SATBAYEV UNIVERSITY

Computing & Engineering

Volume 2 (2024), Issue 1, 1-6

https://doi.org/10.51301/ce.2024.i1.01

Establishing a Comprehensive Enterprise Security System

R. Agzam, Kh. Yubuzova*

Satbayev University, Almaty, Kazakhstan

**Corresponding author: k.yubuzova@satbayev.university*

Abstract. The article considers the complex provision of information security of an enterprise using modern technologies and tools. The analysis of the existing network infrastructure was carried out, the main vulnerabilities were identified, including the absence of VLANs, subnets and IDS/IPS systems, which increases the risk of unauthorized access and data leakage. To eliminate the identified shortcomings, a network upgrade was proposed, including the introduction of virtual local area networks (VLANs), subnets and the Snort intrusion detection and prevention system. A test model of a corporate network was created on the GNS3 platform, including a pfSense firewall with an integrated IDS/IPS system, routers, switches and workstations divided into VLANs. Simulations of network attacks using Kali Linux were carried out, which made it possible to demonstrate the effectiveness of the proposed measures. The Snort system successfully detected and recorded attempts to bypass filters and unauthorized scanning, which confirms its suitability for corporate use. The results of the work show that an integrated approach to information security based on traffic isolation, access control and network monitoring significantly reduces the risks of cyber-attacks, increases network stability and improves its manageability. The proposed methods can be recommended for implementation in enterprises seeking to increase the level of security of their information systems.

Keywords: *information security, corporate network, VLAN, subnets, network modeling, traffic, cyber threats.*

1. Introduction

Network security analysis is a key element of enterprise information security. With its help, it is possible to assess the state of the network, identify vulnerabilities and risks, predict threats and develop measures to protect against incidents leading to financial losses and loss of reputation. Today's reality is characterized by the regular emergence of new and sophisticated cyber threats, so regular analysis is necessary to update security mechanisms and policies. In addition, it helps to comply with standards and regulatory requirements for information security, and minimize legal risks. The analysis strengthens the safety culture by increasing employee awareness and reducing the risks associated with the human factor. As a result, he provides management with information for informed decisions on security investments and strategic planning, which is important for the sustainable development and competitiveness of the enterprise.

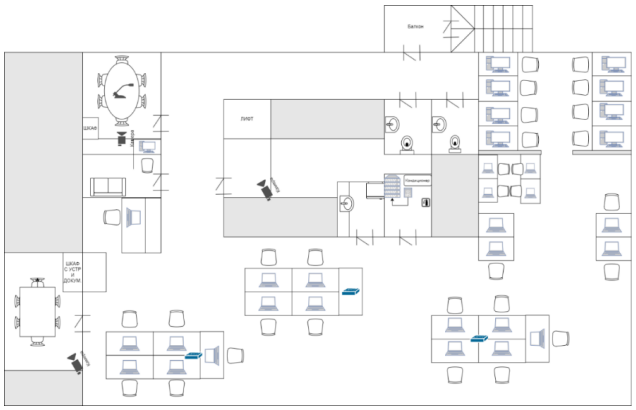

Figure 1. Layout of the enterprise

2. Materials and methods

2.1 Enterprise layout analysis and network devices

During the study, a thorough tour of the office was carried out to create a detailed plan of its location, which facilitated the search for network devices and orientation inside the room (Figure 1).

Analyzing the layout, the following were revealed: the personnel structure and organizational hierarchy, including IT departments, research, quality control, office management, a group of assistants, a call center, a director and his deputy, indicating the number of employees in each.

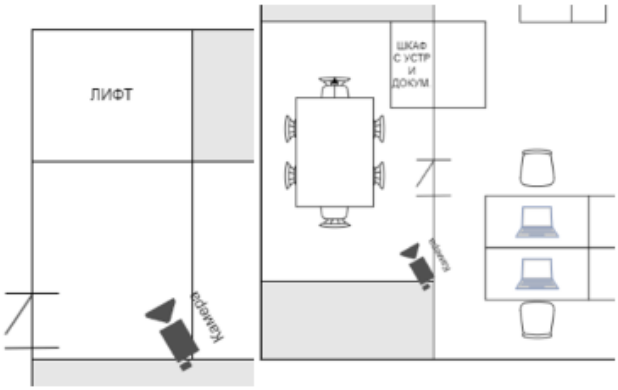

Figure 2. Indoor cameras

Important network equipment is installed in the office: five switches for combining devices into a single local area network and two routers for traffic management and connection to the external Internet. This detail helps to effectively organize the workspace and optimize internal communications.

External and internal protection measures have been implemented to ensure safety. External security is provided by an access control system with personal cards and video surveillance in public places, which prevents unauthorized entry and allows you to control the flow of people. Internal security is supported by video surveillance inside the office, preventing internal threats and acting as a deterrent against unfair actions by employees or visitors (Figure 2).

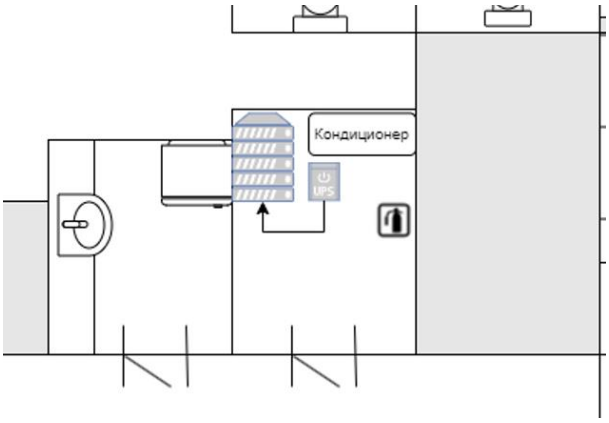

Figure 3. Server protection from high temperature/fire

2.2 Network security Analysis

During the study, a detailed diagram of the enterprise's network infrastructure was developed (Figure 4), which serves as the basis for analyzing the level of network security.

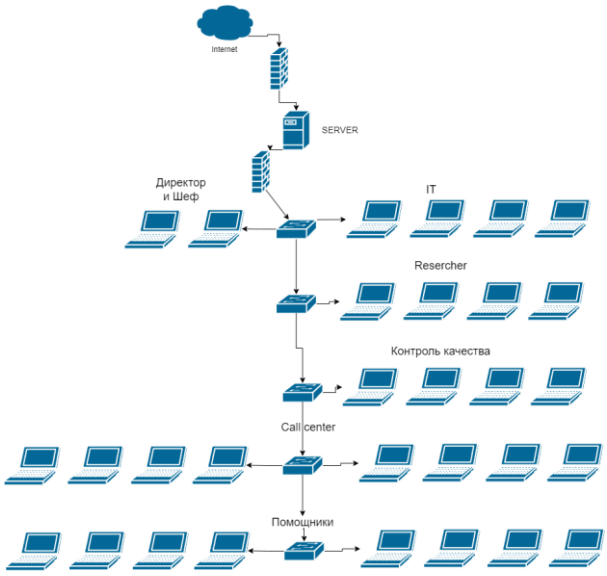

Figure 4. Network infrastructure diagram

At the top level, cloud services and enterprise servers are located, reflecting an external Internet connection and centralized resources. The next layer includes routers and switches that provide communication between servers and end devices. The lower part shows workstations and network storage devices (NAS).

A firewall plays a central role in managing and controlling network traffic between different domains, blocking unauthorized access to corporate data and resources. To enhance the security of network channels, VPN technology is used, which creates a secure tunnel for data transmission, which is especially important for remote employees.

The 802.1X standard is used to enhance access control to network resources, requiring new devices to undergo verification and authentication before connecting to the network. The Zabbix system is used for network monitoring and management (Figure 5), which monitors network traffic, the status of routers and the expiration dates of SSL certificates.

The integration of technologies and tools such as firewall, VPN, 802.1X standard and Zabbix system creates a multi-layered protection system that significantly increases the security level of the enterprise's network infrastructure and allows you to effectively counter modern cyber threats.

Figure 5. Zabbix monitoring system

2.3 Network vulnerabilities

The study revealed disadvantages such as the lack of VLANs (virtual local area networks), which is why all departments use a single network environment, increasing the likelihood of unauthorized employee access to confidential information from other departments and increasing the risk of corporate data leakage.

In addition, there is no comprehensive network security policy, which means that there are no clear guidelines for access management, data protection and responding to security incidents, leaving the network infrastructure without the necessary protection measures. There are also no intrusion detection (IDS) and intrusion prevention (IPS) systems, which deprives the network of the ability to effectively detect anomalies or attacks in real time, increasing the risk of unnoticed intrusions and leaks of confidential information, making the organization vulnerable to various cyber-attacks.

3. Results and discussion

To improve the security and efficiency of the corporate network, it is necessary to modernize, including:

1. Implementation of Virtual Local Area Network (VLAN) technology to divide the network into isolated segments, improving security and preventing unauthorized access between departments;

2. Development and implementation of an information security policy, including access control, data protection,

incident response and staff training, ensuring comprehensive protection of data and resources;

3. Installation of intrusion detection and prevention systems (IDS/IPS), such as Snort, Suricata or Zeek, for real-time detection and blocking of threats, increasing the level of network security.

The use of these measures will reduce the risks of data leakage, prevent unauthorized access, strengthen protection against cyber threats and improve network efficiency. It is recommended to use the GNS3 software to plan and test changes. The implementation should be accompanied by careful planning and, if necessary, the involvement of information security specialists.

3.1 Implementation on the GNS3 platform

A test network was created within the GNS3 platform (Figure 6), which includes a pfSense firewall with an integrated IDS/IPS Snort system. The firewall is connected to an L3 layer router and a switch, which in turn is connected to Kali Linux. The L3 layer router is also connected to three switches to which computers are connected. Each switch is configured on a separate subnet and VLAN corresponding to a separate department of the enterprise. The network configuration has been simplified due to the limitations of computing resources, as GNS3 uses significant hardware resources to emulate each connected device.

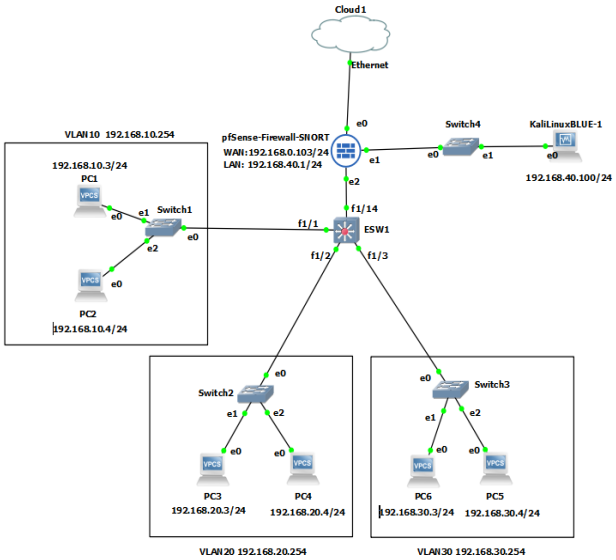

Figure 6. Network infrastructure diagram in GNS3

When scanning the network using Kali Linux, the following alerts were recorded (Figure 9). The last three alerts point to a source with an IP address of 192.168.40.100, which is scanning using unauthorized HTTP methods in an attempt to bypass filters. Under standard conditions, it is recommended to block such an IP address, however, since this is a test environment, there is no need to block it.

3.2 IDS/IPS Snort system tests and results

Kali Linux is used to conduct attack simulations and manage the pfSense firewall via a web interface (Figure 7).

The IDS/IPS Snort system has been installed and configured on the pfSense firewall (Figure 8), which will be used in the future to detect and block suspicious traffic on the network.

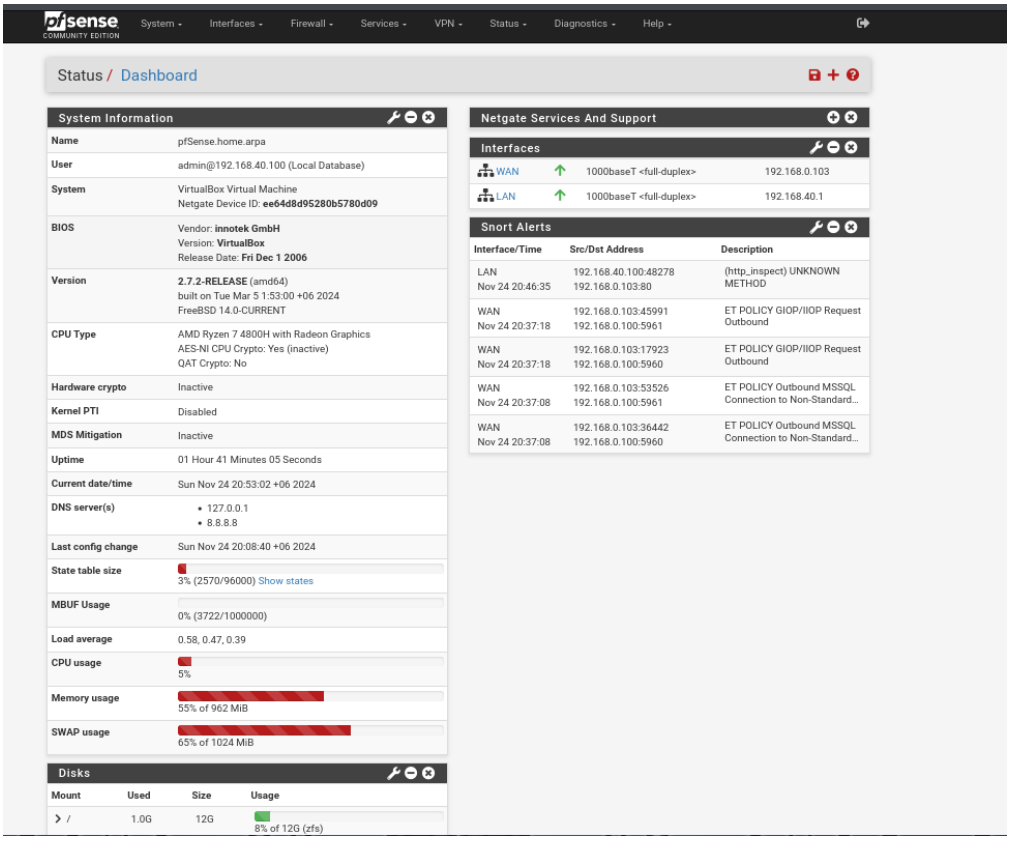

Figure 7. pfSense Web Interface

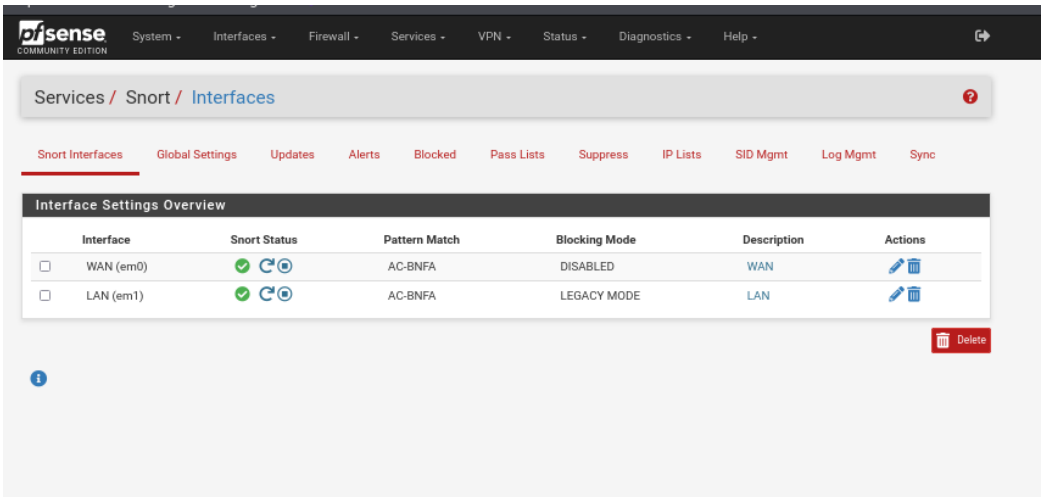

Figure 8. Snort in pfsense

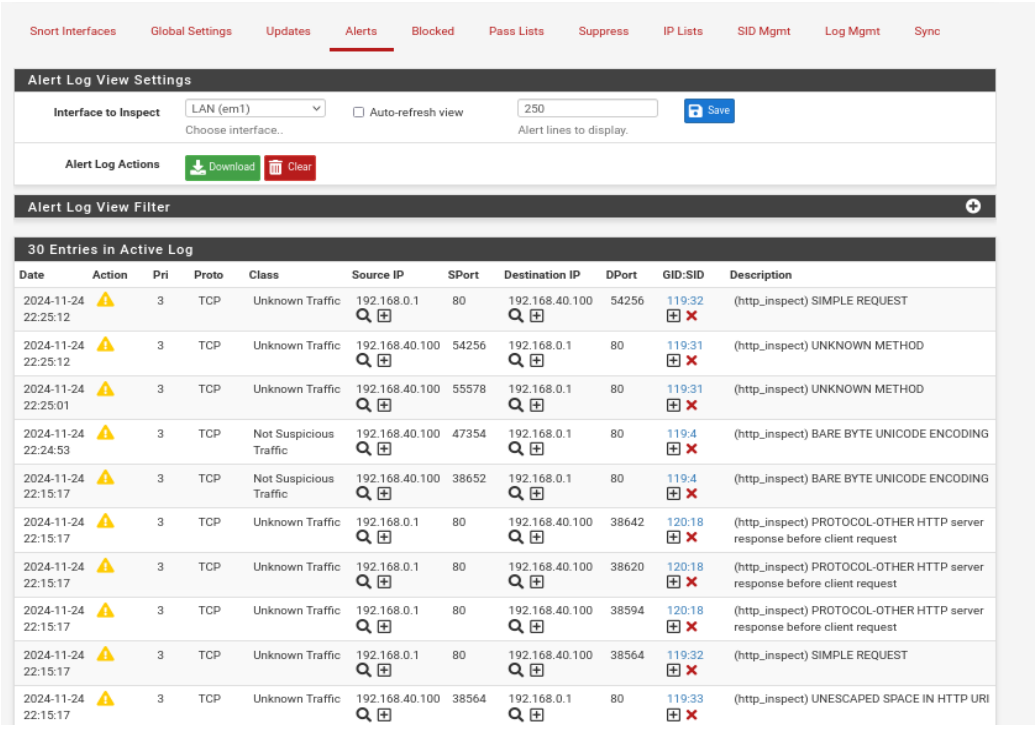

Figure 9. Snort alerts

The use of subnets and VLANs plays a key role in ensuring traffic isolation, which significantly increases security and simplifies network management. These technologies allow devices to be divided into logical groups, regardless of their physical location, which helps to reduce the volume of broadcast traffic and improve overall network performance.

VLANs provide flexibility in network configuration, allowing devices to be combined into a single network segment even when they are located on different switches. This simplifies management and increases the adaptability of the network to changes.

Subnets, in turn, optimize routing, making it easier to monitor IP addresses and prevent unwanted interaction between segments. This separation helps to increase the efficiency of using network resources and simplifies access management.

The integration of IDS/IPS solutions such as Snort, Suricata or Zeek will ensure the detection and prevention of network anomalies and cyber threats in real time. These systems will enhance the network's ability to respond effectively to intrusions and minimize potential data leaks.

GNS3, a powerful network emulator, is recommended for planning and testing these enhancements in a controlled environment. GNS3 allows for the simulation of complex network topologies, enabling the organization to test IDS/IPS configurations and other security upgrades before deployment. This approach supports a proactive stance on security, allowing the identification and resolution of issues in a simulated environment before they impact the live network.

4. Conclusions

During the research, a corporate network model was developed and tested with the integration of modern information security tools such as VLANs, subnets and IDS/IPS systems. A simulation of the real infrastructure was carried out on the GNS3 platform, which made it possible to demonstrate the

effectiveness of the implementation of these technologies for traffic isolation, access control and threat detection.

The results confirm the importance of using an integrated approach to network security, including monitoring, risk management and architecture modernization. These measures not only minimize the threat of cyber-attacks, but also contribute to improving network performance and manageability of information resources.

References

[1] Van Horn, M.J. (2023). Mastering Enterprise Networks. Embry-Riddle Aeronautical University. *Daytona Beach, USA.* https://doi.org/10.15394/eaglepub.2023.1069)

[2] Software. (2024). Netgate Documentation – Configuring the Snort Package. This guide details the steps for installing and configuring the Snort package in pfSense. *Retrieved from:* https://docs.netgate.com/pfsense/en/latest/packages/snort/setup.html

[3] Balogh, Z., Koprda, Š. & Francisti, Jan. (2018). LAN security analysis and design. Department of Informatics, Faculty of Natural Sciences, Constantine the Philosopher University in Nitra. *Nitra, Slovakia. Retrieved from*: https://ieeexplore.ieee.org/document/8746912

[4] Official website of Snort. Retrieved *from*: https://www.snort.org/

[5] Official website of Kali Linux. *Retrieved from*: https://www.kali.org/

Кәсіпорын қауіпсіздігінің кешенді жүйесін құру

Р. Агзам, Х. Юбузова*

Satbayev University, Алматы, Қазақстан

**Корреспонденция үшін автор: k.yubuzova@satbayev.university*

Аңдатпа. Мақалада заманауи технологиялар мен құралдарды пайдалана отырып, кәсіпорынның ақпараттық қауіпсіздігін кешенді қамтамасыз ету қарастырылады. Қолданыстағы желілік инфрақұрылымға талдау жүргізілді, негізгі осалдықтар анықталды, оның ішінде VLAN, ішкі желілер және IDS/IPS жүйелерінің болмауы, бұл рұқсатсыз кіру және деректердің ағып кету қаупін арттырады. Анықталған кемшіліктерді жою үшін виртуалды жергілікті желілерді (VLAN), ішкі желілерді және Snort басып кіруді анықтау және алдын алу жүйесін енгізуді қамтитын желіні жаңарту ұсынылды. GNS3 платформасында корпоративтік желінің сынақ үлгісі жасалды, оның ішінде біріктірілген IDS/IPS жүйесі бар pfSense брандмауэр, маршрутизаторлар, коммутаторлар және VLAN-ға бөлінген жұмыс станциялары. Kali Linux көмегімен желілік шабуылдарды модельдеу жүргізілді, бұл ұсынылған шаралардың тиімділігін көрсетуге мүмкіндік берді. Snort жүйесі сүзгілерді және рұқсатсыз сканерлеуді айналып өту әрекеттерін сәтті анықтап, тіркеді, бұл оның корпоративтік пайдалануға жарамдылығын растайды. Жұмыс нәтижелері трафикті оқшаулауға, қол жеткізуді басқаруға және желіні бақылауға негізделген ақпараттық қауіпсіздікке кешенді көзқарас кибершабуылдар қаупін айтарлықтай төмендететінін, желінің тұрақтылығын арттыратынын және оны басқару мүмкіндігін жақсартатынын көрсетеді. Ұсынылған әдістерді өздерінің ақпараттық жүйелерінің қауіпсіздік деңгейін арттыруға ұмтылатын кәсіпорындарға енгізу үшін ұсынуға болады.

Негізгі сөздер: *ақпараттық қауіпсіздік, корпоративтік желі, VLAN, ішкі желілер, желіні модельдеу, трафик, киберқауіптер.*

Создание комплексной системы безопасности предприятия

Р. Агзам, Х. Юбузова*

Satbayev University, Алматы, Казахстан

**Автор для корреспонденции: k.yubuzova@satbayev.university*

Аннотация. В статье рассмотрено комплексное обеспечение информационной безопасности предприятия с использованием современных технологий и средств. Проведен анализ существующей сетевой инфраструктуры, выявлены основные уязвимости, в том числе отсутствие VLAN, подсетей и систем IDS/IPS, что повышает риск несанкционированного доступа и утечки данных. Для устранения выявленных недостатков была предложена модернизация сети, включающая внедрение виртуальных локальных сетей (VLAN), подсетей и системы обнаружения и предотвращения вторжений Snort. На платформе GNS3 была создана тестовая модель корпоративной сети, включающая межсетевой экран pfSense с интегрированной системой IDS/IPS, маршрутизаторы, коммутаторы и рабочие станции, разделенные на VLAN. Было проведено моделирование сетевых атак с использованием Kali Linux, что позволило продемонстрировать эффективность предложенных мер. Система Snort успешно обнаружила и зафиксировала попытки обхода фильтров и несанкционированного сканирования, что подтверждает ее пригодность для корпоративного использования. Результаты работы показывают, что комплексный подход к информационной безопасности, основанный на изоляции трафика, контроле доступа и мониторинге сети, существенно снижает риски кибератак, повышает стабильность сети и

улучшает ее управляемость. Предложенные методы могут быть рекомендованы к внедрению на предприятиях, стремящихся повысить уровень безопасности своих информационных систем.

Ключевые слова: *информационная безопасность, корпоративная сеть, VLAN, подсети, сетевое моделирование, трафик, киберугрозы*.

Received: 28 November 2023
Accepted: 16 March 2024
Available online: 31 March 2024