ZERO TRUST ARCHITECTURE FOR SECURING UNIVERSITY NETWORKS

Baliyev Firdavs
Student, Faculty of Cybersecurity Tashkent University of Information Technologies named after Muhammad Al-Khwarizmi
bolievfirdavs0@gmail.com
Yesbosinova Nursulu Perdebayevna
Scientific adviser: Acting associate professor,
Department of Uzbek and Foreign Languages
Tashkent Institute of Textile and Light Industry
https://doi.org/10.5281/zenodo.22075241

Abstract: This article examines how Zero Trust Architecture can improve the security of university networks. It applies zero trust principles to the mixed environment of students, teachers, researchers, guests, personal devices, laboratories, and cloud services. The paper proposes an identity-centered architecture based on continuous verification, least-privilege access, device posture, microsegmentation, data classification, and centralized monitoring. It also presents a practical migration approach and discusses cost, privacy, usability, and legacy-system challenges.

Keywords: zero trust architecture, university network, identity security, least privilege, microsegmentation, continuous verification

Introduction. University networks are designed for openness and collaboration. They connect students, academic staff, administrators, researchers, contractors, guests, laboratories, libraries, cloud platforms, and personal devices. This diversity supports education but also creates a broad attack surface. A stolen student password, an unmanaged laptop, a vulnerable laboratory device, or an incorrectly shared cloud resource can provide an attacker with an entry point. Traditional perimeter security is insufficient when users and services operate both inside and outside the campus network.

Zero trust changes the security question from 'Is this connection inside the network?' to 'Should this subject, using this device and context, access this specific resource now?' NIST defines zero trust as an approach that grants no implicit trust solely because of network location or asset ownership [1]. Authentication and authorization are performed before access to a resource is established, and decisions can be continuously reevaluated. For universities, this approach can limit lateral movement while preserving the flexibility required for teaching and research.

Main Body. Security requirements of a university environment. A university cannot apply one access rule to every person and device. A student may need a learning platform and laboratory software but should not reach payroll records. A lecturer may manage course data without receiving administrative privileges on research servers. A guest should receive internet access without visibility into internal systems. Zero trust supports these distinctions by protecting individual resources and evaluating identity, device condition, requested action, data sensitivity, location, and risk. The objective is not to distrust people. It is to remove automatic technical trust and reduce the damage that one compromised account or device can cause. Access should be limited to the minimum resources required for a defined purpose and period. Sessions involving sensitive systems should receive stronger controls, while low-risk academic services can use simpler policies to avoid unnecessary disruption. Core components

of the proposed architecture. The first component is a central identity provider that maintains reliable user roles and supports strong authentication. The second is device posture assessment, which checks whether an endpoint is registered, updated, encrypted, protected, and free from known critical risks. The third is a policy decision function that combines identity, device, resource sensitivity, and threat information. A policy enforcement point then allows, restricts, or blocks the requested connection.

CISA organizes zero trust maturity around five pillars: identity, devices, networks, applications and workloads, and data [2]. Applied to a university, identity policies define who may act; device policies determine whether the endpoint is acceptable; network controls isolate services and limit movement; application controls protect web systems and APIs; and data controls classify, encrypt, log, and restrict sensitive information. Visibility, analytics, automation, and governance connect these pillars into one operational model. A typical access decision illustrates how the components cooperate. When a student opens the learning platform, the policy system confirms the account, checks the requested application, evaluates device risk, and grants only the permissions assigned to the course role. The same account attempting to reach a finance database is denied because the role and purpose do not match. A managed staff laptop may be allowed to open administrative records after strong authentication, while an unknown device may receive read-only access, additional verification, or no access. If the device becomes noncompliant or behavior changes during the session, the policy can be reevaluated. This adaptive process is more precise than treating every connection on campus Wi-Fi as trusted and every external connection as dangerous.

Practical design for university networks. The university should begin with an inventory of users, devices, applications, services, and important data flows. High-value resources such as identity systems, finance, student records, research repositories, and administrative portals should receive priority. Phishing-resistant authentication and appropriate identity assurance can strengthen access to these resources; NIST SP 800-63-4 provides current guidance for identity proofing, authentication, and federation [3]. Privileged accounts should be separated from ordinary accounts and activated only when administrative work is required.

Network access should be divided by resource and function rather than by one trusted campus zone. Microsegmentation can separate student systems, staff services, laboratories, Internet of Things devices, and management interfaces. Application gateways can evaluate each request before it reaches a service. Cloud applications should use federated identity and granular authorization instead of shared credentials. For cloud-native services, policies should also use application and service identities rather than depending only on IP addresses or subnets [4].

Central logging should collect authentication events, endpoint posture, policy decisions, network activity, and changes to sensitive data. Analytics can identify impossible travel, unusual downloads, new devices, repeated access failures, or privilege escalation. The response can range from requesting additional authentication to isolating a device or terminating a session. Monitoring must be proportionate and governed so that security does not become unnecessary surveillance.

Implementation roadmap. A university should migrate incrementally. The first stage is governance: assign ownership, define critical services, map data, and document existing access paths. The second stage strengthens identity, multi-factor authentication, device management,

and logging. The third stage pilots resource-based access for a small number of important applications. Later stages extend segmentation, automation, and continuous policy evaluation. NIST SP 1800-35 demonstrates that zero trust can be assembled through interoperable technologies and provides example implementations and lessons for deployment [5].

Challenges and limitations. Universities often operate legacy systems, specialized laboratory equipment, and unmanaged research devices that cannot support modern agents or authentication. Budgets and cybersecurity staffing may also be limited. Strict policies can interrupt classes, examinations, or experiments if availability and recovery are not considered. The solution is a risk-based migration with documented exceptions, compensating controls, tested recovery procedures, and regular consultation with academic and administrative users.

Conclusion. Zero Trust Architecture is well suited to university networks because it protects resources without assuming that the campus network, a familiar user, or an institution-owned device is automatically safe. Its strongest contribution is the combination of verified identity, device posture, least privilege, segmentation, data protection, and continuous monitoring. This combination can reduce lateral movement and contain incidents while still supporting remote learning, cloud services, research collaboration, and personal devices. Successful adoption requires more than purchasing security products. The university must understand its resources, define access policy, improve identity governance, measure risk, train users, and implement changes gradually. A carefully planned zero trust program therefore becomes not only a network-security project, but a long-term model for protecting the university's digital mission.

Adabiyotlar, References, Литературы:

1. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. NIST Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207
2. Cybersecurity and Infrastructure Security Agency (CISA). (2023). Zero Trust Maturity Model, Version 2.0. https://www.cisa.gov/zero-trust-maturity-model
3. Temoshok, D., Proud-Madruga, D., Choong, Y. Y., Galluzzo, R., Gupta, S., LaSalle, C., Lefkovitz, N., & Regenscheid, A. (2025). Digital Identity Guidelines. NIST Special Publication 800-63-4. https://doi.org/10.6028/NIST.SP.800-63-4
4. Chandramouli, R., & Butcher, Z. (2023). A Zero Trust Architecture Model for Access Control in Cloud-Native Applications in Multi-Cloud Environments. NIST Special Publication 800-207A. https://doi.org/10.6028/NIST.SP.800-207A
5. Yesbosinova, N. (2026). The pedagogical and psychological essence of developing teachers' writing skills. в international conference on health & technology (Т. 2, Выпуск 1, сс. 10–12). Zenodo. https://doi.org/10.5281/zenodo.18194399