

Tetyana Derkach¹, Andrii Dmytrenko¹, Lina Klochko²

¹National University “Yuri Kondratyuk Poltava Polytechnic”, Poltava, Ukraine

²Geological Bureau BEG SA, Switzerland

A COMPREHENSIVE APPROACH TO ENSURING THE CYBERSECURITY OF CORPORATE NETWORK INFRASTRUCTURE

Abstract. Relevance. The rapid development of digital technologies, the widespread implementation of corporate information systems, and the continuous increase in the number of cyber threats necessitate the improvement of approaches to protecting corporate network infrastructure. Traditional protection methods based on the use of separate software or hardware security tools do not provide an adequate level of resistance to modern cyberattacks, which are characterized by complexity, multiple attack vectors, and the ability to bypass individual security mechanisms. Therefore, the development of a comprehensive multi-layered cybersecurity system aimed at ensuring the confidentiality, integrity, and availability of the information resources of enterprises, institutions, and organizations is highly relevant. **Subject of the research:** modern approaches, models, protocols, and technologies for ensuring the cybersecurity of corporate network infrastructure. **Purpose of the research:** to substantiate a comprehensive approach to designing secure corporate computer networks based on multi-layered protection and the integrated application of modern network security technologies. **Research objectives.** To analyze the role of the Open Systems Interconnection reference model as a methodological basis for designing secure computer networks; to identify the main information security threats affecting corporate networks; to investigate the implementation of security mechanisms at the physical, data link, network, and application layers; to examine the principles of the Defense in Depth concept; to analyze the capabilities of the AAA, RADIUS, SSH, ACL, VLAN, Port Security, DHCP Snooping, and Dynamic ARP Inspection models, protocols, and technologies; and to determine the advantages of their integrated application for improving the cybersecurity of corporate network infrastructure. **Research methods.** The study employs the methods of systems analysis, comparison, generalization, classification, and systematization of scientific and technical information. A structural and functional approach is applied to analyze security mechanisms at different layers of the OSI model. The method of modelling a comprehensive corporate network security architecture is also used. **Research results.** The main threats to the information security of corporate networks are identified, including MAC Spoofing, MAC Flooding, ARP Spoofing, ARP Cache Poisoning, Man-in-the-Middle attacks, unauthorized device connections, the compromise of user and administrator accounts, and violations of access control policies. The Defense in Depth concept, which involves creating several complementary layers of protection against external and internal cyber threats, is analyzed. It is established that the application of a multi-layered approach makes it possible to minimize the consequences of the compromise of individual network components and ensure the continuity of information systems even when particular attacks are successfully implemented. The capabilities of the AAA model for centralized access management to information resources are examined, together with the operating principles of the RADIUS protocol as a means of centralized authentication, authorization, and accounting of user activities. The advantages of using the cryptographically protected SSH protocol for the secure administration of network equipment are identified. The application of Access Control Lists for implementing security policies and controlling communication between corporate network segments is investigated. Port Security, DHCP Snooping, and Dynamic ARP Inspection technologies aimed at countering data-link-layer attacks and unauthorized device connections are analyzed. It is established that the logical segmentation of the network environment using VLAN technology is an effective mechanism for improving cybersecurity, as it enables the localization of cyber incidents, limits the lateral movement of attacks, and supports the implementation of the principle of least privilege. **Conclusions.** The highest level of protection of corporate network infrastructure is achieved through the integrated application of AAA, RADIUS, SSH, ACL, VLAN, Port Security, DHCP Snooping, and Dynamic ARP Inspection technologies in accordance with the principles of the Defense in Depth concept. The proposed approach provides centralized access control, increases the protection of information resources, improves the manageability of the network environment, reduces the risk of cyberattack propagation, and meets modern requirements for designing secure corporate information systems.

Keywords: cybersecurity; corporate network; network infrastructure; information security; Defense in Depth; AAA; RADIUS; SSH; ACL; VLAN; Port Security; Dynamic ARP Inspection; OSI model, access control.

1. Introduction

1.1 Relevance of the Topic

The rapid development of digital technologies, the widespread implementation of corporate information systems, and the increasing number of network services significantly increase the requirements for ensuring the cybersecurity of modern computer networks. Almost all business processes of enterprises, institutions, and organizations operate on the basis of corporate network infrastructure, which provides information exchange among users, servers, databases, and cloud services, the use of which requires a separate cybersecurity risk assessment when selecting a cloud provider [1–3].

At the same time, the expansion of digitalization is accompanied by a constant increase in the number of cyber threats aimed at violating the confidentiality, integrity, and availability of information. Attacks focused on exploiting vulnerabilities in network protocols, configuration errors in active equipment, weaknesses in authentication systems, and deficiencies in access control mechanisms are particularly dangerous. Successful implementation of such attacks may result in the compromise of corporate information resources, disruption of business continuity, financial losses, and reputational risks [4–6].

Under modern conditions, information security can no longer be limited to the use of individual software or

hardware protection tools. A comprehensive approach is required, combining modern technologies for network segmentation, centralized access management, cryptographic protection of data transmission channels, monitoring systems, and control of network activity. Therefore, the study of modern threats to corporate computer networks and the development of effective mechanisms for their neutralization are among the current areas of cybersecurity and network technology development. The relevance of this approach is confirmed by modern international recommendations for building multilayered protection of network infrastructure [7–9].

1.2 Literature Review and Problem Statement

The issue of ensuring the information security of corporate computer networks is the subject of research by both Ukrainian and foreign scholars. A significant contribution to the development of the theoretical foundations of network security has been made by W. Stallings, A. S. Tanenbaum, J. Postel, D. Comer, as well as the authors of international ISO/IEC standards and IETF recommendations [10, 11].

Practical aspects of building secure corporate networks are addressed in the recommendations of the U.S. National Institute of Standards and Technology (NIST), particularly in the SP 800 series documents, which define modern approaches to building network infrastructure protection systems, applying firewalls, access control policies, and information security management [12].

Considerable attention in modern research is paid to the use of the Defense in Depth concept, centralized user authentication, AAA mechanisms, the RADIUS protocol, network segmentation using VLAN, Access Control Lists (ACL), Port Security technology, and cryptographic protection of administrative access using SSH. However, most scientific works consider individual security tools without a comprehensive analysis of their interaction within a corporate network [13, 14].

Thus, the development of a comprehensive approach to ensuring the cybersecurity of corporate network infrastructure remains relevant. Such an approach combines modern protection technologies while taking into account current threats and the practical features of operating local computer networks [11].

1.3 Aim and Objectives of the Study

The purpose of the article is to study modern threats and vulnerabilities of corporate computer networks, analyze the mechanisms of their occurrence, and substantiate a comprehensive approach to ensuring the cybersecurity of network infrastructure based on the use of modern authentication, access control, network segmentation, and cryptographic protection technologies.

To achieve this purpose, the following objectives were defined:

- to study modern threats to the information security of corporate computer networks;
- to analyze vulnerabilities of protocols at different layers of the OSI model;

- to investigate the implementation mechanisms of the most common network attacks;
- to evaluate the effectiveness of modern technologies for protecting corporate networks;
- to substantiate a comprehensive approach to building secure corporate network infrastructure.

2. Materials and Methods

2.1 Corporate Network Architecture and the OSI Model

The Role of the OSI Model in Building Secure Network Infrastructure. The design of modern corporate computer networks requires a systematic approach to organizing data transmission processes, resource administration, and information security. The conceptual basis for building network systems is the Open Systems Interconnection (OSI) reference model, standardized by the International Organization for Standardization in ISO/IEC 7498-1. This model defines the logical structure of network communications and provides a unified approach to designing, analyzing, and protecting information systems [15].

The OSI model consists of seven interconnected layers: physical, data link, network, transport, session, presentation, and application. Each layer performs a defined set of functions and interacts only with adjacent layers, which ensures architectural modularity and simplifies the implementation of protection mechanisms [10].

In the field of cybersecurity, the OSI model is used as a methodological basis for identifying potential threats, analyzing vulnerabilities, and implementing protection tools at different stages of information processing. This approach makes it possible to form a multilayered security system in which the compromise of one layer does not lead to a complete disruption of network infrastructure functioning [16].

For corporate networks, the ability to correlate specific cyber threats with the corresponding layers of the OSI model is of particular importance.

Levels of Information Protection in a Corporate Network. Effective information security requires the implementation of protective mechanisms at all layers of network interaction. Within the OSI model, each layer has its own set of potential threats and corresponding countermeasures [1].

At the physical layer, the main protection tasks include controlling access to network equipment, cable infrastructure, and server rooms. Physical security is implemented through access control systems, video surveillance, backup power supply, and protection against unauthorized network connections [9].

At the data link layer, the priority direction of protection is ensuring the security of switching equipment and controlling connected devices. The most common threats at this layer include MAC Spoofing, MAC Flooding, ARP Spoofing, and unauthorized connection of user devices. To minimize these risks, Port Security, Dynamic ARP Inspection, DHCP Snooping, and network access authentication mechanisms are used [17].

At the network and transport layers, routing mechanisms and data-flow control play a key role. Protection at these layers is implemented using Access Control Lists (ACL), firewalls, intrusion detection and prevention systems (IDS/IPS), network segmentation, and packet filtering in accordance with established security policies [18].

The application layer is of particular importance for corporate networks because it is where users interact with network services and information resources. Application-layer protection involves the use of authentication and authorization mechanisms, multifactor authentication, centralized account management, cryptographic protection of data transmission channels, and information security event monitoring tools [12].

Implementation of the Defense in Depth Principle in a Corporate Network. One of the key concepts of modern cybersecurity is the Defense in Depth principle, which involves building several complementary security layers to protect information resources from external and internal threats [14].

The main idea of the concept is that no single security mechanism can guarantee absolute protection of network infrastructure.

Therefore, a security system must consist of a set of interconnected organizational, software, and hardware tools, each of which performs its own protective function.

If one layer is compromised, an attacker encounters additional barriers, which significantly complicates the implementation of an attack [7].

2.2 Analysis of Modern Technologies for Protecting Corporate Networks

Effective cybersecurity of corporate network infrastructure requires the integrated use of modern protection technologies that cover different layers of network interaction and implement the principle of multilayered defense (Defense in Depth).

During the design of a secure corporate network, a number of technologies aimed at ensuring access control, protecting network equipment, preventing unauthorized connections, and countering common network attacks were analyzed.

These technologies include AAA, RADIUS, SSH, ACL, Port Security, and Dynamic ARP Inspection [17].

AAA Technology as the Basis of Centralized Access Control. In corporate networks, the TACACS+ protocol may also be used alongside RADIUS to implement the AAA model. It is used for centralized control of authentication, authorization, and accounting, particularly during network equipment administration [19].

One of the key concepts of modern network security is the AAA (Authentication, Authorization, Accounting) model, which provides centralized management of access to information resources.

This model involves the implementation of three interrelated processes: user authentication, authorization of user actions, and accounting of performed operations [12].

Authentication is used to confirm the identity of a user or network device before access to system resources is granted. Authorization determines the list of permitted actions after successful authentication. Accounting ensures the registration and storage of information on all login attempts, executed commands, and user network activity [10, 12].

Use of the RADIUS Protocol for Centralized Authentication. The practical implementation of the AAA model in corporate networks is often carried out using the RADIUS (Remote Authentication Dial-In User Service) protocol. This protocol provides centralized authentication, authorization, and accounting of users during access to network resources [10, 11].

The operating principle of RADIUS is based on interaction among a client, a network device, and an authentication server.

After receiving an access request, the network device transmits the user credentials to the RADIUS server, which verifies their validity and returns a decision to grant or deny access [10, 11].

2.3 Secure Administration of Network Equipment Using SSH

Secure management of network infrastructure is an important component of ensuring the cybersecurity of corporate networks.

Traditional remote administration protocols, such as Telnet, transmit credentials and service information in clear text, creating conditions for their interception and subsequent system compromise [16].

To eliminate these shortcomings, modern networks use the SSH (Secure Shell) protocol, which provides secure remote management of network devices by creating a cryptographically protected communication channel between a client and a server [20].

2.4 Access Control Lists as a Network Traffic Filtering Mechanism

Access Control Lists (ACL) are among the most widespread tools for protecting network infrastructure. This technology makes it possible to regulate the passage of network traffic in accordance with defined security rules and implement access policies among different segments of a corporate network [16].

ACLs are sets of rules that define permitted or prohibited actions for network packets based on parameters such as source IP address, destination IP address, port number, protocol type, and data transmission direction [18].

2.5 Port Security Technology for Protecting Switching Equipment

One of the most common threats at the data link layer is the connection of unauthorized devices to a corporate network. To minimize this risk, Port Security technology is used on switches.

The operating principle of Port Security consists in limiting the number of allowed MAC addresses on a specific physical switch port. The administrator may define permitted devices manually or automatically store the MAC addresses of connected equipment.

When a security policy violation is detected, the switch may perform various actions: generate an incident message, block traffic, or automatically disable the port. This approach makes it possible to effectively counter MAC Spoofing attacks, unauthorized equipment connections, and attempts to gain access to corporate resources.

2.6 Dynamic ARP Inspection as a Means of Countering ARP Attacks

ARP Spoofing and ARP Cache Poisoning attacks pose a significant threat to corporate networks, as they allow an attacker to substitute records in the ARP tables of network nodes and intercept network traffic [16].

To counter these attacks, Dynamic ARP Inspection (DAI) technology is used. It ensures verification of the authenticity of ARP messages within the network. The operating principle of DAI is based on analyzing the correspondence between IP addresses and MAC addresses using a trusted database formed by the DHCP Snooping mechanism.

When an ARP message is received, the switch checks its correctness. If a mismatch is detected between the declared IP address and the physical address of the device, the packet is blocked and the event is recorded in the security log.

3. Development and Research Results

3.1 Proposed Multilayered Security Architecture

In the proposed corporate network architecture, the Defense in Depth principle is implemented through the combination of several protection layers.

At the physical infrastructure layer, access control to server equipment and switching devices is provided. At the data link layer, Port Security and VLAN-based network segmentation are used to limit the possibility of unauthorized connections and lateral movement of attacks [2].

At the network layer, ACLs are applied to regulate interaction among individual network segments and implement the principle of least privilege.

At the application layer, a centralized authentication system based on the RADIUS protocol is implemented, while network equipment administration is performed exclusively through the secure SSH protocol [17].

Continuous monitoring of network activity, analysis of event logs, and auditing of user actions are also important components of multilayered protection. The integrated use of these mechanisms makes it possible to ensure a high level of corporate network resilience against modern cyber threats, reduce the risks of compromising information resources, and increase the overall reliability of information infrastructure functioning [12].

Thus, the OSI model serves as a methodological basis for building secure corporate networks, while the implementation of the Defense in Depth principle ensures the formation of a multilayered security system capable of effectively countering modern threats to information security.

3.2 Implementation of Centralized Access Management Based on AAA and RADIUS

Within the proposed architecture, the AAA model is used as the basis for centralized management of user and administrator access.

Authentication is performed before access to network resources is granted, authorization determines the permitted resources and operations, and accounting ensures the recording of login attempts, executed commands, and user network activity. This approach enables the consistent application of access policies and provides traceability of actions within the corporate network [9].

Within the proposed corporate network architecture, the RADIUS server functions as the central node for authenticating users and network equipment administrators, ensuring the implementation of the principle of centralized access management.

3.3 Implementation of Secure Administration via SSH

In the proposed network architecture, SSH is used as the main mechanism for remote administration of switches, routers, and server equipment, ensuring the secure execution of configuration and diagnostic operations [18].

3.4 Implementation of Inter-Segment Communication Control

In the context of a VLAN-segmented architecture, ACLs perform an important function in controlling inter-segment interaction.

They allow limiting user access to critical servers, regulating interaction among structural departments of an enterprise, and implementing the principle of least privilege [13].

3.5 Implementation of Port Security

Within the proposed architecture, Port Security is used to protect the user ports of access switches, which significantly increases the level of network connection control [17].

3.6 Results of the Comparative Analysis

The results of the comparative analysis of corporate to systematize the obtained results, the selected corporate network protection technologies were compared according to four main criteria: their functional purpose, the corresponding layer of the OSI model, the principal threats they counteract, and the practical advantages of their implementation.

This comparison makes it possible to determine the role of each security mechanism within the proposed multilayered architecture and to identify how the analyzed technologies complement one another.

Particular attention was paid to the distribution of security functions among the application, network, and data link layers.

The results of the comparative analysis are presented in Table 1.

Table 1 – Comparative Characteristics of Corporate Network Protection Technologies

Technology	Main purpose	OSI model layer	Main threats countered	Advantages of use
AAA	Authentication, authorization, and user activity auditing	Application	Unauthorized access, privilege abuse	Centralized access management and user activity auditing
RADIUS	Centralized authentication of users and devices	Application	Use of local accounts, weak access control	Single point of management for security policies
SSH	Secure remote administration	Application	Password interception, Man-in-the-Middle attacks	Data encryption and protection of administrative sessions
ACL	Control and filtering of network traffic	Network	Unauthorized access between network segments	Flexible configuration of access policies
Port Security	Control of device connections to switch ports	Data link	MAC Spoofing, unauthorized equipment connection	Protection of physical network access points
Dynamic ARP Inspection	Verification of ARP message authenticity	Data link	ARP Spoofing, ARP Poisoning, MITM attacks	Protection of ARP interaction integrity
VLAN	Logical network segmentation	Data link	Lateral movement of attacks, data leakage	Traffic isolation and incident localization
DHCP Snooping	Control of DHCP traffic	Data link	Rogue DHCP, DHCP Starvation	Formation of a trusted IP–MAC correspondence database

Network protection technologies are presented in Table 1.

As shown in Table 1, none of the considered technologies provides complete protection of a corporate network by itself.

Each mechanism is aimed at neutralizing a particular class of threats and operates at the corresponding layer of the OSI model. The highest effectiveness is achieved through the integrated use of access control, network segmentation, and network interaction protection technologies. Such an approach makes it possible to implement a multilayered cybersecurity system that meets modern requirements for corporate network infrastructure.

Thus, the results of the analysis indicate that the integrated use of AAA, RADIUS, SSH, ACL, Port Security, and Dynamic ARP Inspection forms a multilayered protection system for a corporate network.

The combination of these mechanisms provides centralized access control, secure administration of network equipment, protection against data-link-layer attacks, and effective management of information flows, which corresponds to modern requirements for building secure corporate information systems [9].

4. Discussion of Research Results

The use of the AAA model significantly increases the information security level of a corporate network due to centralized access-right management, reduced risk of unauthorized actions, and the possibility of security event auditing. In modern corporate networks, AAA is a basic

component of Identity and Access Management (IAM) systems.

The main advantage of using RADIUS is the centralization of account management and security policy processes.

An administrator is able to manage access to all network resources from a single center, which considerably simplifies administration and increases the level of control over information infrastructure. In addition, the use of RADIUS makes it possible to implement detailed auditing of user actions and ensure compliance with the information security requirements of the corporate environment [12].

The main advantages of SSH are confidentiality of transmitted data, protection against credential interception, information integrity, and authentication of the communicating parties. The use of SSH makes it possible to significantly reduce the risks of Man-in-the-Middle attacks and unauthorized access to network equipment [16].

In the proposed network architecture, SSH is used as the main mechanism for remote administration of switches, routers, and server equipment, ensuring the secure execution of configuration and diagnostic operations.

The application of ACLs significantly reduces the risks of lateral movement within a corporate network and increases the effectiveness of information flow control.

The use of Dynamic ARP Inspection makes it possible to prevent Man-in-the-Middle attacks, ensure the integrity of addressing processes in the local network,

and increase the level of trust in network interactions among nodes of the corporate infrastructure [13].

The combined use of Port Security and DHCP Snooping strengthens control at the data link layer.

Port Security restricts device connections through physical switch ports, while DHCP Snooping prevents the operation of unauthorized DHCP servers and creates a trusted IP–MAC address binding database.

The integration of VLAN segmentation and ACL-based traffic filtering is particularly important for limiting the lateral movement of attacks. VLANs isolate individual user groups and network resources, whereas ACLs regulate permitted communication between the created segments.

5. Conclusions

As a result of the study, modern threats to the information security of corporate computer networks were analyzed and the most critical vulnerabilities of network infrastructure were identified. It was established that the main sources of risk remain attacks at the data link layer of the OSI model, the use of insecure administration protocols, weaknesses in authentication mechanisms, and an insufficient level of network segmentation.

It is shown that effective cybersecurity can be ensured only through the integrated application of modern protection technologies. The most effective mechanisms include centralized user authentication based on the AAA model and the RADIUS protocol, the use of the cryptographically protected SSH protocol, the application of Port Security, Access Control Lists, Dynamic ARP Inspection technologies, and logical network segmentation using VLAN.

Conflict of Interest

The authors declare that they have no conflicts of interest related to this study, including financial, personal, authorship-related, or any other conflicts that could have influenced the research and the results presented in this article.

Funding

The study was conducted without financial support.

Data Availability

No data are associated with this manuscript.

Use of Artificial Intelligence Tools

The authors confirm that artificial intelligence technologies were not used in the preparation of this work.

REFERENCES

1. Kurose, J. F., and Ross, K. W. (2025), *Computer Networking: A Top-Down Approach*, 9th ed., Pearson, New York, 864 p. available at: <https://www.pearson.com/en-us/subject-catalog/p/computer-networking-a-top-down-approach/P200000013385>
2. Buriachok, V. L., Hulak, H. M., and Tolubko, V. B. (2024), *Information and cyberspaces: security problems, methods and means of counteraction*, textbook, Magnolia-2006, Lviv 2024. 448 p. available at: https://magnolia.lviv.ua/wp-content/uploads/2024/04/INF-TA-KIBERPROSTORY-pidruchnyk_zmist.pdf
3. Khomchak, M. (2025), “Cybersecurity risk assessment for selecting a cloud provider”, *Cybersecurity: Education, Science, Technique*, no. 27, pp. 549–559, doi: <https://doi.org/10.28925/2663-4023.2025.27.773>
4. Derkach, T. M., Holovko, H. V., Dmytrenko, A. O., and Klochko, L. A. (2026), “Analysis of threats and vulnerabilities of computer networks and substantiation of a comprehensive approach to ensuring their cybersecurity”, *Control, Navigation and Communication Systems*, no. 2, pp. 73–80, doi: <https://doi.org/10.26906/SUNZ.2026.2.073>
5. Derkach, T. M., and Lavrenko, M. (2024), “Cyberspace: analysis of threats and protection methods”, *Innovative Education: Problems and Prospects of Scientific Research*, Proceedings of the 50th International Scientific and Practical Conference, Stuttgart, December 4–6, pp. 112–115, available at: <https://reposit.nupp.edu.ua/handle/PolNTU/18104>
6. Korchenko, O., Ivanchenko, E., Bakalinsky, O., Myalkovskyi, D., and Zubkov, D. (2024), “Method for assessing the level of cybersecurity improvement of critical infrastructure facilities of the state”, *Science-Based Technologies*, no. 61(1), pp. 3–20, doi: <https://doi.org/10.18372/2310-5461.61.18509>
7. Anderson, R. (2020), *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley, Hoboken, 1248 p., available at: <https://www.cl.cam.ac.uk/archive/rja14/book.html>
8. Easttom, C. (2024), *Network Defense and Countermeasures*, Springer, William Easttom II, 412 p. available at: https://books.google.com.ua/books/about/Network_Defense_and_Countermeasures.html?hl=ar&id=NFTDwAAQBAJ&redir_esc=y
9. Stewart, J. M., Chapple, M., and Gibson, D. (2024), *ISC2 CISSP Certified Information Systems Security Professional Official Study Guide*, 10th ed.: Wiley, Hoboken, ISBN 978-1-394-25470-5, 1248 p., available at: <https://www.wiley.com/en-us/ISC2+CISSP+Certified+Information+Systems+Security+Professional+Official+Study+Guide%2C+10th+Edition-p-9781394254705>
10. Tanenbaum, A. S., and Wetherall, D. J. (2011), *Computer Networks*, 5th ed. Upper Saddle River: Pearson, 2011. 960 p. available at: <https://www.pearson.com/en-us/subject-catalog/p/computer-networks/P200000003188>
11. Lakhno, V., Yerbolat, K., Bagdat, Y., Kryvoruchko, O., Desiatko, A., Tsiutsiura, S., and Tsiutsiura, M. (2022), “A model for protecting the local network of an educational institution”, *Cybersecurity: Education, Science, Technique*, no. 18, pp. 6–23, doi: <https://doi.org/10.28925/2663-4023.2022.18.623>
12. (2024), *NIST Cybersecurity Framework (CSF) 2.0*, National Institute of Standards and Technology, available at: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
13. (2018), *IEEE Computer Society. IEEE Standard for Virtual Bridged Local Area Networks (IEEE 802.1Q)*, IEEE, New York, available at: https://standards.ieee.org/standard/802_1Q-2018.html
14. Derkach, T. M., and Prykhodko, R. (2025), “Intrusion detection system as a key element of multilayered cyber protection of information systems”, *Research in Science, Technology and Economics*, Proceedings of the 5th International Scientific and Practical Conference, Luxembourg, December 10–12, 2025, pp. 308–311, available at:

- <https://reposit.nupp.edu.ua/handle/PoltNTU/20866>
15. (1994), ISO/IEC 7498-1:1994. *Information Technology – Open Systems Interconnection – Basic Reference Model*, available at: <https://www.ecma-international.org/wp-content/uploads/s020269e.pdf>
 16. Stallings W. (2017), *Network Security Essentials: Applications and Standards*, 6th ed., Pearson, Boston, 464 p., available at: <https://www.pearson.com/en-us/subject-catalog/p/network-security-essentials/P200000003180>
 17. Cisco Systems. Catalyst 2960 and 2960-S Switches Software Configuration Guide, Cisco IOS Release 15.2(1)E. Cisco, 2013. available at: <https://www.cisco.com>
 18. Odom W. (2024), *CCNA 200-301*, vol. 1, Official Cert Guide, Cisco Press, 1087 p., available at: <https://faspc.com/academy/Ebook/Cisco/CCNA%20200-301%20Official%20Cert%20Guide%20Volume%201%20Second%20Edition.pdf>
 19. Ylonen T., and Lonvick C. (2006), *The Secure Shell (SSH) Protocol Architecture: RFC 4251*, IETF, available at: <https://www.rfc-editor.org/rfc/rfc4251>
 20. Dahm, T., Ota, A., Medway Gash, D.C., Carrel, D., and Grant, L. (2020), *RFC 8907: The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol*, IETF, Fremont, 66 p., DOI: <https://doi.org/10.17487/RFC8907>

Received (Надійшла) 01.07.2026

Accepted for publication (Прийнята до друку) 09.09.2026

Publication date (Дата публікації) 25.09.2026

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Деркач Тетяна Миколаївна – доктор філософії, доцент, доцент кафедри комп'ютерних та інформаційних технологій і систем, Національний університет "Полтавська політехніка імені Юрія Кондратюка", Полтава, Україна

Tetyana Derkach – PhD, Associate Professor, Associate Professor of the Department of Computer and Information Technologies and Systems, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine

e-mail: tanider@ukr.net; ORCID Author ID: <https://orcid.org/0000-0001-8062-9105>

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57204846765>

Дмитренко Андрій Олександрович – доктор філософії, доцент, доцент кафедри будівельних конструкцій, Національний університет "Полтавська політехніка імені Юрія Кондратюка", Полтава, Україна;

Andrii Dmytrenko – PhD, Associate Professor, Associate Professor of Department of building structures, National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine;

e-mail: andmyt@ukr.net; ORCID Author ID: <https://orcid.org/0000-0002-8715-7646>;

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57217604473>.

Ключко Ліна Андріївна – доктор філософії, інженер-геотехнік, геологічне бюро BEG SA, Швейцарія

Lina Klochko – Ph.D., Geological Bureau BEG SA, Switzerland

e-mail: lina.dmitrenko@gmail.com; ORCID Author ID: <http://orcid.org/0000-0002-6064-2887>;

Scopus Author ID: <https://www.scopus.com/authid/detail.uri?authorId=57217278708>.

Комплексний підхід до забезпечення кібербезпеки корпоративної мережевої інфраструктури

Т. М. Деркач, А. О. Дмитренко, Л. А. Ключко

Анотація. Актуальність. Стрімкий розвиток цифрових технологій, широке впровадження корпоративних інформаційних систем і зростання кількості кіберзагроз зумовлюють необхідність удосконалення захисту корпоративної мережевої інфраструктури. Традиційні методи, засновані на використанні окремих програмних або апаратних засобів, не забезпечують належної стійкості до сучасних багатовекторних кібератак. Тому актуальним є формування комплексної багаторівневої системи, спрямованої на забезпечення конфіденційності, цілісності та доступності корпоративних інформаційних ресурсів. **Предмет дослідження:** підходи, моделі, протоколи та технології забезпечення кібербезпеки корпоративної мережевої інфраструктури. **Мета дослідження:** обґрунтування комплексного підходу до побудови захищених корпоративних мереж на основі багаторівневого захисту та інтегрованого застосування сучасних технологій мережевої безпеки. **Завдання дослідження.** Проаналізувати роль моделі OSI у проєктуванні захищених мереж; визначити основні загрози; дослідити механізми захисту на різних рівнях мережевої взаємодії; розглянути концепцію Defense in Depth; проаналізувати технології AAA, RADIUS, SSH, ACL, VLAN, Port Security, DHCP Snooping і Dynamic ARP Inspection та переваги їх комплексного застосування. **Методи дослідження.** Використано методи системного аналізу, порівняння, узагальнення та систематизації науково-технічної інформації, структурно-функціональний підхід і моделювання комплексної архітектури безпеки корпоративної мережі. **Результати дослідження.** Визначено основні загрози корпоративним мережам, зокрема MAC Spoofing, MAC Flooding, ARP Spoofing, ARP Cache Poisoning, Man-in-the-Middle, несанкціоноване підключення пристроїв, компрометацію облікових записів і порушення політик доступу. Проаналізовано концепцію Defense in Depth та встановлено, що багаторівневий підхід обмежує наслідки компрометації окремих компонентів мережі. Розглянуто застосування AAA і RADIUS для централізованого управління доступом, SSH – для захищеного адміністрування, ACL – для контролю міжсегментної взаємодії, а Port Security, DHCP Snooping і Dynamic ARP Inspection – для протидії атакам каналного рівня. Встановлено, що VLAN-сегментація сприяє локалізації кіберінцидентів, обмеженню горизонтального поширення атак і реалізації принципу найменших привілеїв. **Висновки.** Комплексне застосування AAA, RADIUS, SSH, ACL, VLAN, Port Security, DHCP Snooping і Dynamic ARP Inspection відповідно до концепції Defense in Depth забезпечує централізований контроль доступу, захищене адміністрування, сегментацію мережі та протидію поширеним мережевим атакам.

Ключові слова: кібербезпека; корпоративна мережа; мережева інфраструктура; інформаційна безпека; Defense in Depth; AAA; RADIUS; SSH; ACL; VLAN; Port Security; Dynamic ARP Inspection; модель OSI; контроль доступу.