CYBERSECURITY CHALLENGES OF SMART UNIVERSITY INFRASTRUCTURE: A LAYERED THREAT ANALYSIS AND MITIGATION FRAMEWORK

Khusenov Murodjon Zokhirovich

Associate Professor, Department of Artificial Intelligence and Information Security, Bukhara State University, Bukhara, Uzbekistan

E-mail: m.z.xusenov@buxdu.uz ORCID: 0000-0002-1533-3102

Abstract. The transformation of universities into smart campuses — saturated with Internet of Things devices, smart classrooms, integrated information systems and cloud services — substantially expands their attack surface while the protection mechanisms developed for traditional IT infrastructure prove insufficient for resource-constrained and heterogeneous IoT environments. This article systematizes the cybersecurity problems of smart university infrastructure on the basis of a layered analysis. Following the three-tier architecture of smart campus systems (perception, network, application), the principal asset groups and threats of each layer are identified: from weak default credentials and firmware vulnerabilities of end devices, through rogue access points, man-in-the-middle attacks and IoT botnets at the network layer, to phishing, ransomware and breaches of personal data at the application and data layer. A mitigation framework is proposed that organizes governance, technical and human-oriented measures along the functions of the NIST Cybersecurity Framework 2.0 and the requirements of ISO/IEC 27001, taking into account the budget and staffing constraints typical of universities. The results are oriented towards the higher education institutions implementing digital transformation, including the universities of Uzbekistan in the context of the national cybersecurity strategy for 2026–2030.

Keywords: *smart campus; smart university; Internet of Things; cybersecurity threats; layered security; threat modelling; NIST CSF; higher education*

1. Introduction

The concept of the smart campus describes a university whose physical and informational environment is integrated by means of the Internet of Things (IoT) and data-driven services. In the research literature smart campus systems are conventionally described by a three-layer architecture: the perception layer of sensors, cameras, access controllers and smart classroom devices; the network layer transporting their data; and the application layer of services and analytics — and it is precisely at the junctions of these layers that the principal challenges and limitations of such systems are localized [1]. Typical services include smart classrooms with connected projection and videoconferencing equipment, card- and biometric-based access control, energy and climate monitoring, campus Wi-Fi covering tens of thousands of personal devices, learning management and student information systems, and research computing.

This integration creates an attack surface that is qualitatively broader than that of a traditional university network. Universities accumulate data that are attractive to attackers — academic records, financial and health information, results of unpublished research — and connected devices, from cameras to building controllers, become entry points and amplifiers of attacks [2, 3]. Analyses of IoT security emphasize that many deployed devices are legacy products with known but unpatched vulnerabilities, and that the compromise of a single device can open the path to lateral movement across the organizational network [4]. The reality of this scenario at scale was demonstrated by the Mirai botnet, which assembled hundreds of thousands of weakly protected IoT devices and produced some of the largest distributed denial-of-service attacks recorded at that time [5]. At the same time, studies of smart university systems conclude that traditional security mechanisms are insufficient or ineffective for IoT environments with their resource-constrained devices and heterogeneous protocols [6], and analyses of university smart campus practice document misconfiguration and interoperability

problems as systematic sources of vulnerability [7]. Reviews of the smart campus domain place cybersecurity among its decisive development trends [8].

For the Republic of Uzbekistan the problem is current rather than prospective: the strategy “Digital Uzbekistan — 2030” stimulates the digitalization of education [9], the Law “On Cybersecurity” No. LRU-764 establishes the legal framework of protection [10], and the national cybersecurity strategy for 2026–2030 introduces concrete obligations — cybersecurity units in state organizations, multi-factor authentication for state information systems, a register of outsourcing service providers — that directly concern state universities [11]. The aim of this study is to systematize the cybersecurity problems of smart university infrastructure and to substantiate a framework of mitigation measures applicable under the resource constraints of higher education institutions. The objectives are: (i) to construct a layered model of the assets of the smart university; (ii) to identify and structure the threats of each layer; (iii) to organize mitigation measures into an implementable framework.

2. Materials and Methods

The study is based on the analysis of publications of 2018–2026 on smart campus and IoT security — peer-reviewed articles, conference papers, book chapters and documented practitioner analyses — retrieved from IEEE Xplore, SpringerLink, ERIC and recognized professional sources, complemented by the normative documents applicable to university infrastructure.

Threat analysis was performed by the method of layered threat modelling: assets were distributed across the three tiers of the smart campus architecture substantiated in the literature — perception, network, application [1] — and for each tier the threats documented in the analysed corpus were identified and qualitatively assessed by the combination of likelihood and impact, which determined their priority in the mitigation framework. The framework itself was constructed by mapping the selected measures onto the six functions of the NIST Cybersecurity Framework 2.0 — Govern, Identify, Protect, Detect, Respond, Recover [12] — and verifying their compatibility with the

requirements for information security management systems of ISO/IEC 27001:2022 [13]. The study is analytical in character: it synthesizes and structures documented evidence, does not report original incident statistics, and defines the empirical verification of the framework on the infrastructure of a concrete university as the next stage of the research.

3. Results

3.1. Layered asset model. The asset inventory of the smart university is structured by three layers. The perception layer comprises IP video surveillance cameras, smart-card and biometric access controllers, environmental and energy sensors, and the connected equipment of smart classrooms and laboratories. The network layer comprises the campus wireless network serving staff, students and guests, IoT gateways, the wired backbone and the uncontrolled multitude of personal (BYOD) devices. The application and data layer comprises the learning management system, the electronic document flow, the student information system with personal data, research data and computing, and the cloud services to which part of these functions is delegated. The layers are connected by trust relationships, and therefore the compromise of a lower layer propagates upwards: a captured camera or controller becomes a foothold in the network, and the network position opens access to applications and data [4, 6].

Table 1. Layered threat model of smart university infrastructure

Layer	Representative assets	Principal threats	Priority mitigations
Perception	IP cameras; smart-card access controllers; environmental sensors; smart classroom devices	Default and weak credentials; firmware vulnerabilities and tampering; unsupported legacy devices [4, 6]	Device inventory and hardening; credential rotation; firmware and lifecycle management; physical protection of devices
Network	Campus Wi-Fi; IoT gateways; wired backbone; BYOD devices	Rogue access points; man-in-the-middle attacks; DDoS, including IoT botnets [5]; lateral	Network segmentation and VLANs; zero trust access principles; network access control;

Layer	Representative assets	Principal threats	Priority mitigations
		movement from a single compromised node [4]	intrusion detection; DDoS protection
Application and data	LMS; e-document flow; student information system; research data; cloud services	Phishing and account takeover; ransomware; breaches of personal data [2, 3]; misconfiguration and insecure APIs [7]	Multi-factor authentication and SSO; patch management; tested backups; centralized logging and security monitoring

3.2. Threat structure. Table 1 summarizes the threats of each layer with the documented sources. At the perception layer the dominant problems are weak or default credentials, vulnerable and unsupported firmware, and the physical accessibility of devices [4, 6]. At the network layer the heterogeneity of the campus environment produces rogue access points and man-in-the-middle attacks, while the mass of weakly protected devices makes the university both a victim and an unwitting participant of botnet-driven distributed attacks of the Mirai type [5]; the flat topology of many legacy campus networks turns a single compromised device into a path of lateral movement [4]. At the application and data layer the leading threats are phishing-driven account takeover, ransomware against institutional services, and breaches of the personal data of students and staff [2, 3], to which the misconfiguration of services and insecure integration interfaces add a systematic technical cause [7].

3.3. Mitigation framework. The proposed framework organizes measures into three groups projected onto the six functions of NIST CSF 2.0 [12]. The governance group (functions Govern, Identify) comprises: an information security policy for IoT and smart services compatible with ISO/IEC 27001 [13]; a maintained asset register covering devices of all layers; supplier and outsourcing management, including a register of external service providers — a measure that directly echoes the requirements of the national strategy [11]; and risk assessment repeated on architectural changes. The technical group (Protect, Detect) realizes the layer measures of Table 1: hardening and lifecycle management of devices, segmentation and zero trust at the network layer,

multi-factor authentication, patching, backups and centralized monitoring at the application layer. The human-oriented group (Protect, Respond, Recover) comprises continuous awareness training of staff and students against phishing and social engineering, an incident response plan with assigned roles and communication procedures, and recovery exercises that test backups in practice. The framework is deliberately phased: the governance measures and the high-impact technical controls (inventory, segmentation, MFA, backups) form the first stage realizable under constrained budgets, while advanced detection and zero trust constitute the maturity stages.

4. Discussion

The layered analysis demonstrates that the cybersecurity problems of the smart university are systemic rather than local: the threats of the three layers are connected by trust relationships, and therefore isolated point measures — an antivirus on workstations or a firewall at the perimeter — do not change the risk profile created by thousands of heterogeneous connected devices. This conclusion agrees with the position of the literature that traditional mechanisms are insufficient for IoT-saturated university environments [6] and that misconfiguration is a systematic, not incidental, source of vulnerability [7]. The framework therefore places governance — inventory, policy, supplier management — before technology: a university that does not know its devices cannot protect them.

Three aspects deserve separate discussion. First, the ethical dimension: smart campus technologies — cameras, access logs, learning analytics — are simultaneously instruments of monitoring of students and staff, and their protection must be combined with data minimization, transparency of collection and lawful processing of personal data [3]. Second, resource constraints: universities rarely possess the budgets of corporations, and analyses of campus IoT adoption emphasize phased implementation and prioritization [14]; the staged structure of the framework answers this constraint, and the staffing deficit can be partly compensated by involving students of

cybersecurity programmes in the monitoring function as a supervised internship, which simultaneously strengthens practice-oriented education. Third, technological perspective: the literature proposes blockchain-based integrity mechanisms and explainable artificial intelligence for the protection of smart university systems [6]; these directions are promising but at present should be treated as research tracks rather than first-priority operational controls. The limitation of the study is its qualitative character: threat prioritization is based on documented evidence rather than on the incident statistics of a concrete institution; the verification of the framework on the infrastructure of Bukhara State University, with quantitative risk assessment, is planned as the continuation of this work.

5. Conclusion

The smart university combines the data sensitivity of a corporation with the openness of a public institution and the device heterogeneity of an industrial site, which makes its cybersecurity a distinct engineering and organizational problem. The contribution of this article is a layered systematization of this problem: an asset model of the perception, network and application layers; a threat structure of each layer grounded in documented evidence, from weak device credentials and botnet participation to ransomware and personal data breaches; and a phased mitigation framework that organizes governance, technical and human-oriented measures along the functions of NIST CSF 2.0 in compatibility with ISO/IEC 27001. For the universities of Uzbekistan the framework offers a structured path to fulfilling the obligations introduced by the national cybersecurity strategy for 2026–2030 within realistic budgets. Further research will be directed at the empirical verification of the framework, the quantitative assessment of risks on real campus telemetry, and the evaluation of blockchain and explainable AI mechanisms proposed in the literature for smart university systems.

References

1. Internet of Things Based Model for Smart Campus: Challenges and Limitations // IEEE Conference Publication. [Online]. Available: https://ieeexplore.ieee.org/document/9036629

2. Campus Commerce. Utilizing and Safeguarding the Internet of Things on Higher Ed Campuses. 2023. [Online]. Available: https://campuscommerce.com/safeguarding-the-internet-of-things-higher-ed/

3. Capitol Technology University. Smart Classrooms, Connected Dorms: How IoT Is Transforming College Campuses. [Online]. Available: https://www.captechu.edu/blog/smart-classrooms-connected-dorms-how-iot-transforming-college-campuses

4. American Public University. IoT Cybersecurity: Strengthening Defenses against Threats. 2026. [Online]. Available: https://www.apu.apus.edu/area-of-study/information-technology/resources/iot-cybersecurity-strengthening-defenses-against-threats/

5. Antonakakis M. et al. Understanding the Mirai Botnet // Proceedings of the 26th USENIX Security Symposium. USENIX Association, 2017. P. 1093–1110.

6. IoT Security in Smart University Systems // Ouaissa M. et al. (Eds.). Big Data Analytics and Computational Intelligence for Cybersecurity. Studies in Big Data, Vol. 111. Cham: Springer, 2022. DOI: 10.1007/978-3-031-05752-6_16.

7. A Framework of Universities' Smart Campus to Detect and Mitigate Vulnerabilities for IoT Devices // Koc M., Ozturk O. T., Ciddi M. L. (Eds.). Proceedings of the International Conference on Research in Education and Science (ICRES 2023). ISTES Organization, 2023. P. 1681–1694.

8. Sanchez-Torres B., Rodriguez-Rodriguez J. A., Rico-Bautista D., Guerrero C. D. Smart Campus: Trends in cybersecurity and future development // Revista Facultad de Ingenieria. 2018. Vol. 27, No. 47.

9. Decree of the President of the Republic of Uzbekistan No. UP-6079 “On Approval of the Strategy ‘Digital Uzbekistan — 2030’ and Measures for Its Effective Implementation”. October 5, 2020.

10. Law of the Republic of Uzbekistan “On Cybersecurity” No. LRU-764. April 15, 2022.

11. Abdushukurov N. Uzbekistan adopts national cybersecurity strategy to 2030. 2026. [Online]. Available: https://www.nurilla.com/insights/uzbekistan-cybersecurity-strategy-2030.html

12. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg: National Institute of Standards and Technology, 2024.

13. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: International Organization for Standardization, 2022.

14. HashStudioz. IoT in Universities: Building Smart Campuses for Smarter Learning. 2025. [Online]. Available: https://www.hashstudioz.com/blog/iot-in-universities-building-smart-campuses-for-smarter-learning/