

UDC 657.6:658.8:656.61(477.7)

*M. Tarasiuk,**Doctor of Economic Sciences, Professor, Head of the Department of Management and Marketing, Kyiv National Linguistic University**ORCID ID: <https://orcid.org/0000-0001-7081-7217>**N. Biletska,**PhD in Economics, Associate Professor, Vice-Rector for educational and methodical work, Private Higher Educational Establishment "Vinnytsia Institute of designing of clothes and entrepreneurship"**ORCID ID: <https://orsid.org/0000-0001-6622-3614>**I. Smyrnova,**Doctor of Pedagogy, Professor, Assistant Director of Academic and Pedagogical Activities, Danube Institute of National University "Odessa Maritime Academy"**ORCID ID: <https://orcid.org/0000-0003-2085-539>**V. Holovachko,**Bachelor's degree student of the Faculty of Mathematics and Digital Technologies, Uzhhorod National University**ORCID ID: <https://orcid.org/0009-0006-7153-6592>*

DOI: 10.32702/2306-6814.2023.12.59

SECURE IT INFRASTRUCTURE MANAGEMENT WITH VLAN USAGE

*M. B. Тарасюк,**д. е. н., професор, завідувач кафедри менеджменту і маркетингу, Київський національний лінгвістичний університет**Н. В. Білецька,**к. е. н., доцент, проректор з навчально-методичної роботи, ПВНЗ Вінницький інститут конструювання одягу і підприємства**І. М. Смирнова,**д. пед. н., проф., заступник директора з науково-педагогічної діяльності, Дунайський інститут Національного університету "Одеська морська академія"**В. В. Головачко,**здобувач вищої освіти факультету математики та цифрових технологій, Державний вищий навчальний заклад "Ужгородський національний університет"*

БЕЗПЕЧНИЙ МЕНЕДЖМЕНТ ІТ ІНФРАСТРУКТУРИ З ВИКОРИСТАННЯМ VLAN

In the conditions of military operations in Ukrainian enterprises, the security and reliability of IT infrastructure become particularly important. This is because the use of VLANs (Virtual Local Area Networks) is an effective tool for ensuring security and resource allocation. Its application is entirely reasonable even in the context of military operations. This is because it allows for minimal costs: physically divide the network into logical segments based on business processes, configure access control rules for data based on business processes, and create redundant paths for data transmission based on business processes in case there is a risk of damage or destruction of parts of the network infrastructure, and establish priorities for different types of traffic based on business processes. The use of VLANs shapes secure management, whose basic features and processes differ from traditional IT infrastructure management. These outlined differences lead to specific transformations like all business processes within an enterprise. Therefore, the research is focused on identifying the peculiarities of secure IT infrastructure management using VLANs and identifying the characteristics of its impact on the nature of business processes within the enterprise. Research results have demonstrated that VLAN forms a secure management of IT infrastructure, which is a complex of technologies, principles, methods, and tools that are developed to ensure the security and efficiency of managing the information technology infrastructure of an enterprise, adapting its business processes to the conditions of military operations. This adaptation is achieved through processes such as

scaling, network segmentation, access control to data, and traffic labeling. The conclusions drawn indicate that the adaptation of business processes to the conditions of military operations results in their transformation, characterized by the following features: physical division of the enterprise network into logical segments, where unique format business processes can be formed in each segment; optimization of data flow management based on business processes; determination of user groups with different levels of access to network resources and data based on business processes; acquiring the ability to flexibly expand and adapt the network infrastructure to the needs of business process owners.

В умовах військових дій на підприємствах України безпека та надійність ІТ інфраструктури стають особливо важливими. Це зумовлене тим фактом, що використання VLAN (Virtual Local Area Networks) є ефективним інструментом забезпечення безпеки і розподілу ресурсів. Це є цілком доцільним навіть в умовах військових дій, оскільки дозволяє з мінімальними витратами: фізично розділити мережу на логічні сегменти за бізнес-процесами; налаштувати правила контролю доступу до даних за бізнес-процесами; створити резервні шляхи для передачі даних за бізнес-процесами, якщо існує ризик пошкодження або знищення частини мережевої інфраструктури; встановлювати пріоритети для різних типів трафіку за бізнес-процесами. Фактично, використання VLAN формує безпечний менеджмент, базові риси та процеси якого відрізняються від класичного менеджменту ІТ-інфраструктури. Окреслені різниці призводять до специфічних трансформацій в природі всіх бізнес-процесів підприємства. Відтак, дослідження спрямоване на визначення особливостей безпечного менеджменту ІТ-інфраструктури з використанням VLAN та ідентифікацію особливостей його впливу на природу бізнес-процесів підприємства. За результатами дослідження доведено, що VLAN формує безпечний менеджмент ІТ інфраструктури, що є симплексом технологій, принципів, методів та засобів, що за ними формуються, для забезпечення безпеки й ефективності управління інформаційно-технічною інфраструктурою підприємства, що адаптує його бізнес-процеси до умов військових дій. Така адаптація здійснюється через процеси масштабування, сегментації, керування доступом до даних та маркування трафіку. Зроблено висновки, що адаптація бізнес-процесів до умов військових дій формує їх зміни, яким властиві наступні особливості: формування сегментів бізнес-процесів унікального формату; оптимізація управління рухом даних по бізнес-процесах; визначення груп користувачів з різним рівнем доступу до мережевих ресурсів та даних за бізнес-процесами; набуття здатності гнучкого розширення та адаптації мережевої інфраструктури до потреб власників бізнес-процесів.

Key words: business process; workflow; network infrastructure; physical network segmentation; management.

Ключові слова: бізнес-процес; потік робіт; мережева інфраструктура; фізичний розділ мережі; менеджмент.

TARGET SETTING

In the conditions of military operations at enterprises in Ukraine, the security and reliability of the IT infrastructure become particularly important. It is because the use of VLAN (Virtual Local Area Network) is an effective tool for ensuring security and resource allocation, which is quite reasonable even in the context of military operations. It allows for minimal costs: physically divide the network into logical segments based on business processes (thus limiting the potential spread of an attack or its impact on other parts of the network in case one segment is compromised), configure access control rules for data based on business processes (thus limiting access to resources and preventing unauthorized access to critical information), create redundant paths for data transmission based on business processes in case there is a risk of damage or destruction of part of the network infrastructure (thus ensuring an alternative data transmission route that helps maintain network continuity in the

conditions of military operations), and prioritize different types of traffic based on business processes (thus ensuring the reliable and fast transmission of critical data, even in case of limited network bandwidth). Indeed, the use of VLANs contributes to secure management, and its basic features and processes differ from classical IT infrastructure management. These outlined differences lead to specific transformations like all enterprise business processes.

ANALYSIS OF RESEARCH AND PUBLICATIONS

A thorough analysis shows that scientists (V. Buryachok, A. Anosov, V. Semko, V. Sokolov, P. Skladannyi, O. Maslyhan H. Mashika, V. Zelic, A. Kiziun, R. Maslyhan, K. Shafranov, N. Kampov) pay great attention to various aspects of developing secure IT infrastructure management. However, researchers note that there are challenges in understanding the impact of such management

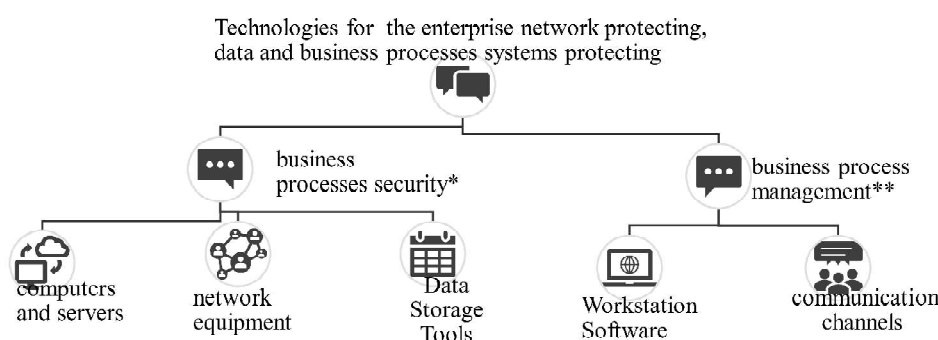


Figure 1. Key components of enterprise secure IT infrastructure management shape changes in its business processes

Note:

*Protection of networks, data, and systems from unauthorized access, viruses, malware, and other threats.

** Tools for monitoring, management, backup, recovery, configuration, and support of the infrastructure.

Source: formed based on [1—2].

on the nature of enterprise business processes, as they can integrate non-specific changes. Nevertheless, the specifics and nature of these changes have not been studied yet. This calls for research in the delineated area.

THE WORDING OF THE PURPOSES OF ARTICLE (PROBLEM)

The article aims to identify the characteristics of secure IT infrastructure management using VLAN and to examine the specific impact of this management approach on the nature of enterprise business processes.

THE PAPER MAIN BODY WITH FULL REASONING OF ACADEMIC RESULTS

The actual use of VLANs forms a secure management of IT infrastructure. It should be considered as a complex of VLAN technologies, principles, methods, and tools that are formed to ensure the security and efficiency of managing the information technology infrastructure of an enterprise, adapting its business processes to the conditions of military operations. Such VLAN imple-

mentation not only establishes fixed control points for all systems and technologies necessary for the functioning and management of IT infrastructure (including network security technologies, data protection, and system security), but it also ensures comprehensive control and configuration of workflow streams for each of the business processes through the following systems: 1) computers and servers; 2) network equipment; 3) data storage devices; 4) workstation software; 5) communication channels. Thus, the key components of enterprise secure IT infrastructure management shape changes in its business processes presented in Figure 1, as provided by us.

The collaborative interaction and functioning of the elements outlined in Figure 1 allow enterprises to ensure the transmission, storage, processing, and protection of information, as well as efficient user work and the execution of business processes. The specific impact and action of secure IT infrastructure management are driven by the fact that IT infrastructure serves as the foundation for business applications, communication systems, email, data storage, information exchange, and many other functions performed within an organization. It is also evident from an analysis of the experience of secure IT infrastructure management using VLANs (Table 1).

In particular, there is a wide range of applications for such management in domestic enterprises, which is focused on:

1. Division of departments and teams. This is relevant for enterprises that have various departments such as production, finance, marketing, IT, and so on. The use of VLANs allows for the separation of these departments into

Table 1. Analysis of experience in secure IT infrastructure management using VLANs

An enterprise secure IT infrastructure management provides	The application areas of secure IT infrastructure management*					
	Division of departments and teams ⁽¹⁾	Guest networks ⁽²⁾	Server segmentation ⁽³⁾	Virtual private networks ⁽⁴⁾	Hot backups ⁽⁵⁾	Network business processes virtualization ⁽⁶⁾
ATB	+	-	-	+	+	+
TEDi Ukraine	-	+	-	+	-	+
BaDM	-	+	+	-	-	+
Philip Morris	-	+	+	+	+	+
Kyivstar	+	+	+	+	+	+
Roshen	+	+	-	+	+	+
Eridon	-	-	+	-	+	+

Note

*Use cases: (1) Network segmentation, providing traffic isolation and access control between segments; (2) Creation of a separate guest network, isolated from the main corporate network; (3) Physical partitioning of servers into separate segments, ensuring security and isolation between them; (4) Creation of a dedicated network segment for VPN traffic, ensuring its isolation from other traffic within the organization; (5) VLAN paths configured as backup routes for data transmission in case of failure of primary routes; (6) Virtualization of internal network organizational interactions within business processes.

Source: formed based on data from economic entities.

separate network segments, providing traffic isolation and access control between them. Each department will have its own VLAN, allowing for the isolation of their traffic from one another. This helps prevent potential threats and preserves the confidentiality of each department's data.

2. Guest networks. It is relevant for enterprises that have business processes involving frequent meetings with clients, partners, or external individuals. In such cases, a separate guest network is created for these workflows (for example, VLAN 10 is configured on

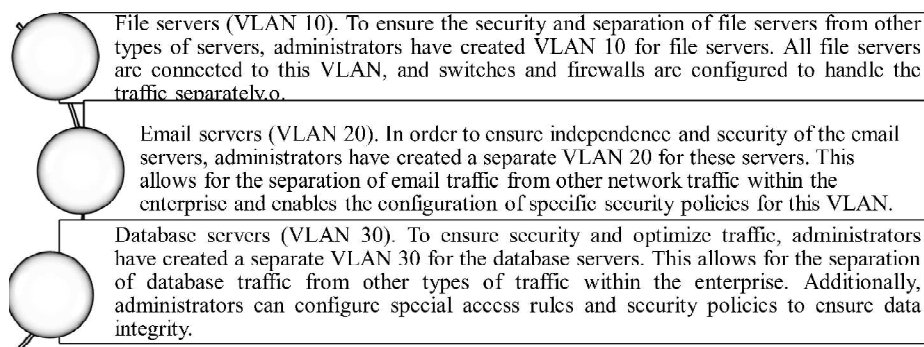


Figure 2. Server Segmentation Practice at Philip Morris Ukraine

Source: formed based on [1; 3].

the network switch for the guest network), which allows them to have access only to a limited set of resources and ensures the isolation of their traffic from the main business process network. Devices placed in the guest hall or conference room, which have access to the guest VLAN, and guest devices (such as laptops or smartphones) connecting to the guest Wi-Fi network, receive an IP address from the guest VLAN 10 and have restricted access to corporate resources. It enables control over guest access to resources and prevents unauthorized access to confidential information circulating within the business process network.

3. Server segmentation. Many enterprises have various servers to support workflows within their business processes, such as file servers, email servers, database servers, and so on. The use of VLANs allows for the physical separation of these servers into distinct segments, ensuring security and isolation between them. For example, at Philip Morris Ukraine, there are three types of servers: File servers (VLAN 10), Email servers (VLAN 20), and Database servers (VLAN 30), each segmented according to their specific nature, as shown in Figure 2. It is evident that this application reduces the risk of compromising all servers simultaneously and facilitates easier traffic management.

4. Virtual private networks (VPN). The use of VLAN can be combined with VPN technology for secure connections to remote workstations or remote offices. VLAN allows for the creation of a separate network segment for VPN traffic, ensuring its isolation from other traffic within the organization. For example, in practice, Kyivstar represents each of its offices and business processes with a separate VLAN, which is isolated from other network segments of the company (according to the logic, Office A — VLAN 10, Office B — VLAN 20). All traffic coming from the remote office is marked using a VLAN tag. At the main office, a VPN server is configured to receive encrypted traffic from the remote office. The use of VLAN can be combined with VPN technology for secure connections to remote workstations or remote offices. VLAN allows for the creation of a separate network segment for VPN traffic, ensuring its isolation from other traffic within the organization. For example, in practice, Kyivstar represents each of its offices and business processes with a separate VLAN, which is isolated from other network segments of the company (according to the logic, Office A — VLAN 10, Office B —

VLAN 20). All traffic coming from the remote office is marked using a VLAN tag. At the main office, a VPN server is configured to receive encrypted traffic from the remote office.

5. Hot backups. The use of VLAN enables the creation of backups that ensure the network's continuity in case of production or technical issues. Paths created with VLAN can be configured as backup routes for data transmission in the event of a failure in primary routes. For

example, in Roshen's practice, there is a primary route for data transmission regarding workflow streams between departments. This route passes through a specific switch and network equipment. However, if this primary route becomes inaccessible due to switch failure or other issues, VLAN functions as a backup route to ensure uninterrupted data transmission for workflow streams. In the case of Kyivstar, an additional VLAN has been created on another switch to provide an alternative path for data transmission between company departments. This VLAN is physically separated from the primary route and has its own switches and network equipment. In the event of a failure in the primary route, using VLAN as a backup route allows Kyivstar experts to redirect traffic through an alternative path. This is achieved by reconfiguring the switches and network equipment to route the traffic through the backup VLAN. Hot backups help ensure the continuity of system operations and reduce the impact of adverse events on business activities.

6. Network business processes virtualization. The use of VLAN is an important component of internal network virtualization in organizational interactions within business processes. Virtualization enables the creation of virtual network environments for different workflow streams, which are physically separated from the infrastructure. For example, in Eridon, there are marketing, development, and finance departments, each with its own networking and security needs. The use of VLAN has allowed Eridon's experts to create virtual network segments for each department and their associated workflow streams. Each segment has its own access rules, security policies, and network device configurations. The VLAN for the marketing department at Eridon has access to specialized resources such as marketing systems or data analytics tools. The development department at Eridon has its own VLAN with access to development servers and tools. The finance department has its own VLAN with enhanced security measures and restricted access to financial data. Thus, the use of VLAN allows for traffic management and security within these virtual networks, simplifying the deployment and management of network resources involved in business processes.

According to modern practices of secure management, the interaction of its elements using VLAN entails specific features that help ensure the security, efficiency, and

manageability of the IT infrastructure and its networks (Figure 3).

Therefore, the areas of application of secure IT infrastructure management considered above allow to distinguish the following aspects:

1. Network segmentation of the enterprise. VLAN allows physically dividing the enterprise network into logical segments, each of which can host business processes of a unique format aimed at creating coordinated conditions for activities, developing new and modifying existing products, selling active products, resource allocation, personnel reproduction, technological resource reproduction, and so on. Each segment has an owner (who is also the owner of the business process), thus it can have its own access rules, security policies, and configuration of network devices.

Defined network segmentation allows for: ensuring traffic isolation for each business process (traffic passing through one VLAN does not intersect with traffic passing through other VLANs. This is achieved by physically dividing the network into logical segments, each with its own VLAN identifier); restricting the potential spread of attacks or impact on other parts of the network; configuring access rules. Each VLAN can have its own access rules and security policies; create configurations for network devices such as switches or routers. Any network segmentation into logical segments allows businesses to effectively manage network resources and maintain optimal performance.

2. Traffic marking. Protocols such as IEEE 802.1Q are used for traffic tagging and separating it from other network segments. Each packet has a VLAN tag that allows for:

- 1) Identifying the segment to which it belongs.
- 2) Properly processing and directing traffic within VLANs to routers and switches.
- 3) Setting priorities for traffic processing within VLANs, which affects Quality of Service (QoS) and real-time data transmission.
- 4) Avoiding collisions and conflicts between different

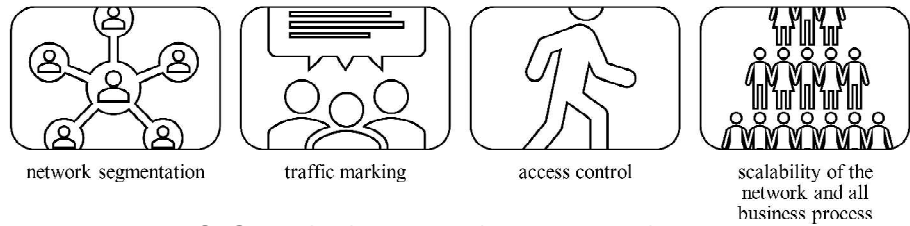


Figure 3. Specific features of secure IT infrastructure management using

Source: formed based on [1; 3; 5].

types of traffic passing through a single physical network device.

5) Increasing the efficiency of network bandwidth utilization by segregating traffic into different VLANs and limiting its propagation to occupied resources.

Traffic tagging through VLAN allows for efficient management of data flow across business processes, which have a physical form and digital representation in the network. This enables the establishment of display priorities, and security, and reduces conflicts. This is particularly important for core business processes that constitute the primary operations, as tagged traffic allows visualizing all the processes and workflows within the resource utilization of business processes, ensuring the quality of service and data security.

3. Access Control. Using VLAN allows for:

- 1) Configuring access control rules at the switch level.
- 2) Configuring access control rules at the network device level.
- 3) Controlling the interaction between systems and users, systems and devices, taking into account their access rights to specific network segments.
- 4) Preventing unauthorized access to critical data or systems by configuring user authentication, authorization, and accounting.

By implementing access control, business process owners can define user groups with varying access levels to network resources. For example, an owner can create separate VLANs for administrators, regular employees, and guests. Each VLAN will have its own access rules, allowing control over which resources each user group can access. An individual VLAN can be created for confidential data, such as financial records or customer personal information. It will restrict access to these data only to authorized users, and a higher level of security provided. It is especially crucial in military operations where information security and confidentiality are crucially important. Access control using VLAN ensures that only authorized users gain access to the necessary resources.

4. The scalability of a network and all business processes. The use of VLAN allows for network scalability by:

- 1) dividing the network into logical segments;

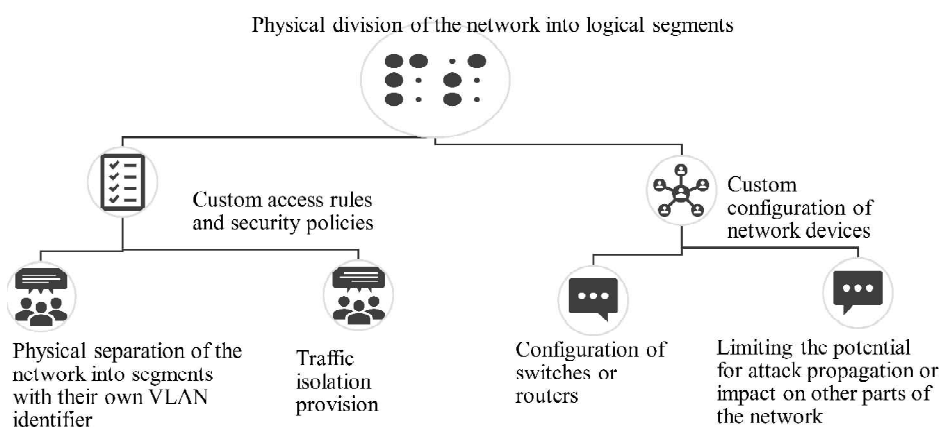


Figure 4. Elements of enterprise network segmentation using VLANs

Source: formed based on [1; 3; 4; 5].

2) managing traffic distribution and limiting its occupancy in each segment;

3) providing the ability to add new networks without the need for physical reconfiguration of IT infrastructure;

4) distributing network load by moving devices and users.

The scalability provided by using VLAN allows businesses to flexibly expand and adapt their network infrastructure to the needs of the owners' business processes (which are determined by the specifics of design, development, execution, and efficiency of the business processes). Under these conditions, all business processes that govern the functioning of the enterprise are formed within separate logical segments capable of scalability. This contributes to ensuring the efficiency, reliability, and productivity of the network in the face of changing requirements and business growth.

CONCLUSIONS FROM THIS STUDY AND PROSPECTS FOR FURTHER EXPLORATION IN THIS AREA

According to the research findings, it has been proven that VLAN (Virtual Local Area Network) forms a secure management of IT infrastructure, which is a complex of technologies, principles, methods, and tools designed to ensure the security and efficiency of enterprise information technology management. It adapts its business processes to the conditions of military operations. This adaptation is achieved through processes such as scaling, network segmentation, data access control, and traffic labeling. Conclusions have been drawn that the adaptation of business processes to the conditions of military operations brings about changes characterized by the following features:

1. Physical division of the enterprise network into logical segments, each of which can accommodate business processes of a unique format. These processes include activities such as establishing coordinated conditions of operation, developing new and modifying existing products, active product sales, resource allocation, personnel management, and technological infrastructure maintenance. Each segment can have its own data access rules, security policies, and network device configurations.

2. Traffic marking using VLAN enables effective management of data flow across business processes, which have a physical form and digital representation in the network. This allows for establishing priorities, ensuring security, and reducing conflicts. This is particularly important for core business processes that constitute the primary operations of the business.

3. Through access control, owners of business processes can define different user groups with varying levels of access to network resources. For instance, an owner can create separate VLANs for administrators, regular employees, and guests. This allows for granular control over who can access specific resources and helps maintain security and data integrity within the network.

4. The scalability of VLAN usage allows enterprises to flexibly expand and adapt their network infrastructure to the needs of business process owners. Under such conditions, all business processes that govern the functioning of the enterprise are formed within separate logical segments that can be scaled. This contributes to ensuring the efficiency, reliability, and productivity of the

network in the face of changing requirements and business growth.

The results obtained by the authors can be used to study optimal VLAN configurations for supporting different types of business processes. Furthermore, these results provide a basis for a systematic assessment of the impact of different VLAN configurations on productivity, security, and the efficiency of executing business processes.

Література:

1. Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. — К.: КУБГ, 2019. — 218 с.

2. Гусєва О. Ю. Легомінова С. В. Діджиталізація - як інструмент удосконалення бізнес-процесів, їх оптимізація, Економіка. Менеджмент. Бізнес, 2018, Вип. 1. С. 33—39.

3. PricewaterhouseCoopers database (2023) PwC report "SMART management models". URL: https://www.pwc.com/content/pwc/userReg/login.en_gx.html?redirectUrl=g0V-55lpsw21J2UMYgbIH5kctcJLK2-lwWPau2GN84=&referrer=g0V-55lpsw21J2UMYgbIH5kctcJLK2lwWPau2GN84=&parentPagePath=/content/pwc/gx/en.

4. Савицька О. М., Салабай В. О. Особливості діджиталізації бізнесу компанії в умовах розвитку індустрії 4.0. Ефективна економіка. 2020. No 10. — URL: <http://www.economy.nayka.com.ua/?op=1&z=8266> (дата звернення: 20.04.2023). DOI: 10.32702/2307-2105-2020.10.65

5. Services sphere cluster management: virtualization and methodological aspects: монографія / [Authorsteam: Mashika Hanna, Zelic Victoria, Kiziun Alla, Maslyhan Roman et al.]. — Odesa: KUPRIENKO SV, 2023, 131 с.

References:

1. Buryachok, V. L., Anosov, A. O., Semko, V. V., Sokolov, V. YU. and Skladanny, P. M. (2019), *Tekhnolohiyi zabezpechennya bezpeky merezhevoyi infrastruktury* [Technologies for ensuring network infrastructure security], KUBH, Kyiv, Ukraine

2. Husieva, O.Yu and Lehominova, S.V. (2018), "Digitalization — as a tool for improving business processes, their optimization", *Ekonomika. Menedzhment. Biznes*, vol. 1, pp. 33—39.

3. PricewaterhouseCoopers database (2023) PwC report "SMART management models". Available at: https://www.pwc.com/content/pwc/userReg/login.en_gx.html?redirectUrl=g0V-55lpsw21J2UMYgbIH5kctcJLK2-lwWPau2GN84=&referrer=g0V-55lpsw21J2UMYgbIH5kctcJLK2lwWPau2GN84=&parentPagePath=/content/pwc/gx/en.

4. Savytska, O. and Salabai, V. (2020), "Specific features of the digitalization of the company's business in the conditions of development of industry 4.0", *Efektivna ekonomika*, [Online], vol. 10, Available at: <http://www.economy.nayka.com.ua/?op=1&z=8266> (Accessed 21 Apr 2023). DOI: 10.32702/2307-2105-2020.10.65

5. Mashika, H. Zelic, V. Kiziun, A. and Maslyhan, R. (2023), *Services sphere cluster management: virtualization and methodological aspects*, KUPRIENKO SV, Odesa, Ukraine.

Стаття надійшла до редакції 29.05.2023 р.