GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 13, Issue 5 May (2025)

PROBLEMS OF TEACHING NETWORK TECHNOLOGIES AND THEIR SOLUTIONS

Rajabova Gulchekhra Salomovna
Bukhara State Pedagogical Institute at Teacher
gulchexra301010@gmail.com

ABSTRACT

This work analyzes the main problems encountered in the process of teaching network technologies, which are an integral part of modern information and communication technologies, and explores ways to address them. In particular, it highlights factors such as difficulties in developing students' practical skills, lack of modern equipment and software tools, teacher qualifications, and the relevance of curricula. The research proposes the use of innovative pedagogical approaches, virtual laboratories, simulators, and online platforms to solve these issues. The annotation serves to promote the development of digital competencies through the implementation of improved methods for effective teaching of network technologies.

Keywords: Network technologies, Information and Communication Technologies (ICT), Innovations in education, Virtual laboratories, Simulators, Curriculum, Practical skills, Qualified personnel, Online learning platforms, Interactive teaching methods, Digital competencies, Technical infrastructure, Network security, Distance education, Modern educational methodology.

INTRODUCTION

The modern education system, its goals and objectives, must align with the challenges of educational development that contribute to the progress of our republic. The current state of global scientific and technological advancement, the management of the country's socio-economic development, and the significance of intellectual potential in shaping the future underscore the importance of timely and relevant information. Moreover, the rapid development of science and technology, especially in societies where modern information technologies are widely implemented, leads to frequent updates in knowledge across various fields. This places on learners the dual responsibility of quickly acquiring new knowledge and continuously engaging in independent learning.

Effectively organizing pedagogical education processes based on modern information technologies requires:

the collaboration of educators, software developers, and relevant specialists in creating distance learning courses and electronic literature;

the distribution of tasks among educators;

the improvement of the educational process organization and the monitoring of pedagogical effectiveness.

The integration of modern information technologies into the educational process contributes to:

Students acquiring professional knowledge;
deeper comprehension of scientific disciplines through modeling of studied phenomena and processes;
the expansion of students' independent learning opportunities due to diverse forms of educational activity;
the individualization and differentiation of the learning process through interactive communication tools;
the adoption of strategies for mastering educational materials by leveraging artificial intelligence systems;
the development of information culture as a member of the information society;
and the enhanced interest and engagement in scientific fundamentals through the presentation of studied phenomena and processes using computer technologies.

The government of our country is carrying out several initiatives aimed at forming and developing the information support system for higher education, reforming higher education institutions in accordance with the requirements of the "National Program for Personnel Training," creating and implementing appropriate state educational standards, providing educational institutions with necessary textbooks and literature, involving leading scientists and highly qualified specialists in this process, and training and improving the qualifications of professors and teachers in leading educational institutions of developed countries. Among these efforts, it is also necessary to improve the effectiveness of teaching the subject *"Network Technologies"* in higher education institutions and to enhance its educational and methodological support.

A systematic approach is required for the content of teaching materials and teaching methods of the *"Network Technologies"* course. The main issue is selecting topics within the course structure clearly, logically, and on a scientific basis, which entails specific didactic requirements, such as: linking theory to practice, ensuring inter- and intra-disciplinary connections, distributing study time effectively, and incorporating core rules, laws, and concepts into the systematization of knowledge with logical analysis of the educational material.

The primary goal of teaching the *"Network Technologies"* course is to provide students with theoretical and scientific knowledge related to network methodologies and technologies, network management, and network architecture design. The objective is to develop in students modern methods of working with network technologies, the ability to develop network software, and skills in operating network management systems.

Analysis shows that the *"Network Technologies"* course should emphasize theoretical and scientific content in lectures, as practical, laboratory, and independent study sessions focus on exploring software capabilities used to develop information systems.

When selecting content for this course, criteria such as the holistic development of future specialists, a high level of scientific and practical relevance, alignment with real educational capabilities, and conformity with the designated time and hours for studying the subject should be applied.

Research analysis reveals that the volume of information provided in the *"Network Technologies"* course is very large. Therefore, the course curriculum should be designed to fully cover all relevant materials on network technologies.

The development of global networks and the emergence of new technologies for obtaining, processing, and transmitting information have attracted individuals and organizations to the Internet. Many organizations have decided to connect their local networks to global ones and currently use WWW, FTP, Gopher, and other servers. The ability to transmit commercial or classified government information over global networks has created a need for qualified specialists in information security systems.

Using global networks is not limited to searching for "interesting" information — it also involves performing commercial and other critical tasks. The absence of protective measures during such activities can result in significant losses.

Any organization connected to the Internet must address the following issues:

Hacking of the organization's computer systems;

Interception of data transmitted via the Internet by malicious actors;

Damage to organizational operations.

The Internet was not initially designed as a secure network. Current issues in this field include:

Easy access to sensitive data;

IP address spoofing;

Vulnerabilities in TCP/IP protocols;

Improper configuration of many websites;

Complex configuration procedures.

To connect local networks to global ones, a network security administrator must address the following:

Establish protection against threats from the global network;

Provide data concealment capabilities for global network users.

Some protective methods include:

Blocking access via unauthorized network addresses;

Using the Ping utility to flood network packets;

Combining allowed network addresses with blocked ones;

Blocking by using prohibited network protocols;

Enforcing password selection for network users;

Modifying routing tables using REDIRECT-type ICMP packets;

Changing routing tables using non-standard RIR packets;

Establishing connections using DNS spoofing.

Unauthorized access during restricted times poses risks in several areas of global networking, including:

Local areas;

Local-global network convergence;

Transmitting critical information via global networks;

Uncontrolled segments of global networks.

The main components of any information network are servers and workstations.
Servers hold information or computing resources, while workstations are used by employees. In general, any computer can function as either a server or a workstation, and as such, they are susceptible to potential security attacks. To prevent these attacks, the concept of a firewall was introduced. This software operates in conjunction with multiple security-enforcing systems. Firewalls and gateways, along with physical and logical data protection methods, ensure secure information transmission within the network.

The firewall and its functions are critical, including the following:
A firewall is a protection tool used to control access to data between a trusted network and an untrusted one.
It is a multi-component system that serves as a strategy to protect an organization's information resources from the Internet. It also acts as a guard between the organization's network and the Internet.
The main function of the firewall is to provide centralized control over data access.
The firewall performs the following security measures:
Blocks unauthorized traffic, i.e., restricts the flow of messages across the network;
Directs incoming traffic to internal systems;
Protects vulnerable parts of internal systems by hiding them from external attacks;
Logs all traffic;
Hides internal data such as network topology, system names, network devices, and user identifiers from the Internet;
Ensures reliable authentication.
In many sources, the term "firewall" is also referred to as a **brandmauer** or **Fire Wall**—they all refer to the same concept.
A firewall is a system that divides a general network into two segments, serving as an inter-network protection tool and a set of rules that govern the conditions for data packet transmission across boundaries.
Typically, a firewall protects internal networks from global networks such as the Internet. It should be noted that firewalls can also protect against corporate networks, not just the Internet. However, no firewall can provide complete protection for internal networks.
There is a problem with the incomplete protection of Internet services and protocols against data attacks. The root cause of this problem is the Internet's close integration with the UNIX operating system.

TCP/IP (Transmission Control Protocol/Internet Protocol) enables communication across the global Internet and is widely used in networks, but it also fails to ensure adequate protection, as the header of a TCP/IP packet can reveal useful information for hackers.

Email transmission on the Internet is handled by a simple mail transfer protocol (SMTP). One of the major security issues with this protocol is that the user cannot see the actual sender's address. Hackers exploit this by sending large volumes of email, overwhelming the mail server.

A widely used email application on the Internet is **Sendmail**. Messages sent via Sendmail may be intercepted and exploited by hackers.

The Domain Name System (DNS) identifies the names and addresses of users and host computers. DNS stores information about a company's network structure. One issue with DNS is that it's difficult to hide its database from unauthorized users. Hackers often use DNS to gain information about trusted hostnames.

Remote terminal emulation services connect remote systems to each other. Users need to register on a TELNET server and obtain their username and password. A hacker connected to a TELNET server may install a program to capture user credentials.

The World Wide Web (WWW) enables access to information on various servers across the Internet or intranet. One of the key features of WWW is that filtering specific protocols and addresses through firewalls is determined by the network's security policy.

Any organization's network security policy consists of two parts:
Use of network services;
Use of firewalls.
Based on the policy for using network services, a list of allowed services is defined on the Internet. User access to these services is restricted.
Restricting access methods means preventing unauthorized access to Internet services through other means.
Network service access policies are usually based on the following principles:
Deny access from the Internet to the internal network, but allow access from the internal network to the Internet;
Allow limited access from the Internet to internal networks only to authorized systems.

Functional requirements for firewalls include:
Filtering at the network layer;
Filtering at the application layer;
Requirements for administration and setting filtering rules;
Requirements for network authentication tools;
Requirements for logging and accounting.

Intrusion Detection Systems (IDS) detect methods or tools used to attempt unauthorized access that violate system or network security policies. IDS systems have nearly a quarter-century history. Early models and prototypes analyzed audit data from computer systems.
IDS systems are divided into two main classes:
Network Intrusion Detection System (NIDS)
Host Intrusion Detection System (HIDS)

The architecture of IDS includes:

Sensor subsystems that collect and analyze security-related events;

Analyzer subsystems designed to detect suspicious actions or attacks based on sensor data;

A repository that stores analysis results and original data;

A control console that configures the IDS, monitors system states, and tracks incidents detected by analysis subsystems.

NIDS operates as follows:

Inspects traffic allowed into the network;

Blocks harmful or unauthorized packets.

By implementing the listed security stages, it is possible to effectively defend against **Eavesdropping threats**.

Denial-of-Service (DoS) attacks aim to prevent legitimate users from accessing a system or service. These attacks often flood infrastructure resources with access requests, overwhelming the system. DoS attacks may target a single host or an entire network.

Before launching an attack, the target is thoroughly analyzed—identifying vulnerabilities in security tools, operating systems, and peak usage periods. Based on this, a special program is developed and sent to high-ranking servers. These servers then distribute it to their registered users.

Users, knowingly or unknowingly, install the program thinking it came from a trusted server. This could occur on thousands or even millions of computers. The program activates at a specified time, sending continuous requests to the target server. As the server struggles to handle these requests, it becomes overwhelmed and unable to perform its main functions, essentially becoming inoperable.

The most effective methods of protecting against denial-of-service (DoS) attacks are as follows:

Firewall technology;

IPsec protocol.

A firewall is considered the first line of defense between internal and external perimeters. In information and communication technology (ICT), a firewall manages incoming and outgoing data, providing protection by filtering data, inspecting information based on specified criteria, and deciding whether packets are allowed into the system. The firewall examines all packets passing through the network in both directions (incoming and outgoing) and determines whether to allow them based on predefined rules. Additionally, the firewall serves as a protective barrier between two networks, guarding the secured network from exposure to open external networks. One of the main advantages of firewalls, particularly their packet filtering functionality, is that it offers effective protection against DoS attacks.

Packet filters control the following:

Physical interface — where the packet originates;

Source IP address;

Destination IP address;

Source and destination transport ports.

However, due to certain limitations, a firewall alone cannot provide full protection against DoS attacks:

Design flaws — various firewall technologies may not cover all intrusion paths into the protected network;

Implementation weaknesses — as firewalls are complex software (or hardware-software) systems, they are prone to errors. Moreover, there is no universal methodology to test implementation quality and verify that all specified features are realized;

Operational issues — managing firewalls and configuring them according to a security policy is complex, and in many cases, incorrect configurations occur.

These limitations can be addressed by using the IPsec protocol. In summary, proper use of firewalls and the IPsec protocol can provide adequate protection against DoS attacks.

Firewall Architecture

Firewalls are also known as security walls. Firewalls are often integrated with other technologies, such as routing. Many technologies associated with firewalls are actually components of other systems. For example, Network Address Translation (NAT) is often considered a firewall technology, but in fact, it is a routing technology. Many firewalls also include content filtering capabilities needed to enforce security policies in organizations that do not require stringent security. Firewalls without filtering capabilities may include open intrusion detection systems (IDS) that respond to attacks.

Firewalls are typically located at network boundaries. In this case, it can be said that a firewall has both external and internal interfaces, often referred to as unprotected and protected interfaces, respectively. For example, it is possible to implement a policy preventing certain types of files from being sent outside the network.

The diagram (not included here) illustrates border routing with packet filtering capabilities, allowing the routing of filtered packets to the appropriate destination. This network topology was used by the first defense institution. It receives packets from untrusted networks like the Internet and controls access based on its operations, such as blocking SNMP, allowing NTTRG, and more. The diagram also shows the intermediate network between the border router, DNS server, and internal firewall.

Current Methods Used in Intrusion Detection Systems (IDS):

Statistical methods;
Expert systems;
Neural networks.

Statistical Method: The main advantage of the statistical approach is the use of a well-established mathematical statistics framework and adaptability to user-specific characteristics.

Expert Systems: An expert system is composed of a set of rules that embody the knowledge of human experts. Using expert systems is a common method for detecting attacks, where information about attacks is expressed in the form of rules. These rules may be written as sequences of actions or signatures. When any of these rules are triggered, a decision is made that unauthorized activity has occurred. A significant advantage of this approach is the elimination of false positives. An expert system's database must contain scenarios of most known attacks and be regularly updated to remain relevant. However, failure to update or manual updates by administrators can weaken the system's effectiveness. A major disadvantage is the inability to detect unknown attacks. Even minor changes to known attacks can disrupt detection.

Neural Networks: Most intrusion detection methods analyze the monitored environment using rules or statistical approaches. The monitored environment may include log files or network traffic. This analysis relies on a predefined set of rules created by the administrator or the intrusion detection system.

Intrusion Detection Systems (IDS) help identify attempts or tools used to breach system or network security policies. IDS technologies have a history of nearly a quarter of a century. The initial models and prototypes of IDS analyzed computer system audit data. IDS is classified into two main types:

Network-based Intrusion Detection System (NIDS);
Host-based Intrusion Detection System (HIDS).

Modern Requirements for Firewalls

The main requirements are to ensure the security of the internal network and to fully control external connections and communication sessions.

The filtering system must have powerful and flexible management tools to fully and simply enforce the organization's security policy.

The firewall must operate without being noticeable to users and must not interfere with legitimate actions.

To prevent overloading or system failure due to a high volume of requests, the firewall's processor must be fast enough to handle incoming and outgoing traffic effectively during peak times.

The security system must be protected from any external unauthorized influence, as such threats may compromise the organization's confidential information.

The firewall management system must enable centralized enforcement of a unified security policy, including remote branches.

The firewall must have user authentication tools to authorize external access, allowing organization staff to access the network even during business trips.

REFERENCES:

1. Karimov A.A., Raxmonov U.M. – Kompyuter tarmoqlari. – Toshkent: “Fan va texnologiya”, 2020.
2. Tursunov B.X. – Axborot-kommunikatsiya texnologiyalari. – Toshkent: “Yangi asr avlodi”, 2019.
3. Rustamov Sh.S. – Tarmoq xavfsizligi asoslari. – Toshkent: “Innovatsiya”, 2021.
4. Qodirov Sh.Q., Xaitov N.N. – Kompyuter tarmoqlari va ularni loyihalash. – Toshkent, 2018.
5. O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta'lim vazirligi. – Tarmoq texnologiyalari bo‘yicha o‘quv dasturi (bakalavriat uchun).
6. Таненбаум Э. – Компьютерные сети (5-е издание). – СПб: Питер, 2018.
7. Cisco Networking Academy – Introduction to Networks (ITN). – Cisco Press, 2022.
8. GNS3, Cisco Packet Tracer – Tarmoq simulyatsiyasi uchun qo‘llanmalar (onlayn resurslar).
9. UNESCO ICT Competency Framework for Teachers. – Paris, 2018.
10. Navoiy nomidagi Toshkent Davlat pedagogika universitetining ilmiy jurnali – “Pedagogik mahorat”, 2022–2024 yillarda chop etilgan maqolalar.
11. Rajabova G.S. The Methodology of Teaching Graphic Elements in the Python Programming Language. // “Maktabgacha va maktab ta’limi” Pedagogik, psixometodologik va tabiiy fanlarga ixtisoslashgan ilmiy jurnal. 2025 yil, mart, № 3-son. –B.223-227
12. Rajabova G.S. The practice of using digital technologies in education. // “European Journal of Economics, Finance and Business Development”. ISSN (E): 2938-3633. Volume 2, Issue 6, June – 2024, -B.24-28
13. Jurayeva N.O. Fundamentals of Organizing Students' Independent Work Using Mobile Applications. Child Studies in Asia-Pacific Contexts, 2022. –P -255-266
14. Jurayeva N.O. ORGANIZATION OF SELF-STUDY OF STUDENTS IN THE HIGHER EDUCATION SYSTEM USING DIGITAL TECHNOLOGIES. Western European Journal of Linguistics and Education, 2024. –P 105-107
15. Jurayeva N.O., Jurayeva Z.O.The possibility of using educational technologies that improve professional skills and its essence. E3S Web of Conferences, 2024