МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ

ВІСНИК
ЧЕРКАСЬКОГО ДЕРЖАВНОГО ТЕХНОЛОГІЧНОГО УНІВЕРСИТЕТУ

Науковий збірник

Том 29,
№ 4. 2024

ЧЕРКАСИ
2024

ISSN: 2306-4412
E-ISSN: 2708-6070

Засновник:
Черкаський державний технологічний університет

Рік заснування: 1996

Рекомендовано до друку та поширення
через мережу Інтернет Вченою радою
Черкаського державного технологічного університету
(протокол № 5 від 16 грудня, 2024 р.)

Державна реєстрація: Ідентифікатор медіа R30-04613.
Рішення Національної ради України з питань телебачення і радіомовлення
№ 1916, протокол № 17 (30.05.2024 р.).

Науковий збірник входить до переліку наукових фахових видань України
Категорія «Б». Спеціальність:
122 – Комп'ютерні науки, 123 – Комп'ютерна інженерія, 125 – Кібербезпека,
126 – Інформаційні системи та технології, 151 – Автоматизація та комп'ютерно-інтегровані технології, 172 – Телекомунікації та радіотехніка
(наказ МОН України від 28 грудня 2019 року № 1643)

Науковий збірник представлено у міжнародних наукометричних базах даних, репозитаріях та пошукових системах: Bielefeld Academic Search Engine (BASE), Crossref, CiteFactor, Litmaps, Ulrich's Periodicals Directory, WorldCat, Directory of Open Access Journals (DOAJ), Open Ukrainian Citation Index (OUCI), Наукова періодика України, Національна бібліотека України імені В. І. Вернадського (НБУВ), Dimensions, UCSB Library, Google Академія, German Union Catalogue of Serials (ZDB), Бібліотека Університету Осло, Бібліотека Університету Халла, SOLO - Search Oxford Libraries Online, Інститут Європейського університету, Бібліотека Лейпцизького університету (UBL), Бібліотека Кембриджського університету

Адреса редакції:
Черкаський державний технологічний університет
18006, бульв. Шевченка, 460, м. Черкаси, Україна
E-mail: info@bulletin-chstu.com.ua
https://bulletin-chstu.com.ua/uk

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
CHERKASY STATE TECHNOLOGICAL UNIVERSITY

BULLETIN
OF CHERKASY STATE TECHNOLOGICAL UNIVERSITY

Scientific Collection

Volume 29,
No. 4. 2024

CHERKASY
2024

ISSN: 2306-4412
E-ISSN: 2708-6070

Founder:
Cherkasy State Technological University

Year of foundation: 1996

Recommended for printing and distribution
via the Internet by the Academic Council
of Cherkasy State Technological University
(Minutes No. 5 of December 16, 2024)

State Registration: Media identifier R30-04613.
Decision of the National Council of Television and Radio Broadcasting of Ukraine
No. 1916, Minutes No. 17, dated 30.05.2024.

The scientific collection is included in the list of Professional Scientific Publications of Ukraine
Category "B". Specialties: 0613 – Software and applications development and analysis,
0611 – Computer use, 0612 – Database and network design and administration,
0714 – Electronics and automation
(Order of the Ministry of Education and Science of Ukraine No. 1643, dated December 28, 2019)

The scientific collection is presented in the international scientometric databases, repositories and scientific systems: Bielefeld Academic Search Engine (BASE), Crossref, CiteFactor, Litmaps, Ulrich's Periodicals Directory, WorldCat, Directory of Open Access Journals (DOAJ), Open Ukrainian Citation Index (OUCI), Scientific Periodicals of Ukraine, Vernadsky National Library of Ukraine (VNLU), Dimensions, UCSB Library, Google Scholar, German Union Catalogue of Serials (ZDB), University of Oslo Library, University of Hull Library, SOLO - Search Oxford Libraries Online, European University Institute, Leipzig University Library (UBL), Cambridge University Library

Editors office address:
Cherkasy State Technological University
18006, 460 Shevchenko Blvd., Cherkasy, Ukraine
E-mail: info@bulletin-chstu.com.ua
https://bulletin-chstu.com.ua/en

Редакційна колегія

Editorial Board

Зміст / Contents

BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en Vol. 29 No. 4. 2024

UDC 004.72
DOI: 10.62660/bcstu/4.2024.10

Comparative analysis of different virtual switches to improve the efficiency of networks of different configurations

Oleksandr Berestovenko*
Postgraduate Student
National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"
03056, 37 Beresteiskyi Ave., Kyiv, Ukraine
https://orcid.org/0000-0003-4887-4674

Abstract. The aim of the study was to determine the optimal type of virtual switch to ensure maximum efficiency of computer networks of various configurations, taking into account their technical characteristics, capabilities, and level of integration. A comparative analysis of the performance and functionality of virtual switches was conducted. The main results showed that the Cisco Nexus 1000V provides excellent performance and low latency (0.5-2 milliseconds), making it ideal for environments where network speed and responsiveness are critical. Open vSwitch is highly scalable and memory efficient, with up to 9 gigabits per second of bandwidth and moderate Central Processing Unit usage, making it suitable for scalable virtualised environments. VMware vSwitch, with a bandwidth of 6-8 gigabits per second, has good integration into the VMware environment and easy configuration. Moreover, Virtual Packet Processing was found to provide the best throughput, reaching values between 20 and 50 gigabits per second, and also exhibits low latency in the range of 0.3-0.5 milliseconds, making it the optimal choice for environments with high bandwidth requirements. At the same time, the Bridge Virtual Switch has the lowest Central Processing Unit load (5-10%), which allows maintaining performance even with limited hardware resources. The other switches, namely Hyper-V Virtual Switch, Juniper Contrail Virtual Router, CloudStack Virtual Router, and Huawei CloudEngine vSwitch, demonstrated good performance and can be useful for environments with lower bandwidth and scalability requirements. The results showed that the choice of a virtual switch depends on specific requirements, as each switch has its own advantages and limitations that determine its optimality for different network configurations

Keywords: bandwidth; component scalability; system integration and performance; data processing; latency reduction

INTRODUCTION

With the rapid development of information technology, virtualisation is becoming an integral part of computer networks. One of the key elements of virtualisation is virtual switches, which provide data transfer between virtual machines and the physical network. Thanks to their ability to optimise the use of hardware resources and support high scalability, virtual switches play an important role in building Software-Defined Networking (SDN) and cloud environments. At the same time, the constant growth of data transmitted, the need to minimise latency and optimise resource utilisation create the need for systematic analysis of their performance.

Despite the significant attention paid to network virtualisation, the issues of choosing the optimal virtual switch for different configurations remain poorly understood. There is a wide range of solutions available, but the lack of clear guidelines for their use in specific environments makes it difficult for network engineers and architects to make decisions. The problem lies in the need to take into account many parameters such as

Article's History: Received: 15.08.2023; Revised: 22.10.2024; Accepted: 16.12.2024.

Suggested Citation:
Berestovenko, O. (2024). Comparative analysis of different virtual switches to improve the efficiency of networks of different configurations. *Bulletin of Cherkasy State Technological University*, 29(4), 10-20. doi: 10.62660/bcstu/4.2024.10.

*Corresponding author

throughput, latency, CPU (Central Processing Unit) and memory usage, and scalability. Existing research often focuses on specific aspects of switches, leaving gaps in understanding their overall performance.

R. Olifirenko (2021) emphasised that virtualisation of network resources remains the "missing link" in cloud computing, despite the automation of other components. The researcher pointed out that hypervisors increase the flexibility of SDN networks, although this is often accompanied by a decrease in performance, which requires improved methods of integration with SDN controllers. The results of V. Dumitrak (2020) demonstrated methods for implementing Network Function Virtualisation (NFV) in modern infrastructures, focusing on the use of Information-Centric Networking and SDN. This has made it possible to increase the efficiency of using network resources and introducing new services, improving the adaptability of networks to changing loads.

In turn, G. Bueno *et al.* (2022) showed how integrating NFV with SDN can improve the efficiency of network infrastructure. They pointed out that the use of a common SDN controller to manage NFV allows for optimising resource allocation and improving scalability by reducing data transmission delays. Researchers K. Wang *et al.* (2024) proposed an automated tool for diagnosing and localising errors in virtual private cloud networks. The tool uses a modular network model to accurately reflect the functions of real-world components of such networks and can analyse large networks with tens of thousands of components, making it effective for detecting errors in complex configurations.

Moreover, Y. Wang *et al.* (2022) pointed out the problem of dynamic resource allocation and packet scheduling for virtual switches in vehicle Internet networks. They demonstrated a mathematical model of this problem and optimisation algorithms that significantly improve the efficiency of resource allocation and data transmission in complex environments with high dynamicity of cognitive services. The results of the study by K. Yalda *et al.* (2024) compared centralised and distributed SDN architectures for Internet of Things (IoT) networks. The results showed that distributed architectures provide better fault tolerance and reduced use of the controller's CPU.

On the other hand, M.C. Lucas-Estañ *et al.* (2024) investigated the impact of different 5G network architectures and configurations on telemanipulated driving. The results showed that Mobile Edge Computing networks are the best due to high bandwidth requirements compared to centralised networks, and control channel settings can help reduce the impact of video processing time on the scalability of the service. Authors Y. Yang *et al.* (2021) proposed models for the effective implementation of virtual data centres, taking into account the possibility of placing virtual switches on physical switches. At the same time, researchers F. Ahmmed *et al.* (2024) showed that the use of virtual Multiple Input Multiple Output technologies for routing in wireless sensor networks significantly improves energy efficiency compared to traditional methods, in particular Single Input Single Output. This allows optimising network paths and reducing energy costs for data transmission, which can help improve the performance of networks with high energy saving requirements.

The purpose of the study was to identify the most effective virtual switches for optimising the operation of computer networks of various configurations, which was not fully covered by previous research. The tasks included conducting a comparative analysis of virtual switches and studying the effectiveness of their integration into existing network infrastructures with different configurations.

MATERIALS AND METHODS

To achieve the research goal, a detailed review and comparative analysis of the most common virtual switches, including Open vSwitch (OVS), Cisco Nexus 1000V (CNV), and VMware vSwitch (VMS), was carried out. It was found out how these switches affect the efficiency of computer networks of various configura tions, evaluating their performance, functionality and architectural features. A review of various tools for OVS environments, namely OpenFlow, Virtual Local Area Network (VLAN), Generic Routing Encapsulation (GRE), and Virtual Extensible Local Area Network (VXLAN), is conducted (Rashelbach *et al.*, 2022). For a CNV switch, these are VLAN, Private VLAN, and VXLAN, and for a VMS, VLAN and Network Interface Card (NIC) (Mehta, 2015). The review of the architectures of these switches included an analysis of their structural components and mechanisms that ensure their effective operation in different network configurations.

Additionally, architecture diagrams of the listed virtual switches were developed. The OVS switch diagram included various components, including the SDN controller, OVS User-Space Components, which included the Command Line Interface and Application Programming Interface (API), and the OVS Kernel Module (Pfaff *et al.*, 2015). The CNV switch circuit was based on the Virtual Supervisor Module (VSM) and Virtual Ethernet Module (VEM). It included such components as Access Control List, Quality of Service (QoS), and Application Centric Infrastructure. As for the VMS architecture diagram, it focused on the NIC component. The comparative analysis of the performance and functionality of OVS, CNV and VMS switches included such parameters as throughput (Gbps), average latency (ms), CPU usage, Random Access Memory and scalability. In addition, the advantages and disadvantages of using each of these virtual switches were outlined.

Other, less popular virtual switches such as Hyper-V Virtual Switch (HVVS), Juniper Contrail Virtual Router (JCVR), Vector Packet Processing (VPP), CloudStack Virtual Router (CSVR), OpenContrail vRouter (OCR),

Big Virtual Switch (BVS), and Huawei CloudEngine vSwitch (HCES) were analysed. The platforms for using these switches were specified, namely Hyper-V and Azure for the HVVS switch (Detecting bottlenecks in..., 2022), Juniper Contrail for JCVR (Contrail Networking and..., 2023), Apache CloudStack for CSVR (Configuring AutoScale with..., n.d.), OpenContrail for OCR (OpenContrail vRouter, 2024), and cloud platforms for HCES (CloudEngine 1800V virtual..., 2018). Moreover, companies and projects such as the Fast Data Project for VPP (Vector Packet Processing, n.d.) and Big Switch Networks for BVS (Poller, 2017) were reviewed. These switches were compared by such parameters as throughput (Gbps), latency (ms), CPU utilisation (%), memory (MB), and scalability. Based on the comparison of all the virtual switches analysed in this study, namely OVS, CNV, VMS, HVVS, JCVR, VPP, CSVR, OCR, BVS, HCES, recommendations were formulated to select the most suitable solutions for optimising the operation of virtual networks depending on the specifics of the tasks and performance requirements.

RESULTS

Virtualised switches are key components of modern SDNs that provide efficient traffic management, scalability, security, and performance. OVS, for example, is one of the most popular software-defined switches designed to meet the requirements of virtualised environments and SDN. Its functionality, modular architecture, and cross-platform compatibility make it widely used in modern data centres. The OVS supports a wide range of network protocols, making it a flexible and versa tile solution for a variety of environments, including:

- OpenFlow is an SDN management protocol that allows dynamically changing traffic routing and provides centralised network management;
- VLAN – provides isolation of network segments within the physical infrastructure;
- GRE and VXLAN are tunnelling protocols that enable the creation of scalable networks on top of existing physical networks;
- integration with virtualisation platforms, as OVS is compatible with Elastic Sky X Integrated Virtual Machine (VMware ESXi), Kernel-based Virtual Machine and other platforms, allowing to effectively manage traffic between virtual machines.

The OVS architecture demonstrates the interaction between the operating system kernel, user space, SDN controller, and virtual machines (Fig. 1). This architecture has a modular structure consisting of several main components:

- OVS Kernel Module is a component that works at the operating system kernel level, is responsible for fast network traffic processing and provides low latency and high performance;
- the OVS User-Space Daemon is a component that performs management, configuration, and monitoring functions, as well as provides an API for interacting with SDN controllers such as OpenDaylight or Ryu;
- SDN controller – a component that allows centrally managing network flows using the OpenFlow protocol.

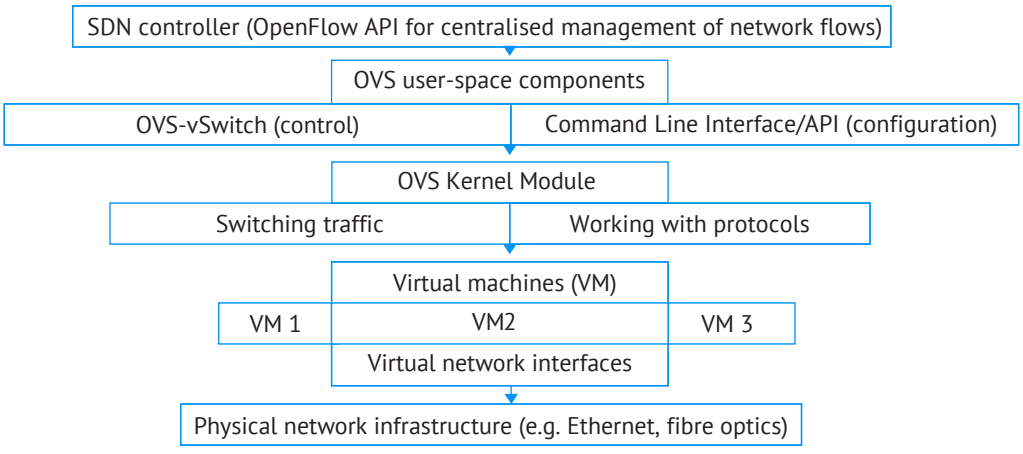

Figure 1. Diagram of the OVS architecture

Source: created by the author

OVS is widely used in a variety of areas, including data centres, cloud and container environments, SDN, and telecommunications. In data centres, OVS is used to communicate between virtual machines on the same server or between servers, as well as to build tunnel networks using VXLAN or GRE. This allows efficiently scaling one's network infrastructure and providing traffic isolation across VLANs. In cloud environments, OVS helps to create logical networks on top of the physical infrastructure. For example, in OpenStack, it acts as the main network element, providing convenient management through the Neutron module.

In container platforms such as Kubernetes, OVS orchestrates networks for containers, providing connectivity between them and integrating with the Container Networking Interface for scalable management.

Moreover, in SDN environments, OVS integrates with controllers such as OpenDaylight for centralised traffic management. This allows for the implementation of complex routing policies, adapting to changes in the network. In telecommunications, OVS is used to build NFV and organise high-speed services in IoT or 5G networks.

In turn, the CNV virtual switch is an important element of modern SDN, providing high performance, flexibility, and security in virtualised environments. It is an enterprise solution specifically designed to integrate virtual networks with physical infrastructure, making it a popular choice in large data centres. CNV supports a number of functionalities that ensure its adaptability to the needs of modern virtualised environments, including:

- VLAN – network segmentation to increase security and isolate traffic between virtual machines;
- Private VLAN is an additional layer of isolation for traffic between separate organisational units;
- VXLAN is a protocol for building scalable virtual networks on top of physical infrastructure;
- Standardised port settings that are automatically applied to virtual interfaces, which simplifies network management.

The CNV architecture is based on two main components: VSM and VEM (Fig. 2). The VSM is the central management unit that acts as the controller for all switches in the network. It provides centralised management, configuration, monitoring, and provides APIs for integration with virtualisation management platforms such as VMware vCenter. For its part, the VEM is located on each server running virtual machines. It directly handles traffic between virtual machines on the server and transmits it to the physical network or other hosts.

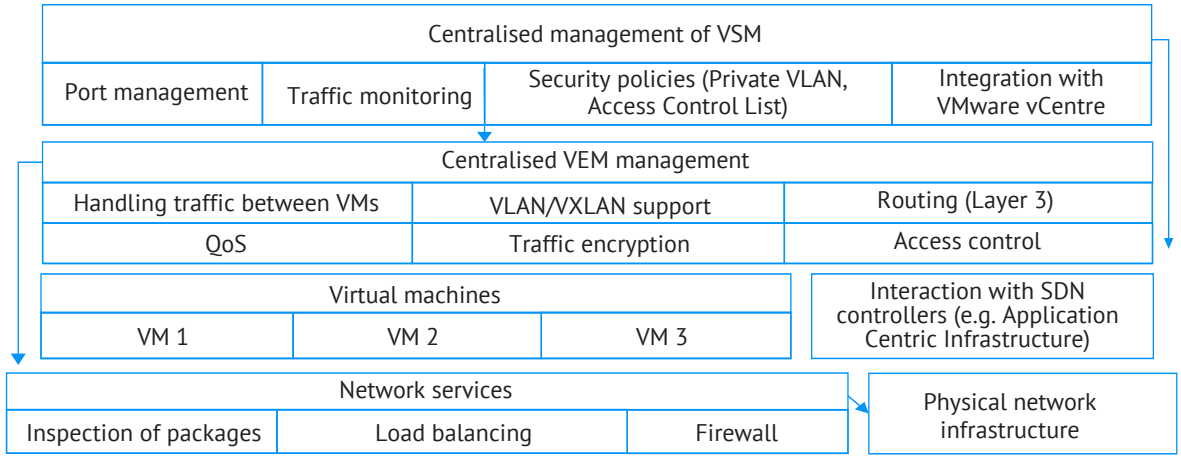

Figure 2. Diagram of the CNV architecture

Source: created by the author

CNV is widely used in data centres, cloud environments and enterprise networks. In data centres, it integrates virtual networks with the physical infrastructure, allowing operators to centrally manage traffic between virtual machines and configure security and segmentation policies using VLANs and Private VLANs. For example, in multi-zone data centres, CNV is used to clearly distinguish zones by access level and isolate critical resources.

In cloud environments, this virtual switch is often used to build virtual networks that scale with VXLAN, allowing logical networks to be created on top of physical infrastructure. In enterprise networks, the CNV provides standardised configuration through standardised port settings, simplifying the deployment of new services and minimising human error. In addition, CNV supports integration with management platforms such as VMware vCenter and SCVMM (Microsoft System Center Virtual Machine Manager), which allows automating network management processes. This makes it indispensable in large corporate environments where it is necessary to dynamically scale resources and ensure stable network operation.

On the other hand, the VMS virtual switch is a key element of VMware's virtualisation network infrastructure that allows virtual machines on the same ESXi server to exchange traffic with each other or with a physical network. Thanks to its ease of integration, scalability, and high performance, vSwitch has become the standard in enterprise and data centre environments. VMS supports the following functionalities:

- VLAN, which provides logical network segmentation, increasing security and isolating traffic between virtual machines;
- NIC Teaming, which combines multiple physical network adapters to increase bandwidth and provide fault tolerance;
- traffic shaping, which allows the administrator to restrict incoming or outgoing traffic for load balancing;
- security policies that control access to network resources through features such as Promiscuous Mode, MAC Address Changes, and Forged Transmissions.

A VMS functions as the virtual equivalent of a physical switch (Fig. 3). Its structure includes virtual ports that are used to connect virtual network interfaces of virtual machines to the virtual switch. It also contains port groups with defined configuration parameters, such as VLAN IDs or security policies, and physical network adapters that connect the vSwitch to the physical network.

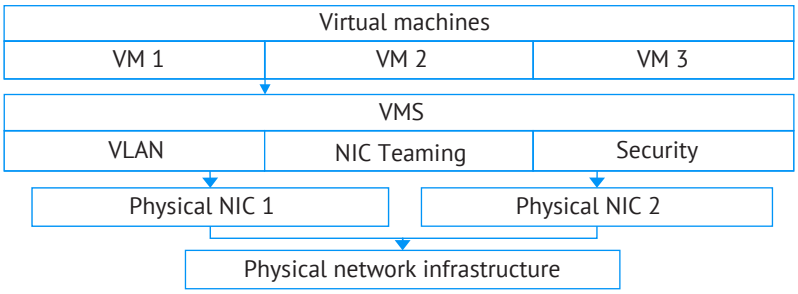

Figure 3. VMS architecture diagram

Source: created by the author

Overall, VMS is the basic solution for network virtualisation in large data centres. Its VLAN and NIC Teaming features provide the flexibility to build segmented and fault-tolerant networks. In cloud environments, such as VMware Cloud Foundation, vSwitch is used to aggregate virtual machines into logical networks. This allows quickly configuring and scaling resources as needed. On the other hand, a VMS is suitable for creating isolated networks needed for software or configuration testing. In SDN, the VMS is the component that routes traffic between virtual machines and hosts, integrating with solutions such as Network Security eXtension to implement complex security and routing policies.

In addition to the virtual switches already mentioned, it is worth paying attention to HVVS, JCVR, VPP, CSVR, OCR, BVS, and HCES. For example, HVVS is a virtual switch from Microsoft that is integrated into the Hyper-V platform. It provides VLAN support, traffic isolation, QoS, and security features such as Address Resolution Protocol and Dynamic Host Configuration Protocol protection. It is suitable for building enterprise networks and integrating with the Azure platform. JCVR is a software-based router and switch that is part of the Juniper Contrail platform. It provides routing functionality, network isolation, and traffic management in SDN and cloud environments. It supports integration with OpenStack. VPP is a high-performance software switch and router developed by the Fast Data Project. It is focused on low latency and high throughput. It is widely used in NFV and SDN. CSVR is a solution integrated into the Apache CloudStack platform that provides routing, Network Address Translation, Virtual Private Network, and firewall functions for cloud environments. It is effective for creating isolated networks in multi-tenant environments. OCR is a component of the OpenContrail platform that provides virtual switch and router functions. It supports VXLAN tunnelling and Multiprotocol Label Switching, providing scalability and flexibility in building SDN. BVS is an SDN solution from Big Switch Networks that provides centralised traffic management and scalability. It is used to build private and hybrid clouds with VLAN and VXLAN support. HCES is a virtual switch that provides high performance, integration with cloud management platforms, and support for SDN controllers. It is designed for enterprise environments and large data centres.

In summary, OVS improves the efficiency of networks in various configurations with its modular architecture and support for a wide range of protocols such as VLAN, GRE, and VXLAN, enabling scalable and optimised networks in cloud, container, and on-premises environments. Its integration with SDN controllers provides centralised management in large distributed networks, while in small environments it makes efficient use of resources. CNV delivers high performance in networks of varying complexity through clear segmentation and centralised management, which is important for large data centres and cloud environments. Its support for VXLAN allows networks to scale over physical infrastructure, and its standardised port settings simplify management in enterprise networks, providing adaptability to changing loads. As for VMS, it integrates seamlessly with VMware vSphere to automate traffic management and simplify virtual machine deployment in virtualisation environments, optimising network performance in enterprise configurations. Other switches, such as HVVS, JCVR, VPP, CSVR, OCR, BVS, and HCES, also offer specific solutions for different needs, from SDN and NFV scalability to security and traffic isolation in multi-tenant environments. This demonstrates the wide range of functionality that virtual switches offer to improve the efficiency of networks in various configurations.

To improve the efficiency of networks of various configurations, it is important to evaluate the performance and functionality of virtual switches. To determine the optimal solutions for different network environments, a comparative analysis of the most popular virtual switches should be conducted: OVS, CNV, and VMS (Table 1).

Table 1. Comparison of OVS, CNV and VMS

Parameter	OVS	CNV	VMS
Bandwidth (Gbps)	Up to 9	Up to 10	6-8
Average latency (ms)	1-3	0.5-2	2-5
CPU usage	Moderate	Low	Moderate
Using Random Access Memory	Effective	High	Moderate
Scalability	High	High	Medium

Source: created by the author based on R. Mehta (2015), A. Rashelbach *et al.* (2022)

Consequently, OVS has high scalability and memory efficiency, making it a flexible solution for SDN environments. CNV demonstrates the best performance with low latency and efficient CPU usage, but requires significant memory resources. And VMS integrates well into the VMware ecosystem and is suitable for virtualised environments, but is limited in scalability and slightly inferior in performance. In addition, it is worth considering the advantages and limitations of each switch.

OVS has a number of advantages that make it a popular choice for modern virtualised environments. High performance is achieved through optimisation at the operating system kernel level, which allows for efficient network traffic processing even in complex and busy environments. Configuration flexibility is provided by support for multiple network protocols and compatibility with SDN controllers, which allows OVS to adapt to the needs of different users. Scalability is achieved through support for tunnelling, such as VXLAN and GRE, which allows for the integration of virtual and physical networks. In addition, the OVS architecture is optimised for efficient resource utilisation, making it suitable for environments with limited hardware. At the same time, this switch also has disadvantages, such as complexity of configuration, which requires high skills, and increased CPU requirements when working with numerous virtual machines or tunnels.

CNV also offers significant benefits, including deep integration with corporate networks, allowing it to be easily integrated with existing infrastructure. CNV's security is backed by support for Private VLANs and flexible access policies, which ensures reliable data protection. VXLAN technology allows creating scalable virtual networks on top of physical infrastructure, and centralised management through VSM makes it easy to administer. However, the disadvantages of this solution are its high cost, the need for in-depth knowledge of networking technologies for configuration, and limited compatibility with non-VMware platforms.

The VMS stands out for its seamless integration with the VMware ecosystem, including ESXi, vCenter and Network Security eXtension, for easy management. An intuitive interface and standard templates simplify configuration, while support for security and redundancy policies increases network reliability. VMS flexibility is provided through the use of VLAN and NIC Teaming, which allows for segmentation and load balancing. The main disadvantages are limited analytics and integration with SDN solutions, high dependence on VMware infrastructure, and the need for additional licences to use advanced features such as VMware Distributed Switch. It is also important to compare other virtual switches (Table 2).

Table 2. Comparison of HVVS, JCVR, VPP, CSVR, OCR, BVS and HCES

Parameter	HVVS	JCVR	VPP	CSVR	OCR	BVS	HCES
Bandwidth (Gbps)	5-15	10-30	20-50	5-20	10-25	15-50	20-40
Delay (ms)	~0.8	~0.5	~0.3	~0.9	~0.4	~0.2	~0.3
CPU load (%)	10-20	15-25	5-10	10-30	10-20	5-15	5-20
Memory (MB)	30-50	40-70	25-60	30-80	35-70	25-50	30-60
Scalability	Medium	High	Very high	Medium	High	Very high	High

Source: created by the author based on Configuring AutoScale with using CloudStack virtual router (n.d.), Detecting bottlenecks in a virtualized environment (2022), Contrail Networking and Security User Guide (2023)

This means that the VPP switch is best suited for networks with high bandwidth requirements, such as those in data centres or telecommunications environments. The BVS offers the lowest latency, making it the best choice for applications that require fast response times, such as financial systems or real-time. VPP and BVS also have the lowest CPU load, which is important for maintaining performance in systems with limited hardware resources. They are leaders in terms of RAM efficiency, which is suitable for systems with limited resources. In addition, these switches demonstrate the highest level of scalability, making them effective for large distributed environments. On the other hand, HVVS is the easiest to configure, making it a good choice for small teams or environments with minimal specialisation requirements. For distributed networks or SDN environments, JCVR or OCR should be considered due to their high scalability.

OVS, CNV, and VMS were chosen because of their popularity, versatility, and wide integration into various network configurations. They are the standard for many organisations due to their proven efficiency and ease

of use. At the same time, VPP and BVS switches achieve the best technical performance. The VPP is the leader in terms of throughput and low CPU load, while the BVS provides the lowest latency. JCVR and OCR have the highest scalability, which is best suited for distributed and cloud environments.

DISCUSSION

The results of the study showed that the choice of a virtual switch depends on the specific requirements of the network configuration, as each switch has its own advantages and limitations in terms of performance, scalability, and integration in different environments. S. Rush (2020) focused on the use of virtual switches in automotive systems to replace physical components, in particular in the context of functional safety and network security. Compared to the current study, which focuses on comparing the performance of virtual switches in networks of different configurations, the aforementioned study focuses on specific applications in automotive systems. Therefore, this study covers more general networking solutions for virtualised environments. In addition, A. Alnaim (2024) focused on the security of virtual networks in the context of 5G, emphasising the importance of ensuring the security of virtual networks through the flexibility of virtual functions. Whereas the current study focuses on analysing the performance of virtual switches for different network configurations, other work focuses on the security of virtualised systems. Thus, the current work complements A. Alnaim (2024) research by focusing on switch performance and integration into different environments where security is an important consideration.

The authors O.G. Lira *et al.* (2024) focused on automating the network configuration process by using large language models to generate and verify settings with minimal human involvement. Whereas the current work analyses the performance of virtual switches, the results of the above researchers focus on the automation of network configurations. Therefore, the current study complements the approach of the above work by emphasising the importance of switch performance and its integration into different network environments. Meanwhile, Y. Wang *et al.* (2018) analysed the optimisation of hash tables for flow classification in virtual switches, which is an important component of network efficiency, in particular in the context of SDN. However, the current study focuses on the performance of switches, while the above work on hash tables focuses more on the theoretical aspects of flow classification and hash table optimisation to improve switch performance. The results of the present study extend this by considering not only optimisation but also a practical comparison of different virtual switches for different types of network configurations.

In turn, P.M. Rekha & M. Dakshayini (2015) focused on managing virtual networks with SDN and using the OpenFlow architecture to improve QoS in cloud data centres. Similar to the current work, these researchers focus on configuring virtual switches to optimise network performance, and analyse the role of SDN and OpenFlow in the context of network efficiency. However, their approach is more focused on QoS management in a multi-user environment, while the current study focuses on comparing switch performance for different types of network configurations. Therefore, the current study complements the aforementioned work by considering the broader aspects of virtual switch integration and network performance in different environments. Regarding the work of C. Wang *et al.* (2024), they investigated the use of large language models to simplify the configuration of network devices and the development of routing algorithms, minimising errors due to the translation of high-level policies and requirements into low-level network configurations. Compared to the current research, which focuses on analysing the performance of virtual switches in different networks, the study of language models focuses on automating configurations using artificial intelligence. Therefore, this study complements the work of these authors by focusing on the efficiency of switches and their integration into various network configurations.

On the other hand, V.K. Tchendji *et al.* (2018) focused on the use of virtual switches to increase the resilience of virtual networks to failures by proposing traffic redirection schemes to ensure QoS. This work examines the effectiveness of virtual switches, but focuses on solutions for network recovery in the event of a failure. Similarly, the current work analyses the performance of switches in different network configurations, which also demonstrates the importance of virtual switches in ensuring network efficiency and reliability. Thus, the study confirms the conclusions of these authors, emphasising the importance of virtual switches for network scalability and stability. Additionally, S. Sadrhaghighi *et al.* (2022) presented Open Virtual Tap (OVT), which uses OpenFlow switches to monitor traffic in virtual networks, focusing on the efficiency of flow mirroring. In the current study, OpenFlow is considered as a management protocol in OVS, providing flexibility and centralised traffic management in SDN. Thus, OpenFlow is a common aspect of both works, but the current work focuses on switch performance, while the authors of the other work investigated its role in traffic analysis.

The results of the study by Z. Guo *et al.* (2023) presented ConfigReco, a configuration recommendation tool that uses graph neural networks to create templates based on the network operator's intentions. The difference from the current study is the emphasis on automating manual configuration, as the work in this paper focuses on analysing the performance of virtual switches in different network environments. Both approaches complement each other, as ConfigReco provides templates for efficient network configuration, which can be applied to virtual switches to optimise

their integration into networks. In addition, L. Zhu *et al*. (2020) investigated the effectiveness of SDN controllers, particularly in the context of specialised networks such as IoT and blockchain, and compared their performance across different networks. In contrast, the current work focuses on the effectiveness of virtual switches such as OVS, VMS, and CNV, as well as their integration with different networks. In other words, this study complements the aforementioned work by extending their findings by comparing the performance of switches in the context of different network configurations and virtualisation.

For their part, I. Alam *et al*. (2020) focused on the integration of SDN and NFV for IoT, analysing their architecture, security, and management, with a focus on IoT challenges. They also highlighted key issues such as scalability and flexibility. Similarly, current work has looked at the use of SDN and NFV, specifically through virtual switches, namely OVS and CNV, to provide scalability, security, and performance in virtualised environments. Hence, the current work focuses more on the performance of specific virtual switches in different network configurations, including telecoms, IoT and 5G, which is an extension of the second study. The authors D. Bringhenti *et al*. (2023) proposed a method for automating firewall configuration in virtualised networks to improve security by reducing the number of firewalls and configuration settings required. Their approach focuses on optimising network security by minimising configuration errors. The current work focuses on virtual switch configurations, particularly in the context of traffic management, scalability, and security. This work has the advantage of evaluating not only security, but also performance and scalability, which is critical for environments with high traffic and resource requirements, such as data centres and 5G networks.

As for the work of J.V.G. de Oliveira *et al*. (2021), they proposed the implementation of NFV as programmable rules distributed among SDN switches to improve performance and scalability in packet-intensive environments. Compared to the current study, which focuses on comparing switch performance, the work of the above researchers focuses on combining hardware and software SDN switches to optimise processing speed and instantiation flexibility. This approach complements the current study by increasing the performance and scalability of virtual networks under high traffic loads. In turn, K. Marzuki *et al*. (2023) focused on the use of OVS in the context of Proxmox to manage traffic between virtual machines and external communications using VLANs. The study focused on automating virtual network configuration with Ansible, which reduces configuration time and human error. The current study also examined OVS, but focused on its performance and capabilities in the context of scalability and efficiency of virtual switches in network configurations. In addition, various aspects of virtual switches such as throughput, latency, and resource utilisation were compared, providing a deeper understanding of the functional features of OVS compared to other switches such as CNV and VMS.

A. Singh (2019) looked at CNV as a virtualisation solution targeting VMware environments, with a particular focus on automating the management of VEM and VSM components through the Python API, which significantly reduces manual intervention. The current study also analysed CNVs, but in a broader context. It not only investigated the management features of this switch, but also compared its performance, latency, resource utilisation, and scalability with other popular virtual switches. This made it possible to formulate comprehensive recommendations for choosing the optimal solution depending on the specifics of the network environment, making the approach of the current study more universal. Moreover, A. Abdou *et al*. (2018) and L. Patrão (2024) focused on a basic overview of VMware vSphere, its functionality, and basic concepts such as the differences between vSphere and ESXi hosts.

Compared to other works, the current study focuses on a detailed performance analysis of popular virtual switches and compares them. The uniqueness of the work lies in the emphasis on practical comparison of different switches in the context of different network scenarios, making it an addition to existing virtualisation and network management approaches.

CONCLUSIONS

The study identified the optimal virtual switches for different network configurations depending on key technical parameters. In particular, it was found that CNV provides the best performance with low latency (0.5-2 ms) and a high level of integration, making it optimal for environments with critical speed and reliability requirements. OVS proved to be highly efficient with scalability, up to 9 Gbps throughput, and moderate CPU usage, which is suitable for scalable virtualised environments. VMS has shown good integration into VMware environments with 6-8 Gbps bandwidth. The highest throughput (20-50 Gbps) was demonstrated by Virtual Packet Processing, making it the best choice for environments with high bandwidth requirements, while Bridge Virtual Switch has the lowest CPU load (5-10%). Other switches, such as Juniper Contrail Virtual Router and Huawei CloudEngine vSwitch, performed satisfactorily for environments with lower scalability requirements.

Limitations include the lack of testing of switches on platforms with Advanced Risc Machines processors, which are becoming increasingly popular in cloud and embedded solutions due to their energy efficiency. In addition, the study did not analyse switch performance in HPC environments, which could have yielded a wider range of results. And the sample of switches selected was limited to popular and less popular solutions, while there are other models that may also be important for specialised environments.

To improve the efficiency of virtual switches in different environments, it is advisable to focus on expanding the analysis of their integration with technologies such as next-generation networks that require low latency and high throughput. Tests on energy-efficient processors of the Advanced Risc Machines architecture will help determine their effectiveness in resource-constrained environments. Additionally, it is important to develop standardised benchmarking methodologies to take into account the specific requirements of different network configurations, which will allow for the creation of optimal solutions for specialised environments such as IoT or HPC.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Abdou, A., van Oorschot, P.C., & Wan, T. (2018). Comparative analysis of control plane security of SDN and conventional networks. *IEEE Communications Surveys & Tutorials*, 20(4), 3542-3559. doi: 10.1109/COMST.2018.2839348.

[2] Ahmmed, F., Rahman, A., Hossain Emon, M., & Rahman Enam, M. (2024). Enhancing energy efficiency in wireless sensor networks using virtual MIMO technology. *Global Mainstream Journal of Innovation, Engineering & Emerging Technology*, 3(2), 27-42. doi: 10.62304/jieet.v3i02.93.

[3] Alam, I., Sharif, K., Li, F., Latif, Z., Karim, M.M., Biswas, S., Nour, B., & Wang, Y. (2020). A survey of network virtualization techniques for Internet of Things using SDN and NFV. *ACM Computing Surveys*, 53(2), article number 35. doi: 10.1145/3379444.

[4] Alnaim, A.K. (2024). Securing 5G virtual networks: A critical analysis of SDN, NFV, and network slicing security. *International Journal of Information Security*, 23(6), 3569-3589. doi: 10.1007/s10207-024-00900-5.

[5] Bringhenti, D., Marchetto, G., Sisto, R., Valenza, F., & Yusupov, J. (2023). Automated firewall configuration in virtual networks. *IEEE Transactions on Dependable and Secure Computing*, 20(2), 1559-1576. doi: 10.1109/TDSC.2022.3160293.

[6] Bueno, G., Saquetti, M., Rodrigues, P., Lamb, I., Gaspary, L., Luizelli, M.C., Zhani, M.F., Azambuja, J.R., & Cordeiro, W. (2022). Managing virtual programmable switches: Principles, requirements, and design directions. *IEEE Communications Magazine*, 60(2), 53-59. doi: 10.1109/MCOM.001.2100363.

[7] CloudEngine 1800V virtual switch. (2018). Retrieved from https://carrier.huawei.com/~/media/CNBG/Downloads/Product/Fixed%20Network/b2b/0920/1800-en.pdf.

[8] Configuring AutoScale with using CloudStack virtual router. (n.d.). Retrieved from https://docs.cloudstack.apache.org/en/4.19.1.3/adminguide/autoscale_with_virtual_router.html.

[9] Contrail Networking and Security User Guide. (2023). Retrieved from https://www.juniper.net/documentation/us/en/software/contrail-networking19/contrail-networking-security-user-guide/contrail-networking-security-user-guide.pdf.

[10] De Oliveira, J.V.G., Bellotti, P.C.P., de Oliveira, R.M., Borges Vieira, A., & Chaves, L.J. (2021). Virtualizing packet-processing network functions over heterogeneous OpenFlow switches. *IEEE Transactions on Network and Service Management*, 19(1), 485-496. doi: 10.1109/TNSM.2021.3112403.

[11] Detecting bottlenecks in a virtualized environment. (2022). Retrieved from https://learn.microsoft.com/en-us/windows-server/administration/performance-tuning/role/hyper-v-server/detecting-virtualized-environment-bottlenecks.

[12] Dumitrak, V. (2020). *Methods and means of increasing the efficiency of implementing virtualisation of network functions in modern network infrastructures*. (Master's dissertation, Ternopil Ivan Puluj National Technical University, Ternopil, Ukraine).

[13] Guo, Z., Li, F., Shen, J., Xie, T., Jiang, S., & Wang, X. (2023). ConfigReco: Network configuration recommendation with graph neural networks. *IEEE Network*, 38(1), 7-14. doi: 10.1109/MNET.2023.3336239.

[14] Lira, O.G., Caicedo, O.M., & da Fonseca, N.L.S. (2024). Large language models for zero touch network configuration management. *ArXiv*. doi: 10.48550/arXiv.2408.13298.

[15] Lucas-Estañ, M.C., Coll-Perales, B., Khan, M.I., Gozalvez, J., Avedisov, S.S., Altintas, O., & Sepulcre, M. (2024). 5G network architecture and configuration choices to support teleoperated driving at scale. In *Proceedings of the 100th vehicular technology conference* (pp. 1-6). Washington: IEEE. doi: 10.1109/VTC2024-Fall63153.2024.10758026.

[16] Marzuki, K., Kholid, M.I., Hariyadi, I.P., & Mardedi, L.Z.A. (2023). Automation of open VSwitch-based virtual network configuration using ansible on Proxmox virtual environment. *International Journal of Electronics and Communications Systems*, 3(1), 11-20. doi: 10.24042/ijecs.v3i1.16524.

[17] Mehta, R. (2015). *Network improvements in vSphere 6 boost performance for 40G NICs*. Retrieved from https://surl.li/pmnzmm.

[18] Olifirenko, R. (2021). *An improved way of NFV hypervisor functioning in SDN networks*. (Bachelor's dissertation, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine).

[19] OpenContrail vRouter. (2024). Retrieved from https://docs.mirantis.com/mcp/q4-18/mcp-ref-arch/opencontrail-plan/contrail-vrouter.html.
[20] Patrão, L. (2024). *VMware vSphere essentials: A practical approach to vSphere deployment and management*. Berkeley: Apress. doi: 10.1007/979-8-8688-0208-9.
[21] Pfaff, B., *et al.* (2015). The design and implementation of open vSwitch. In *Proceedings of the 12th USENIX symposium on networked systems design and implementation* (pp. 117-130). Oakland: USENIX.
[22] Poller, J. (2017). *Big switch networks and Dell EMC: Next-generation data center networking*. Retrieved from https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/ESG-Lab-Review-Big-Switch-and-Dell-April-2017.pdf.
[23] Rashelbach, A., Rottenstreich, O., & Silberstein, M. (2022). Scaling open vSwitch with a computational cache. In *Proceedings of the 19th USENIX symposium on networked systems design and implementation* (pp. 1359-1374). Renton: USENIX.
[24] Rekha, P.M., & Dakshayini, M. (2015). Dynamic network configuration and virtual management protocol for open switch in cloud environment. In *Proceedings of the international advance computing conference* (pp. 143-148). Bangalore: IEEE. doi: 10.1109/IADCC.2015.7154687.
[25] Rush, S. (2020). Virtual switches and indicators in automotive displays. *SAE International Journal of Advances and Current Practices in Mobility*, 2(4), 2418-2424. doi: 10.4271/2020-01-1362.
[26] Sadrhaghighi, S., Dolati, M., Ghaderi, M., & Khonsari, A. (2022). Monitoring OpenFlow virtual networks via coordinated switch-based traffic mirroring. *IEEE Transactions on Network and Service Management*, 19(3), 2219-2237. doi: 10.1109/TNSM.2022.3149734.
[27] Singh, A. (2019). *Development of Python API for a network switch*. (Bachelor's dissertation, Jaypee University of Information Technology Waknaghat, Waknaghat, India).
[28] Tchendji, V.K., Yankam, Y.F., & Myoupo, J.F. (2018). Conflict-free rerouting scheme through flow splitting for virtual networks using switches. *Journal of Internet Services and Applications*, 9(1), article number 13. doi: 10.1186/s13174-018-0085-4.
[29] Vector Packet Processing. (n.d.). Retrieved from https://www.netgate.com/resources/articles-vector-packet-processing.
[30] Wang, C., Scazzariello, M., Farshin, A., Ferlin-Reiter, S., Kostic, D., & Chiesa, M. (2024). NetConfEval: Can LLMs facilitate network configuration? *Proceedings of the ACM on Networking*, 2, article number 7. doi: 10.1145/3656296.
[31] Wang, K., Zhao, C., Chu, J., Shi, Y., Lu, J., Lyu, B., Zhu, S., Cheng, P., & Chen, J. (2024). LFVeri: Network configuration verification for virtual private cloud networks. *IEEE/ACM Transactions on Networking*, 32(6), 5475-5490. doi: 10.1109/TNET.2024.3469386.
[32] Wang, Y., Gobriel, S., Wang, R., Tai, T.-Y.C., & Dumitrescu, C. (2018). Hash table design and optimization for software virtual switches. In *Proceedings of the 2018 afternoon workshop on Kernel bypassing networks* (pp. 22-28). New York: Association for Computing Machinery. doi: 10.1145/3229538.3229542.
[33] Wang, Y., Wang, X., Huang, Z., Li, W., & Xu, S. (2022). Joint optimization of dynamic resource allocation and packet scheduling for virtual switches in cognitive internet of vehicles. *EURASIP Journal on Advances in Signal Processing*, 2022, article number 32. doi: 10.1186/s13634-022-00862-7.
[34] Yalda, K., Hamad, D.J., & Tapus, N. (2024). Comparative analysis of centralized and distributed SDN environments for IoT networks. *Journal of Control Engineering and Applied Informatics*, 26(3), 84-91. doi: 10.61416/ceai.v26i3.9164.
[35] Yang, Y., Guo, S., Liu, G., & Yi, L. (2021). Fine granularity resource allocation of virtual data center with consideration of virtual switches. *Journal of Network and Computer Applications*, 175, article number 102916. doi: 10.1016/j.jnca.2020.102916.
[36] Zhu, L., Karim, M., Sharif, K., Xu, C., Li, F., Du, X., & Guizani, M. (2020). SDN controllers: A comprehensive analysis and performance evaluation study. *ACM Computing Surveys*, 53(6), article number 133. doi: 10.1145/3421764.

Порівняльний аналіз різних віртуальних комутаторів для підвищення ефективності функціонування мереж різної конфігурації

Олександр Берестовенко
Аспірант
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
03056, просп. Берестейський, 37, м. Київ, Україна
https://orcid.org/0000-0003-4887-4674

Анотація. Мета роботи полягала у визначенні оптимального типу віртуального комутатора для забезпечення максимальної ефективності роботи комп'ютерних мереж різних конфігурацій, з огляду на їхні технічні характеристики, можливості та рівень інтеграції. Було проведено порівняльний аналіз продуктивності та функціональних можливостей віртуальних комутаторів. Основні результати показали, що Cisco Nexus 1000V забезпечує відмінну продуктивність та низьку затримку (0,5-2 мілісекунд), що робить його ідеальним для середовищ, де критичні швидкість та реакція мережі. Open vSwitch характеризується високою масштабованістю і ефективним використанням пам'яті, з пропускною здатністю до 9 гігабіт на секунду і помірним використанням процесора, що робить його підходящим для масштабованих віртуалізованих середовищ. VMware vSwitch, із пропускною здатністю 6-8 гігабіт на секунду, має хорошу інтеграцію у середовище VMware та зручне налаштування. Більше того, виявлено, що Virtual Packet Processing забезпечує найкращу пропускну здатність, досягаючи значень від 20 до 50 гігабіт на секунду, а також демонструє низьку затримку в межах 0,3-0,5 мілісекунд, що робить його оптимальним вибором для середовищ із високими вимогами до пропускної здатності. У той самий час, Bridge Virtual Switch має найменше навантаження на процесор (5-10 %), що дозволяє зберігати продуктивність навіть за обмежених апаратних ресурсів. Інші комутатори, а саме Hyper-V Virtual Switch, Juniper Contrail Virtual Router, CloudStack Virtual Router та Huawei CloudEngine vSwitch продемонстрували хорошу ефективність і можуть бути корисними для середовищ з меншими вимогами до пропускної здатності та масштабованості. Отримані результати показали, що вибір віртуального комутатора залежить від специфічних вимог, оскільки кожен комутатор має свої переваги та обмеження, що визначають його оптимальність для різних мережевих конфігурацій

Ключові слова: пропускна здатність; масштабованість компонентів; інтеграція та продуктивність систем; обробка даних; зниження затримок

BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en

Vol. 29 No. 4. 2024

UDC 004.5:004.032.26
DOI: 10.62660/bcstu/4.2024.21

Optimisation of intelligent system algorithms for poorly structured data analysis

Mykola Demchyna*
PhD in Technical Sciences, Associate Professor
King Danylo University
76018, 35 Ye. Konovalets Str., Ivano-Frankivsk, Ukraine
https://orcid.org/0009-0002-9161-4843

Taras Styslo
Senior Lecturer
King Danylo University
76018, 35 Ye. Konovalets Str., Ivano-Frankivsk, Ukraine
https://orcid.org/0000-0002-2377-7985

Serhii Vashchyshak
PhD in Technical Sciences, Associate Professor
King Danylo University
76018, 35 Ye. Konovalets Str., Ivano-Frankivsk, Ukraine
https://orcid.org/0000-0002-1753-1540

Abstract. Integration of heterogeneous types of medical data using modern deep learning methods can improve the accuracy and efficiency of diagnosing complex diseases, such as cardiovascular diseases, which is relevant for personalised medicine and reducing the risk of medical errors. The study aimed to present the development of a decision support system for improving the diagnosis of cardiovascular diseases by integrating heterogeneous types of medical data. To create the knowledge base, data from real clinical scenarios were used, which underwent the stages of cleaning, standardisation, and semantic analysis using specialised medical dictionaries. The system demonstrated high efficiency due to its ability to integrate text, image and signal data into a single analysis process. The efficiency was evaluated by such metrics as accuracy, completeness, F1-score, and predictive values of positive and negative results. The introduction of transformers ensured a 15% increase in diagnostic accuracy compared to traditional methods, and the use of a hybrid computing approach reduced model training time by 30% and enabled the processing of up to 1 TB of data per day. Additionally, the integration of heterogeneous types of medical data into the system has improved the personalisation of diagnostics, accounting for individual patient characteristics such as medical history, genetic factors, or comorbidities. Transformer attention mechanisms improved resistance to noise and data gaps, which ensures reliable results even with incomplete or inaccurate information. Optimisation of the models reduced delays in data processing, which is critical for prompt clinical decision-making. In addition, transformers have proven their ability to dynamically scale to process new types of data without losing efficiency, opening opportunities

Article's History: Received: 16.07.2024; Revised: 11.10.2024; Accepted: 16.12.2024.

Suggested Citation:
Demchyna, M., Styslo, T., & Vashchyshak, S. (2024). Optimisation of intelligent system algorithms for poorly structured data analysis. *Bulletin of Cherkasy State Technological University*, 29(4), 21-31. doi: 10.62660/bcstu/4.2024.21.

*Corresponding author

for further expansion of the system's functionality. The system has also increased the productivity of clinical specialists by automating routine tasks, allowing doctors to focus on more complex aspects of treatment

Keywords: artificial intelligence; knowledge base; decision support; neural networks; knowledge mining; classification algorithms; adaptive systems

INTRODUCTION

Modern medicine is facing increasing challenges in analysing large volumes of unstructured data, including text-based physician notes, medical imaging, and signal data. Traditional approaches to processing such information are often ineffective due to the limited ability to integrate heterogeneous data types into a single analysis process. This limits the accuracy of diagnosis and the speed of clinical decision-making, especially in the context of complex diseases such as cardiovascular disease.

The integration of artificial intelligence (AI) and neural networks in medicine creates new opportunities for improving the quality of diagnosis and treatment. Modern neural network architectures, such as multilayer perceptron (MLP), recurrent neural networks (RNN), convolutional neural networks (CNN), and transformers, improve the efficiency of various data format processing. The use of transformers with attention mechanisms enables complex pattern detection between text, image, and signal data, which is critical for medical research. The study by J. Meng & Z. Wang (2022) proposes a model that integrates transformer and RNN mechanisms to better understand the context of words and phrases, achieving an 18% increase in classification accuracy. Transformers provide a deeper analysis of long-term dependencies between words, while RNNs efficiently process text sequences, considering the local context. This combination not only increases the classification accuracy but also improves the model's ability to work with heterogeneous text data containing complex semantic relationships.

Z. Shen (2023) addressed the optimisation of data visualisation platforms based on Artificial Intelligence (AI). In particular, the study described approaches to interactive data analysis in real-time, which can reduce rendering time by 25%. The study emphasised the use of adaptive algorithms for processing large amounts of data, which ensures the smooth operation of platforms and their ability to scale. The study also emphasised the importance of integrating different data sources and applying effective methods to reduce computational costs, which is critical to ensuring the high performance of systems in real-time. D. Kushnir *et al.* (2021) analysed the use of deep neural networks for semantic text analysis. The main idea is to integrate vector representation of words (word embeddings) with transformers for natural language analysis. The results show that the model provides a 12% increase in text classification accuracy compared to classical machine learning methods.

The review analysis by C. Gambella *et al.* (2021) covered modern optimisation problems in machine learning. The authors reviewed methods for optimising hyperparameters, ways to avoid overfitting problems, and an approach to model selection. Improvement of the computational efficiency of algorithms, which can significantly reduce model training time without losing accuracy, was also prioritised. In addition, the authors analysed the role of hybrid computing approaches that combine local and cloud resources to ensure the scalability and adaptability of machine learning. The study emphasised the importance of integrating heterogeneous data and using transformative architectures to improve the accuracy of analysis and stability of models in different environments.

A. Wilson & M.R. Anwar (2024) discussed adaptive machine learning algorithms for processing multivariate data. A new approach to data dimensionality reduction using stochastic methods was proposed, which significantly reduces computation time without loss of accuracy. The process of integrating neural networks for analysing poorly structured data was emphasised. Three types of architectures were compared: multilayer perceptron (MLP), recurrent neural networks (RNN), and transformers. MLPs were used to process structured data, such as test results, RNNs were used to analyse text records, while transformers provided image processing and integration with other data. The results showed that transformers had the highest accuracy in diagnosis, outperforming traditional methods by 15%, while RNNs demonstrated significantly better text processing compared to other approaches.

N. Abbas & S. Gasmi (2024) analysed in detail the approaches to optimising machine learning algorithms, in particular for natural language processing and text analytics. The authors addressed the development of efficient methods for processing streaming data in real-time, which is critical in modern dynamic information systems. The main goal of the study was to improve the performance of algorithms by reducing delays in data processing and optimising the use of computing resources. T.B. Brown *et al.* (2020) analysed natural language processing models that can perform tasks with a minimum number of examples (few-shot learning). The authors demonstrated how large language models, such as GPT-3, can adapt to new tasks without the need for large amounts of training data. The key task was to optimise the resources required to process large amounts of data without losing the accuracy of the results. For this purpose, a hybrid learning methodology that combines local data processing with cloud computing was used. A detailed analysis of the system performance was conducted: the model training time was reduced by 30% due to parameter optimisation, and the

use of cloud computing resources allowed processing up to 1 terabyte of data per day.

The study aimed to develop and evaluate the effectiveness of a decision support system (DSS) for medical diagnoses that integrated heterogeneous data types to improve the accuracy of cardiovascular disease diagnosis. As part of the study, a knowledge base was created that included data from real clinical scenarios that went through the stages of cleaning, standardisation and semantic analysis. The development of a methodology for data integration and neural network optimisation was emphasised.

MATERIALS AND METHODS

The research was based on the development of a decision support system (DSS) for medicine that can integrate heterogeneous types of medical data. For this purpose, a knowledge base was created that includes information from various sources: textual records of doctors, laboratory data, computed tomography (CT) images and electrocardiographic (ECG) signals. Ethical approval covered all aspects of the study, including procedures for data collection, processing, analysis and storage. The Ethics Committee reviewed whether the study met ethical standards, including the informed consent of patients (if required) or the appropriate legal basis for using anonymised data. This correlated with the principles stipulated in the World Medical Association's Declaration of Helsinki (1964), the Law of Ukraine No. 2297-VI (2010), and the European General Data Protection Regulation (GDPR) (2016). All the steps were designed to comply with the principles of transparency, responsibility and security of data processing. Particular attention was devoted to standardisation of text data, which was processed using natural language processing (NLP) methods such as tokenisation, text normalisation and semantic analysis using specialised medical dictionaries.

Different neural network architectures were used to integrate the data into the system, with appropriate optimisation algorithms to ensure that each model was trained efficiently. Multilayer Perceptron (MLP) was used to analyse structured data such as laboratory parameters. The Adaptive Moment Estimation (AdamW) algorithm was used to train this model, which provides fast convergence and stability when dealing with structured numerical data. Recurrent neural networks (RNNs) were used to process sequential text records, such as medical reports, to allow for context. For this model, the RMSprop algorithm was used, which works well with sequential data and avoids the problem of exploding or disappearing gradients typical of RNNs. Transformers were used to integrate text, image, and signal data. Attention mechanisms detected complex patterns between heterogeneous data. They were trained using the AdamW algorithm (adaptive optimisation with weight decay), which reduces the risk of over-computing gradients and improves regularisation, which is critical when working with large datasets and complex architectures. Convolutional Neural Networks (CNNs) were used to analyse medical images, in particular CT images. For their optimisation, the SGD (Stochastic Gradient Descent) algorithm with momentum was used, which provides high efficiency in computer vision tasks such as image classification and segmentation. Both RNNs and transformers were used to process ECG signals. The RNNs used the RMSprop algorithm, which improved the efficiency and consistency of physiological data, while the transformers were trained using AdamW, ensuring stable convergence and reducing the risk of overfitting.

These optimisation algorithms were carefully selected following the specifics of the data being processed and the architecture of the neural network. This was used to achieve high efficiency and accuracy of the system, ensuring high-quality integration of text, image and signal data within a single analytical process. The study results were evaluated using a sample from the control set of patients whose data were not used during the model training phase. This limited overtraining and ensured the independence of the evaluation. The sample included cases with varying degrees of complexity, covering mild, moderate and severe forms of disease, to represent the full range of clinical scenarios. To increase the objectivity of the assessment, heterogeneity of the data, including textual records of doctors, images of medical examinations (e.g., CT scans), electrocardiographic (ECG) signals and laboratory indicators, were prioritised. Additionally, proportionality in terms of age and gender characteristics of patients was addressed to avoid bias in statistical results, as well as comorbidities that could complicate diagnosis. All patient data was anonymised, in compliance with ethical principles and legal standards, such as the Law of Ukraine No. 2297-VI (2010) and the European General Data Protection Regulation (GDPR) (2016). This ensured the legality and transparency of the information collection and analysis process. This approach ensured the most objective assessment of the effectiveness of the developed system.

To evaluate the system's performance, the models were benchmarked using metrics such as accuracy, recall, F1-score, and clinically relevant indicators such as the positive predictive value (PPV) and negative predictive value (NPV). The models were trained on large volumes of labelled data, which ensured high diagnostic accuracy. In addition, the computational efficiency of the developed system was evaluated, including model training time and performance when processing large data sets. To optimise computational costs, a hybrid approach was used, combining local computing and scaling in the cloud environment.

RESULTS

The first step was to evaluate the effectiveness of traditional approaches such as individual MLP architectures that provided intermediate results when analysing

structured data, such as laboratory results. Such approaches proved to be useful in cases where the information was clearly structured and easily formalised. However, during the processing of contextual factors (e.g., the sequence of textual notes from doctors describing a patient's medical history) or the complex structure of image data, the accuracy of MLP models was not high enough. RNN architectures were more efficient at analysing text containing descriptions of symptoms, doctors' opinions, and recommendations. Due to the memory mechanism and the ability to account for the temporal sequence, RNN models demonstrated better completeness, and F1-score compared to MLPs when processing text data. However, their ability to integrate different types of data and consider images or signals remained limited, as RNNs mainly focused on sequential text input.

The use of transformers has become a key step towards achieving the highest performance. Due to their attention mechanisms, transformers can identify relevant pieces of information in different types of data, compare them with each other, and build complex links between medical records, CT images, and ECG signals (Zhang *et al.*, 2024). Experiments have shown that transformative architectures can achieve 15% higher accuracy than traditional methods that work with only one type of data or combine data less efficiently. This result suggests that transformers can detect complex patterns that other models have failed to capture. This is especially important for medical diagnostics, where even small correlations between different indicators can be critical. Table 1 illustrates the accuracy, precision, recall, and F1-score scores for the three main types of neural models: MLPs, RNNs, and Transformers.

Table 1. Comparison of the efficiency of different neural network architectures for the diagnosis of cardiovascular diseases

Architecture	Accuracy	Precision	Recall	F1-score
MLP	0.82	0.79	0.80	0.795
RNN	0.87	0.85	0.84	0.845
Transformers	0.95	0.93	0.92	0.925

Source: compiled by the authors

Following Table 1, the MLP architecture has the lowest results among the models considered. This can be attributed to the fact that multilayer perceptrons are effective with structured data but lose efficiency in situations where it is necessary to integrate information from different sources. RNN architectures have significantly improved the accuracy and completeness rates compared to MLPs by processing textual data in a consistent form, which allows for a better understanding of the contextual information available in medical history. However, the limitations of RNNs in simultaneously integrating complex visual and signal characteristics did not allow them to achieve transformer-like performance.

Transformer architectures proved to be the leaders across the board. Their ability to accommodate different data formats and identify complex relationships between them allowed them to significantly exceed the accuracy achieved by other models. In addition, transformers ensured that the results remained stable even when new data types were included or updated. This approach is especially important for medical applications where examination protocols may change periodically, or new research methods may appear. Given the above results, it is possible to argue that transformers are best suited to the needs of complex medical diagnostics, as they provide the most accurate and reliable results when working with heterogeneous, poorly structured data.

A critical aspect of medical diagnostics is not only the accuracy but also the speed of results. In situations where a clinical decision needs to be made within a limited time, it is also important to evaluate the performance of the models, i.e., their ability to learn quickly and process large amounts of information. To this end, a detailed analysis of training time and computational costs for different architectural approaches was conducted. The experiment considered both local computing resources and the cloud infrastructure, which made it possible to scale the load and ensure the processing of up to 1 TB of data per day. As a result of optimising hyperparameters and applying a hybrid computing approach, model training time was reduced by 30% compared to standard methods that relied solely on local resources or did not use optimisation strategies. Table 2 illustrates the average model training time on a benchmark dataset (approximately 500 GB), as well as the amount of data that can be processed per day after optimisation. Table 2 shows the results for MLP, RNN, and transformers, addressing the use of hybrid infrastructure.

Table 2. Computational efficiency of different neural network architectures in medical data processing

Model	Learning time (hours)	Processing volume per day (GB)
MLP	10	600
RNN	12	700
Transformers	7	1,000

Source: compiled by the authors

Table 2 shows that MLP models were trained relatively quickly, but their limited ability to integrate complex data negatively affected the final accuracy and usefulness in a clinical context. RNNs require more time to learn due to the processing of sequential information and context-preservation mechanisms. However, even with longer training times, RNNs did not reach the accuracy of transformers. In turn, the transformers proved to be optimal not only in terms of accuracy but also in terms of computational efficiency, as their training time was only 7 hours on average, and the implemented hybrid infrastructure allowed processing up to 1 TB of data per day, which is 30% faster than previous approaches. Such computational optimisation is extremely important as modern medical systems generate large amounts of data, and their prompt processing is one of the key conditions for timely diagnosis.

The quick large amounts of data processing, combined with the high accuracy of transformational models, means that the developed DSS can provide reliable results in real-time or close to it. This significantly increases the value of the system for medical practice, as clinicians can make complex diagnostic decisions quickly and confidently. For example, in the case of suspected acute cardiac conditions such as myocardial infarction, a timely and accurate diagnosis can save a patient's life by allowing them to start appropriate treatment immediately. While traditional methods require several hours to analyse a complex data set, the new system, thanks to transformers and a hybrid computing approach, can provide a preliminary decision much faster. In addition to time and computational aspects, an important criterion for the system's effectiveness is the ability to integrate and analyse different types of medical data simultaneously. To confirm this, additional experiments were conducted to evaluate the diagnostic accuracy when new sources of information were added sequentially. Initially, only textual records of medical histories were used, then laboratory values were added, and then CT scans and ECG signals were connected. The results showed that the transformers demonstrated a steady improvement in accuracy and F1-score with each new type of data. This means that the model is not "overloaded" with additional information, but rather successfully forms interconnections, improving the quality of its predictions. For a medical diagnostic system, this result is extremely valuable, as it confirms that the introduction of new data sources (e.g., new types of visual examinations or more accurate sensory signals) will allow the model to dynamically improve its estimates without the need for a fundamental rebuilding of the entire architecture.

In medical practice, it is necessary to account for individual patient characteristics, such as pre-existing conditions, and reactions to certain drugs or genetic markers. With transformers, the model was able to focus on key segments of medical data relevant to a particular patient. This became apparent when analysing cases with atypical symptoms or comorbid conditions when traditional methods or simpler neural network models could not detect hidden patterns. Transformational architectures, on the contrary, can identify unique patterns and form more accurate and personalised diagnostic recommendations based on them. This confirms the importance of this approach for the development of personalised medicine, as more accurate diagnostics pave the way for better and more individually tailored treatment regimens, reducing the risk of inadequate therapy and side effects. In addition, the analysis of the results shows that the introduction of transformers contributes to greater resilience of the system to noise and data errors. Medical data often has a heterogeneous structure, containing not only different formats but also different quality. For instance, doctors' text records may contain spelling errors, abbreviations or acronyms, and images may contain shooting artefacts. ECG signals can be interfered with by patient movement or electrical interference. Traditional processing methods are often vulnerable to such distortions and can either ignore or misinterpret some of the information. Transformers, on the other hand, can dynamically determine which parts of the data should be given more attention and which parts can be partially ignored as noise, thanks to their attention mechanisms. This increases the reliability of the system and provides better results even with incomplete or poorly structured data.

In a real-world clinical setting, a medical decision support system must not only be accurate and efficient but also easy to use. The study concentrated mainly on quantitative evaluation of the results but also considered qualitative aspects. For instance, the time taken to complete a diagnostic decision is reduced not only due to faster data processing but also due to the preparation of more generalised and understandable recommendations for doctors. The transformer-based model provided summary information in the form of concise text messages or annotations on images. This allowed clinicians to quickly evaluate the proposed diagnoses and recommendations. This functionality proved to be extremely useful in situations where doctors were faced with many patients and limited time for each of them. Another aspect of practical importance is the scalability of the system. The results showed that the implemented hybrid infrastructure and the use of transformers allow the system to easily adapt to the growth of data or the emergence of new sources of information (Meng & Wang, 2022). Combining transformers with CNN increases the efficiency of integrating text, numeric, and visual data, which is especially important for systems that work with multimodal data in real-time (Zhang *et al.*, 2024).

In modern healthcare facilities, data volumes are growing rapidly as new examination methods are introduced (e.g., fractional imaging analysis, biometric sensors, patient data from smart devices). The ability to scale quickly without losing accuracy is a crucial factor in ensuring the system's long-term relevance and

efficiency. The results confirmed that the proposed architecture is well suited for such conditions, as the models can be updated or retrained on new data sets without significantly reducing the quality of diagnosis. Notably, the introduction of transformers and hybrid computing approaches contributes to better resource utilisation. The optimisation of hyperparameters and adaptive load balancing between local and cloud resources reduced the time and cost of processing without compromising the quality of the results (Nedosnovanyi *et al.*, 2023). This can have significant economic value for healthcare facilities that want to improve diagnostic efficiency without the need for massive investments in new equipment or expensive computer clusters. Instead, by using cloud computing and adapting the system architecture, data processing can be scaled to meet the needs and resources available.

Another important aspect is the system's ability to work with unstructured data, which includes textual notes from doctors, laboratory values, images, and signals. The study results confirmed that the use of deep neural networks significantly improves the analysis of such data. The use of neural networks for semantic text analysis can significantly improve the classification accuracy of poorly structured information (Kushnir *et al.*, 2021). Cognitive computing is also used to effectively analyse unstructured data (Chen *et al.*, 2020). Another aspect of practical importance is the scalability of the system. The implemented hybrid infrastructure makes it easy to adapt to the growth of data volumes or the emergence of new sources of information. The use of AI strategies allows for optimising big data processing in dynamic environments (Oza & Domadiya, 2023; Smetaniuk & Tsisar, 2024).

An important consequence of improved accuracy and speed of data processing is increased confidence in the decision support system. Doctors and other medical professionals need to be confident that the proposed diagnosis is reliable and justified. If the model is highly accurate and stable across different data sets, they will be more willing to use the system in their daily practice. This, in turn, can lead to wider adoption of DSS in the clinical process, increased standardisation of diagnostic decisions, and ultimately improved medical outcomes for patients.

The use of transformers improves the accuracy and speed of data processing but also lays the foundation for further development of medical DSS in the direction of integrating new types of data, improving the interpretation of results and increasing the trust of the medical community. The results obtained confirm that the system can be used in real clinical settings and can contribute to improving the quality of medical services and the processes of diagnosing cardiovascular diseases. Thus, the results of the experiments indicate the high efficiency and prospects of using transformable architectures and hybrid computing approaches in decision support systems for medical diagnostics. Comparison with traditional approaches (MLP, RNN) has demonstrated a significant advantage of transformers in terms of accuracy, completeness, prediction accuracy and F1-score, as well as better computational efficiency and the ability to quickly process large volumes of heterogeneous data. The practical benefit is the ability to significantly reduce diagnostic time, increase the level of treatment personalisation, and provide more reliable and scalable tools for medical practice. The data obtained confirm that the integration of various types of data – text, image, signal and structured – within a single decision support system is quite achievable and brings tangible benefits.

DISCUSSION

The obtained results demonstrate the effectiveness of using transformable architectures and hybrid computing approaches for medical decision support systems (DSS) capable of processing poorly structured data of various natures (text, images, signals). A 15% increase in the accuracy of cardiovascular disease diagnosis compared to traditional methods and a 30% reduction in model training time demonstrate the feasibility of the chosen approach. These results are in line with the general trend in artificial intelligence (AI), machine learning (ML), and natural language processing (NLP) research, where transformers, multitasking learning (MTL), hybrid computing platforms, and hyperparameter optimisation have become key elements in building effective systems.

Numerous studies emphasise the importance of using modern neural architectures and optimisation strategies for processing low-structured data. For instance, I. Malyha & S. Shmatkov (2022) combined word embeddings with multitasking learning, increasing the accuracy of text contextualisation by 15%. This approach is particularly promising for clinical case analysis, where semantic aspects of the text – including contextual nuances and terminological variations – are critical. Considering such works inspires the integration of MTL into the developed system, which can further improve the accuracy of medical record analysis. Similar ideas were expressed by Y. Zhang & Q. Yang (2022), who emphasised the potential of MTL to simultaneously solve several interrelated tasks, such as disease classification, symptom analysis, and complication prediction. The 20-30% increase in model accuracy due to MTL is a strong argument in favour of implementing this approach for medical DSS. This will allow the system to account for the diversity of data, including textual descriptions, images, and signals, by jointly training several complementary objective functions.

G. Zhang *et al.* (2024) demonstrated the benefits of combining transformers and CNNs to integrate textual, visual, and numerical data, which increased the accuracy of analysis by 25%. This integration is particularly relevant for systems that consider CT images of the cardiovascular system, ECG signals, and text records.

The combination of CNNs for image processing with transformers that can integrate text and signal data opens new opportunities for creating complex models that consider all aspects of medical data. A review by R. Rueda *et al.* (2024) analysed the application of machine learning methods for exacerbation detection and clustering in patients with chronic obstructive pulmonary disease (COPD). The authors reviewed approaches to analysing time series and multivariate data to identify precursors of exacerbations and automatically group patients according to the nature of the disease. The paper emphasises the importance of using machine learning to improve the quality of medical care for patients with COPD, focusing on the possibility of early intervention and a personalised approach to treatment. S.V. Mahadevkar *et al.* (2024) addressed the capabilities of transformers and NLP algorithms to analyse poorly structured documents, reducing analysis time by 30%. This is especially important in real-world clinical settings when doctors need prompt recommendations and diagnostic conclusions. Integration of such solutions will ensure faster detection of critical patterns in medical information and timely response to changes in the patient's condition.

The effectiveness of model training depends not only on the choice of architecture but also on the optimal setting of hyperparameters. H. Fatima & S. Gasmi (2023) demonstrated that dynamic tuning of hyperparameters can speed up the learning process by 40% without losing accuracy. The use of such strategies in DSS facilitates faster adaptation of models to new data while reducing overall computational costs. The relevance of this aspect is also confirmed by N.L. Rane *et al.* (2024), where optimised algorithms such as AdamW and Ranger can reduce training time by 15-25% without compromising accuracy.

A critical part of the system's effective operation is scalability and the ability to process large amounts of data in real-time. S. Kumar Rachakatla *et al.* (2023) emphasise that the introduction of AI-oriented approaches and cloud technologies can reduce data processing time by 35% and increase analysis efficiency by 20%. This is of particular importance for the medical DSS, as healthcare systems constantly generate large amounts of information that need to be analysed quickly. Cloud-based infrastructure provides flexibility and scalability, can be used to quickly adapt to the growth of data or the connection of new sources. A hybrid approach to the integration of structured and unstructured data is considered extremely promising. J.G. Turet & A.P.C.S. Costa (2022) proposed an effective combination of different sources of information for public safety systems. Similar methods can be adapted to DSS, including additional clinical databases or new types of signals. D. Baviskar *et al.* (2021) demonstrated the possibilities of automated document processing in the legal and medical fields, which can reduce data processing time by 30%. This highlights the versatility of the proposed approaches and confirms the potential for their scaling to other industries.

The expediency of improving approaches to processing poorly structured data was confirmed by the results of the research by S. Singh & S. Hooda (2023). The study proposes strategies for pre-processing and model adaptation that reduce classification errors by 20%. Optimisation of data analysis workflows can improve the performance of models in real-world conditions. The proposed approaches demonstrate efficiency in working with large amounts of information and ensure the stability of results when integrating new data sources.

The review paper by R. Cong *et al.* (2024) addressed the multidimensional selection of features based on an optimisation strategy for the causal analysis of medical data. The authors proposed an innovative approach to the selection of relevant characteristics that allow for the efficient identification of key variables for analysing relationships in complex medical systems. Particular attention was devoted to the use of optimisation methods to overcome the problem of high-dimensional data, which is typical for medical research. The authors also analysed the impact of various types of noise and missing data on the accuracy of models and proposed strategies to minimise them. In addition, the paper emphasises the importance of interpreting the results for decision-making in clinical practice. The inclusion of adaptive optimisation algorithms not only improved the quality of the analysis but also ensured the flexibility of the system for use in environments with limited computing resources. The study emphasises the potential of a multidimensional approach to improve diagnostic accuracy and treatment effectiveness based on causal models. S. Chen *et al.* (2020) propose cognitive computing to analyse customer information and improve the effectiveness of marketing strategies, which increases by 20%. While this study has a different focus, similar approaches can be applied to analyse patient feedback, optimise clinical services, and improve the quality of care. Lastly, tools that improve the understanding of context and intentions in data have universal value.

The adaptive control systems mentioned by B. Zohuri (2024), which use AI to adapt to changing environmental conditions, can be useful for healthcare facilities. Their application can provide dynamic resource optimisation, improve the stability of medical systems, and allow flexible responses to changing clinical protocols or the emergence of new diagnostic methods. S. Jain *et al.* (2021) investigated deep learning approaches for processing unstructured text data. The proposed transformer architecture for integrating different text formats increases the extraction of key data by 28%, which is especially useful for analysing complex clinical records where important details may be scattered across different parts of the document. This increase in the efficiency of information extraction contributes to faster diagnostic recommendations. Z. An *et al.* (2023) examined the intelligent design of complex

products and the reduction of their creation time by 20%. Similar principles can be used to create and improve medical protocols, personalised treatment plans, or new algorithms for DSS. Optimising processes with AI make systems more flexible, adaptive, and focused on rapid innovation.

Acceleration of model training without loss of accuracy was addressed by K. Karthick (2024) in an analysis of optimisers and mechanisms for their adaptation. Reducing training time by 30% through the right choice of optimisers was identified as a key aspect for systems that manage medical data that are frequently updated and expanded. Ensuring that new models can be trained quickly, or existing models can be retrained with up-to-date data is critical to maintaining the accuracy and relevance of recommendations.

The potential of machine learning methods for optimisation tasks in communication networks was demonstrated by H. Dahrouj *et al*. (2021). Although the focus of this study is on network infrastructure, the proposed algorithms for improving bandwidth, reducing latency, and integrating different types of data are relevant to the medical field. For instance, accelerating the transfer and processing of information between hospital subsystems (laboratory results, CT scans, ECG data) will allow the DSS to respond more quickly to clinical changes. H. Lu & Y. Li (2020) examined cognitive computing and the processing of semi-structured information. According to the results, the use of deep neural networks and NLP techniques can reduce data analysis time by 20% and increase decision-making accuracy by 18%. Similar approaches can be integrated into a DSS for detailed analysis of mixed types of information, including data from medical devices, laboratory systems, and patient records. Lastly, D. Van De Berg *et al*. (2022) demonstrated data-driven optimisation techniques for managing engineering processes, increasing system performance by 25%. Although the field of engineering is different from the medical field, the general approaches to optimisation, streaming data analysis, and automated decision-making are universal. The ability to quickly adapt systems to new conditions, update models, and test different information processing options will allow DSS to support doctors in their daily work even more effectively.

Given the prospects for further development, it is possible to conclude that the integration of MTL will increase the accuracy and flexibility of the DSS, allowing the model to simultaneously solve several clinically important tasks. The use of optimised learning algorithms, adaptive optimisers, dynamic hyperparameter tuning mechanisms and cloud technologies will help reduce data processing time and improve the overall efficiency of the system. Expanding the range of data types, including non-standard medical formats, as well as the use of explanatory artificial intelligence (XAI) techniques will increase clinicians' confidence in the results of the DSS and facilitate the system's implementation in real medical practice. Thus, the use of transformers and related modern data processing methods creates the preconditions for the emergence of new generations of medical DSS capable of quickly and accurately analysing large amounts of diverse information, providing personalised recommendations for each patient, and effectively scaling to the needs of modern medicine. Comparison with the results of other studies confirms the high relevance and scientific novelty of the chosen approach.

CONCLUSIONS

A study on the development and evaluation of the effectiveness of a decision support system for medical diagnosis of cardiovascular diseases that integrates heterogeneous types of data using neural networks, in particular transformers, shows the significant potential of this approach for modern medicine. The proposed architecture of the DSS, which processes text records, images, and signals, demonstrated the possibility of effective integration of poorly structured data of different natures in a single analytical process. The Transformers significantly improved the system's ability to detect key patterns and relationships between data using an attention mechanism, which increased the diagnostic accuracy by 15% compared to traditional methods.

The achieved level of accuracy and stable results when using new data sources are the result of an optimal combination of different types of neural networks. The use of multilayer perceptrons, recurrent and convolutional neural networks in combination with transformers allowed each of the subsystems to focus on specific aspects of analysis: MLP – on structured indicators, RNN – on sequential text records, CNN – on visual data, and transformers – on the complex integration of these formats. Such a multimodal model better considers the contextual and individual characteristics of patients, which is important in the context of personalised medicine and the provision of quality healthcare services. An equally important achievement was the introduction of a hybrid computing approach that combined local and cloud resources. This made it possible to reduce model training time by 30% and process up to 1 TB of data per day. The use of optimisation techniques and adaptive optimisers ensured the speed of analysis, which is critical in situations where rapid clinical decision-making is required. Thus, computational efficiency and scalability have become key factors in implementing a system suitable for real-world clinical settings where the amount of data is constantly growing.

The results of the study confirmed that transformers not only improve the accuracy and speed of diagnostics but also contribute to increasing the system's resistance to noise and incomplete data. This helps to ensure the reliability and predictability of decisions made by the decision support system and reduces the risk of medical errors. In this regard, the introduction of such DSS can significantly improve the quality of diagnostic

procedures, optimise resource allocation in healthcare facilities, and support doctors in their daily practice.

The findings correlate with current trends in artificial intelligence and machine learning, with special attention paid to multimodal data, multitasking, hyperparameter optimisation, scalability, and the use of cloud technologies. A promising area for further research is the introduction of explanatory artificial intelligence (XAI) approaches, which will increase the transparency of the decision-making process and the trust of doctors in the system's results. It is also possible to expand the list of data types (e.g., genetic or wearable device signals), which will contribute to even greater personalisation and accuracy of diagnosis. Thus, the developed DSS has all the prerequisites to become the basis for future generations of intelligent medical systems, increasing the effectiveness of treatment, reducing time and resources, and improving the quality of life of patients.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Abbas, N., & Gasmi, S. (2024). Optimizing machine learning techniques for big data analysis in natural language processing and text analytics. *ResearchGate*. doi: 10.13140/RG.2.2.15547.84002.

[2] An, Z., Bu, W., Wu, Z., & Li, D. (2023). Intelligent design of complex products based on extraction and reconstruction of key dimensions. In *2023 China automation congress (CAC)* (pp. 7966-7970). Chongqing: IEEE. doi: 10.1109/cac59555.2023.10450557.

[3] Baviskar, D., Ahirrao, S., Potdar, V., & Kotecha, K. (2021). Efficient automated processing of the unstructured documents using artificial intelligence: A systematic literature review and future directions. *IEEE Access*, 9, 72894-72936. doi: 10.1109/ACCESS.2021.3072900.

[4] Brown, T.B., *et al*. (2020). Language models are few-shot learners. *ArXiv*. doi: 10.48550/arXiv.2005.14165.

[5] Chen, S., Kang, J., Liu, S., & Sun, Y. (2020). Cognitive computing on unstructured data for customer co-innovation. *European Journal of Marketing*, 54(3), 570-593. doi: 10.1108/ejm-01-2019-0092.

[6] Cong, R., Deng, O., Nishimura, S., Ogihara, A., & Jin, Q. (2024). Multiple feature selection based on an optimization strategy for causal analysis of health data. *Health Information Science and Systems*, 12, article number 52. doi: 10.1007/s13755-024-00312-8.

[7] Dahrouj, H., *et al*. (2021). An overview of machine learning-based techniques for solving optimization problems in communications and signal processing. *IEEE Access*, 9, 74908-74938. doi: 10.1109/access.2021.3079639.

[8] European General Data Protection Regulation (GDPR). (2016, April). Retrieved from https://surl.li/wwepce.

[9] Fatima, H., & Gasmi, S. (2024). Optimization strategies in machine learning for improved big data analysis and natural language processing. *ResearchGate*. doi: 10.13140/RG.2.2.28130.75208.

[10] Gambella, C., Ghaddar, B., & Naoum-Sawaya, J. (2021). Optimization problems for machine learning: A survey. *European Journal of Operational Research*, 290(3), 807-828. doi: 10.1016/j.ejor.2020.08.045.

[11] Jain, S., Jain, S., & Jain, A.K. (2021). Deep learning approach towards unstructured text data utilization: Development, opportunities, and challenges. In A. Sharaff, G. Sinha & S. Bhatia (Eds.), *New opportunities for sentiment analysis and information processing* (pp. 29-49). New York: IGI Global Scientific Publishing. doi: 10.4018/978-1-7998-8061-5.ch002.

[12] Karthick, K. (2024). Comprehensive overview of optimization techniques in machine learning training. *Control Systems and Optimization Letters*, 2(1), 23-27. doi: 10.59247/csol.v2i1.69.

[13] Kumar Rachakatla, S., Ravichandran, P., & Reddy Machireddy, J. (2023). Advanced data science techniques for optimizing machine learning models in cloud-based data warehousing systems. *Australian Journal of Machine Learning Research & Applications*, 3(1), 396-419.

[14] Kushnir, D., Ocherklevich, O., & Paramud, Ya. (2021). Deep neural network model for text semantic analysis based on word embeddings. In *Proceedings of the 11th international conference on advanced computer information technologies (ACIT)* (pp. 718-721). Deggendorf: IEEE. doi: 10.1109/acit52158.2021.9548393.

[15] Law of Ukraine No. 2297-VI "On the Protection of Personal Data". (2010, June). Retrieved from https://www.president.gov.ua/documents/2297vi-11567.

[16] Lu, H., & Li, Y. (2020). Cognitive computing for intelligence systems. *Mobile Networks and Applications*, 25(4), 1434-1435. doi: 10.1007/s11036-019-01428-y.

[17] Mahadevkar, S.V., Patil, S., Kotecha, K., Soong, L.W., & Choudhury, T. (2024). Exploring AI-driven approaches for unstructured document analysis and future horizons. *Journal of Big Data*, 11, article number 92. doi: 10.1186/s40537-024-00948-z.

[18] Malyha, I., & Shmatkov, S. (2022). Machine learning methods for solving semantics and context problems in processing textual data. *Bulletin of V.N. Karazin Kharkiv National University, Series "Mathematical Modeling. Information Technology. Automated Control Systems"*, 56, 35-42. doi: 10.26565/2304-6201-2022-56-03.

[19] Meng, J., & Wang, Z. (2022). Intelligent algorithms of English semantic analysis based on deep learning technology. In *2022 IEEE Asia-Pacific conference on image processing, electronics and computers (IPEC)* (pp. 1530-1533). Dalian: IEEE. doi: 10.1109/IPEC54454.2022.9777363.
[20] Nedosnovanyi, O., Cherniak, O., & Golinko, V. (2023). Comparative analysis of cloud services for geoinformation data processing. *Information Technologies and Computer Engineering*, 20(2), 50-57. doi: 10.31649/1999-9941-2023-57-2-50-57.
[21] Oza, R.R., & Domadiya, D.H. (2023). Analysis of unstructured data using artificial intelligence. *International Journal of Creative Research Thoughts*, 11(5), 969-973.
[22] Rane, N.L., Mallick, S.K., Kaya, Ö., & Rane, J. (2024). Techniques and optimization algorithms in deep learning: A review. In *Applied machine learning and deep learning: Architectures and techniques* (pp. 59-79). Yakutiye: Deep Science Publishing. doi: 10.70593/978-81-981271-4-3_3.
[23] Rueda, R., Fabello, E., Silva, T., Genzor, S., Mizera, J., & Stanke, L. (2024). Machine learning approach to flare-up detection and clustering in chronic obstructive pulmonary disease (COPD) patients. *Health Information Science and Systems*, 12, article number 50. doi: 10.1007/s13755-024-00308-4.
[24] Shen, Z. (2023). Algorithm optimization and performance improvement of data visualization analysis platform based on artificial intelligence. *Frontiers in Computing and Intelligent Systems*, 5(3), 14-17. doi: 10.54097/fcis.v5i3.13836.
[25] Singh, S., & Hooda, S. (2023). A study of challenges and limitations to applying machine learning to highly unstructured data. In *2023 7th international conference on computing, communication, control and automation (ICCUBEA)* (pp. 1-6). Pune: IEEE. doi: 10.1109/ICCUBEA58933.2023.10392115.
[26] Smetaniuk, O., & Tsisar, D. (2024). Digital economy as a foundation for creating digital strategies of enterprises. *Innovation and Sustainability*, 4(3), 68-75. doi: 10.31649/ins.2024.3.68.75.
[27] Turet, J.G., & Costa, A.P.C.S. (2022). Hybrid methodology for analysis of structured and unstructured data to support decision-making in public security. *Data & Knowledge Engineering*, 141, article number 102056. doi: 10.1016/j.datak.2022.102056.
[28] Van De Berg, D., Savage, T., Petsagkourakis, P., Zhang, D., Shah, N., & del Rio-Chanona, E.A. (2022). Data-driven optimization for process systems engineering applications. *Chemical Engineering Science*, 248(B), article number 117135. doi: 10.1016/j.ces.2021.117135.
[29] Wilson, A., & Anwar, M.R. (2024). The future of adaptive machine learning algorithms in high-dimensional data processing. *International Transactions on Artificial Intelligence*, 3(1), 97-107. doi: 10.33050/italic.v3i1.656.
[30] World Medical Association's Declaration of Helsinki. (1964, June). Retrieved from https://www.wma.net/policies-post/wma-declaration-of-helsinki/.
[31] Zhang, G., Fu, C., & Zhou, H. (2024). Research on key technologies of deep learning techniques in unstructured data processing. *Applied Mathematics and Nonlinear Sciences*, 9(1). doi: 10.2478/amns-2024-3175.
[32] Zhang, Y., & Yang, Q. (2022). A survey on multi-task learning. *IEEE Transactions on Knowledge and Data Engineering*, 34(12), 5586-5609. doi: 10.1109/TKDE.2021.3070203.
[33] Zohuri, B. (2024). Artificial intelligence and machine learning driven adaptive control applications. *Journal of Material Sciences and Engineering Technology*, 2(4). doi: 10.61440/JMSET.2024.v2.27.

Оптимізація алгоритмів інтелектуальних систем для аналізу слабоструктурованих даних

Микола Демчина

Кандидат технічних наук, доцент
Університет Короля Данила
76018, вул. Є. Коновальця, 35, м. Івано-Франківськ, Україна
https://orcid.org/0009-0002-9161-4843

Тарас Стисло

Старший викладач
Університет Короля Данила
76018, вул. Є. Коновальця, 35, м. Івано-Франківськ, Україна
https://orcid.org/0000-0002-2377-7985

Сергій Ващишак

Кандидат технічних наук, доцент
Університет Короля Данила
76018, вул. Є. Коновальця, 35, м. Івано-Франківськ, Україна
https://orcid.org/0000-0002-1753-1540

Анотація. Інтеграція різнорідних типів медичних даних із використанням сучасних методів глибокого навчання дозволяє підвищити точність та ефективність діагностики складних захворювань, таких як серцево-судинні, що має вирішальне значення для персоналізованої медицини та зниження ризику медичних помилок. Метою роботи було представити розробку системи підтримки прийняття рішень, спрямованої на покращення діагностики серцево-судинних захворювань шляхом інтеграції різнорідних типів медичних даних. Для створення бази знань були використані дані реальних клінічних сценаріїв, що пройшли етапи очистки, стандартизації та семантичного аналізу за допомогою спеціалізованих медичних словників. Система продемонструвала високу ефективність завдяки здатності інтегрувати текстові, зображувальні та сигнальні дані в єдиний процес аналізу. Ефективність оцінювалася за такими метриками, як точність, повнота, F1-score, а також прогностичні значення позитивних і негативних результатів. Впровадження трансформерів забезпечило підвищення точності діагностики на 15 % порівняно з традиційними методами, а використання гібридного підходу до обчислень дозволило скоротити час навчання моделей на 30 % і обробляти до 1 ТБ даних на добу. Додатково, інтеграція різнорідних типів медичних даних у системі дала змогу покращити персоналізацію діагностики, враховуючи індивідуальні особливості пацієнтів, такі як анамнез, генетичні фактори чи супутні захворювання. Завдяки механізмам уваги трансформерів система демонструє стійкість до шуму та пропусків у даних, що забезпечує надійність результатів навіть за умови неповної або неточної інформації. Оптимізація моделей сприяла зменшенню затримок в обробці даних, що є критично важливим для оперативного прийняття клінічних рішень. Крім того, трансформери довели свою здатність динамічно масштабуватися для обробки нових типів даних без втрати ефективності, відкриваючи можливості для подальшого розширення функціоналу системи. Система також підвищила продуктивність клінічних фахівців завдяки автоматизації рутинних завдань, що дозволило лікарям зосередитися на складніших аспектах лікування

Ключові слова: штучний інтелект; база знань; підтримка прийняття рішень; нейромережі; видобування знань; алгоритми класифікації; адаптивні системи

BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en

Vol. 29 No. 4. 2024

UDC 004.75
DOI: 10.62660/bcstu/4.2024.32

Microservices architecture for ERP systems

Serhii Slivka*
Postgraduate Student
Odesa Polytechnic National University
65044, 1 Shevchenko Ave., Odesa, Ukraine
https://orcid.org/0009-0003-1704-1415

Abstract. Traditional enterprise resource planning (ERP) systems built on the principle of monolithic architecture are becoming less and less effective in a modern business environment. The growing complexity of production processes, the increase in data volumes and the need to adapt quickly to changes pose significant challenges for such systems. The study aimed to analyse and develop methods for transitioning from a monolithic architecture to a microservice architecture in ERP systems to ensure their scalability, flexibility and security. A comprehensive analysis of the client-server architecture of ERP systems and their main components, including relational databases and structured query language (SQL) queries, was conducted. The principles of functions and procedures, interaction between tables, and query creation in systems with many users were investigated. The study also addressed modern strategies for decomposing monolithic systems into microservices, including methods of data synchronisation and component management. Security aspects and risks of transition to microservice architecture were emphasised. Approaches to the transformation of ERP systems based on microservice architecture were developed, which reduces management complexity, increases productivity and reduces risks in business processes. Mechanisms for effective synchronised data exchange between components and ensuring their reliability were proposed. The study determined that microservice architecture enables independent scaling of individual system elements, increasing fault tolerance and performance under high loads. Common issues, including incorrect balances and errors in reports, were investigated and resolved. The developed approaches can be used to modernise ERP systems of large enterprises, especially in the manufacturing sector, where high performance and accuracy of data processing are important

Keywords: client-server; scalability; stakeholder; critical path; critical event; automation; cloud technologies

INTRODUCTION

The rapid development of information technology and the growing need for efficient business process management are creating new challenges for businesses of all sizes. Traditional monolithic enterprise resource planning (ERP) systems are becoming less effective due to the increasing complexity of business processes, growing data volumes and the need to quickly adapt to market changes. This problem is particularly acute in the context of ensuring flexibility, scalability and efficiency of corporate systems.

The research relevance of implementing microservice architecture in ERP systems is determined by several factors. There is a need to modernise existing corporate systems to increase their adaptability and efficiency. In the context of digital business transformation, it is critical to ensure the ability to quickly scale and update individual system components. The globalisation of business processes requires the implementation of modern architectural solutions that meet international software development standards.

Article's History: Received: 05.08.2024; Revised: 29.11.2024; Accepted: 16.12.2024.

Suggested Citation:
Slivka, S. (2024). Microservices architecture for ERP systems. *Bulletin of Cherkasy State Technological University*, 29(4), 32-42. doi: 10.62660/bcstu/4.2024.32.

*Corresponding author

Microservices architecture enables the decomposition of complex systems into independent components and their isolated deployment, which makes it particularly beneficial for use in ERP systems. In the context of corporate systems, microservices open great opportunities for improving business processes. The use of microservices allows for independent scaling of individual components, simplifies the development and testing process, allows for the use of different technologies for different services, and guarantees high system availability due to fault isolation.

The study by M. Söylemez *et al*. (2022) addressed the key issues related to the implementation of microservice architecture. Particular attention was devoted to the issues of service coordination, data consistency in distributed systems, and challenges in transaction management. The microservice architecture was noted to significantly increase the scalability and adaptability of systems but requires the introduction of clear standards for interaction between services to avoid performance degradation.

A step-by-step approach to modernising outdated information systems through the integration of microservice architecture was presented by D. Wolfart *et al*. (2021). The authors proposed methods for decomposing a monolithic structure into independent components that support the use of application programming interface (API) gateways to facilitate interaction. It is noted that this approach helps to increase flexibility, reduce support costs and ensure faster adaptation to changes in business processes.

The benefits of moving to a cloud ERP system based on a microservice architecture were analysed by C. Lee *et al*. (2024). The main emphasis was devoted to ensuring the sustainability and adaptability of such systems, which is achieved by dividing the functionality into independent services. The possibilities of using microservices to reduce risks and improve productivity in large enterprises were also investigated.

A.S. Abdelfattah & T. Cerný (2022) highlighted the security challenges of microservice architecture, including API security, authentication, and access control. The authors proposed multi-level solutions to prevent attacks on microservices, emphasising the importance of integrating modern security protocols such as OAuth 2.0. The study emphasised that the security of distributed systems requires careful monitoring of each component.

The issue of improving the efficiency of business processes in service-oriented architectures was considered by T. Górski & A.P. Wozniak (2021). The authors analysed process automation techniques, including reducing delays and increasing the accuracy of transaction processing. The study emphasised that optimisation of such processes contributes to the performance of ERP systems.

The features of the implementation of microservice architecture in cloud applications are analysed in the study by O.C. Oyeniran *et al*. (2024). The authors analysed design templates that help reduce latency, increase scalability, and ensure the stability of systems in high-load environments. The study emphasised that the use of microservices in cloud ERP solutions allows for efficient resource allocation and system stability.

M. Grambow *et al*. (2020) investigate methods for assessing the performance of microservice applications. The authors conducted a comparative analysis of approaches to testing systems in different load scenarios, emphasising the importance of choosing optimal strategies to avoid performance losses. The study noted that effective testing helps reduce risks in the process of system scaling.

The issue of interoperability of microservice architecture components was considered in the study by A. Bayramçavuş *et al*. (2021). The study determined that API standardisation and the implementation of transaction management strategies can achieve data consistency and ensure the stability of distributed systems. Particular attention is devoted to the development of interaction models that minimise the risks of data loss in the process of system scaling.

Existing research in the field of microservices architecture points to a number of unresolved issues that limit the effectiveness of traditional approaches to ERP system development. The main gaps are the complexity of managing distributed transactions, problems with data consistency between services, and challenges related to monitoring and diagnostics of distributed systems. In addition, existing approaches rarely address the specifics of business processes in particular industries, which creates difficulties in implementing and adapting systems.

The study aimed to analyse and optimise approaches to the transition from monolithic to microservice architecture of ERP systems to ensure their scalability, flexibility and security. Practical recommendations were developed for the design and implementation of microservice architecture in ERP systems. The research included the creation of a theoretical model of microservice architecture for ERP systems, exploring the possibilities of ensuring data consistency between services and developing methods for effective monitoring and management of a distributed system.

MATERIALS AND METHODS

The study is based on a theoretical analysis of modern approaches to the architecture of ERP systems, particularly the transition from a monolithic to a microservice structure. The main methodology used was a review of scientific papers, technical documentation and industry standards related to microservice architecture, client-server interactions, database management and security in distributed systems. The principles of distributing computing loads between client and server components of ERP systems, which are key to ensuring their efficiency, were investigated. Attention was devoted to the peculiarities of implementing structured query language (SQL) queries, transaction

management and maintaining data consistency in a multi-user environment.

To model the transition from a monolithic architecture to a microservice architecture, the main approaches to system decomposition were analysed, including the use of API gateways, data synchronisation and transaction management methodologies. The theoretical aspects of mechanisms for integrating microservices with external modules, such as customer relationship management (CRM) systems or electronic document management systems, as well as architectural templates that ensure data consistency and minimise the risk of information loss when components interact were considered.

The theoretical analysis also included modelling ways to scale systems through independent module decomposition, optimisation of SQL queries, and the introduction of indexes to speed up the processing of large amounts of data. The use of cloud technologies as a means of improving the performance and stability of ERP systems, especially under high-load conditions, was investigated. In this context, the theoretical aspects of dynamic resource allocation and the use of automated monitoring tools to maintain system stability were considered.

Additionally, the theoretical study analysed modern approaches to the design of architectural solutions, including the use of programming patterns such as the Strangler Fig Pattern for the gradual transition from monolithic to microservice architecture. This approach was used to integrate new microservice components without interrupting the system operation and minimise the risks during the implementation of changes. The advantages of using standard API gateways to manage the interaction between system components, which is a key aspect for maintaining the scalability and reliability of ERP systems, are considered.

The client-server architecture of ERP systems has several advantages and disadvantages that affect its effectiveness in the corporate environment. To systematise this analysis, a SWOT analysis was employed to assess the strengths and weaknesses of the architecture, as well as identify opportunities for its modernisation and risks. Thus, the study covers a systematic analysis of the key theoretical aspects of the transition to microservice architecture, including its impact on the performance, scalability, security and adaptability of ERP systems, which creates the basis for the development of innovative solutions in this area.

RESULTS AND DISCUSSION

ERP systems are based on a client-server architecture, which enables efficient distribution of computing loads between the client and server sides. The server performs key functions of data processing, database management, and SQL query execution. The client part of the system, in turn, provides interaction with users and enters and displays data in a clear format.

One of the main advantages of this architecture is the ability to scale the system to meet the needs of the enterprise. New modules and users can be added without significant changes to the basic structure of the system. In addition, the versatility of the client-server architecture is ensured by the SQL standard, which is supported by various database management systems and allows the system to be transferred between platforms with minimal effort. However, there are also disadvantages. Significant computing resources are required to support large amounts of information that grow with the development of the enterprise. There are also difficulties in updating software on numerous client devices, which can slow down the process of implementing changes. Table 1 shows the key results of the SWOT analysis of the client-server architecture of ERP systems.

Table 1. SWOT analysis of the client-server architecture of ERP systems

Aspects	Parameters	Advantages	Disadvantages
Strengths	Scalability	Ease of adding new users and modules	Requires scaling of the server infrastructure as the number of users increases
	Productivity	Centralised data processing reduces the load on client devices	Dependence on network bandwidth and server speed
	Compatibility	Employment of SQL ensures versatility and cross-platform integration	High costs of integration with old or non-standard platforms
Weaknesses	Infrastructure	Significant server requirements for processing large amounts of data	Limitations in the rate of infrastructure upgrades
	Administration	The complexity of updating software on numerous client devices	Dependence on administrators' expertise to maintain the system
	Flexibility	Limitations to rapid innovation due to centralised structure	The possibility of a single server failure affecting the entire system
Opportunities	Integration of new technologies	Employment of cloud services to ensure stability and flexibility	The high initial cost of switching to new technologies
	Automation	Implementation of AI for data analysis and load forecasting	The need to adapt the existing system to new functions
	Expansion functionality	Integration of mobile platforms and external systems (CRM, logistics)	Potential conflicts between different modules during integration

Continued Table 1.

Aspects	Parameters	Advantages	Disadvantages
Threats	Cybersecurity	Possible attacks on the server side due to its central role	Increased costs of data security
	Infrastructure risks	Dependence on network bandwidth and server stability	Equipment failure can lead to a shutdown of the entire system
	Technology development	Competition from microservice architectures and new systems	Risk of losing relevance due to lack of fast updates

Source: compiled by the author based on D. Wolfart *et al.* (2021), M. Söylemez *et al.* (2022), C. Lee *et al.* (2024)

The successful functioning of ERP systems depends on effective interaction between stakeholders. Internal customers, such as managers and employees, seek to optimise business processes and receive accurate reports, while system administrators are focused on ensuring stable operation, data protection and user service. The interests of these groups can often conflict, requiring careful communication management.

The support and influence matrix ensures systematisation of stakeholders' interests, identification of their influence on the project and development of individual interaction strategies. This is especially relevant when the system is scaled up when every change affects the work of both groups. For instance, internal customers value flexibility and quick implementation of changes, while administrators prefer stability and risk minimisation. The study devoted significant emphasis to the architecture of ERP systems, as it is the proper design and management of this architecture that ensures stable and efficient operation of corporate systems. One of the key aspects is the interaction between the main stakeholders, as each group has its requirements for the system's functioning. It is necessary to identify how different interests can influence the architectural decisions of ERP systems and what trade-offs need to be factored into their design and implementation. Table 2 provides a comparison of the interests of the main stakeholders of ERP systems, which will clarify how their needs affect the architectural aspects and technical decisions made during the development and implementation of such systems.

Table 2. Comparison of the interests of the main stakeholders of ERP systems regarding architecture and software solutions

Stakeholders	Main interests	Possible conflicts
Internal customers	1. Flexibility and scalability of functions. 2. Easy integration of new modules.	1. The need for constant updates can be at odds with the stability of the system. 2. Flexibility requirements can make it difficult to maintain and upgrade.
System administrators	Stable and reliable operation.	1. Risk of security breaches due to the integration of new modules. 2. Conflicts between stability and the need to introduce new features.
Software developers	1. Transparency and ease of development. 2. Ease of new technology implementation.	1. Complications due to the need to interact with existing components. 2. The use of new technologies may require significant changes to the system.
Users of the ERP system	1. Speed of operation and availability of functions. 2. Intuitive interface.	1. Problems with adapting the interface to the needs of users. 2. The introduction of new features may affect the ease of use of the system.

Source: compiled by the author based on A. Bayramçavuş *et al.* (2021), D. Wolfart *et al.* (2021), M. Söylemez *et al.* (2022)

Changes to ERP systems are an integral part of their operation. The need for changes can be caused by an increase in data volume, an expansion of the list of users, improvements in business processes, or technology development. For effective change management, it is necessary to utilise modern software development lifecycle methodologies, such as Agile or the spiral model. They can be used to integrate changes gradually, minimising risks and ensuring system stability.

Consideration of system changes should also include risk management. For instance, large-scale changes to the system core or databases have a high level of intervention and require thorough testing. Less critical changes, such as customising reports or creating new forms, can be implemented more quickly.

ERP systems actively use SQL to manage relational databases. The interaction between the client and the server is based on a clearly defined mechanism: the client creates a query; the server processes it and returns the results. This structure can be used to optimise the processing of large amounts of data and ensure the reliability of the system.

Figure 1 shows a diagram of SQL in a client-server ERP system. The client part, which runs on the personal computer of the user, generates queries that are transmitted to the server. The server processes these queries by interacting with the database and returns the results in the form of information ready for analysis. This interaction ensures efficient system operation, reduces network traffic, and adapts to the growth in the number of users or data volumes. The use of the SQL standard as the main database management tool facilitates cross-platform compatibility of the system. At the same time, the complexity of integrating new modules or scaling the architecture requires significant attention to change management.

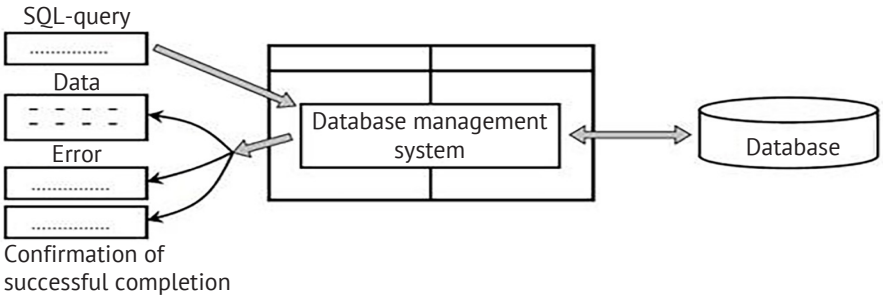

Figure 1. The architecture of SQL queries interaction with the database
Source: compiled by the author based on E.F. Codd (1990), C.J. Date (1975)

ERP system scaling is a major challenge for large enterprises that regularly face an increase in the number of users, changes in business processes, and the need to integrate new modules. The flexibility of the microservices architecture can be used to adapt the system to new conditions without critical failures in its operation. For instance, the implementation of a modular approach to development ensures the independence of each component of the system, which allows making changes locally without affecting other parts. In addition, the use of modern spiral software development lifecycle models, such as Agile or the spiral model, facilitates the integration of updates, as each stage of change is tested and implemented gradually.

One of the key challenges in developing and implementing ERP systems is the need to integrate with other software solutions. To ensure comprehensive management of business processes, the system should combine functionality that covers not only the main but also auxiliary processes, such as logistics management, data analytics, e-commerce, etc. The transition from a monolithic architecture to a microservice architecture is complex and requires careful planning, as it involves significant changes in infrastructure, process design and organisation. One of the most effective methods of transition is to split the monolithic architecture into separate microservices in stages. This avoids the major risks associated with the simultaneous restructuring of the entire system. It is necessary to identify the functional areas of the monolith that can be divided into separate microservices, such as components such as order processing, inventory management, or financial accounting. These areas are then rewritten as separate microservices that can run independently of each other. Microservices should interact through well-defined APIs to ensure their independence and flexibility when changing or scaling.

One of the proven patterns for transition is to use the Strangler Fig Pattern strategy. This strategy consists of the gradual replacement of a monolithic system with microservices. At first, the old monolithic code remains in the system, and gradually its functions are replaced by new microservices. This allows for a safe transition without interrupting the entire system. In addition, API gateways are used for easy integration between old and new components, which minimises the complexity of integration. During the transition, it is also necessary to ensure that development and testing processes are automated to reduce the risk of errors. Microservices require well-defined unit tests that allow for quick detection of errors in the early stages of development. To optimise the testing and deployment of microservices, continuous integration and delivery tools should be used to reduce the risk of errors and improve the speed of deploying new versions.

There are certain risks involved in the transition. One of the main ones is the difficulty of integrating new microservices with the existing monolithic system. To minimise this risk, it is necessary to use a phased migration and the Strangler Fig strategy, as well as clearly define interfaces for interaction between components. Another important risk is data consistency between microservices. The absence of a clear data synchronisation strategy can lead to data discrepancies and errors, so approaches such as Event Sourcing or Command Query Responsibility Segregation should be used to ensure consistency. Another important challenge is the growing complexity of microservices management, which can increase the complexity of monitoring, updating and testing the system. To mitigate this risk, automated monitoring and orchestration tools such as Kubernetes or Docker Swarm should be used.

By migrating to a microservices architecture, companies can significantly increase the flexibility of their

ERP systems, reducing risks and support costs while improving stability and scalability. To achieve a successful outcome, it is necessary to carefully plan the transition, use a phased approach, apply migration templates, automate testing and monitoring processes, and minimise risks through a clear data synchronisation and security strategy. The microservices architecture simplifies the integration of external services and modules through standard APIs and data exchange protocols. For instance, modern ERP systems can interact with electronic document management services or CRM platforms. Such integrations provide end-to-end automation and simplify data transfer between different departments of the enterprise. Integration can be complicated by differences in data formats, external system interfaces, and security requirements. At the same time, the implementation of such changes often requires the cooperation of several teams, which makes it difficult to coordinate the work. To successfully overcome these challenges, it is critical to use unified data exchange standards and effectively manage stakeholder interactions.

Modern ERP systems are actively using data visualisation tools to improve analytics and management decision-making. Graphical reports, interactive dashboards and charts can quickly assess key performance indicators and identify problem areas. Visualisation also contributes to a deeper understanding of complex business processes. Automation of business processes in ERP systems significantly reduces the workload on staff by reducing the number of routine operations. For instance, automatic report generation, inventory management, and payroll functions reduce the time required to complete these tasks and reduce the risk of errors. The modular structure of ERP systems facilitates the adaptation of automation to the specifics of the enterprise. One of the key aspects of ERP systems is ensuring their stability, particularly as the company expands or business processes change. Stability depends on proper server configuration, database maintenance, and system performance monitoring. System administrators perform an important role in this process, as they are responsible for timely software updates, bug fixes, and ensuring that data is available to users.

Problems can arise due to insufficient hardware scalability, an increase in the number of database queries, or incorrect SQL query optimisation. To mitigate risks, system administrators use server and database performance monitoring to identify bottlenecks in the system, automated backups to prevent data loss, and query optimisation and index tuning to speed up database performance. The use of cloud technologies in the client-server architecture of ERP systems can significantly increase the stability and efficiency of such systems due to the ability to dynamically allocate computing resources. This allows ERP systems to adapt to changing business needs and ensure stable operation even under high loads. Cloud computing provides dynamic resource allocation, which can be used to automatically scale the system's capacity depending on the current load. In ERP systems, this is especially critical for companies that experience seasonal peaks in activity, such as retail and logistics, where computing resource requirements may vary depending on sales or the number of transactions.

One of the main advantages of cloud solutions is high availability and fault tolerance. By facilitating data backup in the cloud, which is carried out through geographically distributed data centres, the ERP system can remain available even in the event of hardware failures or local accidents. Cloud providers typically use clustering and load-balancing mechanisms to ensure minimal downtime and improve system stability. Scalability is another important advantage of cloud-based ERP solutions. Companies can start with a limited set of resources and gradually expand the system without significant capital expenditure on new server hardware. This makes it easy to integrate new modules or connect new branches or remote offices, which is important for businesses that are expanding or changing. In addition, cloud technologies can significantly reduce costs. The Pay-as-you-go model allows companies to pay only for the resources they use, making cloud solutions cost-effective. The absence of the need to maintain in-house server hardware also reduces operating costs.

Security and data protection are important aspects when implementing cloud ERP systems. Cloud providers typically offer advanced security features, including data encryption, real-time monitoring, and protection against denial-of-service attacks. Users can access the ERP system through secure channels, such as a virtual private network, which ensures a high level of data protection. Another important advantage is the global availability of cloud ERP systems. Such systems can be accessed from anywhere in the world, which is especially important for international companies or remote teams. Examples of such cloud solutions include Amazon Web Services, which offers services for dynamic resource allocation through EC2, S3 and RDS, and Microsoft Azure, which integrates with ERP systems such as Microsoft Dynamics 365 to ensure stable operation. Also worth mentioning is the Google Cloud Platform, which actively uses data analytics and machine learning technologies in the context of ERP systems.

To successfully implement cloud solutions in ERP systems, companies need to assess several key aspects. It is necessary to verify the compatibility of the existing ERP system with cloud infrastructures, assess the requirements for data security and confidentiality, and address the potential risks associated with dependence on a cloud provider. In summary, cloud technologies provide ERP systems with high stability, efficiency and flexibility, making them an important tool for businesses seeking to optimise their processes and adapt to a rapidly changing environment. In addition, the introduction of continuous monitoring systems can be used

to respond quickly to potential problems, ensuring the smooth operation of the entire platform.

The process of editing ERP systems always involves certain risks, such as module failure, conflicts between old and new components, or configuration errors. To minimise the risks, it is necessary to carefully plan each stage of changes, test new components, and provide feedback from users. One of the most effective approaches is to use the spiral software development lifecycle model. This model can be used to iteratively implement changes, gradually testing each component and reducing the likelihood of major failures. In the case of less critical changes, it is advisable to use the Agile model, which provides flexibility and quick response to new requirements. Ranking risks according to the level of intervention allows administrators to allocate resources more efficiently. For instance, changes to the core of the system require maximum attention and thorough testing, while setting up new forms or reports can be done without significantly affecting other components. Adapting a system often requires upgrading technical equipment and implementing new technologies, such as microservice containers or distributed databases. At the same time, it is necessary to consider the interests of stakeholders to ensure that the adaptation meets the needs of users and does not disrupt the stability of the operation.

The use of a microservice approach can significantly improve the flexibility of the system, ensure its scalability and reduce the risks associated with expanding functionality. This is especially relevant for large enterprises that need to continuously improve processes and adapt to changes in the business environment. A key advantage of microservice architecture is the ability to independently scale individual system components. This ensures greater resilience to loads arising from the growth of data volumes or the number of users. The introduction of a modular approach also helps to reduce the complexity of system management and reduce maintenance costs.

The peculiarities of the transition from monolithic to microservice architecture using hybrid database design were considered by T. Ng *et al*. (2024). The authors analysed approaches to adapting databases for microservices, ensuring compatibility between old and new modules, and improving the efficiency of query processing in distributed systems. Secure microservices and a security framework for user interaction with microservice applications were described by M.I. Elkholy & M.A. Marzok (2022). The authors present methods of authentication, authorisation, and data protection in microservice ecosystems. The automation of business processes implemented as part of the study significantly reduces the time required to perform routine tasks and reduces the number of errors. Optimisation of SQL queries and database management improves system performance, providing fast access to data even under high load conditions. This creates the basis for improving the performance of ERP systems in a dynamic business environment. The study highlighted the integration of ERP systems with external modules and platforms. The use of standard APIs and protocols simplifies the process of data exchange between systems, providing a single information environment. This approach contributes to the creation of integrated business process management solutions that meet the needs of modern enterprises.

Another important aspect considered in the proposed methodology is ensuring the reliability of ERP systems in the process of implementing new modules and functionality. An important factor is to minimise downtime during upgrades and maintain stable system operation even under high load conditions. The use of testing methods in real-life scenarios and modelling of various operating conditions allows identifying potential bottlenecks before the implementation of changes, which significantly reduces the risk of failure. The use of microservice patterns for big data systems was covered by P. Ataei & D. Staegemann (2023). The authors considered ways to improve the processing of large amounts of data through modularity and distribution.

An additional result is the increased security of ERP systems due to the isolation of microservices from each other. This approach minimises the impact of failures in individual components and ensures high availability of the rest of the system. Achieving this level of security is critical for large enterprises that process large amounts of sensitive data. A systematic mapping study of microservices development based on domain-driven design is presented in J. Sangabriel-Alarcón *et al*. (2023). The concepts of domains, strategic modelling, and complexity management in large distributed systems are considered. A generalised description of the principles of microservice architecture is given in the study by V. Božić (2023). The basic concepts, advantages, disadvantages, and prospects for the development of this architecture are considered.

The business process automation implemented in the study not only increases the efficiency of tasks but also helps to improve the interaction between different departments of the enterprise. The integration of data visualisation tools, such as interactive dashboards, ensures quick decision-making for managers based on accurate and up-to-date performance indicators. This creates a transparent environment for resource management and operations planning. The peculiarities of decision-making at the stage of initiating corporate information systems projects were analysed by I. Barskaya *et al*. (2014). The specifics of management decision-making in the process of implementing corporate information systems, particularly the impact of initiation on further stages of the project life cycle, were considered. The main factors that contribute to the successful implementation of such projects are identified.

A study of microservice architecture in the Edge Computing environment was conducted by N. Rathore *et al*. (2020). The study highlights the aspects of adapting microservices to the requirements of edge computing, including reducing latency and improving energy efficiency. The use of microservices and event-oriented architecture for processing large data streams was presented by S. Zhelev & A. Rozeva (2019). The advantages of distributed systems for processing streaming data in real-time were highlighted.

Of particular interest is the possibility of using the proposed approach in combination with modern artificial intelligence technologies. The integration of machine learning algorithms can significantly improve the processes of load forecasting, resource optimisation, and detection of anomalies in the system. Such solutions will allow ERP systems to automatically adapt to changes in the business environment, increasing their efficiency and reliability. The optimisation of enterprise infrastructure using microservices is considered by A.M. Abd-Elwahab *et al*. (2023). The authors analysed methods of adapting infrastructure to the growing needs of businesses and reducing costs.

Further development of the proposed methodology may include its adaptation to the specifics of various industries. For instance, in the manufacturing sector, ERP systems should address the complexity of supply chains, integration with Internet of Things devices to monitor equipment status, and automation of quality control processes. In trade and logistics, real-time inventory management and integration with e-commerce platforms are becoming increasingly important. The concept of creating a minimum viable product and design thinking in the management of IT teams was highlighted by I. Blyznyukova *et al*. (2021). The study focuses on the principles of building a minimum viable product, adapting design thinking to information technology projects, and developing a team management strategy to achieve the goals. Integration with smart enterprise concepts, where ERP systems are a central component of managing all processes, can be a separate area of development. In such conditions, not only microservice architecture plays an important role, but also the ability of ERP systems to support fast data exchange with automated production lines, robotic warehouse systems and other elements of a modern enterprise.

Integration of the proposed methodology with the latest technological approaches can enhance its effectiveness in solving complex problems of modern business. One of the most promising areas is the use of artificial intelligence to optimise management processes in ERP systems. For instance, machine learning algorithms can analyse large amounts of data, predict system failures, optimise resources, and automatically adjust workflows to increase productivity. Approaches to refactoring from monolith to microservices were classified in the study by J. Fritzsch *et al*. (2019). They show various strategies for reorganising systems to increase their flexibility and scalability.

It is also worth noting the importance of automating supply chain management, which is a key component of many ERP systems. Integration of demand forecasting, real-time inventory monitoring and automated logistics management will allow enterprises to reduce costs, minimise the risks of shortages or surpluses and ensure high accuracy of deliveries. Technologies of data integration in national information systems were studied by N. Shakhovska & D. Tarasov (2011). They analysed methods of integrating heterogeneous data sources, building a single database and using modern approaches to information exchange. Optimisation of microservices deployment costs using cluster autoscaling and the Spot pricing model is discussed by D. Edirisinghe *et al*. (2024). The authors present approaches to reducing costs while maintaining high availability. Peculiarities of integration of information systems of instrument-making enterprises were considered by O. Legotchenkov (2016). The study analyses the mechanisms of data integration, the principles of building relational tables and the means of ensuring communication between different information systems to optimise business processes.

Load balancing and service discovery in big data applications based on microservices and Docker Swarm were considered by N. Singh *et al*. (2023). The authors described methods for integrating Docker Swarm to improve data processing efficiency in distributed environments. The role of containerisation in transforming software development and deployment through microservice architecture was analysed by J. Mukaj (2023). The author described the use of Docker and Kubernetes to ensure flexibility, scalability, and reliability.

A separate focus area is integrating ERP systems with future technologies such as quantum computing. Although these technologies are only just beginning to find their way into the corporate environment, in the long run, they can provide unprecedented performance and security in data processing. Preparing an ERP architecture to support such technologies can be a strategic advantage for enterprises. The use of quantum computing in microservice architecture was analysed by S.K. Eddin *et al*. (2024). The potential of quantum microservices to revolutionise data processing and optimise complex computing is explored. Thus, the developed methodology opens wide opportunities for further improvement of ERP systems. Its adaptability, focus on innovation, and ability to integrate with current and future technologies render it a versatile solution that meets not only current but also future business challenges.

CONCLUSIONS

The study substantiates the feasibility of transitioning ERP systems from a monolithic architecture to a microservice architecture that meets modern business challenges, in

particular, increased requirements for scalability, flexibility, performance and security. The results of the analysis showed that microservice architecture facilitates the adaptation of ERP systems to changes in the business environment due to modularity, independent deployment of components and simplified upgrade processes. The use of programming patterns, such as the Strangler Fig Pattern, minimises the risks of system upgrades by ensuring a phased transition to a new architecture.

The study demonstrated that the use of modern tools, such as API gateways, asynchronous interaction and caching technologies, helps optimise the performance of ERP systems in highly loaded conditions. The theoretical analysis has confirmed the effectiveness of using cloud technologies that provide dynamic resource allocation, increase stability and enable rapid scaling. In addition, approaches to the integration of ERP systems with external modules through standardised APIs are considered, which creates a single information space for the enterprise.

Recommendations for the implementation of business process automation solutions and the integration of artificial intelligence algorithms allow ERP systems to adapt to changing business conditions, increasing the efficiency of data and process management. The integration of modern technologies, including artificial intelligence and analytical platforms, creates prospects for automating complex business processes and increasing the competitiveness of enterprises. This research forms the basis for creating flexible, secure and scalable ERP systems that can meet the needs of the globalised market and ensure business stability in the face of dynamic change.

The obtained results created a comprehensive theoretical basis for further research and practical solutions in the field of ERP systems modernisation, in the context of the transition to microservice architecture. The proposed approaches can be the basis for developing innovative ERP solutions that can meet current and future business challenges. Further development of the theoretical foundations will allow these solutions to be adapted to the specific needs of various industries, such as manufacturing, logistics and e-commerce, ensuring their efficiency and sustainable development.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Abdelfattah, A.S., & Cerný, T. (2022). Microservices security challenges and approaches. In R.A. Buchmann, G.C. Silaghi, D. Bufnea, V. Niculescu, G. Czibula, C. Barry, M. Lang, H. Linger & C. Schneider (Eds.), *Information systems development: Artificial intelligence for information systems development and operations*. Cluj-Napoca: Risoprint. doi: 10.62036/ISD.2022.27.

[2] Abd-Elwahab, A.M., Mohamed, A.G., & Shaaban, E.M. (2023). MicroServices-driven enterprise architecture model for infrastructure optimization. *Future Business Journal*, 9, article number 90. doi: 10.1186/s43093-023-00268-3.

[3] Ataei, P., & Staegemann, D. (2023). Application of microservices patterns to big data systems. *Journal of Big Data*, 10(1), article number 56. doi: 10.1186/s40537-023-00733-4.

[4] Barskaya, I., Teslenko, P., & Denysenko, V. (2014). Peculiarities of decision-making at the stage of initiating projects for the creation of information information systems. *Project Management and Production Development*, 1, 32-39.

[5] Bayramçavuş, A., Kaya, M.Ç., & Dogru, A.H. (2021). Interoperability of microservice-based systems. In *Proceedings of the 13th international conference on electrical and electronics engineering* (pp. 594-598). Bursa: IEEE. doi: 10.23919/ELECO54474.2021.9677712.

[6] Blyznyukova, I., Teslenko, P., Danchenko, O., & Melenchuk, V. (2021). The concept of creating a minimum viable product and design-thinking in the IT-project team management. *Bulletin of the National Technical University "KhPI". Series: Strategic Management, Portfolio, Program and Project Management*, 2(4), 11-17. doi: 10.20998/2413-3000.2021.4.2.

[7] Božić, V. (2023). Microservices architecture. *ResearchGate*. doi: 10.13140/RG.2.2.21902.84802.

[8] Codd, E.F. (1990). *The relational model for database management* (2nd ed.). Boston: Addison-Wesley Longman Publishing.

[9] Date, C.J. (1975). *An introduction to database systems*. Boston: Addison-Wesley Longman Publishing.

[10] Eddin, S.K., Salloum, H., Shahin, M.N., Mazzara, M., & Bahrami, M.R. (2024). Quantum microservices: Transforming software architecture with quantum computing. In L. Barolli (Ed.), *Advanced information networking and applications* (pp. 227-237). Cham: Springer. doi: 10.1007/978-3-031-57942-4_23.

[11] Edirisinghe, D., Rajapakse, K., Abeysinghe, P., & Rathnayake, S. (2024). Cost-optimal microservices deployment with cluster autoscaling and spot pricing. In *Proceedings of the 2024 IEEE international conference on cloud computing technology and science (CloudCom)* (pp. 87-94). Abu Dhabi: IEEE. doi: 10.1109/CloudCom62794.2024.00026.

[12] Elkholy, M.I., & Marzok, M.A. (2022). Trusted microservices: A security framework for users' interaction with microservices applications. *Journal of Information Security and Cybercrimes Research*, 5(2), 135-143. doi: 10.26735/QOPM9166.

[13] Fritzsch, J., Bogner, J., Zimmermann, A., & Wagner, S. (2019). From monolith to microservices: A classification of refactoring approaches. In J.-M. Bruel, M. Mazzara & B. Meyer (Eds.), *Software engineering aspects of continuous development and new paradigms of software production and deployment* (pp. 128-141). Cham: Springer. doi: 10.1007/978-3-030-06019-0_10.
[14] Górski, T., & Wozniak, A.P. (2021). Optimization of business process execution in services architecture: A systematic literature review. *IEEE Access*, 9, 111833-111852. doi: 10.1109/ACCESS.2021.3102668.
[15] Grambow, M., Wittern, E., & Bermbach, D. (2020). Benchmarking the performance of microservice applications. *ACM SIGAPP Applied Computing Review*, 20(3), 20-34. doi: 10.1145/3429204.3429206.
[16] Iegorchenkov, O. (2016). Information systems integration of instrument-making enterprise. *Managing the Development of Complex Systems*, 28, 124-129.
[17] Lee, C., Kim, H.F., & Lee, B.G. (2024). A systematic literature review on the strategic shift to cloud ERP: Leveraging microservice architecture and MSPs for resilience and agility. *Electronics*, 13(14), article number 2885. doi: 10.3390/electronics13142885.
[18] Mukaj, J. (2023). *Containerization: Revolutionizing software development and deployment through microservices architecture using Docker and Kubernetes*. (Bachelor's thesis, Epoka University, Tirana, Albania). doi: 10.13140/RG.2.2.23804.51841.
[19] Ng, T., Rawi, A.A.B., Sum, C.S., Tso, E., Yau, P.C., & Wong, D. (2024). Migrating from monolithic to microservices with hybrid database design architecture. In *Proceedings of the 9th international conference on intelligent information technology* (pp. 536-541). New York: Association for Computing Machinery. doi: 10.1145/3654522.3654602.
[20] Oyeniran, O.C., Adewusi, A.O., Adeleke, A.G., Akwawa, L.A., & Azubuko, C.F. (2024). Microservices architecture in cloud-native applications: Design patterns and scalability. *Computer Science & IT Research Journal*, 5(9), 2107-2124. doi: 10.51594/csitrj.v5i9.1554.
[21] Rathore, N., Rajavat, A., & Patel, M. (2020). Investigations of microservices architecture in edge computing environment. In R.K. Shukla, J. Agrawal, S. Sharma, N.S. Chaudhari & K.K. Shukla (Eds.), *Social networking and computational intelligence* (pp. 77-84). Singapore: Springer. doi: 10.1007/978-981-15-2071-6_7.
[22] Sangabriel-Alarcón, J., Ocharán-Hernández, J.O., Cortés-Verdín, K., & Limón, X. (2023). Domain-driven design for microservices architecture systems development: A systematic mapping study. In *Proceedings of the 11th international conference in software engineering research and innovation* (pp. 25-34). León: IEEE. doi: 10.1109/CONISOFT58849.2023.00014.
[23] Shakhovska, N., & Tarasov, D. (2011). Technologies of data integration of information systems of Lviv Polytechnic National University. *Bulletin of Lviv Polytechnic National Univeristy. Series of Information Technology in Higher Education*, 703, 9-20.
[24] Singh, N., Hamid, Y., Juneja, S., Srivastava, G., Dhiman, G., Gadekallu, T.R., & Shah, M.A. (2023). Load balancing and service discovery using Docker Swarm for microservice based big data applications. *Journal of Cloud Computing*, 12(1), article number 4. doi: 10.1186/s13677-022-00358-7.
[25] Söylemez, M., Tekinerdogan, B., & Tahran, A.K. (2022). Challenges and solution directions of microservice architectures: A systematic literature review. *Applied Sciences*, 12(11), article number 5507. doi: 10.3390/app12115507.
[26] Wolfart, D., Assunção, W.K.G., da Silva, I.F., Domingos, D.C.P., Schmeing, E., Villaca, G.L.D., & Paza, D.D.N. (2021). Modernizing legacy systems with microservices: A roadmap. In *Proceedings of the 25th international conference on evaluation and assessment in software engineering* (pp. 149-159). New York: Association for Computing Machinery. doi: 10.1145/3463274.3463334.
[27] Zhelev, S., & Rozeva, A. (2019). Using microservices and event driven architecture for big data stream processing. *AIP Conference Proceedings*, 2172, article number 090010. doi: 10.1063/1.5133587.

Архітектура мікросервісів для ERP-систем

Сергій Слівка
Аспірант
Національний університет «Одеська політехніка»
65044, просп. Шевченка, 1, м. Одеса, Україна
https://orcid.org/0009-0003-1704-1415

Анотація. Традиційні системи управління ресурсами підприємства (ERP), побудовані за принципом монолітної архітектури, стають все менш ефективними в сучасному бізнес-середовищі. Зростаюча складність виробничих процесів, збільшення обсягів даних та необхідність швидкої адаптації до змін створюють значні виклики для таких систем. Метою дослідження були аналіз та розробка методів переходу від монолітної архітектури до мікросервісної в ERP-системах для забезпечення їх масштабованості, гнучкості та безпеки. Проведено комплексний аналіз клієнт-серверної архітектури ERP-систем та їх основних компонентів, включаючи реляційні бази даних і запити на мові структурованих запитів (SQL). Досліджено принципи роботи функцій і процедур, взаємодії між таблицями та створення запитів у системах з великою кількістю користувачів. Також були розглянуті сучасні стратегії декомпозиції монолітних систем на мікросервіси, включаючи методи синхронізації даних та управління компонентами. Наголошено на аспектах безпеки та ризиках переходу до мікросервісної архітектури. Розроблено підходи до трансформації ERP-систем на основі мікросервісної архітектури, що дозволяє знизити складність управління, підвищити продуктивність і знизити ризики в бізнес-процесах. Запропоновано механізми ефективного синхронізованого обміну даними між компонентами та забезпечення їх надійності. Дослідження визначило, що мікросервісна архітектура дає можливість незалежного масштабування окремих елементів системи, підвищуючи відмовостійкість та продуктивність при високих навантаженнях. Були досліджені та вирішені поширені проблеми, включаючи неправильні баланси та помилки у звітах. Розроблені підходи можуть бути використані для модернізації ERP-систем великих підприємств, особливо у виробничому секторі, де важлива висока продуктивність і точність обробки даних

Ключові слова: клієнт-серверна; масштабованість; стейкхолдер; критичний шлях; критична подія; автоматизація; хмарні технології

BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en Vol. 29 No. 4. 2024

UDC 004.056.55:004.75
DOI: 10.62660/bcstu/4.2024.43

Integration of blockchain technologies into cybersecurity systems for critical infrastructure facilities: Prospects and challenges

Viktor Danchuk*
Doctor of Physical and Mathematical Sciences, Professor
National Transport University
01010, 1 M. Omelianovych-Pavlenko Str., Kyiv, Ukraine
https://orcid.org/0000-0003-4282-2400

Mariia Danchuk
PhD in Economic Sciences, Associated Professor
National Transport University
01010, 1 M. Omelianovych-Pavlenko Str., Kyiv, Ukraine
https://orcid.org/0009-0007-3033-3227

Abstract. The purpose of the study was to analyse the potential and main problems of integrating blockchain technologies into the processes of ensuring cybersecurity of critical infrastructure facilities in Ukraine. As part of the work, the potential of blockchain technologies in improving the security of critical infrastructures was analysed, the existing challenges of scaling and performance of such systems were assessed, and the possibilities of international cooperation for implementing innovative solutions in the field of cybersecurity were explored. The paper provided a comprehensive analysis of the prospects for integrating blockchain technologies into cybersecurity systems for critical infrastructure facilities. To ensure the relevance of the study, the technical features of the blockchain, such as consensus mechanisms, data distribution models, and cryptographic methods, were considered. It was found that blockchain technologies provide increased transparency, resistance to cyber threats, and optimisation of access control to critical data. At the same time, the main challenges remain low scalability of systems, limited transaction speed, and high energy costs, which complicates their large-scale implementation. The study also showed that there is a need to adapt regulatory requirements to improve the efficiency of blockchain integration into infrastructure facilities. The study demonstrated the significant potential of blockchain technologies as one of the key components in building sustainable cybersecurity systems. The conclusions of the paper emphasise the need for an interdisciplinary approach to the implementation of technologies, including technical, economic, and regulatory aspects, to increase the level of security of critical infrastructure facilities in the context of growing cyber threats. In addition, the paper highlights the importance of international cooperation, which will combine resources and expertise to create more effective and innovative solutions in the field of cybersecurity

Keywords: distributed ledgers; data management; regulatory aspects; cryptography; digital trust

INTRODUCTION

The development of modern technologies and their integration into critical infrastructure systems create not only new opportunities, but also increase the vulnerability of such objects to cyber threats. Industrial control systems, energy complexes, transport networks, and medical facilities are becoming targets for

Article's History: Received: 08.07.2024; Revised: 25.10.2024; Accepted: 16.12.2024.

Suggested Citation:
Danchuk, V., & Danchuk, M. (2024). Integration of blockchain technologies into cybersecurity systems for critical infrastructure facilities: Prospects and challenges. *Bulletin of Cherkasy State Technological University*, 29(4), 43-52. doi: 10.62660/bcstu/4.2024.43.

*Corresponding author

intruders, threatening national security and stability. In the face of increasing complexity of cyber-attacks, traditional protection methods are often insufficient for the security of such facilities. This highlights the need to apply innovative solutions, among which blockchain technology occupies a special place. Blockchain, originally developed as the foundation of cryptocurrencies, demonstrates potential in a wider range of applications, including cybersecurity. Its key features – decentralisation, immutability of records, and a high level of transparency and reliability – make it a promising tool for protecting data and infrastructure systems. In the context of critical infrastructure, blockchain can be used to improve the security of access control systems, monitor networks, and prevent unauthorised interference. However, the process of integrating blockchain into cybersecurity systems involves a number of challenges. Among them, the high power consumption of some blockchain solutions, limited scalability and the need to ensure compatibility with existing systems stand out. In addition, there are still issues of regulatory regulation and standardisation of such technologies, which complicates their widespread implementation.

The analysis of studies by various researchers demonstrated a wide range of approaches to integrating blockchain technologies into cybersecurity systems. For example, A. Iskryzhytskii & A. Zadorozhnii (2024) emphasised the benefits of decentralised data storage, stressing that the use of blockchain technologies reduces the risk of successful attacks on centralised access points. In turn, N. Mohamed & A.A. Ahmed (2024) investigated the effectiveness of the technology in preventing "man-in-the-middle" attacks and concluded that the use of smart contracts significantly reduced the risks of unauthorised interference. E. Barka *et al.* (2022) focused on using blockchain to control access to critical infrastructure resources. The researchers noted that the introduction of decentralised identifiers improved the reliability of user identification and authentication systems. On the other hand, A. Ali *et al.* (2023) analysed the scalability and power consumption issues of blockchain systems, offering solutions based on hybrid architectures that combine the advantages of blockchain and conventional databases.

Q. Wang & M. Su (2020) studied examples of successful blockchain applications in the energy sector. Their findings showed that the use of technology in energy distribution and smart grid management reduces the likelihood of disruptions due to cyber-attacks. The study by J. Horner & P. Ryan (2019) focused on the regulatory aspects of blockchain implementation, pointing out the need for international standardisation to ensure technology compatibility. D. Kobets & O. Runov (2024) explored the potential of blockchain in medical infrastructure, emphasising its ability to guarantee a high level of protection of medical data, preventing their falsification or unauthorised disclosure. L. Koh *et al.* (2020) analysed the technology's capabilities in transport systems, where blockchain has increased the transparency and reliability of logistics operations. A.A. Zainuddin *et al.* (2024) investigated the synergistic effect of sharing blockchain and artificial intelligence technologies in threat detection systems. Their results highlight that integrating these approaches improves the analysis capabilities and performance of cybersecurity systems. In addition, K. Košťál *et al.* (2019) considered the use of blockchain in the field of monitoring network events. In their study, they argued that a decentralised logging system prevented the possibility of changing or deleting suspicious activity records, which increased the overall level of cybersecurity.

Despite significant advances in blockchain technology applications, several key issues remained unresolved. Methods for integrating blockchain with traditional cybersecurity systems have not been sufficiently studied, especially in conditions of limited computing resources. They also required additional analysis of the issue of scaling blockchain solutions for large-scale critical infrastructure facilities. There were also no comprehensive studies on the cost-effectiveness and profitability of implementing blockchain in such systems. The purpose of the study was to analyse the potential and limitations of using blockchain technologies in cybersecurity systems of critical infrastructure facilities, with an emphasis on their integration, scalability, and cost-effectiveness. The objectives of the study were: to conduct a comparative analysis of existing approaches to the integration of blockchain technologies into the cybersecurity system; to assess the limitations and scalability of blockchain solutions for large infrastructure facilities; to investigate the economic efficiency of using blockchain in the context of improving the sustainability of critical infrastructure.

MATERIALS AND METHODS

Critical infrastructure ensures the functioning of society, economic stability and national security. Therefore, the development of effective methods of its protection has become a key task of modern cybersecurity. The approach to studying this issue was based on the analysis of traditional security methods and innovative technologies, in particular blockchain. At the first stage of the study, an overview of existing solutions was made. Conventional methods, such as multi-level protection, remain the foundation of modern cybersecurity systems. These include the use of firewalls, intrusion detection and prevention systems (IDS/IPS), antivirus software, and data encryption. Such systems are effective against many threats, but face limitations in the face of complex attacks such as "zero-day" or Advanced Persistent Threats (APT).

The main focus was on the analysis of conventional security methods and innovative technologies, in particular blockchain. The territorial boundaries of the study covered Ukraine in order to assess specific challenges and implement technologies in Ukrainian critical

infrastructure. The experience of Ukraine was compared with the leading practices of countries that actively use blockchain in the field of cybersecurity, such as: Israel, the EU countries and the USA (Chowdhury & Gkioulos, 2021; Yu *et al.*, 2021; Joint Statement on..., 2023). Among the areas of implementation of blockchain technologies in Ukraine were considered: energy, financial systems, healthcare, and cybersecurity. The Ukrainian experience was compared with innovations in these countries, which helped to identify common trends and specific challenges (Implementation of blockchain..., 2023; Kozhemiakin, 2023; Shevchuk *et al.*, 2024).

Exploring a multi-level architecture that combines multiple security mechanisms has been key to understanding how different technologies can interact to maximise efficiency. The study also focused on analysing mechanisms such as access control, network segmentation, and artificial intelligence-based solutions for detecting anomalies. Such systems create backup mechanisms that can be activated in the event of an attack, but their implementation often requires significant resources. Further, the potential of the latest technologies, in particular blockchain, was investigated. This technology offers unique cybersecurity solutions due to its decentralised nature, which ensures a high level of data integrity. The study examined ways to use blockchain to control access, monitor threats, and ensure transparency in system management. For example, saving a history of changes and transactions on the blockchain allows quickly identifying possible threats and violations.

Another important stage was the study of the limitations and challenges of implementing blockchain in the Ukrainian critical infrastructure. In particular, attention was paid to regulatory issues, high implementation costs, and the need to adapt to existing management systems. Special attention was paid to the problems of scalability and performance of blockchain technologies. These aspects were critical for applications in infrastructures that require real-time processing of large amounts of data. The analysis focused on solutions such as layer architectures, sharding, and the use of Proof-of-Stake consensus mechanisms. The final stage of the study was based on the limitations and challenges of blockchain implementation.

RESULTS

Ensuring the cybersecurity of critical infrastructure is a key challenge to prevent economic damage, social consequences, and possible threats to national security. In this context, various security approaches are based on the use of both conventional methods and the latest technologies, in particular blockchain. Conventional approaches include the use of multi-level security systems that involve the use of firewalls, IDS/IPS systems, antivirus software, and data encryption tools. These methods provided a basic level of protection, but were not always effective in more complex attacks, such as zero-day attacks or APTs. Centralised architectures often faced problems controlling large amounts of data simultaneously, which made it difficult to detect and neutralise threats in real time. One of the approaches that was actively used was multi-level protection, which combined several types of tools. This included access control, network segmentation, an information security management system that collects, analyses, and responds to incidents in real time, and artificial intelligence-based solutions for predicting and detecting anomalies. A multi-level security system created backup mechanisms that could be activated in the event of an attack on one of the levels, but the implementation of such systems was often expensive and complex.

With the development of technology, it became possible to integrate the latest solutions to improve the effectiveness of protection. Among them were systems based on machine learning and artificial intelligence, which allowed automating the processes of analysing large amounts of data and quickly identifying potential threats. However, the implementation of such solutions required significant investment and a high level of technical training (Ullah *et al.*, 2020). Blockchain technologies offered a new approach to security based on decentralised data storage and management, which allowed changing or deleting them without the consent of all network participants. This provided a high level of data integrity and increased resistance to cyber-attacks. In particular, the blockchain was used to create access control systems, monitor and detect threats, and to save the history of changes and transactions in systems, which increased transparency and control over access to data. Despite all the advantages, the use of blockchain technologies in cybersecurity had its limitations. These included high implementation costs, the need for significant computing resources, and the potential vulnerability to new types of attacks targeting the blockchain technology itself. In addition, the regulation of blockchain systems remained insufficiently clear in many countries, which made it difficult to implement them in existing critical infrastructure frameworks. Consequently, modern approaches to ensuring the cybersecurity of critical infrastructure required a combination of conventional methods with the latest technologies, in particular blockchain, which created new opportunities for strengthening protection, but also posed new challenges that needed to be addressed (Habib *et al.*, 2022).

Scalability and performance are key factors that determine the effectiveness of using blockchain technologies in cybersecurity systems, especially for critical infrastructure facilities. These aspects relate to the ability of blockchain systems to process large amounts of data and the number of transactions in real time, which is important for ensuring their functionality at the level of modern industrial systems (Smith & Dhillon, 2020). The scalability of blockchain technologies was related to their ability to process a large number of

transactions in a certain period of time without losing performance. The blockchain worked on the principle of adding blocks with transactions to the chain using a consensus mechanism, which ensured data security and integrity, but often led to transaction delays, especially in high-load systems.

In addition, technologies can be used to reduce the load on the main blockchain. This included solutions such as a layered architecture, where transaction processing takes place at a second level (for example, a solution based on the Lightning Network in Bitcoin or a solution based on the Polygon platform for Ethereum). Other methods include sharding, which involves splitting data into separate parts, which reduces the load on each individual network node. In this approach, each node processes only a fraction of transactions, which significantly increases the overall network bandwidth. In addition, Proof-of-Stake, instead of the traditional Proof-of-Work, which uses significantly less computing power, allows reducing energy costs and improving performance.

The performance of blockchain systems is measured by the number of transactions they can process per unit of time and the time required to verify transactions (Shapovalova *et al.*, 2024). For critical infrastructure applications, high performance is a prerequisite for smooth system operation. Performance lags lead to delays, which can affect the speed of response to cyber threats (Pacheco *et al.*, 2023). Modern blockchain platforms work to optimise performance using various approaches. For example, platforms that support the concept of hybrid consensus combine various transaction verification mechanisms to ensure fast processing and high security. This allows reducing the cost of processing transactions and increasing the overall speed of the system.

Challenges that arise when implementing scalable and productive blockchain systems include the need for powerful computing resources, which may be economically impractical for some organisations. In addition, the security of these systems can be compromised due to various vulnerabilities associated with new integration methods, which requires detailed testing and additional measures to ensure their sustainability. Thus, issues of scalability and performance of blockchain systems remain important for the implementation of these technologies in critical infrastructure, and require a comprehensive approach, including the development of new technological solutions and optimisation of existing protocols (Nasir *et al.*, 2022).

The protection of critical infrastructure is a particularly important task, as these facilities provide the main functions that support the life of society, economic stability, and national security. Given the growth of cyber-attacks and the complexity of modern threats, the integration of blockchain technologies opens up new prospects for strengthening the cybersecurity of critical objects. Blockchain can become a powerful tool for data protection, access control, and ensuring the transparency and integrity of information systems (Radvanovsky & McDougall, 2023). One of the key advantages of blockchain technologies is decentralisation. In critical infrastructure systems, this means that data is not stored in a single centralised location, which can become the target of a cyberattack. The decentralised structure of the blockchain provides distributed storage of information on many nodes of the network, which makes it difficult to change or delete it without authorisation. This significantly reduces the risks associated with a single-node attack and makes the system more resistant to large-scale cyber-attacks, including DDoS attacks.

Blockchain technologies guarantee data integrity due to cryptographic transaction protection and a hashing mechanism that eliminates unauthorised information changes. This is especially important for critical infrastructure, where ensuring the reliability of data is a prerequisite for proper functioning. In addition, the blockchain provides transparency by being able to track all changes in the system, which allows conducting audits and identifying potential violations in real time. This creates a new level of trust between system participants and makes it difficult to fake or conceal important information (Wei *et al.*, 2020).

Integration of blockchain technologies allows creating effective access control systems for critical infrastructure objects. Smart contracts allow automating the process of granting or revoking access based on certain conditions. Such systems can use decentralised identifiers to authenticate users, which provides a high level of protection against fraud and abuse. If necessary, access can only be restricted to a certain circle of authorised persons, and All Access changes are automatically recorded in the blockchain, which makes the system transparent and controlled. Blockchain-based systems have the potential to detect and prevent cyber-attacks due to their decentralised nature and ability to process data in real time. Blockchain integration with monitoring systems allows creating dynamic anomaly detection mechanisms that help to track unauthorised changes and respond to potential threats in time. Smart contracts can automatically block or restrict access if suspicious activity is detected, which increases the overall level of infrastructure security.

Despite the great potential, the introduction of blockchain technologies in critical infrastructure protection systems is accompanied by some problems. These include the high cost of implementation, the need for significant computing resources, and compatibility issues with existing systems. In addition, the blockchain may have restrictions on the speed of transaction processing, which may affect its application in large systems with high speed requirements (Wisniewski *et al.*, 2022). In general, the integration of blockchain technologies into cybersecurity systems for critical infrastructure facilities opens up new opportunities for strengthening data protection, access control,

and transparency. However, for widespread implementation, it is necessary to overcome certain technical and economic barriers and ensure that new solutions comply with regulatory requirements and safety standards.

In the modern world, technological innovations are becoming the driving force behind development. This is especially relevant for critical infrastructure, which, in the context of global digitalisation and growing cyber threats, requires a radical approach to security and efficiency (Safitra *et al.*, 2023). Blockchain is one of these technologies that, despite its relatively recent emergence, has already proven its ability to change the functioning of many industries. In the energy sector of Ukraine, blockchain opens up new horizons for decentralising network management (Semenenko *et al.*, 2024).

In transport and logistics, blockchain is becoming a key tool for ensuring transparency in supply chains. The use of smart contracts for cargo tracking not only minimises bureaucratic delays, but also creates conditions for combating corruption in customs processes (Pournader *et al.*, 2020). This is especially important for Ukraine, which is an important transport hub in Europe. Healthcare also benefits from blockchain integration. Storing patients' medical data in decentralised systems minimises the risk of loss or theft, while providing quick access for authorised users. Such initiatives contribute to the development of e-health, which is becoming relevant in the context of crises and pandemics. Despite the obvious advantages, the implementation of blockchain faces a number of challenges. These include high initial costs, the need for high technical competence, and insufficient legislative regulation. The issue of cybersecurity of the blockchain infrastructure itself is also important, because errors in smart contracts can become a source of vulnerabilities.

The integration of blockchain technologies into Ukraine's critical infrastructure is a challenge that simultaneously opens up significant prospects. Energy, transportation, healthcare, and finance are already demonstrating the effectiveness of this technology in combating cyber threats, corruption, and inefficiency. The success of this process depends on the interaction of the state, business and society, and on the willingness to invest in training, infrastructure and legislative support. For Ukraine, this is an opportunity not only to strengthen its infrastructure, but also to become a leader in innovation in the region. Table 1 shows the prospects for implementing blockchain technologies in the critical infrastructure of Ukraine.

Table 1. Implementation of blockchain technologies in critical infrastructure of Ukraine: key areas and opportunities

Scope of application	Research/Projects in Ukraine	Quantitative data/Results
Energy	Pilot project of blockchain systems for energy consumption accounting	Reducing energy losses in a pilot project
Healthcare	Development of a system for storing medical data on the blockchain	Medical records are more protected from unauthorised access as part of testing
Financial sector	Blockchain integration for banking transactions	Reducing the time of international transfers
Transport and logistics	Implementation of blockchain solutions for cargo tracking	Delivery efficiency increased transparency of customs procedures
Electoral systems	Pilot project of electronic voting on the blockchain	Participants rated system security as high
Government infrastructure management	Using blockchain in the land cadastre	Cadastre records are stored in a decentralised system

Source: developed by the authors based on Implementation of blockchain technology in healthcare in 2023 (2023), S. Kozhemiakin (2023), M. Shevchuk *et al.* (2024)

Table 1 shows that blockchain technologies have significant potential in modernising Ukraine's critical infrastructure. Due to its decentralised nature, blockchain can provide transparency and security in industries such as energy, transportation, healthcare, and the financial sector. Significant steps have already been taken in the implementation of this technology in 2024, in particular, in projects to decentralise energy networks and pilot initiatives to use the e-Hryvnia. Such examples indicate prospects for improving the efficiency of resource management and the resilience of systems to cyber-attacks.

However, for the widespread adoption of blockchain in critical infrastructure, a number of challenges must be overcome. These include insufficient funding, the need for high technical competence, and imperfect legislative regulation. Solving these problems requires coordinated efforts by the state, business, and educational institutions. Ukraine has every chance to become an innovator in the use of blockchain in critical industries, which will increase its competitiveness and ensure greater reliability of national systems. Ukraine is actively developing international cooperation in the field of blockchain technologies to ensure cybersecurity of critical infrastructure facilities. The main areas of this interaction are the exchange of experience, implementation of advanced technical solutions and joint development of the latest security systems.

Despite significant prospects, Ukraine faces numerous challenges. This includes instability of domestic

funding and insufficient legal framework to support innovation. For example, the lack of uniform standards and regulations in the field of blockchain solutions complicates their implementation at the national level. In addition, the need for harmonisation with international law requires time and considerable resources. However, cooperation with international partners allows to overcome these barriers, gradually strengthening the cyber defence of critical facilities in the country. Table 2 shows Ukraine's international cooperation in the implementation of blockchain technologies for cybersecurity of critical infrastructure.

Table 2. International cooperation of Ukraine in the implementation of blockchain technologies for cybersecurity of critical infrastructure

Country	Area of cooperation	Prospects	Challenges
USA	Exchange of experience, training of experts, support of Ukrainian initiatives	Access to innovative solutions, joint projects in the field of cybersecurity	Unstable political situation in Ukraine, restrictions on funding
EU	Technological assistance, implementation of blockchain solutions for public administration	Use of Estonia's best practices, integration with European standards	Differences in legislation and infrastructure readiness levels
Israel	Joint research in the field of cybersecurity, exchange of analytical data on threats	Development of advanced technologies to protect critical systems	Maintaining a stable level of security in the face of global threats
Poland	Development of regional cooperation programmes in the field of cybersecurity of critical infrastructure	Strengthening regional security, creating compatible solutions for blockchain platforms	Lack of a unified system of standards in the region

Source: developed by the authors based on Israel and Ukraine face shared cyber threats (2023), Joint Statement on the United States-European Union 9th Cyber Dialogue in Brussels (2023)

Ukraine has a significant potential for using blockchain technologies in cybersecurity, because these technologies provide decentralised, transparent, and reliable data exchange. Due to partnership with leading countries in this area, such as the United States and Israel, Ukraine gets access to the latest solutions. In particular, the use of blockchain can improve the protection of state registers, monitor data in real time, and optimise the management of critical infrastructure. The integration of these technologies helps to ensure the continuity of systems even during cyber-attacks, which is a key task for the country in modern conditions.

An important aspect is the development of the regulatory framework for blockchain implementation. Ukraine is actively working to harmonise its laws with international standards, which makes it possible to simplify cooperation with other countries. For example, the adoption of laws on digital assets and regulation of blockchain technologies creates a favourable environment for attracting foreign investment and technology. Moreover, it helps to increase the level of trust in Ukrainian cybersecurity projects.

However, to achieve success, it is necessary to overcome significant challenges. Ukraine needs more funding for the development of blockchain infrastructure and training of specialists in this field. In addition, it is necessary to strengthen cooperation with regional partners, such as Poland, to create common protection systems. Strengthening these relations and utilising international experience will allow Ukraine to integrate blockchain into its systems and become one of the leaders in this field in Eastern Europe.

DISCUSSION

Ensuring the cybersecurity of critical infrastructure is crucial for preventing economic losses, social consequences, and threats to national security. The presented results confirm that the integration of conventional approaches with modern technologies, such as blockchain, allows creating more effective security systems. The main elements of multi-level protection are firewalls, IDS/IPS systems, antivirus software, and data encryption tools. Despite their basic effectiveness, such methods are not always able to counteract complex attacks, such as APT or zero-day attacks. Centralised architectures often face problems handling large amounts of data, which makes it difficult to detect threats in real time. K. Yu *et al.* (2021) investigated the effectiveness of conventional methods of protecting critical infrastructure, in particular the use of multi-level security systems. Their results confirm that firewalls and IDS/IPS provide a basic level of protection, but are not always effective against modern threats, such as zero-day attacks. This is consistent with current results, but the researchers emphasise a greater reliance on the human factor in incident response, which was not the main focus of the current study. This creates the need to introduce new technologies to improve security efficiency. N. Chowdhury & V. Gkioulos (2021) investigated the effectiveness of conventional critical infrastructure security tools, such as multi-level security systems. They noted that while firewalls and IDS/IPS provide a basic level of protection, they are not always effective enough against the latest threats, especially zero-day attacks. This correlates with current results, but the research-

ers emphasise the greater role of the human factor in Incident Response, which was not the main focus of this study. This highlights the need to introduce innovative technologies to improve the effectiveness of protection.

C. Große *et al*. (2021) conducted a study of conventional approaches to protecting critical infrastructure, in particular, the use of firewalls, IDS/IPS systems, and antivirus software. They note that while these methods provide a basic level of protection, they are not effective enough to deal with more complex threats, such as APT or zero-day attacks. In addition, centralised architectures face difficulties when processing large amounts of data, which makes it difficult to quickly detect threats. The researchers also emphasise that the human factor plays an important role in responding to incidents, which increases the need to introduce new technological solutions to improve security. The current results describe in more detail the practical implementation of blockchain technologies in Ukraine, in particular, in the energy, healthcare, and transport sectors, and focus on international cooperation.

Blockchain technologies offer a decentralised approach to data storage and management, which significantly increases their resistance to cyber-attacks. The immutability of data in the blockchain creates a high level of integrity and transparency, which is critical for monitoring and managing access to information systems. D. Berdik *et al*. (2021) investigated cybersecurity and blockchain technologies, namely, the use of blockchain to ensure the protection of information systems in real time. They focused on the benefits of a decentralised approach to data storage and management, improving the integrity and transparency of information, and automating access processes through smart contracts. The implementation of the blockchain allows automating access processes using smart contracts that ensure the accuracy of meeting specified conditions. The current results also identified the advantages of a decentralised architecture, in particular, in the context of reducing the risks of attacks on a single data storage point, which coincides with the authors' results. However, the current study focuses more on the use of blockchain specifically for critical infrastructure, while the researchers focus more on general aspects of cybersecurity.

The main challenges remain high implementation costs, the need for significant computing resources, and unresolved compatibility issues with existing systems. In addition, the regulation of blockchain technologies in many countries is still at an early stage, which can make it difficult to integrate them into critical infrastructure. Performance limitations of blockchain systems, such as slow transaction processing, also affect their applicability in large-scale systems with high speed requirements. I. Tibrewal *et al*. (2022) analysed the use of blockchain technologies in critical infrastructure. They argued that the main advantage is transparency and the inability to change data, but noted that blockchain is too expensive and difficult to implement in small organisations. This is consistent with current findings, although the researchers do not focus on scalability issues, which are considered critical in the current paper. T.R. Vance & A. Vance (2019) investigated the application of blockchain technologies in critical infrastructure, focusing on their ability to provide transparency and protect data from changes. However, they also emphasised the high cost and complexity of integrating these technologies into small organisations. This is consistent with the current results, but the researchers did not address the scalability issues that are key in the current study. M.K. Hasan *et al*. (2022) investigated the implementation of blockchain technologies in the field of protecting critical infrastructure, paying attention to their ability to guarantee data openness and protection against unauthorised changes. However, they noted that the significant costs and complexity of implementation limit the use of these technologies in small organisations. In contrast to this approach, the current paper focuses on scalability, which is crucial for a successful blockchain application.

The success of using a blockchain largely depends on its ability to process large amounts of data in real time. Second-tier technologies, such as the Lightning Network or sharding, offer solutions to reduce the load on the underlying blockchain. Replacing the Proof-of-Work consensus mechanism with Proof-of-Stake reduces energy costs and improves productivity. C.T. Nguyen *et al*. (2019) investigated the performance of blockchain systems and proposed the use of hybrid approaches, such as Proof-of-Stake. They concluded that these methods can significantly improve the speed of real-time transaction processing. The current study also considered this approach, but focused more on implementation issues due to the complexity of settings and compatibility with existing systems. However, critical infrastructure requires careful testing of these solutions to ensure that they are resistant to new types of attacks.

M. Warkentin & C. Orgeron (2020) explored the legal aspects of implementing blockchain technologies in developing countries, in particular, in the context of national security. They noted that insufficiently regulated legislation creates serious barriers to the widespread adoption of these technologies in critical infrastructure. This coincides with the current conclusions, which pointed out the need to develop a regulatory framework for regulating the use of blockchain. However, the researchers focused more on the legal aspects, while the current study focused on the technical and economic problems of implementation. R. Zambrano (2020) considered the legal challenges that arise when implementing blockchain technologies in developing countries, with a focus on national security. He emphasised that the lack of developed legislation is a serious barrier to the integration of blockchain into critical infrastructure, as countries must create appropriate regulations for the successful implementation of these technologies. The current results focused more on the severity of the barriers created by insufficient legislative development, while the researcher focused

on the fact that countries should create the necessary regulations for the implementation of technologies.

Ensuring the cybersecurity of critical infrastructure requires combining traditional approaches with modern technologies, such as blockchain, to create more sustainable and effective security systems. The analysis shows that although conventional methods provide a basic level of security, their limitations in countering modern threats, centralised architecture and dependence on the human factor emphasise the need for innovative solutions. Blockchain shows significant potential through transparency, data immutability, and decentralisation, but its integration into critical infrastructure faces scalability, cost, and compatibility challenges. Effective application of these technologies requires both technological improvement and adaptation of the regulatory framework.

CONCLUSIONS

In the course of the study, a comprehensive analysis of modern approaches to ensuring cybersecurity of critical infrastructure facilities was carried out, with an emphasis on the integration of blockchain technologies. It was established that ensuring cybersecurity is a key task for preventing economic losses, social consequences, and potential threats to national security. Conventional methods, such as multi-level security systems using firewalls, IDS/IPS systems, antivirus software, and data encryption tools, provide a basic level of protection. However, their effectiveness is often limited in the face of complex attacks, such as zero-day attacks or APTs. Centralised data management systems have also been vulnerable to scalability and real-time issues.

With the development of technology, it became possible to implement the latest solutions, in particular, based on machine learning, artificial intelligence, and blockchain technologies. Blockchain allows creating decentralised data storage and management systems, which ensures their integrity, transparency and increases resistance to cyber-attacks. In particular, the technology has found application in access control, monitoring and detecting threats, and in maintaining the history of changes and transactions. However, the introduction of blockchain is accompanied by challenges. These include high implementation costs, significant computing resource requirements, compatibility issues with existing systems, and limited transaction processing speed in large-scale systems. It was noted that solutions such as multi-layer architectures, sharding, and hybrid consensus mechanisms are being actively developed to overcome these limitations.

The analysis revealed that the integration of blockchain technologies into the critical infrastructure of Ukraine has significant potential. The implementation of pilot projects in the fields of energy, transport, healthcare, and finance confirmed the effectiveness of blockchain in the fight against cyber threats, corruption, and inefficiency. In particular, blockchain helped to increase the level of data protection, reduce transaction processing time, and increase the transparency of processes. Limitations of the study were the complexity of fully evaluating the effectiveness of blockchain technologies due to the lack of large-scale practical implementations and limited data on their impact on real cyber threats. Further research should focus on developing solutions to improve the scalability and performance of the blockchain, and adapting these technologies to the specifics of critical infrastructure.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Ali, A., Ali, H., Saeed, A., Ahmed Khan, A., Tin, T.T., Assam, M., Ghadi, Y.Y., & Mohamed, H.G. (2023). Blockchain-powered healthcare systems: Enhancing scalability and security with hybrid deep learning. *Sensors*, 23(18), article number 7740. doi: 10.3390/s23187740.

[2] Barka, E., Kerrache, C.A., Benkraouda, H., Shuaib, K., Ahmad, F., & Kurugollu, F. (2022). Towards a trusted unmanned aerial system using blockchain for the protection of critical infrastructure. *Transactions on Emerging Telecommunications Technologies*, 33(8), article number e3706. doi: 10.1002/ett.3706.

[3] Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. *Information Processing & Management*, 58(1), article number 102397. doi: 10.1016/j.ipm.2020.102397.

[4] Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, 40, article number 100361. doi: 10.1016/j.cosrev.2021.100361.

[5] Große, C., Olausson, P.M., & Wallman-Lundåsen, S. (2021). Left in the dark: Obstacles to studying and performing critical infrastructure protection. *Electronic Journal of Business Research Methods*, 19(2), 58-70. doi: 10.34190/ejbrm.19.2.2509.

[6] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future Internet*, 14(11), article number 341. doi: 10.3390/fi14110341.

[7] Hasan, M.K., Alkhalifah, A., Islam, S., Babiker, N.B.M., Habib, A.K.M.A., Aman, A.H.M., & Hossain, M.A. (2022). Blockchain technology on smart grid, energy trading, and big data: Security issues, challenges, and recommendations. *Wireless Communications and Mobile Computing*, 2022(1), article number 9065768. doi: 10.1155/2022/9065768.

[8] Horner, J., & Ryan, P. (2019). Blockchain standards for sustainable development. *Journal of ICT Standardization*, 7(3), 225-248. doi: 10.13052/jicts2245-800X.733.
[9] Implementation of blockchain technology in healthcare in 2023. (2023). Retrieved from https://stfalcon.com/uk/blog/post/implementation-of-blockchain-technology-in-healthcare.
[10] Iskryzhytskii, A., & Zadorozhnii, A. (2024). Study of available methods and technologies for decentralized storing and administration of public data. *Technical Sciences and Technologies*, 2(36), 137-150. doi: 10.25140/2411-5363-2024-2(36)-137-150.
[11] Israel and Ukraine face shared cyber threats. (2023). Retrieved from https://www.fdd.org/analysis/2023/11/13/israel-and-ukraine-face-shared-cyber-threats/.
[12] Joint Statement on the United States-European Union 9th Cyber Dialogue in Brussels. (2023). Retrieved from https://surl.li/ooyrtk.
[13] Kobets, D., & Runov, O. (2024). Integration of blockchain technologies in the personnel potential management system of medical institutions. *Innovation and Sustainability*, 4(1), 112-119. doi: 10.31649/ins.2024.1.112.119.
[14] Koh, L., Dolgui, A., & Sarkis, J. (2020). Blockchain in transport and logistics – paradigms and transitions. *International Journal of Production Research*, 58(7), 2054-2062. doi: 10.1080/00207543.2020.1736428.
[15] Košťál, K., Helebrandt, P., Belluš, M., Ries, M., & Kotuliak, I. (2019). Management and monitoring of IoT devices using blockchain. *Sensors*, 19(4), article number 856. doi: 10.3390/s19040856.
[16] Kozhemiakin, S. (2023). *Blockchain in Ukraine is used at the state level: 4 main areas are named*. Retrieved from https://hub.obozrevatel.com/ukr/blokchejn-dlya-ukraintsiv-yak-zastosue-kriptotehnologiyu-mintsifru.htm.
[17] Mohamed, N., & Ahmed, A.A. (2024). AI in combatting man-in-the-middle attacks: A comprehensive review. In *Proceedings of the 15th international conference on computing communication and networking technologies* (pp. 1-6). Kamand: IEEE. doi: 10.1109/ICCCNT61001.2024.10725789.
[18] Nasir, M.H., Arshad, J., Khan, M.M., Fatima, M., Salah, K., & Jayaraman, R. (2022). Scalable blockchains – a syste matic review. *Future Generation Computer Systems*, 126, 136-162. doi: 10.1016/j.future.2021.07.035.
[19] Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. *IEEE Access*, 7, 85727-85745. doi: 10.1109/ACCESS.2019.2925010.
[20] Pacheco, M., Oliva, G., Rajbahadur, G.K., & Hassan, A. (2023). Is my transaction done yet? An empirical study of transaction processing times in the Ethereum blockchain platform. *ACM Transactions on Software Engineering and Methodology*, 32(3), article number 59. doi: 10.1145/3549542.
[21] Pournader, M., Shi, Y., Seuring, S., & Koh, S.C.L. (2020). Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. *International Journal of Production Research*, 58(7), 2063-2081. doi: 10.1080/00207543.2019.1650976.
[22] Radvanovsky, R., & McDougall, A. (2023). *Critical infrastructure: Homeland security and emergency preparedness*. Boca Raton: CRC Press. doi: 10.4324/9781003346630.
[23] Safitra, M.F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability*, 15(18), article number 13369. doi: 10.3390/su151813369.
[24] Semenenko, O., Nozdrachov, O., Chernyshova, I., Melnychenko, A., & Momot, D. (2024). Innovative technologies to improve energy efficiency and security of military facilities. *Machinery & Energetics*, 15(4), 147-156. doi: 10.31548/machinery/4.2024.147.
[25] Shapovalova, N., Dotsenko, I., Trachuk, A., & Skrynnikov, I. (2024). Applying artificial intelligence tools for time series analysis. *Journal of Kryvyi Rih National University*, 22(1), 46-51. doi: 10.31721/2306-5451-2024-1-58-46-52.
[26] Shevchuk, M., Zhulinskyi, M., Kupchok, V., Mykhailiv, A., & Kukoreno, M. (2024). Using blockchain technology to increase the efficiency of energy industry enterprises. *Scientific Notes of Lviv University of Business and Law*, 40, 704-709. doi: 10.5281/zenodo.10637407.
[27] Smith, K.J., & Dhillon, G. (2020). Assessing blockchain potential for improving the cybersecurity of financial transactions. *Managerial Finance*, 46(6), 833-848. doi: 10.1108/MF-06-2019-0314.
[28] Tibrewal, I., Srivastava, M., & Tyagi, A.K. (2022). Blockchain technology for securing cyber-infrastructure and internet of things networks. In A.K. Tyagi, A. Abraham & A. Kaklauskas (Eds.), *Intelligent interactive multimedia systems for e-healthcare applications* (pp. 337-350). Singapore: Springer. doi: 10.1007/978-981-16-6542-4_17.
[29] Ullah, Z., Al-Turjman, F., Mostarda, L., & Gagliardi, R. (2020). Applications of artificial intelligence and machine learning in smart cities. *Computer Communications*, 154, 313-323. doi: 10.1016/j.comcom.2020.02.069.
[30] Vance, T.R., & Vance, A. (2019). Cybersecurity in the blockchain era: A survey on examining critical infrastructure protection with blockchain-based technology. In *Proceedings of the IEEE international scientific-practical conference problems of infocommunications, science and technology* (pp. 107-112). Kyiv: IEEE. doi: 10.1109/PICST47496.2019.9061242.

[31] Wang, Q., & Su, M. (2020). Integrating blockchain technology into the energy sector – from theory of blockchain to research and application of energy blockchain. *Computer Science Review*, 37, article number 100275. doi: 10.1016/j.cosrev.2020.100275.
[32] Warkentin, M., & Orgeron, C. (2020). Using the security triad to assess blockchain technology in public sector applications. *International Journal of Information Management*, 52, article number 102090. doi: 10.1016/j.ijinfomgt.2020.102090.
[33] Wei, P., Wang, D., Zhao, Y., Sah Tyagi, S.K., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems*, 102, 902-911. doi: 10.1016/j.future.2019.09.028.
[34] Wisniewski, M., Gladysz, B., Ejsmont, K., Wodecki, A., & Van Erp, T. (2022). Industry 4.0 solutions impacts on critical infrastructure safety and protection – a systematic literature review. *IEEE Access*, 10, 82716-82735. doi: 10.1109/ACCESS.2022.3195337.
[35] Yu, K., Tan, L., Mumtaz, S., Al-Rubaye, S., Al-Dulaimi, A., Bashir, A.K., & Khan, F.A. (2021). Securing critical infrastructures: Deep-learning-based threat detection in IIoT. *IEEE Communications Magazine*, 59(10), 76-82. doi: 10.1109/MCOM.101.2001126.
[36] Zainuddin, A.A., Sairin, H., Mazlan, I.A., Muslim, N.N., & Wan Sabarudin, W.A.S. (2024). Enhancing IoT security: A synergy of machine learning, artificial intelligence, and blockchain. *Data Science Insights*, 2(1), 9-19.
[37] Zambrano, R. (2020). Taming the beast: Harnessing blockchains in developing country governments. *Frontiers in Blockchain*, 2, article number 27. doi: 10.3389/fbloc.2019.00027.

Інтеграція блокчейн-технологій у системи забезпечення кібербезпеки для об'єктів критичної інфраструктури: перспективи та виклики

Віктор Данчук

Доктор фізико-математичних наук, професор
Національний транспортний університет
01010, вул. М. Омеляновича-Павленка, 1, м. Київ, Україна
https://orcid.org/0000-0003-4282-2400

Марія Данчук

Кандидат економічних наук, доцент
Національний транспортний університет
01010, вул. М. Омеляновича-Павленка, 1, м. Київ, Україна
https://orcid.org/0009-0007-3033-3227

Анотація. Дослідження було спрямоване на аналіз потенціалу та основних проблем інтеграції блокчейн-технологій у процеси забезпечення кібербезпеки об'єктів критичної інфраструктури в Україні. У рамках роботи здійснювалися аналіз потенціалу блокчейн-технологій у підвищенні рівня захищеності критичних інфраструктур, оцінка існуючих викликів масштабування та продуктивності таких систем, а також вивчення можливостей міжнародної співпраці для впровадження інноваційних рішень у сфері кібербезпеки. У роботі проведено всебічний аналіз перспектив інтеграції блокчейн-технологій у системи забезпечення кібербезпеки для об'єктів критичної інфраструктури. Для забезпечення релевантності дослідження враховувалися технічні особливості блокчейну, такі як механізми консенсусу, моделі розподілу даних та криптографічні методи. Було виявлено, що блокчейн-технології забезпечують підвищення рівня прозорості, стійкості до кіберзагроз та оптимізацію управління доступом до критичних даних. Водночас основними викликами залишаються низька масштабованість систем, обмежена швидкість транзакцій і високі енергетичні витрати, що ускладнює їх широкомасштабне впровадження. Дослідження також показало, що існує потреба в адаптації регуляторних вимог для підвищення ефективності інтеграції блокчейну в інфраструктурні об'єкти. Дослідження продемонструвало значний потенціал блокчейн-технологій як одного з ключових компонентів у побудові стійких кібербезпекових систем. Висновки роботи акцентують на необхідності міждисциплінарного підходу до впровадження технологій, що включає технічні, економічні та регуляторні аспекти, для підвищення рівня захищеності об'єктів критичної інфраструктури в умовах зростання кіберзагроз. Крім того, у роботі підкреслено важливість міжнародної співпраці, яка дозволить об'єднати ресурси та експертизу для створення більш ефективних та інноваційних рішень у сфері кібербезпеки

Ключові слова: розподілені реєстри; управління даними; регуляторні аспекти; криптографія; цифрова довіра

BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en

Vol. 29 No. 4. 2024

UDC 004.056.5:004.8
DOI: 10.62660/bcstu/4.2024.53

Improving cybersecurity with artificial intelligence

Nazar Zaplatynskyi*
Master
Lviv National University of Nature Management
80831, 1 Volodymyr Velykyi Str., Dubliany, Ukraine
https://orcid.org/0009-0002-7767-8795

Pavlo Lub
PhD in Technical Sciences, Associate Professor
Lviv National University of Nature Management
80831, 1 Volodymyr Velykyi Str., Dubliany, Ukraine
https://orcid.org/0000-0001-9600-0969

Serhiy Zaporozhtsev
PhD in Technical Sciences, Associate Professor
Lviv National University of Nature Management
80831, 1 Volodymyr Velykyi Str., Dubliany, Ukraine
https://orcid.org/0000-0002-8250-2834

Abstract. The study aimed to explore the possibilities of using artificial intelligence to improve cybersecurity systems in the context of increasing complexity and frequency of cyber threats. Analysis of the effectiveness of integrating machine and deep learning methods into the processes of detecting, assessing and neutralisation threats, as well as identification of the strengths and weaknesses of such approaches, were emphasised. The study substantiated the need to combine the technological capabilities of artificial intelligence with expert human experience to ensure comprehensive and adaptive protection of information systems. The study examined the potential application of artificial intelligence to improve cybersecurity systems, given the growing threats and complexity of modern cybercrime. The impact of machine learning and deep learning technologies on improving the effectiveness of traditional methods of protecting information systems was analysed. The study noted that despite the unchanged basic motivations of cybercriminals, their methods were becoming more sophisticated, which required new approaches to detecting and neutralising threats. The use of artificial intelligence was defined as one of the most promising areas of cybersecurity development, as it allows for the automation of risk assessment and incident response processes, reducing response times and increasing overall security efficiency. Particular attention was devoted to an analysis of the strengths and weaknesses of artificial intelligence in the context of cybersecurity. The necessity of integrating artificial intelligence with human intuition and experience was substantiated, as the combination of these components proved to be the most effective approach to ensuring comprehensive security. In addition, the potential risks and concerns associated with the use of artificial intelligence in cybersecurity were explored. The study concluded that a holistic approach that considers both technical and social aspects is needed to increase the maturity of cybersecurity systems. The importance of socially responsible use of artificial intelligence was emphasised to minimise potential threats and ensure the resilience of cyber systems to new challenges. The practical value of the study is to develop recommendations for

Article's History: Received: 13.08.2024; Revised: 21.11.2024; Accepted: 16.12.2024

Suggested Citation:
Zaplatynskyi, N., Lub, P., & Zaporozhtsev, S. (2024). Improving cybersecurity with artificial intelligence. *Bulletin of Cherkasy State Technological University*, 29(4), 53-61. doi: 10.62660/bcstu/4.2024.53.

*Corresponding author

the introduction of artificial intelligence into existing cybersecurity systems, which allows them to increase their resilience to new and complex cyber threats, as well as to identify potential risks and shortcomings in existing approaches to information security

Keywords: machine learning; neural networks; network traffic analysis; threat detection; automatic recognition; adaptive response

INTRODUCTION

Cybersecurity is becoming increasingly relevant in the modern digital world due to the growing complexity and frequency of cyber threats. Traditional defence methods are becoming insufficiently effective in the face of new, more sophisticated attacks, which requires the development of new approaches and technologies. Artificial intelligence (AI) technologies offer significant potential to improve cybersecurity systems by providing faster and more accurate threat detection and adaptive response to new challenges. However, despite considerable academic interest in this topic, there are still gaps in understanding the full potential of AI for cybersecurity, as well as how it can be effectively integrated into existing security systems.

Research in the field of cybersecurity using AI has been going on for several years, and many scientists have been focusing their efforts on studying various aspects of this topic. For example, the study by S.P. Samyuktha *et al*. (2022) discusses the use of AI to improve cybersecurity practices, emphasising the need to protect the huge amounts of data generated by modern technologies such as the Internet of Things and cloud computing. The authors explain that AI and machine learning technologies, such as big data analytics and deep learning, are being actively used to protect against cyber threats, including intrusion and malware detection. The article also discusses various methodologies and datasets that can be used to create effective AI-enabled cybersecurity solutions.

R. Das & R. Sandhane (2021) discuss the importance of automation to effectively manage the complexity of operations, and the scale of information used to protect cyberspace. The researcher notes that traditional technologies with fixed implementations are difficult to apply to successfully combat cyber threats, but the problem can be solved using machine learning methods. The article also assesses the modern applications of AI in cybersecurity, for edge protection and strategic decisions, and emphasises that certain cybersecurity problems can only be effectively addressed by implementing AI approaches. Artificial intelligence provides instant access to information, helping to cope with the data flow in cybersecurity, which is causing significant structural changes in the industry. The study by N.N. Abbas *et al*. (2019) visualised the hotspots, trends, and emerging applications of AI, providing businesses and governments with useful information for strategic planning. For the first time, the study offers a holistic view of the global distribution of AI research in cybersecurity, including the use of heat maps to analyse geographic areas of activity.

A.M. Shamiulla (2019) explored the impact of artificial intelligence on various areas of human life, including language processing, speech recognition, finance, and robotics. The author also examines the threats associated with the use of AI, including cybercrime and security vulnerabilities. The main focus is on the need for research to ensure control over AI and its safe use. L. Lazic (2019) explores the role of artificial intelligence in enhancing cybersecurity, in particular, the ability of machine learning to identify anomalies and improve threat detection strategies. Particular attention is devoted to obfuscation and de-obfuscation methods for Android applications, including a Low-Level Virtual Machine (LLVM) based platform to improve these processes. It also analyses the AndrODet system, which uses online training to identify the three main obfuscation methods in mobile applications.

X. Feng *et al*. (2020) analysed the role of artificial intelligence in forecasting and modelling, emphasising its importance for strategic planning in crises such as the COVID-19 pandemic. The authors highlight the cybersecurity issues that are necessary to ensure the accuracy of AI models and prevent their distortion. X. Feng *et al*. (2020)propose integrating security measures at every stage of AI development, focusing on the balance between technological, social, and political aspects. The study by A. Anandita Iyer & K.S. Umadevi (2023) analysed the impact of AI on current approaches to cybersecurity, with a focus on the speed of alert processing and filtering of critical information. The author also highlights the lack of visual interfaces for more efficient data analysis, which is an important component for improving results. The article examines the structural changes that have emerged in the field of cybersecurity due to the use of AI, as well as current trends and research in a geographical context.

The study by L. Chan *et al*. (2019) reviewed the current state of AI development in cybersecurity, presenting case studies and applied solutions to help a wider range of stakeholders, including executives, engineers, researchers, educators, innovators, entrepreneurs, and students, better understand the field. Particular attention is paid to existing problems and unresolved issues in the use of AI in cybersecurity. In addition, the paper provides practical conclusions and recommendations for businesses and government agencies on management policies in this area.

Based on the analysis of existing scientific works, it is possible to conclude that although AI technologies have significant potential for improving cybersecurity,

there are still some unresolved issues and limitations that require further study. This concerns the adaptability and reliability of AI algorithms, as well as their ability to work effectively in conditions of limited computing resources. The study aimed to identify and analyse modern approaches to the use of artificial intelligence technologies to improve cybersecurity, as well as to develop recommendations for their effective integration into existing security systems. Particular attention was devoted to the exploration of the possibilities of machine learning and deep neural networks for analysing network traffic, detecting malware, and responding adaptively to new threats. The problematic issue of the study is to determine the optimal methods of using AI to improve the effectiveness of cybersecurity, in the context of their ability to adapt to new challenges and ensure high accuracy of threat detection.

MATERIALS AND METHODS

For the analysis, scientific publications, studies and articles describing modern technologies and methods used to detect cyber threats, such as malware, abnormal behaviour in networks, zero-day attacks, etc., were used. The reviewed materials were used to compare different approaches to threat detection using machine and deep learning algorithms, as well as assess their advantages and disadvantages. The main materials used in the research include scientific articles from journals, conferences and books covering the application of machine and deep learning methods in cybersecurity, including works on algorithms such as support vector machines (SVMs), decision trees, naive Bayesian classifiers and neural networks. These algorithms are widely used to process large amounts of data in real-time, allowing for early detection of anomalies and threats. The methods and materials used in this study were used to consider in detail the potential and limitations of machine and deep learning in the field of cybersecurity. The analysis of existing approaches and methodologies contributes to a deeper understanding of how these technologies can be applied to detect and neutralise cyber threats, as well as identify their strengths and weaknesses. As the study focuses on theoretical analysis, it also provides an opportunity to assess the effectiveness of integrating machine and deep learning algorithms into existing information security systems. This was used to build an understanding of how to optimise the use of these technologies in real-world conditions, considering the limitations and needs of modern security systems, as well as to predict the directions of their further development and adaptation to new types of cyber threats.

RESULTS

In the context of cybersecurity, machine learning and deep learning are key tools for detecting and neutralising cyber threats. Comparison of these methods assessed their capabilities and limitations, which is critical for the development of effective information resource protection systems. Machine learning, as a sub-branch of artificial intelligence, is based on the use of algorithms that learn from historical data to make decisions or predictions (Fig. 1).

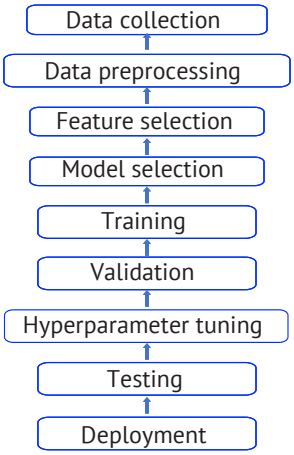

Figure 1. Machine learning algorithm
Source: compiled by the authors

In the field of cybersecurity, these methods are widely used to detect malware, analyse network traffic, and identify abnormal system behaviour (Chan *et al.*, 2019). Algorithms such as support vector machines, decision trees, naive Bayesian classifiers, and others allow efficient processing of large amounts of data with acceptable accuracy and speed. However, their effectiveness can be reduced when processing complex, non-linear dependencies that are typical of modern cyber threats. Deep learning, in turn, is a subset of machine learning that uses multi-layer neural networks to model complex patterns and relationships in data (Jain, 2021). Due to their ability to automatically extract relevant features from raw data, deep neural networks are highly effective in pattern recognition, natural language processing, and time series analysis. In the context of cybersecurity, deep learning is used to detect complex attacks, such as zero-day attacks, and analyse the behavioural characteristics of users and systems. Deep learning has been observed to outperform traditional machine learning methods in the face of large amounts of data and high pattern complexity. Due to the nonlinear nature of neural networks, deep learning can model complex relationships that may be invisible to simpler algorithms. This is relevant in cybersecurity, where threats are constantly evolving and taking on new forms (Macas *et al.*, 2022). However, deep models often require significant computational resources for training and operation, which can be a limiting factor in real-world settings.

Machine learning, despite its simplicity, has the advantages of faster learning and lower resource requirements. This makes it suitable for use in systems with limited computing capabilities or where fast, real-time data processing is required. However, these methods may

be less effective in detecting novel or complex attacks, as their performance is highly dependent on the quality and representativeness of the training data. In addition, deep learning is prone to the "black box" problem, where it is difficult to interpret how the model makes certain decisions (Sarker *et al.*, 2021). This can be critical in cybersecurity, where it is important to understand the reasons why a security system is triggered for further analysis and response. Machine learning, especially interpreted models such as decision trees or logistic regression, provides more transparent results, making them easier to interpret and more trustworthy for security professionals. The choice between machine learning and deep learning depends on the specific requirements and application. In cases where the speed and transparency of the model are important, machine learning may be more appropriate. Where complex, high-dimensional data needs to be analysed and hidden patterns discovered, deep learning offers powerful tools (Kant & Johannsen, 2022). The best approach may be to combine these methods, leveraging the strengths of each to build more effective and adaptive cybersecurity systems.

The development of models for integrating artificial intelligence algorithms with existing security systems is a key aspect of improving cybersecurity. This involves the creation of effective mechanisms that combine the capabilities of machine and deep learning algorithms with traditional security tools. The main goal is to increase the ability of systems to detect and neutralise complex and constantly evolving cyber threats. Integrating AI algorithms into existing security systems requires careful consideration of the architecture and interaction interfaces. AI algorithms must be adapted to the specific conditions and requirements of each system, considering their security protocols, standards, and policies (Mishra, 2023). This ensures smooth interaction between system components and minimises the risk of conflicts or malfunctions.

An important aspect is to ensure that AI algorithms are compatible with existing authentication, authorisation and access control mechanisms. This helps preserve data integrity and confidentiality, as well as comply with regulatory requirements and security standards, such as ISO/IEC No. 27001:2022 (2022). Models are being developed that take into account potential vulnerabilities and provide mechanisms to protect against the exploitation of algorithms by malicious actors. Optimising algorithm performance is another critical factor. AI algorithms need to efficiently process large amounts of data in real-time, which requires optimising computing resources and using high-performance computing platforms. This ensures rapid detection of threats and timely response to them, which is crucial in preventing potential security incidents. In addition, mechanisms are being developed to continuously update and train algorithms based on new threat data. This allows systems to adapt to new types of attacks and improve their effectiveness over time. The system is also scalable, enabling it to meet growing security requirements and handle increased data volumes without losing performance.

Artificial intelligence (AI) is increasingly important in cybersecurity (Trofymenko *et al.*, 2024). It opens new opportunities for detecting and neutralising cyber threats, but it also comes with certain challenges and limitations. A critical analysis of the strengths and weaknesses of AI in cybersecurity allows for a deeper understanding of the potential and risks associated with this technology. One of the main advantages of using AI in cybersecurity is its ability to process large amounts of data in real-time. Using machine learning and deep learning techniques, AI can analyse network traffic, user behavioural patterns, and system logs, identifying anomalies that may indicate the presence of cyber threats (Fig. 2). This can ensure quick response to attacks and minimisation of potential damage. In addition, AI can detect new, previously unknown threats, including zero-day attacks, which is a significant advantage over traditional signature-based security methods.

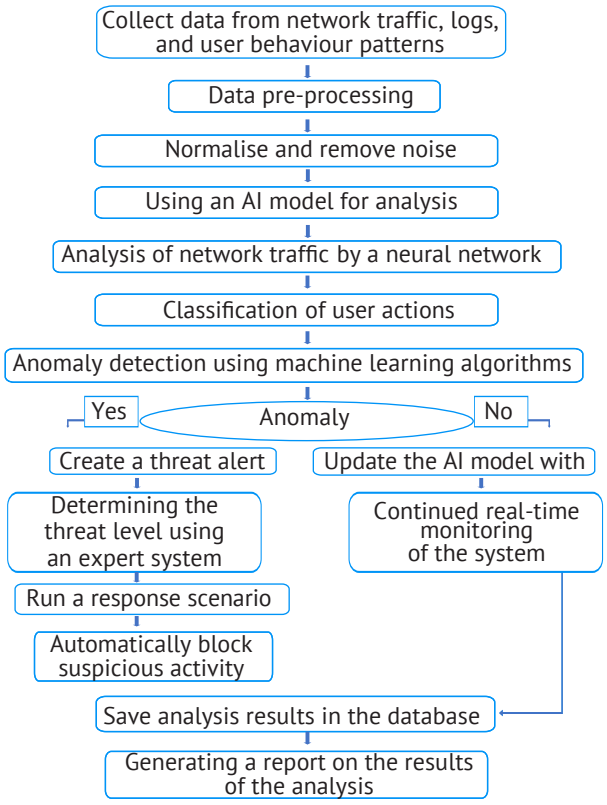

Figure 2. AI algorithm in cybersecurity
Source: compiled by the authors

Artificial intelligence also contributes to the automation of cybersecurity processes, which reduces the burden on human resources and increases the efficiency of security teams. Automated systems can continuously monitor the network, analyse threats, and even make decisions to block suspicious activity on their own (Goyal *et al.*, 2023). This is especially important in

the context of the growing complexity and frequency of cyber threats, when the human factor may not be able to keep up with the dynamics of events.

However, the use of AI in cybersecurity has its weaknesses. One of the key issues is the vulnerability of AI algorithms to attacks on the AI systems themselves. For instance, data poisoning techniques can be used by attackers to inject incorrect or manipulated data into training sets, leading to erroneous system decisions. Additionally, there are attacks based on spoofing or manipulating input data that can trick AI models into classifying malicious activity as safe. Another limitation is the problem of interpretability of AI models, especially deep neural networks. In cybersecurity, it is important not only to detect a threat but also to understand the causes and mechanisms of its occurrence to further eliminate vulnerabilities. The complexity of AI models can complicate this process, which can negatively impact the effectiveness of response and remediation. It can also create difficulties in the context of compliance with regulatory and security standards, which often require transparency and explanation of decisions.

Another important aspect is the dependence on high-quality and representative data to train AI models. If the training data does not reflect the full range of possible threats or contains biases, this can lead to poor system performance in real-world conditions (Dash *et al.*, 2022). Collecting and anonymising such data can be difficult due to privacy restrictions and legislation governing the processing of personal data. In addition, the use of AI can create a false sense of security and lead to a lack of vigilance on the part of cybersecurity professionals. Excessive trust in automated systems can lead to the missed detection of complex or atypical attacks that were not predicted by AI models (Nobles, 2024). This highlights the importance of combining automated solutions with expert human analysis. Ethical and privacy issues must also be considered. The use of AI in cybersecurity may involve the processing of large amounts of personal and confidential data, which requires compliance with strict data protection standards (ISO/IEC No. 27001:2022, 2022). Improper or unethical use of such data can lead to violations of users' rights and legal consequences for organisations.

Based on these aspects, the use of AI in cybersecurity has both significant potential and serious challenges. Maximising the benefits requires careful planning, proper design and implementation of systems, as well as continuous monitoring and improvement of models. It is important to ensure that algorithms are transparent and interpretable and that they are integrated with expert systems and human analysis. Cyber threats are becoming increasingly dynamic and complex, requiring the development of effective countermeasures. The development of theoretical scenarios can be used to model possible attacks and identify strategies to neutralise them using artificial intelligence. This involves analysing current trends in cybercrime, identifying new attack vectors, and forecasting their development.

The use of artificial intelligence in this process can be used to create models that can adapt to changing conditions. Machine learning and deep learning algorithms can analyse large amounts of data in real-time, identifying hidden patterns and anomalies that may indicate a potential threat. This is especially relevant in countering zero-day attacks that exploit unknown system vulnerabilities. One of the key aspects is modelling multi-vector attacks that combine different methods of penetration and exploitation of vulnerabilities. To do this, it is necessary to develop scenarios that consider the combined actions of attackers, including phishing, software exploits and social engineering. Artificial intelligence can help predict such complex threats by analysing the relationships between various events and compromise indicators.

It is also necessary to address the dynamics of changing tactics and techniques of cybercriminals. Continuously updating threat models using machine learning allows security systems to stay one step ahead of attackers. This includes the implementation of self-updating models that learn from new data and adjust their predictions to the current situation. In addition to technological solutions, counteraction scenarios should consider the human factor. The development of theoretical models that simulate user reactions to different types of attacks helps to identify possible vulnerabilities related to human behaviour. This may include analysing susceptibility to phishing attacks or the use of weak passwords. These aspects can be used to develop more comprehensive security strategies that combine technical tools with staff training.

DISCUSSION

The results of this study are consistent with the findings of other cybersecurity and artificial intelligence (AI) scholars, emphasising the importance of integrating modern technologies to improve the effectiveness of information resource protection systems. M.M. Yamin *et al.* (2021) analysed the use of AI as a weapon in cyber-attacks, demonstrating how AI can be used to create more sophisticated and complex threats. This underscores the need for continuous improvement of defence systems capable of withstanding new types of attacks that use AI to bypass traditional defence methods.

W.S. Admass *et al.* (2024) examined the current state of cybersecurity, identifying the main challenges and promising areas of development. The authors emphasised the need to integrate AI to provide adaptive defences in response to dynamic threats, which is in line with the findings of this study on the importance of using AI to automate risk assessment and incident response processes, increasing the efficiency and effectiveness of cybersecurity systems. N. Kaloudi & J. Li (2020) provide a comprehensive overview of the AI-driven cyber threat landscape, highlighting the

diversity and complexity of modern attacks. They note that AI can be used for both defence and attack, requiring defenders to adopt the latest techniques and technologies. This is consistent with the findings that defence systems need to be constantly evolving and adapting to new challenges.

R. Walters & M. Novak (2021) examine the interplay between cybersecurity, AI, data protection, and law. They emphasise the importance of compliance with legal norms and standards when using AI in cybersecurity, which is an important aspect of this study, which focuses on the socially responsible use of AI to minimise potential risks and ensure user confidence in security systems. M. Binhammad *et al*. (2024) explored the role of AI in digital identity protection, highlighting the potential of machine learning to detect and prevent fraudulent activity. They demonstrate how AI can be used to ensure the security of personal data and prevent identity theft, which correlates with the conclusion that AI needs to be integrated with human expertise to ensure comprehensive security.

S.K. Shandilya *et al*. (2022) developed an AI-supported test platform for adaptive defence inspired by natural processes. The results show that the use of AI in cybersecurity simulations can significantly improve the ability of systems to adapt and self-learn, supporting the study's recommendations to combine automated methods with expert human expertise to create more resilient defence systems. A. Ali *et al*. (2022) consider the use of AI as a horizon event in cybersecurity, analysing how AI can transform threat prediction and protection. They emphasise the potential of AI to create proactive defence systems that anticipate and respond to threats before they occur. This is in line with the conclusion that it is necessary to develop models capable of predicting and adapting to new threats. M. Tetaly & P. Kulkarni (2022) discuss whether AI is a threat or a cybersecurity solution, noting that while AI can significantly improve the effectiveness of defence systems, there are risks of misuse, which require careful regulation and ethical standards. This underscores the importance of the ethical use of AI, which is also considered in this study, which focuses on the socially responsible use of AI to minimise potential risks and ensure user confidence in security systems. S.A. Jawaid (2023) analyses the relationship between AI and cybersecurity, considering how AI can improve security methods and create new types of threats. The author emphasises the need to balance the use of AI for protection with the management of its potential risks, which correlates with the study's recommendations for a comprehensive approach to the use of AI in cybersecurity.

M.H.B.A. Alkareem *et al*. (2023) investigated the linguistic aspects of crime in the world with the help of AI-enabled cybersecurity. They show how AI can be used to analyse language patterns in criminal communications, which helps to detect and predict criminal activity. This underscores the importance of using AI in integrated security systems, where it is important to consider various aspects of cybersecurity, including technical, social, and linguistic. J. Ebenezer Taiwo Akinsola *et al*. (2022) consider the use of AI in the design of user interfaces for modelling cybersecurity threats. They demonstrate how AI can be used to create intuitive and adaptive interfaces that improve user interaction with security systems and contribute to the overall effectiveness of cybersecurity. A. Lakhani (2024) analyses the revolutionary impact of AI on cybersecurity, opening the future of digital defence. The author emphasises that AI can significantly improve the ability of systems to detect and respond to threats but also requires continuous improvement and adaptation to new challenges. This correlates with the conclusion that AI technologies in cybersecurity need to be continuously developed and adapted.

D. Aggarwal *et al*. (2023) examine the role of AI in cybersecurity through anomaly and predictive analysis. They demonstrate how machine learning techniques can be used to detect anomalies in network data and predict potential threats, allowing defence systems to be proactive and effective. This highlights the importance of using AI to predict and prevent threats, which is a key aspect of the research. However, despite significant progress, there are serious challenges, such as model interpretability, resource optimisation, and ethical aspects of AI use. This requires a comprehensive approach to the development and implementation of AI technologies in cybersecurity, where it is important not only to improve technical aspects but also to consider social and ethical factors.

Integrating AI with other security and analytical methods, as well as using AI to analyse different types of data, can significantly improve the ability of systems to detect and respond to complex and emerging threats. This underscores the importance of a multidisciplinary approach to cybersecurity, where AI acts as a powerful tool in the complex of measures to protect information systems. Further theoretical and practical research should be aimed at developing more effective, adaptive and interpretable protection models, as well as at integrating human expertise with automated protection systems. Thus, the study results confirm the importance of using modern AI methods to improve cybersecurity systems. The joint efforts of scientists, engineers, and cybersecurity professionals will help create a safer and more resilient digital environment that can effectively counter current and future cyber threats.

CONCLUSIONS

The study determined that the use of artificial intelligence methods, in particular machine and deep learning, significantly improves the efficiency of cybersecurity systems. An analysis of existing approaches has shown that deep neural networks are able to detect complex patterns and anomalies that are typical of modern cyber threats, providing a high level of

accuracy and speed of response. Auto-encoders and recurrent neural networks proved to be particularly effective, demonstrating the ability to self-learn and adapt to new types of attacks, which confirms their suitability for dynamic cybersecurity environments.

Research has also shown that generative adversarial networks (GANs) can be effectively used to create realistic attack patterns, allowing defence systems to better prepare for previously unknown threats. This confirms the need to integrate advanced artificial intelligence techniques to increase the adaptability and proactivity of cybersecurity systems. However, the study determined that deep models often require significant computing resources, which can limit their use in resource-limited environments. Critical analysis has shown that the interpretability of deep learning models remains a significant challenge. Despite their high accuracy in detecting threats, the difficulty of understanding the models' decision-making mechanisms poses risks to the trust of security professionals. This underscores the need to develop explainable artificial intelligence methods that would increase transparency and trust in automated security systems.

The analysis of the study results demonstrated that the use of artificial intelligence technologies in cybersecurity has significant potential to improve the efficiency of security systems. However, an important aspect is the optimisation of the resource consumption of artificial intelligence algorithms, which is critical for their effective use in real-world conditions. The study found that modern machine learning methods, including neural networks, can significantly improve the accuracy of detecting complex and emerging cyber threats. However, for their effective implementation, it is necessary to address the resources used to train and apply these algorithms, as high computing requirements may be a limitation in practical use. This highlights the need for further research and development of more efficient, less resource-intensive approaches to integrate AI into cybersecurity systems.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Abbas, N.N., Ahmed, T., Shah, S.H.U., Omar, M., & Park, H.W. (2019). Investigating the applications of artificial intelligence in cyber security. *Scientometrics*, 121(2), 1189-1211. doi: 10.1007/s11192-019-03222-9.

[2] Admass, W.S., Munaye, Y.Y., & Diro, A.A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2, article number 100031. doi: 10.1016/j.csa.2023.100031.

[3] Aggarwal, D., Sharma, D., & Saxena, A.B. (2023). Role of AI in cyber security through anomaly detection and predictive analysis. *Journal of Informatics Education and Research*, 3(2), 1846-1849. doi: 10.52783/jier.v3i2.314.

[4] Ali, A., Septyanto, A.W., Chaudhary, I., Hamadi, H.A., Alzoubi, H.M., & Khan, Z.F. (2022). Applied artificial intelligence as event horizon of cyber security. In *2022 international conference on business analytics for technology and security* (pp. 1-7). Dubai: IEEE. doi: 10.1109/icbats54253.2022.9759076.

[5] Alkareem, M.H.B.A., Nasif, F.Q., Ahmed, S.R., Miran, L.D., Algburi, S., & ALmashhadany, M.T. (2023). Linguistics for crimes in the world by AI-based cyber security. In *2023 7th international symposium on innovative approaches in smart technologies* (pp. 1-5). Istanbul: IEEE. doi: 10.1109/isas60782.2023.10391610.

[6] Anandita Iyer, A., & Umadevi, K.S. (2023). Role of AI and its impact on the development of cyber security applications. In V. Sarveshwaran, J.I.-Z. Chen & D. Pelusi (Eds.), *Artificial intelligence and cyber security in industry 4.0* (pp. 23-46). Singapore: Springer. doi: 10.1007/978-981-99-2115-7_2.

[7] Binhammad, M., Alqaydi, S., Othman, A., & Abuljadayel, L.H. (2024). The role of AI in cyber security: Safeguarding digital identity. *Journal of Information Security*, 15(2), 245-278. doi: 10.4236/jis.2024.152015.

[8] Chan, L., Morgan, I., Simon, H., Alshabana, F., Ober, D., Gentry, J., Min, D., & Cao, R. (2019). Survey of AI in cybersecurity for information technology management. In *2019 IEEE technology & engineering management conference* (pp. 1-8). Atlanta: IEEE. doi: 10.1109/temscon.2019.8813605.

[9] Das, R., & Sandhane, R. (2021). Artificial intelligence in cyber security. *Journal of Physics Conference Series*, 1964(4), article number 042072. doi: 10.1088/1742-6596/1964/4/042072.

[10] Dash, B., Ansari, M.F., Sharma, P., & Ali, A. (2022). Threats and opportunities with AI-based cyber security intrusion detection: A review. *International Journal of Software Engineering & Applications*, 13(5), 13-21. doi: 10.5121/ijsea.2022.13502.

[11] Ebenezer Taiwo Akinsola, J., Akinseinde, S., Kalesanwo, O., Adeagbo, M., Oladapo, K., Awoseyi, A., & Kasali, F. (2022). Application of artificial intelligence in user interfaces design for cyber security threat modeling. In *Software usability*. London: IntechOpen. doi: 10.5772/intechopen.96534.

[12] Feng, X., Feng, Y., & Dawam, E.S. (2020). Artificial intelligence cyber security strategy. In *2020 IEEE intl conf on dependable, autonomic and secure computing, intl conf on pervasive intelligence and computing, intl conf on cloud and big data computing, intl conf on cyber science and technology congress* (pp. 328-333). Calgary: IEEE. doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00064.

[13] Goyal, S.B., Rajawat, A.S., Solanki, R.K., Majmi Zaaba, M.A., & Long, Z.A. (2023). Integrating AI with cyber security for smart Industry 4.0 application. In *2023 international conference on inventive computation technologies* (pp. 1223-1232). Lalitpur: IEEE. doi: 10.1109/icict57646.2023.10134374.
[14] International Standard (ISO/IEC) No. 27001:2022 "Information Security, Cybersecurity and Privacy Protection". (2022, October). Retrieved from https://www.iso.org/standard/82875.html.
[15] Jain, J. (2021). Artificial intelligence in the cyber security environment. In *Artificial intelligence and data mining approaches in security frameworks* (pp. 101-117). Hoboken: Wiley. doi: 10.1002/9781119760429.ch6.
[16] Jawaid, S.A. (2023). Artificial intelligence with respect to cyber security. *Journal of Advances in Artificial Intelligence*, 1(2), 96-102. doi: 10.18178/jaai.2023.1.2.96-102.
[17] Kaloudi, N., & Li, J. (2020). The AI-based cyber threat landscape: A survey. *ACM Computing Surveys*, 53(1), article number 20. doi: 10.1145/3372823.
[18] Kant, D., & Johannsen, A. (2022). Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs). *Electronic Imaging*, 34, article number MOBMU-387. doi: 10.2352/ei.2022.34.3.mobmu-387.
[19] Lakhani, A. (2024). *How AI is revolutionizing cybersecurity: Unlocking the future of digital protection*. Retrieved from https://cloud-computing.tmcnet.com/features/articles/459618-how-ai-revolutionizing-cybersecurity-unlocking-future-digital-protection.htm.
[20] Lazic, L. (2019). Benefit from AI in cybersecurity. In *11th international conference on business information security*. Belgrade: Belgrade Metropolitan University.
[21] Macas, M., Wu, C., & Fuertes, W. (2022). A survey on deep learning for cybersecurity: Progress, challenges, and opportunities. *Computer Networks*, 212, article number 109032. doi: 10.1016/j.comnet.2022.109032.
[22] Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences*, 13(10), article number 5875. doi: 10.3390/app13105875.
[23] Nobles, C. (2024). The weaponization of artificial intelligence in cybersecurity: A systematic review. *Procedia Computer Science*, 239, 547-555. doi: 10.1016/j.procs.2024.06.206.
[24] Samyuktha, S.P., Kavitha, P., Kshaya, V.A., Shalini, P., & Ramya, R. (2022). A survey on cyber security meets artificial intelligence: AI-driven cyber security. *Journal of Cognitive Human-Computer Interaction*, 2(2), 50-55. doi: 10.54216/JCHCI.020202.
[25] Sarker, I.H., Furhad, M.H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science*, 2(3), article number 173. doi: 10.1007/s42979-021-00557-0.
[26] Shamiulla, A.M. (2019). Role of artificial intelligence in cyber security. *International Journal of Innovative Technology and Exploring Engineering*, 9(1), 4628-4630. doi: 10.35940/ijitee.a6115.119119.
[27] Shandilya, S.K., Upadhyay, S., Kumar, A., & Nagar, A.K. (2022). AI-assisted computer network operations testbed for nature-inspired cyber security based adaptive defense simulation and analysis. *Future Generation Computer Systems*, 127, 297-308. doi: 10.1016/j.future.2021.09.018.
[28] Tetaly, M., & Kulkarni, P. (2022). Artificial intelligence in cyber security – a threat or a solution. *AIP Conference Proceedings*, 2519(1), article number 030036. doi: 10.1063/5.0109664.
[29] Trofymenko, O., Sokolov, A., Chykunov, P., Akhmametieva, H., & Manakov, S. (2024). AI in the military cyber domain. *Technologies and Engineering*, 25(4), 85-92. doi: 10.30857/2786-5371.2024.4.8.
[30] Walters, R., & Novak, M. (2021). *Cyber security, artificial intelligence, data protection & the law*. Singapore: Springer. doi: 10.1007/978-981-16-1665-5.
[31] Yamin, M.M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications*, 57, article number 102722. doi: 10.1016/j.jisa.2020.102722.

Вдосконалення кібербезпеки за допомогою штучного інтелекту

Назар Заплатинський

Магістр
Львівський національний університет природокористування
80831, вул. Володимира Великого, 1, м. Дубляни, Україна
https://orcid.org/0009-0002-7767-8795

Павло Луб

Кандидат технічних наук, доцент
Львівський національний університет природокористування
80831, вул. Володимира Великого, 1, м. Дубляни, Україна
https://orcid.org/0000-0001-9600-0969

Сергій Запорожцев

Кандидат технічних наук, доцент
Львівський національний університет біоресурсів і природокористування
80831, вул. Володимира Великого, 1, м. Дубляни, Україна
https://orcid.org/0000-0002-8250-2834

Анотація. Метою дослідження було вивчення можливостей застосування штучного інтелекту для вдосконалення систем кібербезпеки в умовах зростання складності та частоти кіберзагроз. Особлива увага приділялася аналізу ефективності інтеграції методів машинного та глибинного навчання в процеси виявлення, оцінки та нейтралізації загроз, а також визначенню сильних та слабких сторін таких підходів. Дослідження було спрямоване на обґрунтування необхідності поєднання технологічних можливостей штучного інтелекту з експертним людським досвідом для забезпечення комплексного та адаптивного захисту інформаційних систем. У дослідженні розглядалися потенційні можливості застосування штучного інтелекту для вдосконалення систем кібербезпеки, враховуючи зростаючі загрози та складність сучасних кіберзлочинів. Аналізувався вплив технологій машинного навчання та глибинного навчання на підвищення ефективності традиційних методів захисту інформаційних систем. Відзначалося, що незважаючи на незмінність основних мотивів кіберзлочинців, їхні методи ставали дедалі витонченішими, що вимагало від захисників нових підходів до виявлення та нейтралізації загроз. Використання штучного інтелекту розглядалося як один з найперспективніших напрямків розвитку кібербезпеки, оскільки це дозволяє автоматизувати процеси оцінки ризиків та реагування на інциденти, знижуючи час реагування та підвищуючи загальну ефективність захисту. Особлива увага приділялася аналізу сильних і слабких сторін штучного інтелекту в контексті кібербезпеки. Обґрунтовувалася необхідність інтеграції штучного інтелекту з людською інтуїцією та досвідом, оскільки поєднання цих компонентів виявилося найефективнішим підходом для забезпечення комплексної безпеки. Окрім того, досліджувалися потенційні ризики та занепокоєння, пов'язані з використанням штучного інтелекту в кібербезпеці. Було зроблено висновок, що для підвищення зрілості систем кібербезпеки необхідний цілісний підхід, який враховує як технічні, так і соціальні аспекти. Наголошувалося на важливості соціально відповідального використання штучного інтелекту, щоб мінімізувати потенційні загрози та забезпечити стійкість кіберсистем до нових викликів. Практична цінність дослідження полягає в розробці рекомендацій щодо впровадження штучного інтелекту в існуючі системи кібербезпеки, що дозволяє підвищити їх стійкість до нових та складних кіберзагроз, а також виявляти потенційні ризики та недоліки в існуючих підходах до забезпечення інформаційної безпеки

Ключові слова: машинне навчання; нейронні мережі; аналіз мережевого трафіку; виявлення загроз; автоматичне розпізнавання; адаптивне реагування

BULLETIN of Cherkasy State Technological University

Journal homepage: https://bulletin-chstu.com.ua/en Vol. 29 No. 4. 2024

UDC 004.43
DOI: 10.62660/bcstu/4.2024.62

Algorithms and simulation model for the synchronisation subsystem of the noise-resilient communication system based on permutations

Emil Faure
Doctor of Technical Sciences, Professor
Cherkasy State Technological University
18006, 460 Shevchenko Blvd., Cherkasy, Ukraine
https://orcid.org/0000-0002-2046-481X

Artem Skutskyi*
Postgraduate Student
Cherkasy State Technological University
18006, 460 Shevchenko Blvd., Cherkasy, Ukraine
https://orcid.org/0000-0002-8632-1176

Artem Lavdanskyi
PhD in Technical Sciences, Associate Professor
Cherkasy State Technological University
18006, 460 Shevchenko Blvd., Cherkasy, Ukraine
https://orcid.org/0000-0002-1596-4123

Abstract. In modern data transmission systems, one of the key tasks is to ensure the reliability of communication in conditions of noise. This is especially relevant for channels with high bit error rate, in particular, for radio communication channels with intense natural or artificial noise, which limits the use of traditional error correction methods. The purpose of this work was to develop algorithms for communication using code words of non-separable factorial code, which implies the representation of code words in the form of permutations using simplex binary symmetric communication channel with high bit error probability. To build these algorithms, the method of frame synchronisation of non-separable factorial code, which uses majority and correlation processing of fragments received from communication channel, was taken as a basis. Methods and algorithms for noise-resilient transmission of permutations in communication channels with high bit error probability were investigated. A general scheme of the protocol for organisation of simplex communication was developed. An algorithm for detecting false synchronisations under conditions of high noise level in communication channel was proposed. The effectiveness of the protocol for synchronisation of code words of factorial code was studied, advantages of the used approach were identified and presented. A simulation model of the communication system using a simplex binary symmetric communication channel and the possibility of setting the bit error value in it was developed. The structure of the simulation model and the algorithms of its component blocks were presented. Synchronisation parameters were calculated for bit error probability of 0.4, simulation results based on 10,000 tests were presented, which made it possible to experimentally determine synchronisation algorithm parameters. Simulation modelling was performed and the accuracy of determining the boundaries of synchronisation blocks was estimated based on bit error probability in the range from 0.1 to 0.4. An approach was proposed to reduce the error when determining the boundaries of

Article's History: Received: 12.08.2024; Revised: 20.11.2024; Accepted: 16.12.2024.

Suggested Citation:
Faure, E., Skutskyi, A., & Lavdanskyi, A. (2024). Algorithms and simulation model for the synchronisation subsystem of the noise-resilient communication system based on permutations. *Bulletin of Cherkasy State Technological University*, 29(4), 62-74. doi: 10.62660/bcstu/4.2024.62.

*Corresponding author

permutations. The obtained results indicate the effectiveness of the proposed solutions, the consistency of theoretical and practical indicators of the synchronisation subsystem, as well as the possibility of using the developed algorithms to implement a three-pass cryptographic protocol based on permutations

Keywords: simplex binary symmetric channel; factorial coding; statistics; protocol; noise

INTRODUCTION

Information transmission is the basis of modern communication systems, providing data exchange in various environments – rom high-speed fiber-optic networks to wireless systems operating in difficult conditions. The performance of systems depends on the ability to maintain the reliability and integrity of information even under the impact of interference, multipath effect, or other factors of communication channel. That is why the development of effective methods for encoding, synchronisation, and protection of transmitted data is one of the key tasks of modern communication technologies.

Modern data transmission technologies face new challenges, which are caused by the need to ensure high reliability of information transmission even in difficult conditions of signal propagation, in particular in environments with high noise intensity. The security of data transmission technology for IoT is critically important, since these devices interact in environments with a large number of potential threats. The vulnerability of IoT devices can cause leaks of confidential information, disruption of systems, or even large-scale cyberattacks. For example, the study by A. Jahangeer *et al.* (2023) notes that the routing protocol for low-power and lossy networks (RPL), specially designed for IoT, is vulnerable to many attacks, such as selective forwarding, blackhole, sybil, wormhole, and sinkhole attacks, which significantly affects network performance. The authors of the study present an overview of attacks on the RPL protocol, as well as a detailed analysis of machine learning and methods for protection against these threats, which highlights the need to improve IoT security.

I. Ahmad *et al.* (2019) and H. Lee & Y.-C. Ko (2021) point out stringent reliability and latency requirements in 5G cellular technologies. Y. Li *et al.* (2022) propose a structure of a digital copy of a device, which through an IoT network using unmanned aerial vehicles (UAVs) can be used as a mobile auxiliary server for edge computing. Such use requires high reliability of data transmission, a secure communication channel, and transmission delays. Modern research, in particular by Y. Sun *et al.* (2021), actively implements optimised data encoding and transmission algorithms, such as byte-parallel configurable cyclic shift (BP-CCS) algorithm in low-density parity-check (LDPC) encoding, which significantly improves data processing efficiency in 5G protocols.

Non-separable factorial codes have been considered and investigated in the study by E. Faure *et al.* (2022). Such codes offer wide opportunities for using permutations as the basis of the transport mechanism in short-packet communication systems. Such systems can be used in IoT systems as discussed in the study by C.D. Ho *et al.* (2021). A similar system is considered by C. Feng *et al.* (2021). The use of permutations in communication is considered by Y. Yang & L. Hanzo (2023). The study compares it with traditional data encapsulation methods. Non-separable factorial codes allow for the implementation of effective mechanism for joint protection of transmitted data from errors occurring in communication channel, as well as ensuring their security from unauthorised access.

As shown by E. Faure *et al.* (2022), code words of non-separable factorial code are formed from a subset of the set of permutations of length M. To ensure their transmission, permutation symbols are encoded by uniform binary code with fixed code combination length. The redundancy of information transmitted by permutations is a feature of such codes. Due to this, non-separable factorial codes, like permutation codes, are able not only to detect, but also to effectively correct errors that occur in communication channel. For example, the study by M. Gao & K.W. Shum (2024) suggests that in the context of combinatorics, permutation codes can be interpreted as directed t-designs and directed t-packings. This connection stems from the fact that permutation code can correct any d-deletions if and only if all subsequences of code words of n-d length are distinct. In addition, the specific structure of permutations creates favourable conditions for frame synchronisation without the need for additional signals, which simplifies the transmission system operation. Under these conditions, sync word length is equal to permutation length, which guarantees signal consistency between the transmitter and the receiver.

Previous studies have demonstrated the effectiveness of non-separable factorial coding even in situations where the probability of bit errors in communication channel remains high. In particular, in the study by B. Stupka (2024) this makes it possible to create: permutation synchronisation algorithms; algorithms for reliable transmission of permutations in communication systems with short packets. At the same time, the developed synchronisation methods imply knowledge of the moment when sync word bits are received, which is not always achievable in conditions of transmission through noisy communication channels. In addition, the integration of synchronisation and protected transmission procedures within one protocol as of 2024 remains insufficiently studied. The purpose of this study was to develop effective algorithms for the operation of the synchronisation subsystem for simplex noise-resilient communication by permutations, as well as to develop a simulation model for their implementation and research.

MATERIALS AND METHODS

There are two systems connected by communication channel. Data transmission through stationary communication channel (*Ch*) occurs in one direction, from one system to another (simplex type of transmission). For better understanding, the names of the systems are indicated according to their target function: the first system is transmission, respectively: *Tx*, the second system is reception, respectively: *Rx*. Information is transmitted from *Tx* through *Ch* to *Rx*. Communication channel distorts the transmitted signal by superimposing noise on the input signal, resulting in bit error probability . Accordingly, *Rx* receives the signal distorted by communication channel. A graphical representation of the communication scheme is shown in Figure 1.

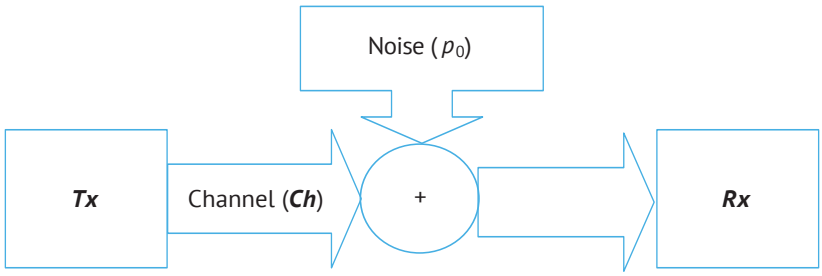

Figure 1. Communication scheme

Source: developed by the authors

Time diagram of the transmission procedure (Fig. 2) shows the components: *Tx*, *Ch*, *Rx*. In addition, there are fragments of information located at the *Tx* output, *Rx* input, *Ch* input and output.

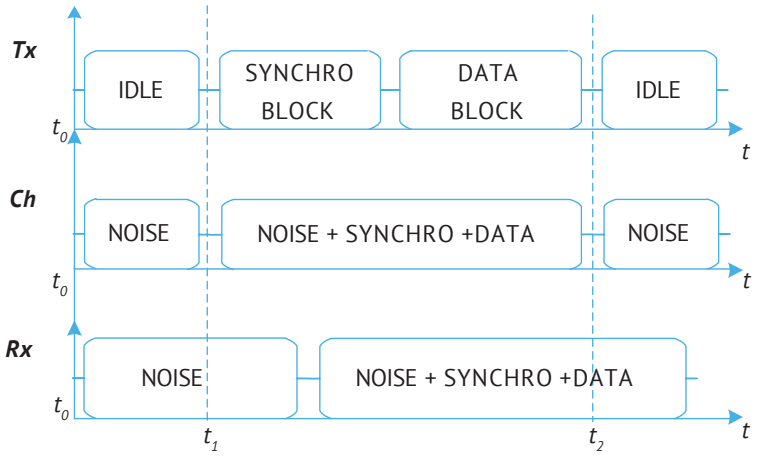

Figure 2. Transmission procedure diagram

Source: developed by the authors

In $[t_0; t_1;]$ time interval *Tx* does not send any data, so the signal level at the input of the channel *Ch* remains constant and zero one. The receiver does not "know" anything about the moment of the start/end of transmission, it constantly processes the input signal. In this case, in $[t_0; t_1;]$ time interval *Rx* receives only noise. Accordingly, during this period of time the probability of bit error in *Rx* is equal to 0.5. In $[t_1; t_2;]$ time interval the transmitter forms a synchronisation block and a data block and sequentially outputs them to the channel.

In the considered transmission procedure, the receiver *Rx* constantly analyses the signal coming from communication channel, since the receiver does not have additional information about the start of transmission from *Tx*, and the *Tx* transmission process can start at any time (asynchronously). Accordingly, the first task for the receiver is to be synchronised with the transmitter to correctly determine the boundaries of transmitted blocks. The second task is to reduce the impact of noise in communication channel on the efficiency of transmission procedures. The solution of these tasks makes it possible to implement a reliable data transmission protocol in communication channels with high bit error probability. In his work, the author B. Stupka (2024) proposes methods for reliable transmission of permutations and demonstrates their effectiveness in the channel with bit error probability $p_0 \leqslant 0.495$. The research by E. Faure *et al.* (2024) is aimed at studying and evaluating the possibility of synchronisation in the channel with $p_0 \leqslant 0.4$. Based on these works, the authors of the study propose the structure of synchronisation block and data block, which is shown in Figure 3.

Figure 3. Structure of synchronisation block and data block

Notes: L_0 – a sync character determined by permutation π that has the maximum value d_{lim} of minimum Hamming distance to all its cyclic shifts; L_{block} – a block of $l_{max\_letters}$ of L_0 sync characters (synchronisation block); W – a word consisting of S characters – cyclic shifts of a sync character L_0: $\{L_1, L_2, \ldots, L_S\}$; W_{block} – a block of l_{max_words} of words W (data block is a frame). Each L_j character is a permutation of symbols of length M. Each symbol is encoded with a binary uniform code. Thus, the length of each symbol is equal to $l_r = \lceil log_2 M \rceil$ bits. Accordingly, the number of bits in a character: $n = M \cdot lr$, the number of bits in synchronisation block L_{block}: $n_L = l_{max\_letters} \cdot M \cdot l_r s$, and the number of bits in data block (frame) W_{block}: $n_w = l_{max\_words} \cdot M \cdot l_r \cdot (n-1)$.
Source: developed by the authors

Permutation synchronisation algorithms with high bit error probability are proposed and researched in the studies by E. Faure *et al.* (2024) and B. Stupka (2024). However, the condition of this study is that the receiver has no knowledge about the beginning of data transmission, and the transmission process can begin at any time. In this case, only the permutation synchronisation algorithm from the study by E. Faure *et al.* (2024) is suitable. This algorithm uses a fixed-size sliding window to ensure a given synchronisation probability, but creates significant redundancy, which increases the transmission overhead. Despite this, its efficiency makes it possible to achieve a theoretical probability of false synchronisation $P_{false\_final} = 2.9 \cdot 10^{-6}$), which makes it promising for applications with high requirements for synchronisation accuracy.

This work uses the frame synchronisation algorithm (synchronisation by characters) without the need to increase the length L_{block} of the synchronisation block. At the same time, the procedures of majority and correlation processing in a sliding window with L_{block} received fragments remain unchanged. A series of cases of false sync detection of the frame synchronisation subsystem is considered as a separate concept. A series of cases for determining false positions of sync character boundaries (a false sync detection series) is a situation when, while searching for the boundaries of a sync character-permutation using a sliding window, the synchronisation subsystem fixes false positions of the boundary for several consecutive shifts of the sliding window. The number of such shifts of the sliding window is the length of the series. To determine the lengths of false sync detection series, a simulation modelling of the frame synchronisation process was carried out. For this purpose, the following parameters of the simulation model were adopted:

- permutation length $M = 8$;
- number of bits to encode the permutation symbol $l_r = 3$;
- bit error rate in communication channel in the absence of transmitter signal $p_{noise} = 0.5$;
- bit error rate in the presence of transmitter signal $p_0 = 0.4$;
- number of tests in the experiment – 10,000.

To ensure the condition of the absence of information about the initial moment of data transmission by the transmitter, the simulation model provides for the formation of a noise block with a length equal to the length of the sliding window of the frame synchronisation subsystem: $L = l_{max\_letters} \cdot M \cdot l_r$ bits. In the conditions of simulation modelling, it is possible to know the start of transmission and the number of bits received by the receiver. Under the condition, the decision on false or true definition of the boundary is formed based on the number of bits received by the l_{rx} receiver, the position of the start of transmission to the synchronisation block (0^{th} bit), the length of sync character fragment and the set of all sync character shifts. Since sync characters in the synchronisation block are arranged sequentially, the sliding window that receives bits is sequential and forms the R refined sequence.

For the next bit reception, the sliding window is shifted by one bit, thus sync character boundary is changed by one. If the frame synchronisation subsystem has determined a boundary that is not equivalent to the calculated boundary from the beginning of synchronisation block transmission, the receiver may set a false boundary of fragments in the synchronisation block. The following expression (1) is the condition for checking the false boundary setting by the frame synchronisation subsystem:

$$S_{false} \rightarrow n_R \neq |l_{rx}|_n, \quad (1)$$

where n_R – the associated cyclic shift of the refined sequence R; l_{rx} – the number of bits received by the receiver Rx. Figure 4 presents a histogram of absolute frequencies of lengths of false sync detection series observed as a result of an experiment with 10,000 tests.

The simulation model, in accordance with the defined algorithm, calculates false sync detection of the synchronisation subsystem under condition (1). If there is a false synchronisation, the run-length counter is incremented. If there is no synchronisation or a true synchronisation occurs, the value of the false synchronisation run-length counter is recorded in the general sample and reset to zero. If the correct sync character

boundary is determined, the current test is completed, and the transition to the next one occurs. From the obtained results of the synchronisation process simulation with the above-defined simulation parameters, the value of the maximum length of the false synchronisation series is $l_{false\_synch} = 4$. The obtained series value makes it possible to form a procedure for increasing the efficiency of input data processing by the receiver *Rx* and successfully receive a frame (block of words) in conditions of high noise intensity.

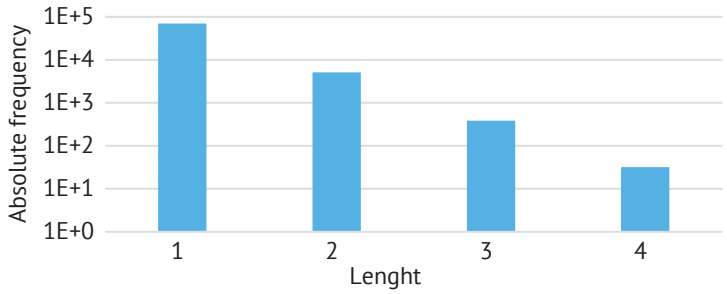

Figure 4. Histogram of absolute frequenciesof false sync detection series
Source: developed by the authors

This procedure is as follows. If the frame synchronisation subsystem run counter exceeds a specified false synchronisation run-length threshold, a decision is made to establish synchronisation. After this, the phase correction process (shifting to the beginning of the boundary of the next fragment of *n* bits) occurs. An attempt to decode the data word begins from the specified position of the next fragment. The algorithm for noise-resilient permutation reception is determined in the study by E. Faure *et al.* (2024). With this procedure, a situation is possible when part of L_0 sync characters of the L_{block} block can be processed by the receiver as characters of the W_{block} block (an error occurs in determining the boundary between L_{block} and W_{block} blocks). The distance from the boundary between L_{block} and W_{block} blocks determined by the synchronisation subsystem to the true boundary is considered to be a numerical value of such an error.

This distance is measured in bits. Based on these expectations, two hypotheses are formed. Hypothesis 1. As a result of performing the frame synchronisation procedure using sync characters, there is an error in determining the boundaries of L_{block} and W_{block} blocks (the error value is not zero). Hypothesis 2. As a result of performing the frame synchronisation procedure using sync characters, there is no error in determining the boundaries of L_{block} and W_{block} blocks (the error value is zero).

RESULTS AND DISCUSSION

Consideration of the structure and algorithms of each component of the simulation model of the data transmission system in accordance with the specified transmission procedure. The structure of the transmitter *Tx* (Fig. 5) presents that:

- the word block W_{block} formation subsystem receives input data in the form of permutation π;
- transmitter settings according to L_0, $l_{max\_letters}$, l_{max_words}, W parameters are set by the user;
- the block L_{block} formation subsystem forms the content of the block in accordance with the specified transmitter parameters;
- the transmission subsystem forms L_{block} and W_{block} blocks according to the set transmission parameters.

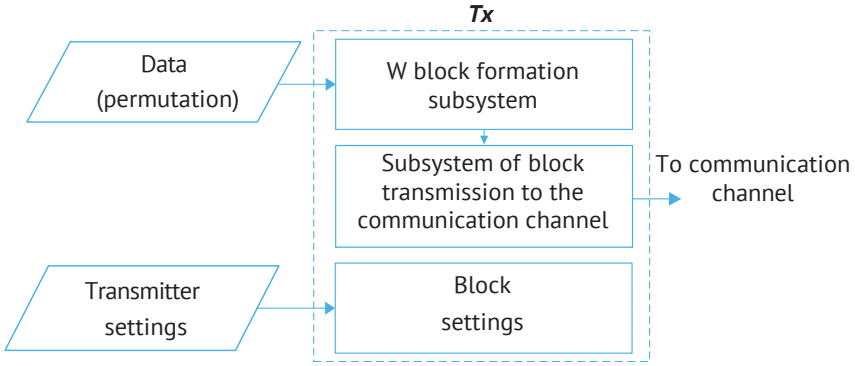

Figure 5. Structure of the transmitter *Tx* system
Source: developed by the authors

The block diagram of the transmitter block operation algorithm (Fig. 6) describes the following sequence of actions:

1. Initialisation. It configures *Tx* based on the entered settings:
   - permutation length *M*;

• number of bits per permutation symbol L_R;
• value L_0 of sync character in the form of a permutation.

Conversion of permutation π into binary representation. Determination of the size of information vectors of synchronisation and data blocks according to $l_{max\_letters}$ and l_{max_words} parameters.

2. Formation of L_{block} and W_{block} blocks from permutations in binary form by combining them into one vector of arrays.

3. Transmission of blocks for output. It transmits bit content of blocks to the transmitter output, to communication channel. Bit-by-bit transmission occurs until the entire content of blocks is transmitted to the output.

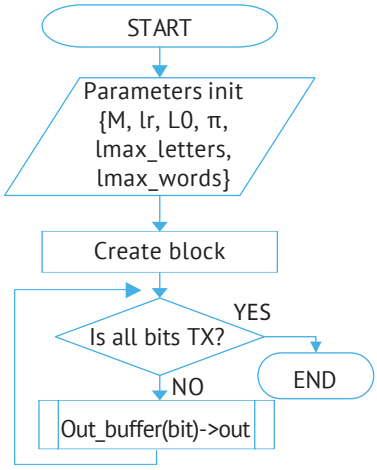

Figure 6. Block diagram of the transmitter *Tx* algorithm
Source: developed by the authors

The structure of the communication channel block *Ch* (Fig. 7) contains:

• input, the channel receives data and transmits it to a noise superposition block;
• noise superposition block that adds generated noise to input data and transmits it to the output;
• noise generation block that generates a distorted signal in accordance with adjustment of false bit rete value set by the user in the form of p_0 value. Generated noise is transmitted to the noise superposition block;
• output that receives data from the noise superposition block and transmits it to the channel output.

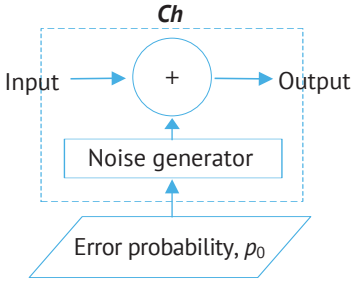

Figure 7. Structure of the communication channel block *Ch*
Source: developed by the authors

The noise superposition block implements the binary symmetric channel (BSC) model. Binary symmetric transmission channel has: an input and an output with an alphabet of binary values that take {1, 0} values (Fig. 8). The output has the probability of false inverted symbol received at p input. The $1-p$ value sets the probability of transmitting the input symbol unchanged, i.e. without distortion.

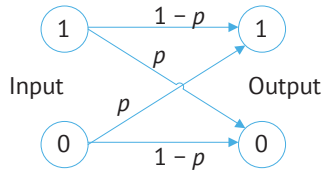

Figure 8. Model of a binary symmetric data transmission channel
Source: developed by the authors

The structure of the receiver block *Rx* (Fig. 9) contains:

• input that receives data from the communication channel system *Ch*;
• input data buffer that accumulates information from the input;
• counter of the number of synchronisation cases that records the length of a series of sync detection of the synchronisation detection subsystem;
• synchronisation detection subsystem that performs data analysis in the input data buffer, the results of the analysis are displayed by increasing or resetting the counter of the number of synchronisation cases;
• phase compensation subsystem that performs phase shift compensation in case the threshold of the synchronisation detection subsystem series is exceeded;
• word processing subsystem that analyses the input data buffer after working out of the phase compensation subsystem;
• output data buffer that stores and displays the decoded information by the word processing subsystem.

The block diagram of the algorithm of the receiver block *Rx* operation is shown in Figure 10.

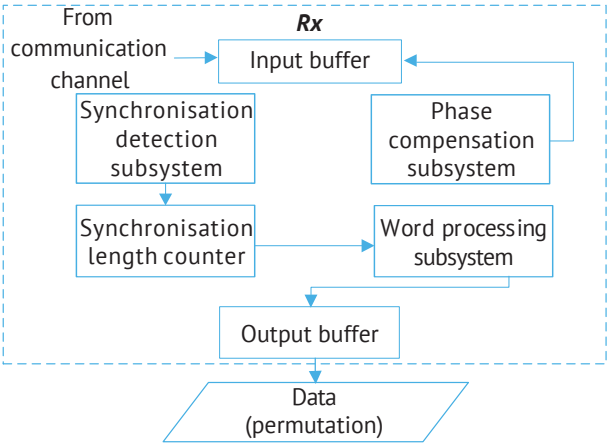

Figure 9. Structure of the receiver block Rx
Source: developed by the authors

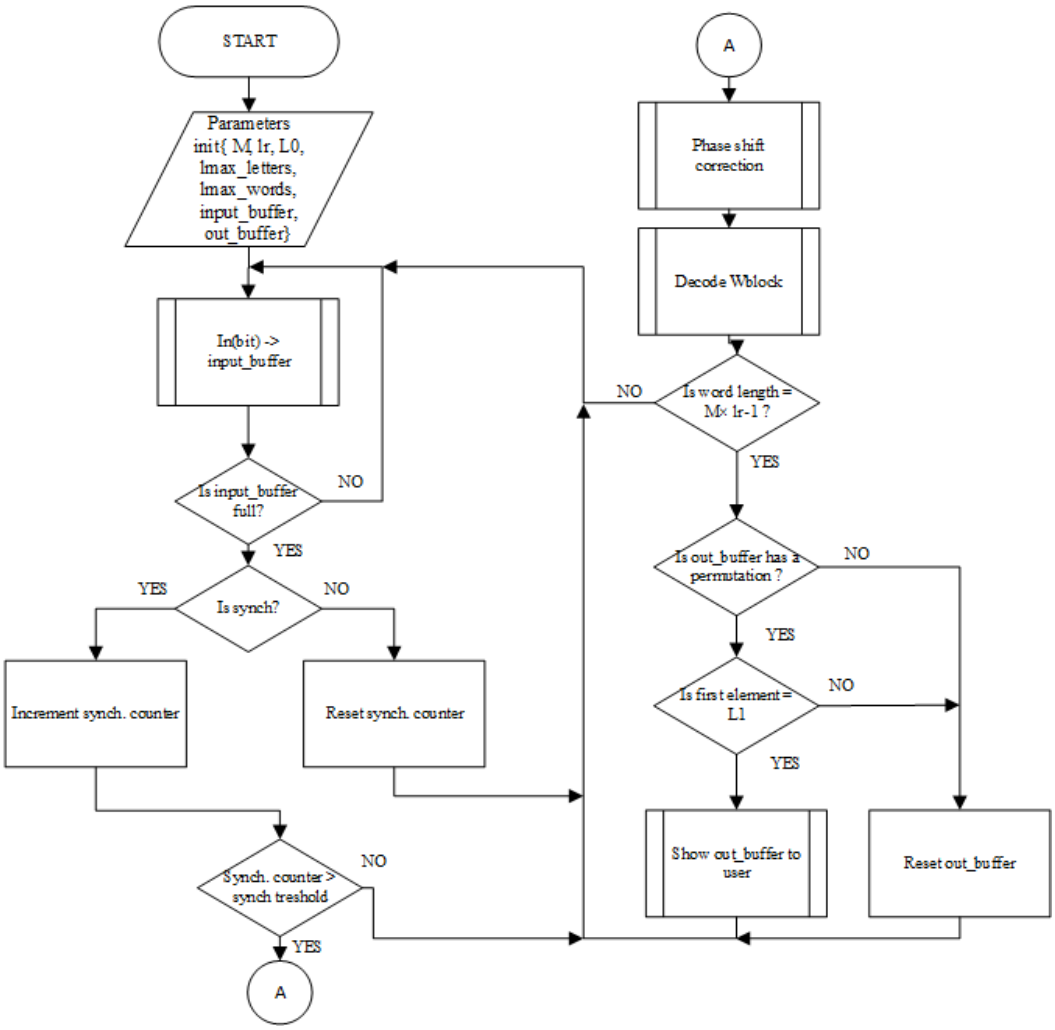

Figure 10. Block diagram of the receiver block Rx operation algorithm
Source: developed by the authors

The receiver block operation algorithm is as follows:

1. Initialisation. It adjusts the receiver according to the settings:

- value of L_0 sync character in the form of a permutation;
- value of the permutation length M;
- number of bits l_r per permutation symbol;
- permutation length n in bits;
- values of all bit and cyclic shifts of L_0 sync character;
- it converts permutation π into a binary representation;
- number of sync characters $l_{max\_letters}$;
- number of words l_{max_words};
- minimum value of the synchronisation series threshold: $l_{synch\_tresh} > l_{false\_synch}$;
- it determines the size of both input and output buffers based on $l_{max\_letters}$ and l_{max_words} parameters.

2. Accumulation of information from the channel. Constant accumulation of bits received at the input of the receiver block and stored in the input data buffer. The buffer has a size equal to the size of synchronisation and data blocks: $l_{rx\_in} = L + W$, bits. The algorithm for recording to the buffer when it is filled can be represented in the form of a queue, first in first out (FIFO). When the buffer is filled with the maximum number of bits l_{rx_in}, the first bit of information by index is deleted. Next bits, starting with index two and ending with l_{rx_in} last bit, are shifted to the left, freeing up space for recording the next bit that comes from communication channel.

3. Synchronisation analysis. Having accumulated l_{rx_in} bits, the receiver analyses a part of the input buffer equal to L bits and forms the refined sequence R. If refined bit sequence is associated with L_0, the synchronisation series counter is incremented. Otherwise, the synchronisation series counter is reset to zero and the transition to receiving the next bit from the input of the receiver block is performed (point 2).

4. Synchronisation series analysis. If the value l_{synch_tresh} of synchronisation series length is exceeded, go to point 5, otherwise receive the next bit (point 2).

5. Phase correction. Based on the obtained data of sync character, the value of the synchronisation phase

shift is determined. For this, the refined sequence R is compared with all cyclic shifts of the sync character. If d_{lim} with a certain shift is present, the number of this j shift is obtained. The number of bits to the boundary of the next $J_{shift} = n - j$ permutation block (fragment) is calculated. If the value of $J_{shift} = 0$, go to point 6, if $J_{shift} \neq 0$, accumulate the number of required J_{shift} (points 2-5).

6. Word block analysis. A data fragment, which is equal to W bits, is selected from the input buffer. The refined sequences for each of $[L_1; L_j]$ characters in the block W_{block} are determined. A comparison with all cyclic shifts of $R \in [L_1; L_j]$ sync character is performed. As a result of the comparison, the identified shift number j for each of refined sequences is obtained. The obtained shift number is recorded to the output buffer. If the word is not recognised after the comparison procedure with L_0 cyclic shifts, clear the output buffer and go to point 2.

7. Word content analysis. The number of entered shifts in the output buffer is counted. When $j = \{1; n-1\}$ shift numbers are accumulated, it is checked whether the numbers are repeated (numbers of word shifts form a permutation). If the numbers are unique, a permuta tion is formed in the buffer, and the contents of the buffer are analysed by index one. If the first number in the output buffer is equal to one (identified with the first cyclic shift of L_1 sync character-permutation), the content of the output buffer is transmitted to the user. A conclusion is formed that the reception of data (transmitted permutation by the transmitter) is completed. If no unique values of j shift numbers have been entered in the buffer or the first number in the output buffer is not equal to one, then clear the output buffer and repeat the reception cycle from point 2.

In the process of testing, the simulation model was experimentally investigated by conducting 1,000 experiments. During the experiment, the data presented in the form of permutation $\pi = (1, 2, 3, \ldots, 23)$ was transmitted for different bit error rate $p_0 = [0.1; 0.4]$ with a step of 0.05. L bits of zero values were transmitted to communication channel, then a synchronisation block L_{block} and a word block W_{block} were formed.

Transmitter system setting parameters:

- permutation length $M = 8$, symbols;
- number of bits per permutation symbol $l_r = 3$, bits;
- value of sync character-permutation $L_0 = (0, 1, 7, 3, 2, 5, 4, 6)$;
- number of sync character blocks $K = 1$;
- number of sync characters in the block $l_{max\_letters} = 75$;
- number of words in the data block $l_{max\_words} = 89$.

Receiver system setting parameters:

- permutation length $M = 8$, symbols;
- number of bits per permutation symbol $l_r = 3$, bits;
- value of sync character-permutation $L_0 = (0, 1, 7, 3, 2, 5, 4, 6)$;
- number of sync character blocks $K = 1$
- number of sync characters in the block $l_{max\_letters} = 75$
- number of words in the data block $l_{max\_words} = 89$.
- minimum value of synchronisation series threshold $l_{synch\_tresh} = 5$.

Based on the results of the experimental study of the simulation model, a sample of the following parameters was formed:

1. The number $N_{frame\_received}$ of data blocks successfully received by the receiver – a situation when the receiver was able to correctly perform synchronisation by characters and decoded the word block – the test was successful.

2. The number N_{frame_lost} of data blocks not received by the receiver – a situation when the receiver was unable to correctly perform synchronisation by characters or correctly performed synchronisation, but incorrectly decoded the word block – the test was not successful.

3. The maximum number of bits from the block L_{block} to the sliding window for analysing the word block W_{block} is $l_{max\_letter\_block}$.

4. The minimum number of bits from the block L_{block} to the sliding window for analysing the word block W_{block} is $l_{min\_letter\_block}$.

5. The number of successfully decoded frames with the maximum number of bits from the block L_{block} to the sliding window for analysing the block W_{block} is $N_{rx\_max\_l}$.

6. The number of successfully decoded frames with the minimum number of bits from the block L_{block} to the block W_{block} is $N_{rx\_min\_l}$.

7. Average transmission time t_μ in seconds.

The results obtained for each $p_0 = [0.1; 0.4]$ with a step of 0.05 as a result of 1,000 tests are given in Table 1.

Table 1. Results of the experiment

BER p_0	0.1	0.15	0.2	0.25	0.3	0.35	0.4
$N_{frame\_received}$	1,000	1,000	1,000	1,000	1,000	1,000	1,000
N_{frame_lost}	0	0	0	0	0	0	0
$l_{max\_letter\_block}$	552	552	552	552	552	552	552
$l_{min\_letter\_block}$	-*	-*	-*	-*	-*	-*	0
$N_{rx\_max\_l}$	1,000	1,000	1,000	1,000	1,000	1,000	988
$N_{rx\_min\_l}$	0	0	0	0	0	0	12
t_μ	0.716	0.706	0.689	0.7	0.7	0.67	0.666

Note: * – value is equal to the maximum number

Source: developed by the authors

To assess the impact of false determination of sync character boundary by the receiver synchronisation subsystem and to check the effectiveness of the receiver operation algorithm, another 1,000 tests were carried out with similar test parameters, the parameter of the minimum value of synchronisation series threshold was set to $l_{synch\_tresh} = -1$ in the receiver block *Rx*. According to the receiver block operation algorithm (Fig. 10), such an indicator turns off the analysis of synchronisation series. The results of the conducted experiment are shown in Table 2.

Table 2. Results of experiments with the turned off mechanism of synchronisation series analysis

BER p_0	0.1	0.15	0.2	0.25	0.3	0.35	0.4
$N_{frame\_received}$	1,000	1,000	1,000	1,000	1,000	1,000	1,000
N_{frame_lost}	0	0	0	0	0	0	0
$l_{max\_letter\_block}$	552	552	552	1,104	1,104	1,104	1,104
$l_{min\_letter\_block}$	-*	-*	-*	552	552	552	552
$N_{rx\_max\_l}$	1,000	1,000	1,000	2	56	317	318
$N_{rx\_min\_l}$	0	0	0	998	944	683	682
t_{μ}	0.68	0.681	0.69	0.736	0.702	0.613	0.488

Note: * – value is equal to the maximum number

Source: developed by the authors

According to the results of the experiment, 1,000 tests were conducted (Table 1). No lost transmitted blocks were recorded during tests, the receiver block reception algorithm with the proposed structure (Fig. 9) successfully received all transmitted fragments through communication channel with $p_0 = [0.1; 0.4]$ with a step of 0.05. Under these conditions, the error in determining the distance between L_{block} and W_{block} blocks did not exceed the value of 552 bits. For $M = 8$ and $l_r = 3$ parameters, this is equal to one word W (phase shift by words). Average synchronisation and decoding time of one frame is 0.666 s with $p_0 = 0.4$. Relative frequency of occurrence of an error in determining the boundary between L_{block} and W_{block} blocks per word for $p_0 = 0.4$ is equal to: $\omega_{word} = \frac{988}{1{,}000} = 0.988$. Relative frequency of occurrence of a zero error in determining the boundary between L_{block} and W_{block} blocks is equal to: $\omega_0 = 1 - \omega_{word} = 0.012$. According to p_0 from 0.1 to 0.35, relative frequency of occurrence of the error in determining the boundary between L_{block} and W_{block} blocks per word is 1.0.

The results of 1,000 tests are shown in Table 2. The algorithm of the receiver block performed the analysis of the synchronisation series length by the l_{synch_tresh} parameter. According to Table 2, no lost transmitted fragments were recorded during tests. The error value for determining the boundary between L_{block} and W_{block} blocks is 1,104 bits, which is equal to $2W$ two words with a p_0 ranging from 0.25 to 0.4. Relative frequencies of error values for determining the boundary between L_{block} and W_{block} blocks are shown in Figure 11. Average synchronisation and decoding time for one test is 0.488 s for $p_0 = 0.4$,

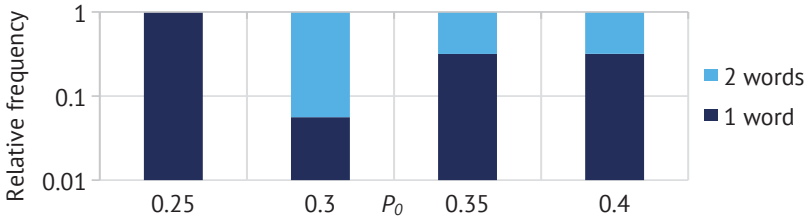

Figure 11. Histogram of relative frequencies of error values for determining the boundary between L_{block} and W_{block} blocks

Source: developed by the authors

The presented simulation model of communication uses binary symmetric channel (BSC) model to simulate the transmission channel. The BSC model can be used for theoretical analysis of data transmission channels, in particular in the tasks of bandwidth calculation, as shown in the study by H. Chen *et al.* (2024), where optimisation using symmetrised KL information is considered. At the same time, the BSC model is a simplified idealisation of real data transmission channels, which has a number of drawbacks in the context of noise simulation:

1. Unrealistic assumption of uniform error distribution. BSC assumes the same error probability for each bit regardless of previous ones. In real channels, errors often have a correlation.

2. Lack of noise type simulation. The BSC model does not take into account physical nature of noise (for example, white Gaussian noise, impulse noise, or interference), which is important in real systems.

3. Limitations of adaptation to the environment. BSC does not take into account variable channel

characteristics, such as dynamic signal-to-noise ratio (SNR), which can change the error probability depending on current conditions. This characteristic is inherent in complex modem systems where information presentation and transmission are implemented using phase and amplitude modulation, where errors depend on signal and noise interaction.

4. Ignoring of packet or symbol losses. In many real channels, not only errors in bit values, but also data loss, which BSC does not simulate, can occur.

5. Non-consideration of spatiotemporal effects. BSC does not take into account the effects of multipath and signal displacement in time, which can significantly affect the quality of transmission.

The study by J. Boiko *et al.* (2022) shows the influence of spatiotemporal effects on the noise resiliece of telecommunication systems with orthogonal frequency-division multiplexing (OFDM) modulation. When implementing the simulation model of the communication system, the phenomenon of signal displacement in time is taken into account by implementing the transmitter in the form of a separate system, as well as transmitting a block of zero bit values with a length of $L = l_{max\_letters} \cdot M \cdot l_r$ into the channel that contains noise after the system passes through communication channel. An alternative to the use of the BSC model implies the following:

1. Binary channel with dependent error probability. To take into account the correlation of errors, it is possible to use models with Markov processes. Thus, V. Vlasenko *et al.* (2023) propose the use of Markov models for quantitative assessment of network reliability, which allows predicting the state of the network and planning preventive measures to ensure its stable operation.

2. Real noise simulation. For a more accurate representation of the environment, it is possible to use channels that take into account the type of noise: a channel with additive white Gaussian noise (AWGN); a channel with impulse noise for cases when interference is short-term and intense. The study by V. Anand Kumar & V. Nandalal (2024), which conducts research and evaluation of the 5G 3GPP cellular network standard, uses several transmission channel models, including both the AWGN channel and the BSC model.

3. Multipath models. For example, Rayleigh or Rice models for simulating multipath effects in wireless networks.

4. Channels with a variable signal-to-noise ratio (SNR).

5. Iterative modelling using realistic simulators.

The overview of the functionality of use of MATLAB software which is shown in the study by D.T. Valentine & B.H. Hahn (2022). The study by J.C. da Silva *et al.* (2021) considers the possibilities of using the NS-3 network simulator to study the LoRAWAN protocol used in IoT. The use of such tools allows for the integration of more complex channel models taking into account real physical effects. To maintain the simplicity and increase the realism of binary symmetric transmission channel, some aspects can be improved by using the Hilbert-Elliot model. H.Q. Ta *et al.* (2022) consider the impact of noise and uncertainty on message throughput using the Gilbert-Elliot model to simulate communication channel. The described approaches will help to increase the accuracy of simulation studies and to ensure greater compliance with real conditions of information transmission.

Word synchronisation and decoding procedure used in the simulation model. In the presence of synchronisation, phase shift compensation occurs only to the boundary of the next sync character fragment, and not to the beginning of the W_{block} block with words, since the receiver does not know where the beginning of the block in the buffer of input information from *Ch* communication channel is. Therefore, having the value of a sync character-permutation, its structure and properties, the receiver block algorithm in the simulation model of communication compensates for the phase shift of the sliding window only until the beginning of the next permutation fragment. When the boundaries of a word block and a character block are incorrectly determined, an error occurs in determining the boundary, which affects the probability of a bit error in the word block. The analysis of the results given in Table 1 with $p_0 = 0.4$ bit error probability in communication channel indicates the presence of an error in determining the boundary of 552 bits. This fragment does not belong to the data block and, accordingly, increases the probability of a bit error in it. This probability can be estimated by expression (2):

$$p_0^* = \frac{l_{max\_letter\_block} \cdot 0.5 + (n_w - l_{max\_letter\_block}) \cdot p_0}{n_w}. \quad (2)$$

For specified model parameters, $p_0^* = 0.401$. The error in determining the boundary occurs due to the fact that the receiver does not know the exact beginning of the block of sync characters-permutations and relies only on information about the structure of information flow. Accordingly, after establishing synchronisation, the system performs phase shift correction to the boundary of the character and assumes that the next block of *W* bits may contain information with words. The reduction in bit error probability when decoding a word depends on accurate determination of the boundary of L_{block} and W_{block} blocks. The use of a mechanism for detecting the synchronisation series threshold exceeding is one of the means for increasing accuracy. The mechanism is represented in the form of a counter showing the length of the series, and in the model algorithm as l_{synch_tresh}.

The effectiveness of the mechanism for detecting the synchronisation series threshold exceeding can be assessed by comparing the results presented in Table 1 and Table 2. Based on the results of two experiments, it is possible to draw a conclusion about the proposed Hypothesis 1 and Hypothesis 2 regarding the synchronisation

series length tracking mechanism. Hypothesis 1 has been confirmed, since after exceeding the threshold for the number of synchronisation cases, phase shift correction, the beginning of analysis and word decoding, the value of the error of determination between L_{block} and W_{block} blocks is not zero. Accordingly, Hypothesis 2 has not been confirmed. However, according to calculated boundary probability of bit error in communication channel for the number of $L_{block} = 1$ and $l_{max\_letters} = 75$ sync character blocks, there are cases where the error in determining the boundary of L_{block} and W_{block} blocks is equal to zero. Table 1 shows the results under conditions of using the mechanism for detecting the synchronisation series threshold exceeding. In this case, the error value is 552 bits. However, as a result of tests, where the mechanism for detecting the synchronisation series threshold exceeding has not been used, the error value for determining the boundary of L_{block} and W_{block} blocks is 1,104 bits (Table 2). Accordingly, the introduction of the mechanism for detecting the synchronisation series threshold exceeding helps to increase the accuracy of determining the boundary of L_{block} and W_{block} blocks. The analysis of synchronisation series helps to reduce the value of the phase shift by words by half and increases the accuracy of word recognition.

Average time taken to decode a word, when using the synchronisation series length tracking mechanism, was 0.666 s with $p_0 = 0.4$. In the absence of the mechanism for detecting the synchronisation series threshold exceeding, this time with the same BER was 0.488 s, which was 26.7% faster. BER in the word block during analysis and decoding increases from 0.401 to 0.402. It is possible to compensate for the error in determining the boundary of L_{block} and W_{block} blocks by performing compensation of the determined boundary after the synchronisation procedure by the value of one word during analysis and decoding by the receiver block. Thus, the error in determining the boundary of sync character and word blocks will decrease from 99.8% to 0.2% under specified model parameters and $p_0 = 0.4$.

The difference between the synchronisation algorithm of E. Faure *et al.* (2024) and the algorithm in the study by B. Stupka (2024) consists in the use of a fixed-size sliding window, where the data received from communication channel is recorded. As a result, the algorithm proposed in the study by E. Faure *et al.* (2024) does not use a dynamic change in values of K and l – the number of blocks (K) of l fragments of length M received from the symbol channel. Therefore, K and l values are constant. They are chosen in such a way as to satisfy the requirements for the probabilities of true and false synchronisation. The length of the sliding window is equal to $K \cdot L \cdot M$ symbols.

Using majority and correlation processing of received fragments, the algorithm of E. Faure *et al.* (2024) makes it possible to achieve a theoretical probability of false synchronisation $P_{false\_final} = 2.9 \cdot 10^{-6}$ for $p_0 = 0.4$, as well as $K = 4$, $l = 85$ and $M = 8$. The presence of significant redundancy is a disadvantage of the frame synchronisation algorithm proposed in the study by E. Faure *et al.* (2024). With an increase in the number of L_{block} blocks having a length of 1,800 bits (for $M = 8$, $l_r = 3$, $l = 75$ parameters) by 4 times, the number of sync character bits in the synchronisation block will be 8,160 bits (for $M = 8$, $l_r = 3$, $K = 4$, $l = 85$ parameters). Such redundancy will result in an increase of overhead by time during transmission/reception. In the study by J.R. Cotrim & J.H. Kleinschmidt (2020), the authors review and evaluate the Long RangeWide Area Network (LoRaWAN) link layer protocol. LoRaWAN is a low-power communication protocol that provides data transmission over distances of up to several kilometers for IoT devices. It operates in radio frequency bands using Long Range (LoRa) technology – spread spectrum modulation, which provides high sensitivity and noise immunity. The study by J.R. Cotrim & J.H. Kleinschmidt (2020) indicates that packet size, spreading factor (SF) and bandwidth are influential factors on the transmission/reception time. The results of the authors' study demonstrate that in the 125 kHz bandwidth of data transmission with a length of 50 bytes and $SF = 7$, the time on air (ToA) is 0.113 s. The calculated channel bandwidth is 3,543.1 bit/s. Using the proposed structure (Fig. 3) and LoRaWAN transmission technology, the number of L_{block} blocks is increased by 4 times and the ToA value will be 2.303 s for the same bandwidth and SF value. The introduction of redundancy leads to a decrease in the "useful" channel bandwidth, since less useful information is transmitted per unit of time, which affects the transmission time. The processing time of received and transmitted information is important when controlling real-time devices or transmitting information in real-time mode.

CONCLUSIONS

The application of algorithms and methods for noise-resilient transmission of permutations through communication channel with high bit error probability was considered and investigated. The structure of the communication system, the synchronisation subsystem, consisting of the synchronisation block L_{block} and the word block W_{block} was solved by conducting simulation modelling of the synchronisation process with 10,000 tests. The maximum length of the series of false determination of sync character boundaries was experimentally determined.

A simulation model of the communication system using a simplex binary symmetric communication channel with $p_0 = 0.4$ was built. The structures and algorithms for the operation of component blocks of the simulation model: transmitter, communication channel, and receiver were presented. The proposed algorithms were tested in the simulation model of communication by conducting 1,000 tests taking into account the mechanism for exceeding the synchronisation series threshold, as well as a simulation modelling of 1,000 transmissions without taking into account the mechanism

for exceeding the synchronisation threshold was conducted in order to assess the impact of the accuracy of determining the boundaries of synchronisation blocks and words. The simulation parameters were presented. The experiments were conducted for a specified range of p_0 = [0.1; 0.4] with a step of 0.05. The simulation modelling has shown that the procedure for taking into account the length of the synchronisation series makes it possible to reduce the error in determining the boundary between L_{block} and W_{block} blocks. The results of the model demonstrate successful information transmission in each of tests with p_0 = 0.4. This indicates the adequacy of the proposed methods and algorithms, which can form the basis for the implementation of the synchronisation subsystem of the noise-resilient communication system based on permutations and be used to implement a three-pass cryptographic protocol.

ACKNOWLEDGEMENTS

This research was funded by the Ministry of Education and Science of Ukraine (Grant No. 0123U100270).

CONFLICT OF INTEREST

None.

REFERENCES

[1] Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019). Security for 5G and beyond. *IEEE Communications Surveys & Tutorials*, 21(4), 3682-3722. doi: 10.1109/COMST.2019.2916180.

[2] Anand Kumar, V., & Nandalal, V. (2024). A comparative design of 5G communication codes. *International Journal of Communication Systems*, 37(18), article number e5954. doi: 10.1002/dac.5954.

[3] Boiko, J., Pyatin, I., Eromenko, O., & Shayuk, D. (2022). Estimation of the effect of carrier frequency offset on the noise immunity of telecommunications with OFDM. *Measuring and Computing Devices in Technological Processes*, 3, 19-26. doi: 10.31891/2219-9365-2022-71-3-3.

[4] Chen, H., Aminian, G., & Bu, Y. (2024). An algorithm for computing the capacity of symmetrized KL information for discrete channels. In *60th annual Allerton conference on communication, control, and computing* (pp. 1-8). Urbana: IEEE. doi: 10.1109/Allerton63246.2024.10735330.

[5] Cotrim, J.R., & Kleinschmidt, J.H. (2020). LoRaWAN mesh networks: A review and classification of multihop communication. *Sensors*, 20(15), article number 4273. doi: 10.3390/s20154273.

[6] Da Silva, J.C., Flor, D.D.L., de Sousa Junior, V.A., Bezerra, N.S., & de Medeiros, A.A.M. (2021). A survey of LoRaWAN simulation tools in ns-3. *Journal of Communication and Information Systems*, 36(1), 17-30. doi: 10.14209/jcis.2021.2.

[7] Faure, E., Baikenov, A., Skutskyi, A., Faure, D., & Abramkina, O. (2024). Algorithms for reliable permutation transmission protocols in noisy communication channels. In *Cybersecurity providing in information and telecommunication systems II* (pp. 40-48). Kyiv: CPITS.

[8] Faure, E., Shcherba, A., Makhynko, M., Stupka, B., Nikodem, J., & Shevchuk, R. (2022). Permutation-based block code for short packet communication systems. *Sensors*, 22(14), article number 5391. doi: 10.3390/s22145391.

[9] Feng, C., Wang, H.-M., & Poor, H.V. (2021). Reliable and secure short-packet communications. *IEEE Transactions on Wireless Communications*, 21(3), 1913-1926. doi: 10.1109/TWC.2021.3108042.

[10] Gao, M., & Shum, K.W. (2024). Efficient encoding and decoding algorithm for a class of perfect single-deletion-correcting permutation codes. *ArXiv*. doi: 10.48550/arXiv.2411.08258.

[11] Ho, C.D., Nguyen, T.-V., Huynh-The, Th., Nguyen, T.-T., da Costa, D.B., & An, B. (2021). Short-packet communications in wireless-powered cognitive IoT networks: Performance analysis and deep learning evaluation. *IEEE Transactions on Vehicular Technology*, 70(3), 2894-2899. doi: 10.1109/TVT.2021.3061157.

[12] Jahangeer, A., Bazai, S.U., Aslam, S., Marjan, S., Anas, M., & Hashemi, S.H. (2023). A review on the security of IoT networks: From network layer's perspective. *IEEE Access*, 11, 71073-71087. doi: 10.1109/ACCESS.2023.3246180.

[13] Lee, H., & Ko, Y.-C. (2021). Physical layer enhancements for ultra-reliable low-latency communications in 5G new radio systems. *IEEE Communications Standards Magazine*, 5(4), 112-122. doi: 10.1109/MCOMSTD.0001.2100002.

[14] Li, Y., Huynh, D.V., Do-Duy, T., Garcia-Palacios, E., & Duong, T.Q. (2022). Unmanned aerial vehicle-aided edge networks with ultra-reliable low-latency communications: A digital twin approach. *IET Signal Processing*, 16(8), 897-908. doi: 10.1049/sil2.12128.

[15] Stupka, B. (2024). *Methods of reliable information transmission in systems with non-separable factorial coding of data with a high probability of bit error*. (PhD tesis, Cherkasy State Technological University, Cherkasy, Ukraine).

[16] Sun, Y., Li, H., Guo, C., & Wang, D. (2021). A 5G-oriented LDPC encoder based on byte-parallel configurable cyclic shift. In *13th international conference on communication software and networks (ICCSN)* (pp. 17-23). Chongqing: IEEE. doi: 10.1109/ICCSN52437.2021.9463607.

[17] Ta, H.Q., Pham, Q.-V., Ho-Van, K., & Kim, S.W. (2022). Covert communication with noise and channel uncertainties. *Wireless Networks*, 28(1), 161-172. doi: 10.1007/s11276-021-02828-3.

[18] Valentine, D.T., & Hahn, B.H. (2022). *Essential MATLAB for engineers and scientists* (8th ed.). Cambridge: Academic Press. doi: 10.1016/C2021-0-01607-2.

[19] Vlasenko, V., Shchavinskyi, Yu., Zaporozhchenko, M., & Tyshchenko, V. (2023). Analysis of technologies for building a data transmission network with high requirements for information security, reliability and delay. *Connectivity*, 163(3), 8-15. doi: 10.31673/2412-9070.2023.032030.
[20] Yang, Y., & Hanzo, L. (2023). Permutation-based short-packet transmissions improve secure URLLCs in the Internet of things. *IEEE Internet of Things Journal*, 10(12), 11024-11037. doi: 10.1109/JIOT.2023.3243038.

Алгоритми та імітаційна модель підсистеми синхронізації системи завадостійкого інформаційного обміну на основі перестановок

Еміль Фауре

Доктор технічних наук, професор
Черкаський державний технологічний університет
18006, бульв. Шевченка, 460, м. Черкаси, Україна
https://orcid.org/0000-0002-2046-481X

Артем Скуцький

Аспірант
Черкаський державний технологічний університет
18006, бульв. Шевченка, 460, м. Черкаси, Україна
https://orcid.org/0000-0002-8632-1176

Артем Лавданський

Кандидат технічних наук, доцент
Черкаський державний технологічний університет
18006, бульв. Шевченка, 460, м. Черкаси, Україна
https://orcid.org/0000-0002-1596-4123

Анотація. У сучасних системах передавання даних однією з ключових задач є забезпечення надійності комунікації в умовах завад. Це є особливо актуальним для каналів із високою ймовірністю бітових помилок, зокрема, для каналів радіозв'язку з інтенсивними природними чи штучними шумами, що обмежує використання традиційних методів корекції помилок. Метою цієї роботи була розробка алгоритмів інформаційного обміну кодовими словами нероздільного факторіального коду, що передбачає представлення кодових слів у вигляді перестановок, симплексним двійковим симетричним каналом зв'язку з високою імовірністю бітової помилки. Для побудови цих алгоритмів за основу взято метод циклової синхронізації нероздільного факторіального коду, який використовує мажоритарну та кореляційну обробку прийнятих з каналу зв'язку фрагментів. Досліджено методи та алгоритми завадостійкого передавання перестановок у каналах зв'язку з високою ймовірністю бітової помилки. Розроблено загальну схему протоколу організації симплексного інформаційного обміну. Запропоновано алгоритм детектування хибних синхронізацій для умов високого рівня шуму в каналі зв'язку. Досліджено ефективність протоколу синхронізації кодових слів факторіального коду, виявлено та представлено переваги використаного підходу. Розроблено імітаційну модель системи інформаційного обміну симплексним двійковим симетричним каналом зв'язку та можливістю задання значення бітової помилки в ньому. Наведено структуру імітаційної моделі та алгоритми роботи її складових блоків. Виконано розрахунок параметрів синхронізації для ймовірності бітової помилки 0,4, представлено результати моделювання за 10 000 випробувань, що дозволило експериментальним шляхом визначити параметри алгоритму синхронізації. Виконано імітаційне моделювання та отримано оцінку точності визначення меж блоків синхронізації за ймовірності бітової помилки в діапазоні від 0,1 до 0,4. Запропоновано підхід, що дозволяє зменшити похибку під час визначення меж перестановок. Отримані результати свідчать про ефективність запропонованих рішень, узгодженість теоретичних і практичних показників роботи підсистеми синхронізації, а також про можливість використання розроблених алгоритмів для реалізації трьохетапного криптографічного протоколу на основі перестановок

Ключові слова: симплексний двійковий симетричний канал; факторіальне кодування; статистика; протокол; шум

ВІСНИК
Черкаського державного технологічного університету

Науковий збірник

Том 29, № 4. 2024

Заснований у 1996 р. Виходить чотири рази на рік

Оригінал-макет видання виготовлено у редакційно-видавничому відділі
Черкаського державного технологічного університету

Відповідальний редактор:
А. Лавданський

Редагування англомовних текстів:
С. Воровський, К. Касьянов

Комп'ютерна верстка:
М. Блімар

Підписано до друку 16 грудня 2024 р.
Формат 60*84/8
Умов. друк. арк. 9
Наклад 50 прим.

Адреса видавництва:
Черкаський державний технологічний університет
18006, бульв. Шевченка, 460, м. Черкаси, Україна
Тел.: +380638013283
E-mail: info@bulletin-chstu.com.ua
https://bulletin-chstu.com.ua/uk

BULLETIN
of Cherkasy State Technological University

Scientific Collection

Volume 29, No. 4. 2024

Founded in 1996. Published four times per year

The original layout of the publication is made in the editorial and publishing department of Cherkasy State Technological University

Managing editor:
A. Lavdanskyi

Editing English-language texts:
S. Vorovsky, K. Kasianov

Desktop publishing:
M. Blimar

Signed for print of December 16, 2024.
Format 60*84/8
Conventional printed pages 9
Circulation 50 copies

Editors Office Address:

Cherkasy State Technological University
18006, 460 Shevchenko Blvd., Cherkasy, Ukraine
Tel.: +380638013283
E-mail: info@bulletin-chstu.com.ua
https://bulletin-chstu.com.ua/en