN:2349-5707 Volume:13,Issue 2, February -2026 eISSN:2349-5715

METHODS OF LIMITING AUTHORIZED ACCESS AND EXIT OF INFORMATION IN COMPUTER NETWORKS

Kodirov Odiljon Jaloldinovich
Andijan State Pedagogical Institute, teacher
Email:odiljon_qodirov@umail.uz
ORCID ID 0009-0006-6865-0714

Abstract: With the widespread use of computer networks and the internet, information security issues are becoming increasingly relevant. This topic is aimed at studying the methods of restricting unauthorized access and leakage of information in computer networks. Information security is especially important in corporate networks, government organizations, and personal computers. Effective application of these methods helps prevent cases of information theft, damage, or misuse in networks.

Keywords: LAN, WAN, information systems, computer networks, unauthorized access, computer viruses.

Currently, large volumes of information are stored in existing information systems, and their protection is one of the most pressing problems.

Modern automated information systems are a development software and hardware complex, and they provide solutions to problems requiring information exchange.

The main sensitive components of information systems are:

- servers on the internet. These servers are disabled: by destroying programs or data files; by overloading servers with excessive unfinished processes; by abruptly filling the system log; by copying files that cause browser programs to fail;
- data transmission channels - programs that form a hidden channel are sent for the purpose of obtaining information through some port;
- Rapid data transmission channels - these channels are loaded with a large number of unnecessary files, and their data transmission speed decreases;
- channels for transmitting news - these channels are filled with outdated information or these channels are completely destroyed;
- Java browsers - Using Java language capabilities created by SUN company, data can be accessed without authorization by creating applets. Java applets are automatically triggered on the network, and as a result, the user can never see what actually happens when using a document, for example, it becomes possible to organize network viruses and send viruses through Java applets, or it becomes possible to own the user's credit card numbers.

Thus, the analysis conducted above shows that currently computer networks have many sensitive parts through which unauthorized access to information is being carried out or databases are being destroyed, resulting in humanity suffering billions of dollars in losses.

Unauthorized access to the resources of computer systems is understood as actions to use, modify, and delete the data of this system.

If computer systems have protection mechanisms against unauthorized access, then unauthorized access actions are organized as follows:

- Remove or change the appearance of the protection mechanism;
- Log in to the system with the name and password of a certain user.

If in the first case it is necessary to change the program or change the system query, then in the second case, unauthorized access is carried out by viewing and using the password of the existing user when entering it through the keyboard.

Methods of implementing programs necessary for unauthorized data acquisition:

- Unauthorized possession of computer system resources;
- unauthorized interference in the process of exchanging messages in the communication channels of the computer network;

pISSN:2349-5707 Volume:13,Issue 2, February -2026 eISSN:2349-5715

- Introduction of software vulnerabilities in the form of viruses.

Often, the weaknesses present in a computer system are called "holes" or "holes." Sometimes programmers themselves leave these "holes" when creating a program, for example:

- for the purpose of easy assembly of the resulting software product;
- to gain secret access to the program after the program is ready.

Necessary commands are poured into the existing "hole," and these commands carry out their work at the right time. Virus-like programs are used to erase or partially modify data and disrupt work sessions.

Currently, the boundary between local area networks (LAN) and global networks (WAN) is disappearing. This, that is, the increase in LAN capabilities, requires further improvement of data protection methods.

When organizing protective equipment, the following should be taken into account:

- a large number of subjects interacting with the system, and in many cases, the lack of control over some users;
- availability of necessary information for the user on the network;
- the use of computers produced by various companies in networks;
- use of various programs in the network system;
- Due to the fact that network elements are located in different countries, the length of communication cables stretched to these countries and their complete control is practically impossible;
- simultaneous use of information resources by several users;
- connection of several systems to the network;
- slight network expansion, i.e., the uncertainty of the system's boundaries and the uncertainty of who works in it;
- multitude of attack points;
- difficulty in controlling system access.

The need for network protection arises in the following cases:

- read other users' arrays;
- read data that has been left in memory;
- bypassing protective measures and copying data carriers;
- working as a hidden user;
- use of software holders;
- use of shortcomings of programming languages;
- deliberate failure of protective equipment;
- Enter and use computer viruses.

When organizing network protection, it is necessary to organize:

- control of the protection system;
- file access control;
- control of data transmission in the network;
- control of access to information resources;
- Control of data distribution to other networks connected to the network.

For information processing, it is necessary to use computers that have passed the necessary verification. The functional completeness of protective equipment is important. In this case, the work of the system administrator and their control are of great importance. For example, users frequently change passwords, and the length of passwords makes them difficult to identify. Therefore, it is important to limit the registration of new users (for example, only during working hours or only at the enterprise where they work). To verify user authenticity, it is necessary to maintain feedback (for example, using a modem). It is possible to use a mechanism for restricting access to information resources and fully transfer its influence to LAN objects.

To protect data transferred between network elements, it is necessary to take the following measures:

pISSN:2349-5707 Volume:13,Issue 2, February -2026 eISSN:2349-5715

- not allowing information to be clarified;
- not allowing analysis of information exchange;
- do not allow messages to be modified;
- prevent hidden connections and quickly identify these cases.

Cryptographic protection methods are used during data transmission on the network. Information about unauthorized access must be recorded in the registration log. Access restrictions to this log must also be implemented using security measures.

The main reason for the complexity of monitoring a computer network is the complexity of monitoring software. In addition, the abundance of computer viruses makes it difficult to monitor the network.

Based on the foregoing, it can be concluded that software tools are the most powerful and effective tool for unauthorized access to data, posing a significant threat to computer information resources, and the fight against them is one of the most pressing problems.

REFERENCES

1. Karl A. Astrom, Bjom Wittenmark. Computer-Controlled Systems: Theory and Design, Third Edition. - USA: Dover Publications, 2011. 576 p.

2. Fritz Klocke. Modeling and Planning of Manufacturing Processes. - Тошкент, 2016. - 658p.

3. Olifer V.G., Olifer N.A. Computer Networks. Principles, technologies, protocols. Textbook. - 3rd edition. St. Petersburg. Peter. 2006.

4. Broydo V.L. Computing Systems, Networks, and Telecommunications. St. Petersburg: Piter. 2003.

5. Botirov T.V., Sattorov O.U., Kadirov Yo'.B., Boboyev A.A Computer Systems and Networks. Textbook.- Navoi-2019. - 443 pages.