CYBERSECURITY AND INFORMATION PROTECTION
КІБЕРБЕЗПЕКА ТА ЗАХИСТ ІНФОРМАЦІЇ

https://doi.org/10.15407/intechsys.2026.03.073
UDC 316.772.5

Ya.M. ANTONUK, Senior Researcher,
Institute of Information Technologies and Systems of the NAS of Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0009-0005-7680-5950
ant@noc.irtc.org.ua
B.A. SHYIAK, Junior Researcher,
Institute of Information Technologies and Systems NAS Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0009-0004-9130-7370
bosh@noc.irtc.org.ua
A.M. MATSAENKO, Senior Researcher, PhD (Engineering),
Institute of Information Technologies and Systems NAS Ukraine,
40, Hlushkova Akad. ave., Kyiv, 03187, Ukraine
https://orcid.org/0000-0003-1149-7318
matsaenko2015@gmail.com
S.L. ARKHANHELSKA, Researcher,
Institute of Information Technologies and Systems NAS Ukraine,
40, Hlushkova Akad. ave., 40, Kyiv, 03187, Ukraine
https://orcid.org/0009-0002-6889-8294
dep125@irtc.oeg.ua

FEATURES OF BUILDING A CYBER DEFENSE SYSTEM FOR A CAMPUS NETWORK OF A RESEARCH INSTITUTION

The paper examines the features of building a cyber-security system for a campus network of a research institution. The specifics of the functioning of the information and communication infrastructure of research institutions in comparison with corporate networks of commercial enterprises are analyzed. The main differences in architecture, user models, the nature of information flows and the profile of cyberthreats for research institutions are identified. A system of principles for building a cyber-security system for a campus network of a research institution is proposed, which includes adaptive network segmentation, a multi-level trust model, the principle of controlled openness, the principle of continuity of scientific services and distributed administration with centralized audit. The need to integrate organiza-

Cite: Antonyuk Ya.M., Shiyak B.A., Matsaenko A.M., Arkhanhelska S.L. PFeatures of Building a Cyber Defense System for a Campus Network of a Research Institution. *Information Technologies and Systems*. 3 (9). 2026. 73—84. https://doi.org/10.15407/intechsys.2026.03.073

© Publisher PH "Akademperiodyka" of the NAS of Ukraine, 2025. This is an Open Access article under the CC BY-NC-ND 4.0 license (https://creativecommons.org/licenses/by-nc-nd/4.0/

tional, technical and procedural mechanisms for cyber-security within a single system for ensuring information security of a research institution is substantiated. A structural model of a cyber-security system for a campus network of a research institution is proposed, focused on ensuring the stability of the functioning of the information infrastructure in the conditions of modern cyberthreats.

***Keywords**: cyber-security, campus network, research institution, information security, network segmentation, Zero Trust, network monitoring.*

Introduction

Modern research activities critically depend on the stable functioning of information and communication infrastructure. Campus networks of scientific institutions provide access to scientific resources, electronic document management, specialized computing services, research results storage systems, cloud platforms, web resources, and international information systems for scientific interaction.

Simultaneously with the increase in the level of digitalization of scientific activity, the number of cyberthreats aimed at the information resources of scientific institutions is significantly increasing. The problem becomes particularly relevant in the context of hybrid cyberthreats, targeted attacks on scientific organizations, the spread of ransomware, compromise of accounts, and attacks on critical information infrastructure.

Unlike corporate networks of commercial enterprises, campus networks of research institutions have a number of specific features, including:

- open nature of academic interaction;
- a significant number of temporary users;
- the need for integration with external scientific resources;
- use of hybrid network infrastructure;
- availability of specialized laboratory segments;
- active use of wireless technologies and remote access;
- constant change in the configuration of network segments in accordance with scientific tasks.

Classic corporate cyber-security models, focused on rigid centralization, access restrictions, and static network structure, do not provide adequate efficiency in the conditions of scientific campus networks. This necessitates the development of adapted principles for building a cyber-security system for scientific and research institutions.

The purpose of the article is to study the features of the functioning of the campus network of a research institution and develop a system of principles for building cyberprotection for such a network, taking into account the specifics of scientific activity.

Analysis of Existing Approaches and Problem Formulation

The issue of ensuring cyber-security of information and communication systems is studied in a significant number of scientific works. The main attention is paid to the issues of network segmentation, access control,

perimeter protection, network activity monitoring, intrusion detection and building cyberincident response systems.

A significant part of modern approaches to building cyberdefense systems is based on corporate security models focused on commercial enterprises. Such models include:

- centralized administration;
- static network structure;
- clearly defined business processes;
- limited number of external integrations;
- minimizing external access;
- strict control of information flows.

For corporate networks, the priority is to ensure the confidentiality of financial, commercial, and service information. Accordingly, cyberdefense systems are focused on maximum isolation of information resources, centralized control, and minimizing changes in the network structure.

At the same time, research institutions operate in fundamentally different conditions. Campus networks of research institutions are characterized by:

— the need to ensure academic openness;
— high intensity of international information interaction;
— a significant number of mobile and temporary users;
— using users' own devices (BYOD);
— constant change in the structure of research segments;
— using heterogeneous software and hardware platforms;
— the availability of specialized scientific equipment.

A feature of scientific institutions is also the combination of administrative, scientific, laboratory and service infrastructure within a single information environment, usually in the form of a mixed campus network [1].

Thus, the use of classic corporate cyberdefense models without adaptation to the — specifics of scientific activity leads to:

— excessive difficulty in accessing information resources;
— reduction in the effectiveness of scientific interaction;
— reduced flexibility of network infrastructure;
— complexity of integrating external services;
— the emergence of a conflict between security requirements and the needs of scientific research.

Therefore, there is a need to develop a specialized approach to building a cyberprotection system for a campus network of a research institution.

Features of the Campus Network of a Research Institution

The campus network of a research institution is a complex multi-level information and communication system that ensures interaction between scientific departments, administrative services, laboratories, service systems, and external information resources.

A typical campus network structure of a research institution includes:

- core network segment;
- server infrastructure;
- user segments;
- wireless networks;
- guest segments;
- laboratory networks;
- remote access systems;
- cloud services;
- backup and archiving tools.

The core segment provides the functioning of backbone data channels, routing, centralized services, authentication and access control systems. It includes server equipment, routers, firewalls, monitoring systems, and backup systems.

The user segment combines employee workstations, laboratory equipment, mobile devices, and wireless access points. One of the features of scientific institutions is the significant number of non-unified software and hardware platforms used to conduct specialized research.

The wireless component of the network plays a particularly important role in the functioning of a modern scientific institution. The use of Wi-Fi networks ensures user mobility, supports guest access, connects mobile research complexes, and operates educational and scientific events.

At the same time, the widespread use of wireless technologies significantly increases the risks of unauthorized access, traffic interception, account compromise, and attacks on network infrastructure [2].

Another characteristic feature is the need to support open scientific interaction. Scientific institutions are actively integrating with external services, international computing platforms, scientific repositories, remote collaboration systems, and cloud resources.

Unlike commercial enterprises, where the concept of maximum isolation of information infrastructure prevails [3, 4], scientific institutions are forced to maintain controlled openness of the network.

Thus, the campus network of a scientific institution is characterized by:

— hybrid structure;
— high dynamism;
— multi-level architecture;
— mixed trust model;
— a significant number of external integrations;
— the need to simultaneously ensure the availability and security of resources.

Threats and Vulnerabilities of the Academic Campus Network

The specifics of the functioning of a campus network of a research institution form a special profile of cyberthreats and vulnerabilities.

The main organizational risks include:

— a significant number of temporary users;
— the difficulty of controlling the level of cyberhygiene of users;
— use of personal devices;
— decentralized administration of individual segments;
— insufficient software unification.

A feature of scientific institutions is the frequent change of user base. The network can be connected to graduate students, interns, participants in scientific projects, invited researchers, and representatives of third-party organizations.

Technical risks include:

— use of outdated equipment;
— the presence of unknown or specialized devices;
— use of open wireless networks;
— insufficient level of segmentation;
— connecting unauthorized equipment;
— use of vulnerable remote access services.

A separate problem is scientific equipment, which often operates under outdated operating systems or specialized software that does not support modern protection mechanisms.

The main information risks include:

— compromising the results of scientific research;
— leakage of confidential scientific data;
— violation of the integrity of scientific archives;
— unauthorized access to grant documentation;
— blocking of critical services by ransomware.

Particularly dangerous are ransomware attacks that can lead to loss of access to the results of many years of research, scientific archives and electronic document management systems, or leakage of personal data, as in the case of the University of Hawaii Cancer Center [5].

In addition, modern cyberthreats are characterized by a high level of automation and the use of artificial intelligence technologies to conduct phishing campaigns, compromise accounts, and bypass protection mechanisms [6].

In this regard, cyberdefense systems of scientific institutions must take into account not only classic threats to information security, but also specific risks associated with the functioning of an open scientific environment.

Principles of Building a Campus Network CyberDefense System

Taking into account the peculiarities of the functioning of research institutions, it is advisable to form a system of principles for building cyberprotection for the campus network.

Principle of adaptive network segmentation

Unlike corporate networks with a static structure, the campus network of a scientific institution must support the ability to dynamically form segments according to the needs of research groups and scientific projects.

Adaptive segmentation involves:

— isolation of critical services;
— separation of guest networks;
— allocation of laboratory segments;
— demarcation of administrative and scientific infrastructure;
— the possibility of rapid network reconfiguration.

The use of adaptive segmentation allows you to minimize the attack surface and limit the spread of cyber-security incidents between network segments.

The Principle of Multi-Level Trust

In a campus network, it is not possible to use a model of complete trust for internal nodes. Users, devices, and services must be treated as potentially untrusted regardless of their physical location on the network.

The implementation of this principle involves:

— using the Zero Trust concept [7];
— constant verification of user authentication;
— multi-factor authentication;
— node behavior control;
— access restrictions based on the principle of least privilege.

The multi-level trust model ensures increased resilience of the cyberdefense system to compromise of individual network segments.

The Principle of Controlled Openness

Scientific activity requires constant interaction with external information resources. Therefore, complete isolation of the network is impossible and contradicts the principles of functioning of the modern scientific environment.

The principle of controlled openness provides for:

— regulated external access;
— use of secure communication channels;
— control of access to public services;
— segmentation of external services;
— constant monitoring of external activity.

This approach allows for a balance between the openness of scientific infrastructure and the necessary level of cyberprotection.

The Principle of Continuity of Scientific Services

For a research institution, the continuity of services related to conducting research is of critical importance.

Critical services include:

— research results storage systems;
— electronic document management servers;
— backup systems;
— scientific repositories;
— computing clusters;
— web resources of scientific projects.

Ensuring continuity of operation involves:

— redundancy of critical components;
— regular backup;
— use of geographically remote copies;
— support for disaster recovery mechanisms;
— monitoring the status of the infrastructure in real time.

The Principle of Distributed Administration with Centralized Audit

In scientific institutions, individual laboratories and scientific units can use their own information resources and local administration mechanisms.

Complete centralization of management in such conditions is ineffective.

Therefore, it is advisable to use a distributed administration model with centralized audit, which provides for:

— local administration of individual segments;
— centralized event logging;
— centralized monitoring;
— unified security policies;
— centralized response to cyberincidents.

The Principle of Integration of Organizational and Technical Measures

The effectiveness of a cyberdefense system is determined not only by technical means, but also by the level of organizational support.

The organizational component should include:

— internal regulations;
— user instructions;
— incident response procedures;
— staff training;
— periodic audits;
— monitoring compliance with security policies.

The integration of organizational and technical mechanisms allows for a comprehensive approach to building a cyberdefense system.

Campus Network Cyber-security System Model

Based on the proposed principles, a multi-level model of the cyber-security system of the campus network of a research institution can be formed.

Structurally, this model includes:
1. Level of physical infrastructure.
2. Level of network interaction.
3. Level of services and information systems.
4. Access control level.
5. Level of monitoring and response.
6. Organizational level.

At the physical infrastructure level, protection is provided for server equipment, power supply systems, data transmission channels, and telecommunications equipment.

The level of network interaction includes:
- firewalls;
- VLAN segmentation;
- IDS/IPS systems;
- VPN technologies;
- network traffic control mechanisms.

The service level covers:
- postal systems;
- web resources;
- file storage;
- scientific information systems;
- cloud services.

The access control layer implements:
- centralized authentication;
- multi-factor authentication;
- privilege control;
- access policies.

The monitoring and response level includes:
- log collection systems;
- SIEM platforms;
- network activity analysis tools;
- incident response procedures.

The organizational level covers:
- regulatory documentation;
- audit procedures;
- user training;
- administration regulations.

The interaction of these levels forms a unified cyberdefense system aimed at ensuring the stability of the functioning of the information infrastructure of a scientific institution.

Practical Implementation of a CyberDefense System in a Scientific Institution

The practical implementation of a cyberdefense system should be based on a comprehensive approach that combines organizational, technical, and procedural mechanisms.

One of the key elements is the creation of a system support unit responsible for:

- network administration;
- infrastructure monitoring;
- incident response;
- user support;
- information security audit.

An important component of the system is the organization of centralized network monitoring. The monitoring system should provide:

- monitoring the status of network nodes;
- network traffic analysis;
- detection of abnormal activity;
- control of resource use;
- prompt informing of administrators.

Significant attention should be paid to logging security events. Centralized log storage allows:

- perform incident analysis;
- detect unauthorized access attempts;
- monitor user actions;
- generate statistics on security events.

To achieve rapid response and analysis of security incidents, it is advisable to implement an ontological expert incident management system [8].

To ensure the stability of the infrastructure, it is necessary to implement a backup system, which should include:

- regular backups;
- isolated storage of copies;
- backup data integrity control;
- periodic testing of recovery procedures.

An important aspect of ensuring cyber-security is increasing user awareness. Staff training should cover:

- cyberhygiene rules;
- detection of phishing attacks;
- safe use of email;
- rules for working with information resources;
- cyberincident response procedures.

In addition, it is necessary to conduct regular information security audits and testing of the security of the information infrastructure. It is also important to simulate social engineering attacks [9].

Conclusions

The article examines the features of building a cybersecurity system for a campus network of a research institution. It is shown that campus networks of research institutions differ significantly from corporate networks of commercial enterprises in terms of structure, user model, nature of in-

formation interaction and cyberthreat profile. It is established that the use of classical corporate models of cybersecurity without adaptation to the specifics of the scientific environment is not effective enough.

A system of principles for building cybersecurity for a campus network of a research institution is proposed, which includes the principle of adaptive network segmentation, of multi-level trust, of controlled openness, of continuity of scientific services, of distributed administration with centralized audit, and principle of integration of organizational and technical protection mechanisms.

The scientific novelty of the work lies in the formalization of the principles of building a cyber-protection system for a campus network of a scientific institution, taking into account the peculiarities of the academic information environment, the need to support open scientific interaction, and the dynamic structure of user segments.

The practical significance of the results obtained lies in the possibility of using the proposed approach to build and modernize cyberdefense systems in institutions of the National Academy of Sciences of Ukraine, higher education institutions, and other research organizations.

DECLARATIONS

***Author contributions*:** Antonyuk Ya.M. analyzed existing approaches to building cybersecurity systems for a campus network of a research institution and identified threats and vulnerabilities of an academic campus network. Shyak B.A. highlighted the features of a campus network of a research institution and the principles of building a campus network cyber protection system. Matsaenko A.M. demonstrated a model of a campus network cybersecurity system. Arkhanhelska S.L. presented a practical implementation of a cyber protection system in a scientific institution

***Use of AI and Tools Usage*:** The authors declare that artificial intelligence tools were used only for language editing and spell checking and were not used for scientific analysis of information and interpretation of results.

***Conflict of Interest*:** The authors declare that they have no financial interests or personal relationships that could influence the presented work.

REFERENCES

1. Antoniuk Ya.M., Shyiak B.A., Tkalya V.H., Arkhanhelska S.L. Telemetry As the Foundation of Predictable QoS in Hybrid Campus Networks. *Information Technologies and Systems*, 2026, Vol. 7 (1), 35–42. https://doi.org/10.15407/intechsys.2026.01.035
2. Scarfone K.A., Mell P.M. Guide to Intrusion Detection and Prevention Systems (IDPS). *National Institute of Standards and Technology Special Publication 800-94*, Gaithersburg, MD, 2007. https://doi.org/10.6028/NIST.SP.800-94
3. What Is Enterprise Network Security? A Complete Guide. URL: https://e.huawei.com/en/knowledge/2024/solutions/enterprise-network/enterprise-network-security [Accessed 25 May. 2026]
4. Enterprise Network Security: A Complete Guide. EPAM SolutionsHub. URL: https://solutionshub.epam.com/blog/post/enterprise-network-security [Accessed 25 May. 2026]
5. Data breach reported by University of Hawai‘i Cancer Center. UpGuard. URL: https://www.upguard.com/news/university-of-hawaii-cancer-center-data-breach-2026-03-02 [Accessed 25 May. 2026]

6. Zdrojewski K. AI-Powered Cyberattacks: A Comprehensive Review and Analysis of Emerging Threats. *Advances in IT and Electrical Engineering*, 2025, Vol. 31, 55–69.
7. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. *National Institute of Standards and Technology Special Publication 800-207*, 2020. https://doi.org/10.6028/NIST.SP.800-207
8. Rozlomii I.O., Babenko V.H., Holovnia V.M. Ontological expert system for identifying vulnerable components in security systems of critical infrastructure facilities. *Telecommunication and information technologies*, 2026, Issue 1, 180–187. https://doi.org/10.31673/2412-4338.2026.019017
9. Korshun N.V., Bondarchuk A.P., Skladannyi P.M., Sokolov V.Yu., Kryzhanivska T.M. Modeling and execution of social engineering attacks. *Telecommunication and information technologies*, 2026, Issue 1, 130–139. https://doi.org/10.31673/2412-4338.2026.019013

Received 26.05.2026
Accepted 20.07.2026
Published 25.08.2026

Я.М. АНТОНЮК, старш. наук. співроб.,
Інститут інформаційних технологій та систем НАН України,
просп. Акад. Глушкова, 40, Київ, 03187, Україна
https://orcid.org/0009-0005-7680-5950
ant@noc.irtc.org.ua
Б.А. ШИЯК, молодш. наук. співроб.,
Інститут інформаційних технологій та систем НАН України,
просп. Акад. Глушкова, 40, Київ, 03187, Україна
https://orcid.org/0009-0004-9130-7370
bosh@noc.irtc.org.ua
А.М. МАЦАЄНКО, канд. техн. наук, старший викладач,
ВІТІ імені Героїв Крут,
https://orcid.org/0000-0003-1149-7318
matsaenko2015@gmail.com
С.Л. АРХАНГЕЛЬСЬКА, наук. співроб.,
Інститут інформаційних технологій та систем НАН України,
просп. Акад. Глушкова, 40, Київ, 03187, Україна
https://orcid.org/0009-0002-6889-8294
dep125@irtc.oeg.ua

ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМИ КІБЕРЗАХИСТУ КАМПУСНОЇ МЕРЕЖІ НАУКОВО-ДОСЛІДНОЇ УСТАНОВИ

Вступ. Сучасна дослідницька діяльність критично залежить від стабільного функціонування інформаційно-комунікаційної інфраструктури. Кампусні мережі наукових установ забезпечують доступ до наукових ресурсів, електронного документообігу, спеціалізованих обчислювальних сервісів, систем зберігання результатів досліджень, хмарних платформ, веб-ресурсів та міжнародних інформаційних систем для наукової взаємодії. Одночасно зі зростанням рівня цифровізації наукової діяльності значно зростає кількість кіберзагроз, спрямованих на інформаційні ресурси наукових установ. Проблема стає особливо актуальною в контексті гібридних кіберзагроз, цілеспрямованих атак на наукові організації, поширення програм-вимагачів, компрометації облікових записів та атак на критичну інформаційну інфраструктуру. На відміну від корпоративних мереж комерційних підприємств, кампусні мережі наукових установ мають низку специфічних особливостей. Класичні моделі корпоративної кібербезпеки, орієнтовані на жорстку централізацію, обмеження доступу та статичну структуру мережі, не забезпечують належної ефективності в умовах наукових

кампусних мереж. Це зумовлює необхідність розробки адаптованих принципів побудови системи кібербезпеки для науково-дослідних установ.

Метою статті є дослідження особливостей функціонування кампусної мережі дослідницької установи та розробка системи принципів побудови кіберзахисту для такої мережі з урахуванням специфіки наукової діяльності.

Методи. В статті сформовано систему принципів побудови кіберзахисту кампусної мережі.

Результати. Проведено аналіз специфіки функціонування інформаційно-комунікаційної інфраструктури наукових установ у порівнянні з корпоративними мережами комерційних підприємств. Визначено основні відмінності архітектури, моделі користувачів, характеру інформаційних потоків та профілю кіберзагроз для науково-дослідних установ. Запропоновано систему принципів побудови кіберзахисту кампусної мережі наукової установи, що включає адаптивну сегментацію мережі, багаторівневу модель довіри, принцип контрольованої відкритості, принцип безперервності наукових сервісів та розподіленого адміністрування з централізованим аудитом. Обґрунтовано необхідність інтеграції організаційних, технічних та процедурних механізмів кіберзахисту в межах єдиної системи забезпечення інформаційної безпеки наукової установи. Запропоновано структурну модель системи кіберзахисту кампусної мережі науково-дослідної установи, орієнтовану на забезпечення стійкості функціонування інформаційної інфраструктури в умовах сучасних кіберзагроз.

Висновки. Показано, що кампусні мережі наукових установ суттєво відрізняються від корпоративних мереж комерційних підприємств за структурою, моделлю користувачів, характером інформаційної взаємодії та профілем кіберзагроз. Встановлено, що використання класичних корпоративних моделей кібербезпеки без адаптації до специфіки наукового середовища є недостатньо ефективним.

Ключові слова: *кіберзахист, кампусна мережа, науково-дослідна установа, інформаційна безпека, сегментація мережі, Zero Trust, мережевий моніторинг.*