ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ
АКАДЕМИЯСЫ» РҚБ

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

РОО «НАЦИОНАЛЬНОЙ
АКАДЕМИИ НАУК РЕСПУБЛИКИ
КАЗАХСТАН»

N E W S

OF THE NATIONAL ACADEMY
OF SCIENCES OF THE REPUBLIC
OF KAZAKHSTAN

SERIES OF PHYSICS AND MATHEMATICS

1 (353)

JANUARY – MARCH 2025

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

«ҚР ҰҒА Хабарлары. Физика-математика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы).

Ақпарат агенттігінің мерзімді баспасөз басылымын, ақпарат агенттігін және желілік басылымды қайта есепке қою туралы ҚР Мәдениет және Ақпарат министрлігі «Ақпарат комитеті» Республикалық мемлекеттік мекемесі **28.02.2025** ж. берген **№KZ20VPY00113741** Куәлік.

Тақырыптық бағыты: *ақпараттық-коммуникациялық технологиялар*

Қазіргі уақытта: *«ақпараттық-коммуникациялық технологиялар» бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*

Мерзімділігі: *жылына 4 рет.*

Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«Известия НАН РК. Серия физико-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*

Свидетельство о постановке на переучет периодического печатного издания, информационного агентства и сетевого издания **№ KZ20VPY00113741.** Дата выдачи **28.02.2025**

Тематическая направленность: *информационно-коммуникационные технологии.*

В настоящее время: *вошел в список журналов, рекомендованных КОКСНВО МНВО РК по направлению «информационно-коммуникационные технологии».*

Периодичность: *4 раза в год.*

Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of Physics and Mathematics
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty).
Certificate **No. KZ20VPY00113741** on the re-registration of the periodical printed and online publication of the information agency, issued on **28.02.2025** by the Republican State Institution «Information Committee» of the Ministry of Culture and Information of the Republic of Kazakhstan
Subject area*: information and communication technologies.*
Currently: *included in the list of journals recommended by the CCSES MSHE RK in the direction of «Information and communication technologies».*
Periodicity: *4 times a year.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 1. Namber 353 (2025). 66–77

https://doi.org/10.32014/2025.2518-1726.325

IRSTI: 81.93.29
UDC: 004.49

G. Aksholak*, A. Bedelbayev, R. Magazov, 2025.
Kazakh National University named after Al-Farabi, Almaty, Kazakhstan.
E-mail: gaksholak@gmail.com

SECURING KUBERNETES: AN ANALYSIS OF VULNERABILITIES, TOOLS, AND FUTURE DIRECTIONS

Aksholak Gulnur – PhD student, Kazakh National University named after Al-Farabi, Almaty, Kazakhstan, E-mail: gaksholak@gmail.com, https://orcid.org/0000-0001-8292-6939;
Bedelbayev Agyn – candidate of sciences in physics and mathematics, associate professor of the Department "Information Systems", Kazakh National University named after Al-Farabi, Almaty, Kazakhstan, agyn08@yandex.ru, https://orcid.org/0000-0001-9839-4156;
Magazov Raiymbek – PhD student, Kazakh National University named after Al-Farabi, Almaty, Kazakhstan, E-mail: Magazovraiko@gmail.com, https://orcid.org/0009-0000-4105-2331.

Abstract. In an era marked by rapid technological evolution, especially within cloud computing and container orchestration, the security of systems like Kubernetes is paramount. In this study, we investigate the security architecture of Kubernetes, emphasizing both its strengths and vulnerabilities. We analyze the core components—such as the master node and worker nodes – highlighting their roles in maintaining scalability and resilience in containerized environments. Our research further explores the various security challenges, including misconfigurations and vulnerabilities identified in recent CVEs (Common Vulnerabilities and Exposures), and the potential impact these issues have on Kubernetes deployments. A significant portion of the analysis is dedicated to recent developments in Kubernetes security, such as the introduction of Kubernetes 1.29 and the Kubernetes Gateway API.

A critical part of our analysis is the comparative evaluation of security tools, including Kube-bench, Sonobuoy, and Kube-hunter. These tools are assessed based on criteria such as usability, customization options, performance overhead, and integration capabilities. Our findings suggest that while these tools provide essential security features, there is still a gap in comprehensive, automated solutions that can address the dynamic and complex nature of Kubernetes environments.

The study offers valuable insights into the current state of Kubernetes security and suggests future directions for research, including the development of AI-driven security solutions that can proactively detect and mitigate threats.

Keywords: Kubernetes, architecture, security, scalability, containerized applications, misconfiguration.

Г.И. Ақшолақ*, А.А. Бедельбаев, Р.С. Мағазов, 2025.
Әл-Фараби атындағы қазақ Ұлттық университеті, Алматы, Қазақстан.
E-mail: gaksholak@gmail.com

KUBERNETES-ТІ ҚОРҒАУ: ОСАЛДЫҚТАРДЫ, ҚҰРАЛДАРДЫ ЖӘНЕ БОЛАШАҚ БАҒЫТТАРДЫ ТАЛДАУ

Ақшолақ Гүлнұр Исатайқызы – PhD докторант, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан, E-mail: gaksholak@gmail.com, https://orcid.org/0000-0001-8292-6939;
Беделбаев Ағын Абдешұлы – физика-математика ғылымдарының кандидаты, Әл-Фараби атындағы Қазақ ұлттық университетінің «Ақпараттық жүйелер» кафедрасының қауым. профессоры, Алматы, Қазақстан, E-mail: agyn08@yandex.ru, https://orcid.org/0000-0001-9839-4156;
Мағазов Райымбек Саламатұлы – PhD докторант, Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан, E-mail: Magazovraiko@gmail.com, https://orcid.org/0009-0000-4105-2331.

Аннотация. Бұлтты есептеулер мен контейнерлерді оркестрациялаудың қарқынды дамыған дәуірінде Kubernetes сияқты жүйелердің қауіпсіздігі бірінші орында тұрады. Бұл зерттеуде біз Kubernetes-тің қауіпсіздік архитектурасын, оның күшті және әлсіз жақтарын зерттейміз. Біз негізгі компоненттерді – мастер (master node) және жұмыс нодтарын (worker nodes) талдай отырып, олардың контейнерленген ортада масштабталу мен орнықтылықты сақтаудағы рөлін айқындаймыз. Зерттеу барысында конфигурациялардың қателіктері мен соңғы CVE (Common Vulnerabilities and Exposures) арқылы анықталған осалдықтар сияқты қауіпсіздік қиындықтары қарастырылады, сондай-ақ бұл мәселелердің Kubernetes ортасына әсері талданады. Зерттеудің маңызды бөлігі ретінде, Kubernetes 1.29 және Kubernetes Gateway API сияқты қауіпсіздік саласындағы соңғы жетістіктер талқыланады.

Біздің талдауымыздың маңызды бөлігі Kube-bench, Sonobuoy және Kube-hunter сияқты қауіпсіздік құралдарының салыстырмалы бағалануына арналады. Бұл құралдар қолайлылық, баптау мүмкіндіктері, өнімділікке әсері және интеграциялау мүмкіндіктері сияқты критерийлер бойынша бағаланады. Зерттеу нәтижелері көрсеткендей, бұл құралдар негізгі қауіпсіздік функцияларын қамтамасыз еткенімен, Kubernetes ортасының күрделі және динамикалық табиғатын шешуге арналған кешенді автоматтандырылған шешімдердің жетіспеушілігі бар.

Зерттеу Kubernetes қауіпсіздігінің қазіргі жағдайы туралы құнды ақпарат береді және болашақ зерттеулерге бағыттар ұсынады, оның ішінде қауіптерді белсенді түрде анықтап, жоюға мүмкіндік беретін жасанды интеллектке негізделген қауіпсіздік шешімдерін әзірлеуге бағыттар ұсынады.

Түйін сөздер: Kubernetes, архитектура, қауіпсіздік, масштабталу, контейнерленген қосымшалар, конфигурация қателіктері.

Г.И. Акшолак*, А.А. Бедельбаев, Р.С. Магазов, 2025.
Казахский национальный университет имени аль-Фараби,
Алматы, Казахстан.
E-mail: gaksholak@gmail.com

ЗАЩИТА KUBERNETES: АНАЛИЗ УЯЗВИМОСТЕЙ, ИНСТРУМЕНТОВ И НАПРАВЛЕНИЙ НА БУДУЩЕЕ

Акшолак Гульнур Исатаевна – докторант, Казахский национальный университет им. аль-Фараби, Алматы, Казахстан, E-mail: gaksholak@gmail.com, https://orcid.org/0000-0001-8292-6939;
Беделбаев Агын Абдешович – кандидат физико-математических наук, доцент кафедры «Информационные системы» Казахского национального университета им. аль-Фараби, Алматы, Казахстан, E-mail: agyn08@yandex.ru, https://orcid.org/0000-0001-9839-4156;
Магазов Райымбек Саламатович – докторант, Казахский национальный университет им. аль-Фараби, Алматы, Казахстан, E-mail: Magazovraiko@gmail.com, https://orcid.org/0009-0000-4105-2331.

Аннотация. В эпоху быстрого технологического развития особенно в сфере облачных вычислений и оркестрации контейнеров, безопасность систем, таких как Kubernetes, имеет первостепенное значение. В этом исследовании мы рассматриваем архитектуру безопасности Kubernetes, акцентируя внимание как на её сильных сторонах, так и на уязвимостях. Мы анализируем основные компоненты — такие как главные узлы (master node) и рабочие узлы (worker nodes), подчеркивая их роль в поддержании масштабируемости и устойчивости в контейнеризованных средах. Наше исследование также затрагивает различные проблемы безопасности, включая неправильные конфигурации и уязвимости, выявленные в последних CVE (Common Vulnerabilities and Exposures), и потенциальное влияние этих проблем на развертывания Kubernetes. Значительная часть анализа посвящена последним достижениям в области безопасности Kubernetes, таким как введение Kubernetes 1.29 и Kubernetes Gateway API.

Ключевым элементом нашего анализа является сравнительная оценка инструментов безопасности, включая Kube-bench, Sonobuoy и Kube-hunter. Эти инструменты оцениваются на основе таких критериев, как удобство использования, возможности настройки, нагрузка на производительность и интеграционные возможности. Наши результаты показывают, что, несмотря на наличие важных функций безопасности, существует разрыв в комплексных автоматизированных решениях, способных справляться с динамической и сложной природой Kubernetes-сред.

Исследование предлагает ценные инсайты в текущее состояние безопасности Kubernetes и предлагает направления для будущих исследований, включая разработку решений безопасности на основе ИИ, способных проактивно обнаруживать и устранять угрозы.

Ключевые слова: Kubernetes, архитектура, безопасность, масштабируемость, контейнеризованные приложения, неправильная конфигурация.

Introduction. In today's rapidly advancing digital landscape, the need for robust and adaptable security measures has never been more critical. With the proliferation of cloud computing and containerization, Kubernetes has emerged as a cornerstone technology, offering unparalleled flexibility, scalability, and automation in managing cloud-native applications. In their comprehensive review, (Senjab, et al., 2023) describe Kubernetes as an open-source platform that simplifies the deployment, scaling, and management of containerized applications by automating infrastructure tasks. However, this evolution has brought about significant challenges, particularly in ensuring the security and integrity of Kubernetes environments. The primary goal of this review is to explore the architecture of Kubernetes, identify its inherent security challenges, and propose advanced methods for mitigating these risks. By addressing these concerns, our work aims to provide a comprehensive understanding of how to protect containerized applications and infrastructures effectively.

The problem at hand revolves around the increasing complexity and dynamic nature of Kubernetes environments, which introduces various vulnerabilities that could be exploited by malicious actors. Our hypothesis is that by implementing continuous monitoring, advanced vulnerability management, and leveraging cutting-edge security tools, it is possible to significantly enhance the security of Kubernetes deployments. To test this hypothesis, we have conducted an extensive review of existing literature, analyzed the latest developments in Kubernetes security, and evaluated various security tools. This study not only synthesizes current knowledge but also identifies gaps and opportunities for further research, particularly in the application of AI and machine learning to proactively detect and mitigate security threats.

Kubernetes Architecture

Kubernetes is architected to provide a highly modular, scalable, and resilient environment for orchestrating containerized applications across a distributed network of computers. This section delves into the intricacies of Kubernetes' architecture.

In the paper, (Karim, et al., 2020) describe Kubernetes as an advanced container orchestration platform designed to automate the management of containerized applications. The platform's architecture is centered around a master-worker model, where the master node manages the cluster's state and orchestrates workloads, while the worker nodes execute the containerized tasks. This architecture, built on RESTful APIs and a highly modular design, allows Kubernetes to efficiently manage large-scale, distributed applications.

The Kubernetes architecture is designed to provide a flexible and extensible environment for deploying and managing containerized applications across a cluster of computers (Fig. 1).

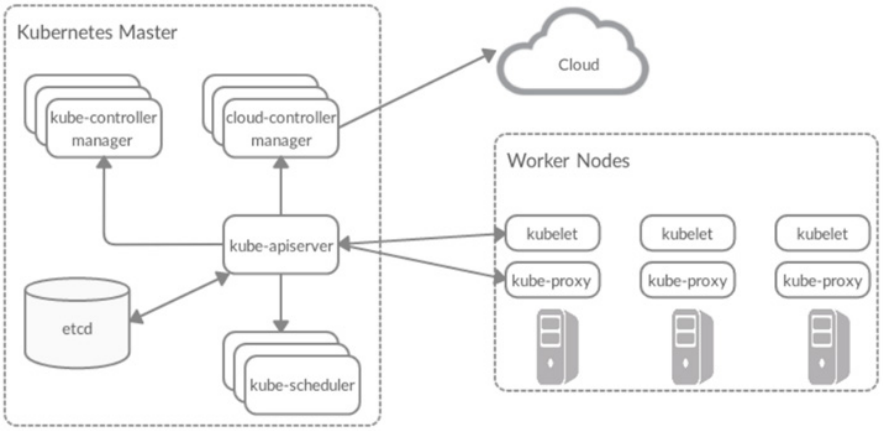

Figure 1. The architecture of a Kubernetes cluster

(Vohra, 2016) provides a detailed exploration of Kubernetes' architecture, focusing on its integration with Docker to manage microservices efficiently. The book highlights Kubernetes' modular and scalable nature, making it a robust choice for managing complex cloud-native applications.

Master Node: The control plane's brain, the master node, oversees the cluster's state, manages replication, and orchestrates rolling updates. Key components like the kube-scheduler and kube-controller-manager work in tandem to optimize resource allocation and ensure self-healing capabilities within the cluster (Thota, 2018). Worker Nodes: Serving as the data plane, worker nodes execute the containerized workloads. Each node, managed by the master, runs multiple pods through essential services such as kubelet and kube-proxy. These nodes ensure that the desired state defined by the master is continuously maintained, providing resilience and scalability to the Kubernetes environment.

Kube-scheduler. Determines where workloads should run based on what it thinks is the optimal node. It uses filtering and scoring to make this decision (Rosso, et al., 2021). Factors taken into account for scheduling decisions include: individual and collective resource requirements, hardware/software/policy constraints, affinity and anti-affinity specifications, data locality, inter-workload interference, and deadlines (Kubernetes Components, 2024).

Kube-controller-manager. Kube-controller is a daemon for self-healing. It is responsible for noticing and responding when nodes go down. It watches etcd for changes to objects such as replication, namespace, and service account controller objects, and then uses the API to enforce the specified state. Kube-controller makes sure the correct number of replications requested exist in the cluster. For example, when a user requests of the system to scale the application into ten instances kube-controller-manager makes sure that if one or more of them go down to spawn replacements, so that the requested number, matches the actual number of pods and the application is running on full capacity (Mytilinakis, 2020).

Cloud-controller-manager. A daemon with similar purpose to kube-controller-manager, but instead of focusing on components within Kubernetes, it focuses on maintaining alignment with the cloud platform that is hosting the Kubernetes cluster. It was originally in the kube-controller manager but because every cloud provider release at a different pace it became a cloud vendor dependent project that gave the cloud providers flexibility in the evolution of IT (Mytilinakis, 2020).

Etcd is a highly-consistent, distributed key-value store that hosts the cluster's state and the all the API objects. In Kubernetes, objects stored in etcd are solely accessed through the api-server (Karim, et al., 2020). Etcd leverages gPRC and TLS, used to store the most sensitive data within a cluster. By default, TLS is enabled including an optional authentication of the client with a certificate (Mytilinakis, 2020).

Kube-apiserver is the gateway and the glue that connects the distributed components together. It receives HTTP RESTful requests, validates the objects and pushes them to etcd. It also provides the front-end to the cluster's shared state through which all the other components interact. DevOps can interact with the API-server either by invoking directly the HTTP API or through a CLI wrapper, entitled kubectl (Karim, et al, 2020). The primary interaction point for all Kubernetes components and users. This is where we get, add, delete, and mutate objects. The API server delegates state to a backend, which is most commonly etcd (Rosso, et al., 2021).

Kubelet. The on-host agent that communicates with the API server to report the status of a node and understand what workloads should be scheduled on it. It communicates with the host's container runtime, such as Docker, to ensure workloads scheduled for the node are started and healthy.

Kube Proxy. Implements Kubernetes services providing virtual IPs that can route to backend Pods. This is accomplished using a packet filtering mechanism on a host such as iptables or ipvs (Rosso, et al., 2021).

This architecture, while robust, introduces several challenges, particularly in maintaining security and managing network traffic across dynamic and distributed environments. The following sections will explore the security challenges inherent in Kubernetes' architecture and propose potential solutions to mitigate these risks.

Materials and Methods

In this study, a comprehensive literature review was conducted to analyze the existing security tools for Kubernetes. The selection criteria for these tools included their relevance to Kubernetes environments, their popularity within the community, and their ability to address identified security gaps. The evaluation of these tools focused on several critical parameters: installation complexity, usability, customization options, performance overhead, and integration capabilities.

The methodology also included a systematic comparison of these tools against established security benchmarks such as the CIS Kubernetes Benchmark and the NIST cybersecurity framework. Additionally, the impact of these tools on the overall

security posture of Kubernetes environments was analyzed through hypothetical scenarios that reflect real-world security challenges.

Kubernetes Vulnerabilities

Kubernetes, while offering scalability and flexibility, introduces complex security challenges, especially concerning vulnerabilities. In the article emphasizes the importance of securing each deployment layer, from Docker containers to Kubernetes nodes, to prevent potential breaches (Vohra, 2016). The rise in identified vulnerabilities, with a 440% increase between 2018 and 2023, underscores the expanding attack surface and the critical need for continuous monitoring and timely patching (Kubernetes vulnerabilities in 2023).

For example, Martin and Hausenblas provide a comprehensive analysis of various attack vectors within Kubernetes, such as CVE-2023-5528, where users can escalate privileges on Windows nodes, and CVE-2023-2728, which allows bypassing the mountable secrets policy (Martin, et al, 2021). This analysis highlights the growing complexity of Kubernetes environments and the necessity of robust security practices.

Security Tools for Kubernets

Based on the findings from the literature review, we identified a list of essential security tools that are commonly used in Kubernetes environments. The tools were categorized into several groups, including image scanning, network security, runtime monitoring, and auditing. Criteria for selection included the tool's relevance, popularity, and coverage of the identified security gaps in Kubernetes deployments.

The security landscape for Kubernetes is vast, with various tools designed to address specific vulnerabilities and challenges. These tools can be categorized based on their primary functions within Kubernetes environments (Table 1) (Top 10 Kubernetes Security Tools in 2023).

Table 1 – Categories of Kubernetes Security Tools

Categories	Security tools
Kubernetes image scanning and static analysis	**Clair** **Checkov**
Security during execution	**Falco**
Kubernetes Network Security	**Calico** **Cilium** **Istio**
Image sharing and secret management	**Vault**
Kubernetes Security Audit	**Kube-bench** **Kube-hunter** **Kubeaudit** **KubeLinter** **Open Policy Agent**
Comprehensive commercial products	**Aqua Security**

Each tool plays a crucial role in strengthening the security posture of a Kubernetes environment. For example, **Kube-hunter** is designed to identify

potential vulnerabilities by simulating attacks within the Kubernetes environment, making it a valuable asset in preemptively detecting security flaws. On the other hand, **Clair** is particularly effective for static analysis and image scanning, helping to ensure that container images are free of known vulnerabilities before deployment.

As we move deeper into securing Kubernetes environments during runtime, **Falco** emerges as a powerful tool that continuously monitors container activity, detecting anomalous behavior that could indicate a security breach. Similarly, **Calico** and **Cilium** provide robust network security by implementing policies that control the communication between containers, ensuring that only authorized traffic flows within the cluster.

Given the critical nature of secret management and image sharing in Kubernetes, tools like **Vault** offer a secure method for managing sensitive information such as API keys and passwords, mitigating the risk of unauthorized access. Additionally, Kubernetes security auditing tools, including **Kube-bench** and **Kubeaudit,** provide a comprehensive overview of cluster security by assessing configurations against established benchmarks.

Recent studies have demonstrated the effectiveness of these tools in identifying and mitigating security risks within Kubernetes clusters. For instance, Alqarni explored the integration of zero-knowledge encryption within Kubernetes to enhance privacy and protect against cloud service provider threats (Alqarni, (2023).

Furthermore, Van der Slik and Wiersma evaluated alternative admission controllers like Gatekeeper and Kyverno, which have been proposed as replacements for the deprecated Pod Security Policies (PSP). Their research underscores the importance of selecting the right security tools to maintain a secure Kubernetes environment (van der Slik, et al., 2021).

In the study (Budigiri, et al., 2021), the authors evaluate performance overheads of eBPF-based solutions by Calico and Cilium, and analyze the security of network policies, highlighting security threats to network policies and outline corresponding state-of-the-art solutions. Their assessment shows that network policies are a suitable low-overhead security solution for low-latency inter-container communication.

Recent Developments in Kubernetes Security

The security landscape of Kubernetes has witnessed significant advancements aimed at addressing both existing and emerging threats. These developments emphasize proactive approaches, enhancing both detection and prevention capabilities within Kubernetes environments.

One such advancement is the introduction of **WARP**, a proactive attack mitigation approach proposed by Bagheri et al. WARP integrates seamlessly with Kubernetes, enabling the prediction of potential attack paths and triggering non-disruptive mitigation actions before these threats can escalate. This approach represents a shift from reactive to proactive security measures, crucial in maintaining the integrity of Kubernetes deployments (Bagheri, et al., 2023). Similarly, Dell'Immagine et al. introduced **KubeHound,** a tool designed to detect 'security smells'—subtle indicators of potential security issues within Kubernetes

deployments. KubeHound's ability to identify issues such as insufficient access control and hardcoded secrets is vital for maintaining secure and compliant Kubernetes environments (Dell'Immagine, et al., 2023).

The dynamic and scalable nature of Kubernetes clusters introduces unique security challenges, particularly in managing network connectivity and enforcing security policies across containerized applications. Verma emphasizes the necessity of implementing robust network security policies within Kubernetes environments, particularly through the integration of Container Network Interface (CNI) plugins. His research demonstrates how tools like port scanners can identify potential vulnerabilities, which can then be mitigated through carefully crafted network policies that enforce secure communication between containers. These insights are critical for developing a comprehensive security strategy that adapts to the evolving threat landscape in cloud-based deployments (Verma, 2024).

Understanding and securing the connectivity between microservices in Kubernetes clusters is critical to maintaining a robust security posture. Bufalino et al. introduced Kubesonde, a tool specifically designed to analyze microservice connectivity within Kubernetes deployments. By utilizing a probing methodology that operates with minimal impact on performance, Kubesonde can reveal discrepancies between declared and actual microservice connectivity, highlighting potential security gaps. Their analysis of 200 cloud applications demonstrated that over 60% exhibited connectivity inconsistencies, emphasizing the need for more stringent network isolation practices in Kubernetes environments (Bufalino, et al., 2023).

The release of **Kubernetes 1.29**, named Mandala (Mandala, 2024), marks a pivotal advancement in Kubernetes security. This version introduces significant features like **KMS V2 encryption** at rest and support for **nftables,** enhancing both security and resource management. These updates, particularly the introduction of sidecar containers and refined access controls, are crucial for bolstering the security and performance of modern cloud-native applications. These updates are crucial for maintaining the security and performance of modern cloud-native applications.

Additionally, the Kubernetes Gateway API, now generally available, offers significant advantages over traditional network ingress controllers, particularly in terms of flexibility and enhanced traffic management. Joslyn explains that the Gateway API allows for more precise routing and better integration with service meshes, which is essential for modern, scalable applications. This development highlights a shift towards more dynamic and secure traffic management solutions in Kubernetes environments (Joslyn, 2024).

These developments underscore a broader trend towards more dynamic and integrated security solutions within Kubernetes. As the platform continues to evolve, so too must the strategies employed to secure it, ensuring that Kubernetes remains resilient against both current vulnerabilities and future threats**.**

Results and Discussion

The comprehensive analysis of various Kubernetes security tools, presented in

Table 2, provides critical insights into their applicability across different security needs within Kubernetes environments. Each tool has been evaluated based on criteria such as installation complexity, usability, customization options, and performance overhead, which are crucial factors when considering the deployment of these tools in real-world scenarios.

Table 2 – Comparative analysis of Kubernetes security tools

Criteria	Kube-bench	Test-infra	Sonobuoy	**Power-fulSeal**	Kubesonde	KubeHunter	Istio
Primary Focus	Security compliance (CIS Benchmark)	Cluster testing (including security)	Confor-mance & custom testing	Chaos Engineering	Network security policies	Vulnerability scanning	Service mesh for micro-services
Installation Complexity	Easy (local or Docker)	Requires Prow CI/CD knowledge	Modular, plugin-based	Configurable via ConfigMap	Medium (Kubernetes & network security)	Moderate (container/ Python source)	Moderate (requires networking knowledge)
Usability	Simple CLI	Sophis-ticated, with a learning curve	Usable, but custom Docker image needed	Easy to configure	Designed for developers/ admins	User-friendly CLI	User-friendly, with CLI & dashboard
Custo-mization Options	Limited security checks	Extensive plugins	High, via custom plugins	Configurable checks	Customizable probing scenarios	Customizable scans (internal/ external)	Extensive (traffic/ security policies)
Testing Scenarios	CIS Benchmark	Varied (security, integration)	Confor-mance & custom	Chaos tests (kill pods/ nodes)pods/ nodes	Probing connectivity (internal/ external)	Vulnerability & misconfiguration scans	Fault injection, traffic shifting
Performance Overhead	Minimal; tests	Depends on selected jobs	Varies (up to an hour)	Continuous, configurable intervals	Minimal	Minimal	Minimal to moderate
Integration	CI/CD pipelines	CI/CD integration	CI/CD integration	Monitoring integrations	Continuous monitoring	CI/CD integration	Strong (CI/CD, observability tools)
Reporting	Detailed reports	TestGrid dashboard	Requires detailed analysis	Continuous feedback	Connectivity graphs	Detailed reports, no built-in visualization	Metrics, logs, traces (Grafana, etc.)
Security Features	Identifies miscon-figurations	Security testing scenarios	Confor-mance compliance	System resilience testing	Connectivity security analysis	Identifies vulnerabilities	Mutual TLS, access controls
Community Support and Updates	Actively maintained	Supported by Kubernetes community	VMware-supported, regularly updated	Active, focused on chaos engineering	Open-source, active community	Open-source, regular updates	Very active, frequent updates

The analysis of Kubernetes security tools revealed several key insights. While tools like Kube-bench and Kube-hunter are effective for identifying vulnerabilities and compliance issues, they have notable limitations. For instance, Kube-bench primarily focuses on static configuration checks and does not provide real-time monitoring capabilities. This limits its effectiveness in dynamic environments where security configurations may change frequently.

Similarly, Kube-hunter, despite its strength in simulating attack scenarios, lacks

integration with continuous deployment pipelines, which makes it less suitable for environments with rapid deployment cycles. This tool also has limitations in identifying complex misconfigurations related to Kubernetes network policies, which are critical for preventing lateral movement of attacks within clusters.

One significant gap identified in the current toolset is the lack of comprehensive automated solutions that integrate both runtime monitoring and static analysis. Most existing tools focus on either one or the other, which can lead to security blind spots in environments where threats evolve rapidly.

To address these gaps, we propose a framework that combines the capabilities of multiple tools to create a more comprehensive security solution. This framework leverages real-time monitoring tools like Falco in conjunction with static analysis tools like Clair to provide a more holistic view of the security posture. Furthermore, we suggest integrating these tools with AI-driven threat detection systems that can predict and mitigate potential security issues before they escalate.

Conclusion

This study highlights the need for a more integrated approach to Kubernetes security. While existing tools provide valuable functionalities, they often operate in isolation, leading to potential security gaps. Our comprehensive analysis demonstrates that current solutions, such as Kube-bench and Kube-hunter, are effective in identifying specific vulnerabilities but lack the capability to provide real-time monitoring and proactive threat mitigation.

The primary scientific contribution of this study is the development of an integrated security framework that combines the strengths of existing tools while addressing their limitations. By leveraging real-time monitoring tools like Falco and static analysis tools like Clair, we propose a holistic approach to securing Kubernetes environments. This framework not only improves the detection and mitigation of security threats but also offers a structured methodology for selecting and deploying security tools in dynamic Kubernetes environments.

Future research should focus on refining and validating the proposed framework in diverse Kubernetes environments. Additionally, exploring the integration of AI-driven threat detection systems could further enhance the framework's capabilities, enabling proactive threat management and automated responses to emerging security challenges.

References

Senjab K., Abbas S., Ahmed N., & Khan A.U.R. (2023). A survey of Kubernetes scheduling algorithms. *Journal of Cloud Computing*, *12*(1), 87. (in English)

Karim Manaouil, Adrien Lebre. Kubernetes and the Edge?. [Research Report] RR-9370, Inria Rennes - Bretagne Atlantique. 2020, pp.19. ffhal-02972686v2f. (in English)

Vohra D. (2016). *Kubernetes microservices with Docker*. Apress. (in English)

Subash Thota. (2018); DOCKER AND GOOGLE KUBERNETICS. *Int. J. of Adv. Res.* **6** (Jul). 984-998] (ISSN 2320-5407). *http://dx.doi.org/10.21474/IJAR01/7449. (in English)*

Rosso J., Lander R., Brand A., & Harris J. (2021). *Production Kubernetes*. « O'Reilly Media, Inc.». (in English)

Kubernetes Components. Available online: *https://kubernetes.io/docs/concepts/overview/components/* (accessed on 20 January 2024). (in English)

Mytilinakis P. (2020). *Attack methods and defenses on Kubernetes* (Master's thesis, Πανεπιστήμιο Πειραιώς). (in English)

Kubernetes vulnerabilities in 2023. *https://www.armosec.io/blog/kubernetes-vulnerabilities-2023/* (accessed on 20 January 2024). (in English)

Martin A., & Hausenblas M. (2021). *Hacking Kubernetes*. «O'Reilly Media, Inc.» (in English)

Top 10 Kubernetes Security Tools in 2023. Available online: *https://www.practical-devsecops.com/kubernetes-security-tools/* (accessed on 22 February 2024). (in English)

Alqarni A. (2023). *Enhancing Cloud Security and Privacy with Zero-Knowledge Encryption and Vulnerability Assessment in Kubernetes Deployments* (Doctoral dissertation, Middle Tennessee State University). (in English)

Van Der Slik, M., Wiersma F., & PwC W.O. (2021). Validating the replacement filtering features of popular alternative admission controllers for Pod Security Policies. (in English)

Budigiri G., Baumann C., Mühlberg J.T., Truyen E., & Joosen W. (2021, June). Network policies in kubernetes: Performance evaluation and security analysis. In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)* (pp. 407-412). IEEE. (in English)

Bagheri S., Kermabon-Bobinnec H., Majumdar S., Jarraya Y., Wang L., & Pourzandi M. (2023, May). Warping the Defence Timeline: Non-disruptive Proactive Attack Mitigation for Kubernetes Clusters. In *ICC 2023-IEEE International Conference on Communications* (pp. 777-782). IEEE. (in English)

Dell'Immagine G., Soldani J., & Brogi A. (2023). KubeHound: Detecting Microservices' Security Smells in Kubernetes Deployments. Future Internet, 15(7), 228. https://doi.org/10.3390/fi15070228. (in English)

Verma V. (2024). Network Security Policies for Containers in Cloud Applications. (in English)

Jacopo Bufalino, Mario Di Francesco, and Tuomas Aura. 2023. Analyzing Microservice Connectivity with Kubesonde. In Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE '23), December 3–9, 2023, San Francisco, CA, USA. ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3611643.3613899. (in English)

Kubernetes v1.29: Mandala. Available online: *https://kubernetes.io/blog/2023/12/13/kubernetes-v1-29-release/* (accessed on 26 January 2024). (in English)

Joslyn H. How the Kubernetes Gateway API Beats Network Ingress. Available online: *https://thenewstack.io/how-the-kubernetes-gateway-api-beats-network-ingress/* (accessed on 26 January 2024). (in English)

CONTENTS

INFORMATION AND COMMUNICATION TECHNOLOGIES

A.Abdiraman, L.Aldasheva, A.Zakirova, B.Mukhametzhanova, I.Orman
GLOBAL ANALYSIS OF MOBILE BROADBAND NETWORK PERFORMANCE: INSIGHTS INTO 5G DEPLOYMENT AND FUTURE 6G CHALLENGES.....5

R. Abdualiyeva, L. Smagulova, A. Yelepbergenova
THE EFFECTIVENESS OF USING CHATGPT IN PROGRAMMING.....17

A.B. Aben, N.M. Zhunissov, G.N. Kazbekova, A.N. Amanov, A.A. Abibullayeva
DEEPFAKE ARTIFICIAL VOICE DETECTION. COMPARISON OF THE EFFECTIVENESS OF THE LSTM AND CNN MODELS.....32

A.A. Aitkazina, N.O. Zhumazhan
DEVELOPMENT OF A BIOTECHNICAL SYSTEM FOR LASER TREATMENT OF SUNFLOWER SEEDS.....49

G. Aksholak, A. Bedelbayev, R. Magazov
SECURING KUBERNETES: AN ANALYSIS OF VULNERABILITIES, TOOLS, AND FUTURE DIRECTIONS.....66

A.T. Akynbekova, A.A. Mukhanova, Salah Al-Majeed, A.G. Altayeva
PROBLEMS OF IMPLEMENTATION OF FUZZY MODELS OF DECISION MAKING IN SOCIAL PROCESSES.....78

K.M. Aldabergenova, M.A. Kantureyeva, A.B. Kassekeyeva, A. Akhmetova, T.N. Esikova
FEATURES AND PROSPECTS FOR THE USE OF DIGITAL PLATFORMS AND INTERNET MARKETING IN THE DEVELOPMENT OF AGRICULTURAL PRODUCTION.....93

A. Yerimbetova, M. Sambetbayeva, E. Daiyrbayeva, B. Sakenov, U. Berzhanova
CREATING A MODEL FOR RECOGNIZING THE KAZAKH SIGN LANGUAGE USING THE DEEP LEARNING METHOD.....108

A.N. Zhidebayeva, S.T. Akhmetova, A.O. Aliyeva, B.O. Tastanbekova, G.S. Shaimerdenova
REVIEW OF DETECTION AND PREVENTION OF OFFENSIVE LANGUAGE VIA SOCIAL MEDIA DATA MINING.....124

K.S. Ivanov, D.T. Tulekenova
ENSURING THE DETERMINABILITY OF MOTION OF AN ADAPTIVE SPACECRAFT DRIVE BY INTRODUCING AN ADDITIONAL VELOCITY CONSTRAINT FORCE.....136

M.N. Kalimoldayev, Z.D. Ormansha, K.B. Begalieva, A.S. Ainagulova, A.O. Aukenova
A BLOCKCHAIN MODEL FOR AGRICULTURAL PRODUCT TRACKING THAT SUPPORTS FEDERAL TRAINING.....151

I. Massyrova, O. Joldasbayev, S. Joldasbayev, A. Bolysbek, S. Mambetov
AUTOMATION OF THE SYSTEM FOR INDUSTRIAL PRACTICE AND INTERNSHIPS FOR STUDENTS IN ORGANIZATIONS OUTSIDE OF THE UNIVERSITY.....168

A.B. Mimenbayeva, G.O. Issakova, G.K. Bekmagambetova, A.B. Aruova, E.K. Darikulova
DEVELOPMENT OF DEEP LEARNING MODELS FOR FIRE SOURCES PREDICTION.....185

K. Momynzhanova, S.Pavlov, Sh. Zhumagulova
MATHEMATICAL MODELS AND PRACTICAL IMPLEMENTATION OF AN OPTICAL-ELECTRONIC EXPERT SYSTEM FOR GLAUCOMA DETECTION.....202

B.O. Mukhametzhanova, L.N. Kulbaeva, Z.B. Saimanova, E.K. Seipisheva, B.M. Sadanova
OPTIMIZATION AND INTEGRATION OF DOCKER TECHNOLOGY IN MODERN INFORMATION SYSTEMS.....218

A.R. Orazayeva, J.A. Tussupov, A.K. Shaikhanova, G.B. Bekeshova, A.D. Galymova
FUZZY EXPERT SYSTEM FOR ASSESSING DYNAMIC CHANGES IN BIOMEDICAL IMAGES OF BREAST CANCER TUMORS.....227

D. Oralbekova, O. Mamyrbayev, A. Akhmediyarova, D. Kassymova
USING KAZAKH NER DATASETS FOR MULTICLASS CLASSIFICATION IN THE LEGAL DOMAIN: A COMPARATIVE STUDY OF BERT, GPT, AND LSTM MODELS.....242

A. Ospanov, A.J. Pedro, T. Turymbetov, K. Dyussekeyev, A. Zhumadillayeva
ADVANCEMENTS IN ERP SYSTEMS THROUGH EMERGING

TECHNOLOGIES, MACHINE LEARNING AND HYBRID OPTIMIZATION TECHNIQUES.....259

K. Rabbany, A. Bekarystankyzy, A. Shoiynbek, D. Kuanyshbay, A. Mukhametzhanov
DETECTION OF SUICIDAL TENDENCIES IN REDDIT POSTS USING MACHINE LEARNING.....270

A. Taukenova
PERSONALIZED ARCHITECTURE: CREATING UNIQUE SPACES WITH DIGITAL TECHNOLOGIES.....283

МАЗМҰНЫ

АҚПАРАТТЫҚ-КОММУНИКАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР

Ә. Әбдіраман, Л. Алдашева, А. Закирова, Б. Мухаметжанова, И. Орман
МОБИЛЬДІ КЕН ЖОЛАҚТЫ ЖЕЛІЛЕРДІҢ ТИІМДІЛІГІНІҢ ЖАҺАНДЫҚ ТАЛДАУ: 5G ЕНГІЗУ ЖӘНЕ 6G БОЛАШАҚ МӘСЕЛЕЛЕРІ.....5

Р.Е. Абдуалиева, Л.А. Смагулова, А.У. Елепбергенова
БАҒДАРЛАМАЛАУДА CHATGPT ҚОЛДАНУ ТИІМДІЛІГІ.....17

А.Б. Абен, Н.М. Жунисов, Г.Н. Казбекова, А.Н. Аманов, А.А. Абибуллаева
DEEPFAKE ЖАСАНДЫ ДАУЫСТЫ АНЫҚТАУ. LSTM ЖӘНЕ CNN МОДЕЛЬДЕРІНІҢ ТИІМДІЛІГІ САЛЫСТЫРУ.....32

Ә.А. Айтқазина, Н.Ө. Жұмажан
КҮНБАҒЫС ТҰҚЫМДАРЫН ЛАЗЕРМЕН ӨҢДЕУГЕ АРНАЛҒАН БИОТЕХНИКАЛЫҚ ЖҮЙЕНІ ДАМЫТУ.....49

Г.И. Ақшолақ, А.А. Бедельбаев, Р.С. Мағазов
KUBERNETES-ТІ ҚОРҒАУ: ОСАЛДЫҚТАРДЫ, ҚҰРАЛДАРДЫ ЖӘНЕ БОЛАШАҚ БАҒЫТТАРДЫ ТАЛДАУ.....66

А.Т. Ақынбекова, А.А. Муханова, Salah Al-Majeed, Г.С. Алтаева
ӘЛЕУМЕТТІК ПРОЦЕСТЕРДЕ ШЕШІМДЕР ҚАБЫЛДАУДЫҢ БҰЛДЫР МОДЕЛЬДЕРІН ЕНГІЗУ МӘСЕЛЕЛЕРІ.....78

К.М. Алдабергенова, М.А. Кантуреева, А.Б. Касекеева, А.Ж. Ахметова, Т.Н. Есикова
АУЫЛ ШАРУАШЫЛЫҒЫ ӨНДІРІСІН ДАМЫТУДА ЦИФРЛЫҚ ПЛАТФОРМАЛАР МЕН ИНТЕРНЕТ-МАРКЕТИНГТІ ҚОЛДАНУДЫҢ ЕРЕКШЕЛІКТЕРІ МЕН ПЕРСПЕКТИВАЛАРЫ.....93

А.С. Еримбетова, М.А. Сәмбетбаева, Э.Н. Дайырбаева, Б.Е. Сәкенов, У.Г. Бержанова
ТЕРЕҢ ОҚЫТУ ӘДІСІН ҚОЛДАНУ АРҚЫЛЫ ҚАЗАҚ ЫМ ТІЛІН ТАНУҒА АРНАЛҒАН МОДЕЛЬ ҚҰРУ.....108

А.Н. Жидебаева, С.Т. Ахметова, А.О. Алиева, Б.О. Тастанбекова, Г.С. Шаймерденова
ӘЛЕУМЕТТІК ЖЕЛІЛЕРДЕН DATA MINING АРҚЫЛЫ БЕЙӘДЕП СӨЗДЕРДІ АНЫҚТАУ ЖӘНЕ АЛДЫН АЛУҒА ШОЛУ.....124

К.С. Иванов, Д.Т. Тулекенова
ЖЫЛДАМДЫҚ БАЙЛАНЫСЫНЫҢ ҚОСЫМША КҮШІН ЕНГІЗУ АРҚЫЛЫ ҒАРЫШ АППАРАТЫНЫҢ БЕЙІМДЕЛГЕН ЖЕТЕК ҚОЗҒАЛЫСЫНЫҢ АЙҚЫНДЫЛЫҒЫН ҚАМТАМАСЫЗ ЕТУ.....136

М.Н. Калимолдаев, З.Д. Орманша, К.Б. Бегалиева, А.С. Айнагулова, А.О. Аукенова
ФЕДЕРАТИВТІ ОҚЫТУДЫ ҚОЛДАЙТЫН АУЫЛШАРУАШЫЛЫҚ ӨНІМДЕРІН БАҚЫЛАУҒА АРНАЛҒАН БЛОКЧЕЙН МОДЕЛІ.....151

И. Масырова, О.К. Джолдасбаев, С.К. Джолдасбаев, А. Болысбек, С.Т. Мамбетов
УНИВЕРСИТЕТТЕН ТЫС ҰЙЫМДАРДА СТУДЕНТТЕРДІҢ ӨНДІРІСТІК ПРАКТИКАСЫ МЕН ТАҒЫЛЫМДАМАСЫН АВТОМАТТАНДЫРУ ЖҮЙЕСІ.....168

А.Б. Мименбаева, Г.О. Исакова, Г.К. Бекмагамбетова, Ә.Б. Аруова, Е.Қ. Дәріқұлова
ӨРТ КӨЗДЕРІН БОЛЖАУ ҮШІН ТЕРЕҢ ОҚЫТУ МОДЕЛЬДЕРІН ӘЗІРЛЕУ.....185

К.Р. Момынжанова, С.В. Павлов, Ш.П. Жұмағұлова, М.Т. Тұңғышбаев
ГЛАУКОМАНЫ АНЫҚТАУҒА АРНАЛҒАН ОПТИКАЛЫҚ-ЭЛЕКТРОНДЫҚ САРАПТАМАЛЫҚ ЖҮЙЕНІҢ МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕРІ МЕН ПРАКТИКАЛЫҚ ІСКЕ АСЫРЫЛУЫ.....202

Б.О. Мухаметжанова, Л.Н. Кулбаева, З.Б. Сайманова, Э.К. Сейпишева, Б.М. Саданова
ЗАМАНАУИ АҚПАРАТТЫҚ ЖҮЙЕЛЕРДЕГІ DOCKER ТЕХНОЛОГИЯСЫН ОҢТАЙЛАНДЫРУ ЖӘНЕ ИНТЕГРАЦИЯЛАУ.....218

А.Р. Оразаева, Д.А. Тусупов, А.К. Шайханова, Г.Б. Бекешова, Ә.Д. Ғалымова
СҮТ БЕЗІ ҚАТЕРЛІ ІСІГІ КЕЗІНДЕ БИОМЕДИЦИНАЛЫҚ КЕСКІНДЕРІНДЕГІ ДИНАМИКАЛЫҚ ӨЗГЕРІСТЕРДІ БАҒАЛАУҒА АРНАЛҒАН АНЫҚ ЕМЕС САРАПТАМА ЖҮЙЕСІ.....227

Д. Оралбекова, О. Мамырбаев, А. Ахмедиярова, Д. Қасымова
ҚАЗАҚ ТІЛІНДЕГІ NER ДЕРЕКТЕР ЖИНАҒЫН ҚҰҚЫҚТЫҚ САЛАДА КӨПСАНАТТЫ ЖІКТЕУ ҮШІН ПАЙДАЛАНУ: BERT, GPT ЖӘНЕ LSTM МОДЕЛЬДЕРІНІҢ САЛЫСТЫРМАЛЫ ЗЕРТТЕУІ.....242

А. Оспанов, П. Алонсо-Жорда, Т. Тұрымбетов, К. Дүйсекеев, А. Жұмаділлаева
ERP ЖҮЙЕЛЕРІНІҢ ЖЕТІЛДІРІЛУІ: ЗАМАНАУИ ТЕХНОЛОГИЯЛАР, МАШИНАЛЫҚ ОҚЫТУ ЖӘНЕ ГИБРИДТІ ОПТИМИЗАЦИЯ ӘДІСТЕРІ.....259

К. Раббани, А. Бекарыстанқызы, Д. Қуанышбай, А. Шойынбек, А. Мұхаметжанов
МАШИНАЛЫҚ ОҚЫТУДЫ ПАЙДАЛАНУ АРҚЫЛЫ REDDIT ПОСТТАРЫНДАҒЫ СУИЦИДТІК ТЕНДЕНЦИЯЛАРЫН АНЫҚТАУ.....270

Ә. Таукенова
ЖЕКЕЛЕНДІРІЛГЕН АРХИТЕКТУРА: ДИДЖИТАЛ ТЕХНОЛОГИЯЛАРМЕН ЕРЕКШЕ КЕҢІСТІКТЕР ЖАРАТУ.....283

СОДЕРЖАНИЕ

ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

А. Абдираман, Л. Алдашева, А. Закирова, Б. Мухаметжанова, И. Орман
ГЛОБАЛЬНЫЙ АНАЛИЗ ЭФФЕКТИВНОСТИ МОБИЛЬНОЙ ШИРОКОПОЛОСНОЙ СЕТИ: ВНЕДРЕНИЕ 5G И БУДУЩИЕ ЗАДАЧИ 6G.....5

Р.Е. Абдуалиева, Л.А. Смагулова, А.У. Елепбергенова
ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ CHATGPT В ПРОГРАММИРОВАНИИ…….....17

А.Б. Абен, Н.М. Жунисов, Г.Н. Казбекова, А.Н. Аманов, А.А. Абибуллаева
ОБНАРУЖЕНИЕ ИСКУССТВЕННОГО ГОЛОСА DEEPFAKE. СРАВНЕНИЕ ЭФФЕКТИВНОСТИ МОДЕЛЕЙ LSTM И CNN……..32

А.А. Айтказина, Н.О. Жумажан
РАЗРАБОТКА БИОТЕХНИЧЕСКОЙ СИСТЕМЫ ДЛЯ ЛАЗЕРНОЙ ОБРАБОТКИ СЕМЯН ПОДСОЛНЕЧНИКА…….……49

Г.И. Акшолак, А.А. Бедельбаев, Р.С. Магазов
ЗАЩИТА KUBERNETES: АНАЛИЗ УЯЗВИМОСТЕЙ, ИНСТРУМЕНТОВ И НАПРАВЛЕНИЙ НА БУДУЩЕЕ……....…….66

А.Т. Акынбекова, А.А. Муханова, Salah Al-Majeed, Г.С. Алтаева
ПРОБЛЕМЫ РЕАЛИЗАЦИИ НЕЧЕТКИХ МОДЕЛЕЙ ПРИНЯТИЯ РЕШЕНИЙ В СОЦИАЛЬНЫХ ПРОЦЕССАХ…….....……78

К.М. Алдабергенова, М.А. Кантуреева, А.Б. Касекеева, А.Ж. Ахметова, Т.Н. Есикова
ОСОБЕННОСТИ И ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ЦИФРОВЫХ ПЛАТФОРМ И ИНТЕРНЕТ-МАРКЕТИНГА В РАЗВИТИИ СЕЛЬСКОХОЗЯЙСТВЕННОГО ПРОИЗВОДСТВА…….……93

А.С. Еримбетова, М.А. Самбетбаева, Э.Н. Дайырбаева, Б.Е. Сакенов, У.Г. Бержанова
СОЗДАНИЕ МОДЕЛИ ДЛЯ РАСПОЗНАВАНИЯ КАЗАХСКОГО ЖЕСТОВОГО ЯЗЫКА С ИСПОЛЬЗОВАНИЕМ МЕТОДА ГЛУБОКОГО ОБУЧЕНИЯ.....108

А.Н. Жидебаева, С.Т. Ахметова, А.О. Алиева, Б.О. Тастанбекова, Г.С. Шаймерденова
ОБЗОР ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ОСКОРБИТЕЛЬНОЙ ЛЕКСИКИ С ПОМОЩЬЮ DATA MINING В СОЦИАЛЬНЫХ СЕТЯХ.…124

К.С. Иванов, Д.Т. Тулекенова
ОБЕСПЕЧЕНИЕ ОПРЕДЕЛИМОСТИ ДВИЖЕНИЯ АДАПТИВНОГО ПРИВОДА КОСМИЧЕСКОГО АППАРАТА С ПОМОЩЬЮ ВВЕДЕНИЯ ДОПОЛНИТЕЛЬНОЙ СИЛЫ СКОРОСТНОЙ СВЯЗИ…….....……..136

М.Н. Калимолдаев, З.Д. Орманша, К.Б. Бегалиева, А.С. Айнагулова, А.О. Аукенова
БЛОКЧЕЙН-МОДЕЛЬ ДЛЯ ОТСЛЕЖИВАНИЯ СЕЛЬСКОХОЗЯЙСТВЕННОЙ ПРОДУКЦИИ С ПОДДЕРЖКОЙ ФЕДЕРАТИВНОГО ОБУЧЕНИЯ…….....…..151

И. Масырова, О.К. Джолдасбаев, С.К. Джолдасбаев, А. Болысбек, С.Т. Мамбетов
АВТОМАТИЗАЦИЯ СИСТЕМЫ ДЛЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ И СТАЖИРОВКИ СТУДЕНТОВ В ОРГАНИЗАЦИЯХ ВНЕ ВУЗА…….....….168

А. Миненбаева, Г. Исакова, Г.К. Бекмагамбетова, А.Б. Аруова, Е.К. Дарикулова
РАЗРАБОТКА МОДЕЛЕЙ ГЛУБОКОГО ОБУЧЕНИЯ ПРОГНОЗИРОВАНИЯ ИСТОЧНИКОВ ПОЖАРОВ……....185

К.Р. Момынжанова, С.В. Павлов, Ш.П. Жумагулова, М.Т. Тунгушбаев
МАТЕМАТИЧЕСКИЕ МОДЕЛИ И ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ ОПТИКО-ЭЛЕКТРОННОЙ ЭКСПЕРТНОЙ СИСТЕМЫ ДЛЯ ВЫЯВЛЕНИЯ ГЛАУКОМЫ…….....202

Б.О. Мухаметжанова, Л.Н. Кулбаева, З.Б. Сайманова, Э.К. Сейпишева, Б.М. Саданова
ОПТИМИЗАЦИЯ И ИНТЕГРАЦИЯ ТЕХНОЛОГИИ DOCKER В СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ……..…….218

А.Р. Оразаева, Д.А. Тусупов, А.К. Шайханова, Г.Б. Бекешова, А.Д. Галымова
НЕЧЕТКАЯ ЭКСПЕРТНАЯ СИСТЕМА ДЛЯ ОЦЕНКИ ДИНАМИЧЕСКИХ ИЗМЕНЕНИЙ В БИОМЕДИЦИНСКИХ ИЗОБРАЖЕНИЯХ ОПУХОЛЕЙ ПРИ РАКЕ МОЛОЧНОЙ ЖЕЛЕЗЫ……...……..227

Д. Оралбекова, О. Мамырбаев, А. Ахмедиярова, Д. Касымова
ИСПОЛЬЗОВАНИЕ НАБОРОВ ДАННЫХ NER НА КАЗАХСКОМ ЯЗЫКЕ ДЛЯ МУЛЬТИКЛАССИФИКАЦИИ В ПРАВОВОЙ СФЕРЕ: СРАВНИТЕЛЬНОЕ ИССЛЕДОВАНИЕ МОДЕЛЕЙ BERT, GPT И LSTM…….....……242

А. Оспанов, П. Алонсо-Жорда, Т. Турымбетов, К. Дюсекеев, А. Жумадиллаева
ПРОДВИЖЕНИЕ ERP СИСТЕМ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ, МАШИННОГО ОБУЧЕНИЯ И ГИБРИДНЫХ МЕТОДОВ ОПТИМИЗАЦИИ…….....…….259

К. Раббани, А. Бекарыстанкызы, Д. Куанышбай, А. Шойынбек, А. Мухаметжанов
ОБНАРУЖЕНИЕ СУИЦИДАЛЬНЫХ ТЕНДЕНЦИЙ В ПУБЛИКАЦИЯХ НА REDDIT С ИСПОЛЬЗОВАНИЕМ МАШИННОГО ОБУЧЕНИЯ……..270

А. Таукенова
ПЕРСОНАЛИЗИРОВАННАЯ АРХИТЕКТУРА: СОЗДАНИЕ УНИКАЛЬНЫХ ПРОСТРАНСТВ С ПОМОЩЬЮ ЦИФРОВЫХ ТЕХНОЛОГИЙ…….....…….283

Publication Ethics and Publication Malpracticein the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Редакторы: *Д.С. Аленов, Ж.Ш.Әден*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 20.03.2025.
Формат 60х881/8. Бумага офсетная. Печать –ризограф.
20,0 п.л. Заказ 1.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19