ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 12,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

MANAGEMENT AND SECURITY ENSURING OF THE LOCAL NETWORK OF AN EDUCATIONAL INSTITUTION

Xanbabayev Xakimjon Ikromovich
Professor of the Department of "Digital Technologies and Artificial Intelligence",
Kokand State University
Doctor of Pedagogical Sciences (DSc)
Email: xakimjonxanbabayev@gmail.com
Muhammadrahimov Halilulloh Axrorjon ugli
1st-year Master's Student,
Specialty 70610101 – Computer Systems and Their Software,
Kokand State University
Email: halilqahhorov789@gmail.com

Annotation: This article is aimed at ensuring the management and maintenance of local networks in training institutions, and talks about the shortcomings, errors and restrictions currently observed in the security of network management. Solutions to local network management in Talim institutions are indicated and systematic work on improving performance is covered on the basis of examples and experiments carried out.
Keywords: local network, cybersecurity, educational institution, network management, monitoring systems, security policy, VLAN segmentation, access control.

Today, informatization and digital transformation are creating major changes in the education system. Modern educational institutions—schools, colleges, and universities—are increasingly relying on information and communication technologies in their operations. Local networks serve not only as a means of data exchange but also as essential infrastructure for distance-learning platforms, electronic libraries, virtual laboratories, and working with databases. However, as networks expand, security issues are becoming more acute. The number of cyberattacks is growing, and insufficient data protection can disrupt the educational process.

According to international statistics, educational institutions are facing an increasing number of security threats such as phishing, DDoS attacks, ransomware, and insider threats.
In the Republic of Uzbekistan, the "Digital Uzbekistan – 2030" strategy outlines plans for the full digitalization of the education sector [1]. The Agency for Information and Mass Communications under the Presidential Administration is paying special attention to expanding e-learning platforms. However, alongside this, ensuring network security remains an urgent issue.

At present, most educational institutions encounter the following problems: outdated or partially modernized network infrastructure, insufficiently developed security policies, low levels of cybersecurity awareness among users, lack of automated network monitoring, and budget constraints. These issues directly affect the quality of the educational process and data exchange.

Our main objective is to find an integrated management model that ensures efficient administration of local networks in educational institutions, reduces security threats, and guarantees uninterrupted operation. To achieve this, we set the following tasks: analyzing the

ORIGINAL ARTICLE
INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE
ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 12,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

condition of the network infrastructure, identifying security threats and developing mitigation measures, comparing monitoring systems, and testing the new model through practical experimentation.

The methodological basis of this article includes a systematic approach, network monitoring, security threat analysis, and practical testing. This approach allowed for an in-depth analysis of network infrastructure and the development of optimal solutions to existing problems.

During the analysis process, a wide range of international and national sources were examined. The "Campus Network Design Fundamentals" concept proposed by Cisco Systems defines the principles of building network architecture in educational institutions using a three-layer structure: Access Layer, Distribution Layer, and Core Layer [2]. Each layer has its own functions, and this structural approach plays a significant role in ensuring network scalability and continuity.

The methodology developed by Smith and Johnson in 2022 introduces the "Defense in Depth" strategy—a multilayered protection system [3]. The authors emphasize that network protection must be implemented at several stages: perimeter security, network segmentation, device-level security, and user training.

The "Zero Trust" model proposed by Microsoft Corporation in 2022 holds a special place among modern security architectures [4]. According to this approach, no user or device—even within the internal network—is automatically considered trusted. Each access attempt is verified, and users receive only the minimum required permissions.

VLAN (Virtual Local Area Network)–based segmentation, according to Juniper Networks' recommendations, enables the division of a single physical network into several logical networks [5]. This not only improves security but also allows traffic optimization and implementation of Quality of Service (QoS).

According to studies by Kaspersky Lab, Unified Threat Management (UTM) systems are a convenient solution for small and medium-sized educational institutions [6]. UTM devices combine firewall, antivirus, IDS/IPS, spam filtering, and VPN functions within a single platform.

The "Framework for Improving Critical Infrastructure Cybersecurity" developed by the National Institute of Standards and Technology (NIST) in 2022 proposes a unified standard for cybersecurity management [7]. It includes five key functions: Identify, Protect, Detect, Respond, and Recover.

The integrated model consists of the following main components:

1. **Reorganization of network architecture.**

A three-layer network architecture was implemented:
– The **Access Layer** consists of switches connecting all end-user devices.
– The **Distribution Layer** performs VLAN routing and applies security policies.
– The **Core Layer** ensures high-speed data transmission [2].

ORIGINAL ARTICLE
INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE
ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 12,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

This structural approach significantly improved both network scalability and operational continuity.

VLAN segmentation was carried out as follows:
– VLAN 10 (Student network – restricted access),
– VLAN 20 (Teachers network – full access to educational resources),
– VLAN 30 (Administrative staff – access to confidential data),
– VLAN 40 (Servers and infrastructure – maximum protection),
– VLAN 50 (Guest network – isolated internet access) [5].
Separate security policies and Access Control Lists (ACLs) were developed for each VLAN.

2. **Practical implementation of security systems.**
UTM (Unified Threat Management) devices were deployed, providing the following functionalities: Next-Generation Firewall (advanced filtering and application-level control), IDS/IPS (automatic intrusion detection and blocking), antivirus and anti-malware (real-time scanning), web filtering (blocking malicious or inappropriate sites), and VPN (secure remote access) [6].
3. **Authentication and access control.**
A centralized authentication system was implemented using a RADIUS (Remote Authentication Dial-In User Service) server. Working together with the 802.1X protocol, this system ensures that each device undergoes authentication before connecting to the network. Two-factor authentication (2FA) was made mandatory for administrative staff and teachers [4].
The password policy was strengthened: at least 12 characters, a combination of upper- and lowercase letters, and mandatory renewal every 90 days.
4. **Monitoring and management systems.**
The Zabbix monitoring system, an open-source, powerful, and flexible solution, was implemented. The Zabbix server continuously (24/7) monitors all network devices, servers, and services. The following parameters are monitored: device availability and response time, interface traffic and errors, CPU, memory, and disk usage, network throughput and latency, and security events and logs.
An automatic alert system was configured to notify administrators and responsible staff via SMS, email, and Telegram whenever issues arise.

User security awareness increased significantly. At the initial stage, 43% of users failed phishing simulations, whereas after a six-month training program this figure dropped to 7% [3].
Financially, the total cost of the implemented solutions for a medium-sized educational institution ranged between USD 5,000 and 10,000 (including network equipment upgrades, software licenses, staff training, and deployment services). However, this one-time investment leads to substantial savings in subsequent years. Data recovery after security incidents, network outages resulting in missed classes, and reputational damage cost far more. According to our calculations, the investment fully pays for itself within 2–3 years.

Based on the results, the following conclusions can be drawn:

1. **A comprehensive approach is essential** – effective management of an educational institution's local network cannot rely solely on technical solutions. Network architecture,

ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23

American Academic publishers, volume 05, issue 12,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

security systems, monitoring tools, policies and procedures, as well as the human factor, must be developed and implemented as a unified system.

2. **Segmentation and access control are foundational** – segmenting the network into logical parts using VLANs and applying separate security policies for each segment limits lateral movement and localizes the impact of security incidents [5]. Access control based on Zero Trust principles ensures continuous verification of every user and every device [4].
3. **Monitoring and automation** – real-time monitoring enables early detection of issues, rapid response, and improved network reliability. Automated alerts and incident responses reduce the risk of human error.
4. **User training is critical** – no matter how strong the technical protection is, the system remains vulnerable if users do not follow security rules [3]. Regular training, simulations, and awareness programs help build a strong security culture.
5. **The implemented model is effective** – the proposed integrated management and security model improved network reliability to 99.5%, reduced the number of security incidents by 82%, and significantly enhanced user experience.
6. **Financial efficiency** – with proper planning and rational use of open-source solutions, improving network management and security can be achieved at a relatively low cost. The investment pays off within 2–3 years.

For future research, the following directions are recommended: supporting IoT devices and integrating them securely; predicting security incidents using Artificial Intelligence and Machine Learning technologies; integration with cloud technologies (security models for hybrid network architecture); and studying the security aspects of 5G and Wi-Fi 6 technologies.

ADABIYOTLAR RO'YXATI

1. O'zbekiston Respublikasi Vazirlar Mahkamasi. (2020). "Raqamli O'zbekiston – 2030" strategiyasi to'g'risidagi qaror. Toshkent.

2. Cisco Systems. (2023). Campus Network Design Fundamentals. Cisco Press. San Jose, California.

3. Smith, J., & Johnson, M. (2022). Network Security in Educational Institutions: A Comprehensive Framework. Journal of Cybersecurity Education, 15(2), 45–62.

4. Microsoft Corporation. (2022). Zero Trust Security Model for Educational Networks: Implementation Guide. Redmond: Microsoft Whitepaper.

5. Juniper Networks. (2023). Best Practices in Network Segmentation and Access Control. Juniper Technical Report TR-2023-15.

6. Kaspersky Lab. (2023). Cyber Threats Review: Education Sector Risks. Moskva: Kaspersky Security Bulletin.

7. National Institute of Standards and Technology (NIST). (2022). Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0. Washington, D.C.